

Swansea University Prifysgol Abertawe

FACULTY OF SCIENCE AND ENGINEERING

STUDENT HANDBOOK

MSc (FHEQ LEVEL 7)

MSc COMMUNICATIONS ENGINEERING DEGREE PROGRAMME

SUBJECT SPECIFIC (PART TWO OF TWO) *MODULE AND COURSE STRUCTURE* 2022/23

DISCLAIMER

The Faculty of Science and Engineering has made all reasonable efforts to ensure that the information contained within this publication is accurate and up-to-date when published but can accept no responsibility for any errors or omissions.

The Faculty of Science and Engineering reserves the right to revise, alter or discontinue degree programmes or modules and to amend regulations and procedures at any time, but every effort will be made to notify interested parties.

It should be noted that not every module listed in this handbook may be available every year, and changes may be made to the details of the modules. You are advised to contact the Faculty of Science and Engineering directly if you require further information.

The 22-23 academic year begins on 19 September 2022

Full term dates can be found here

DATES OF 22-23 TERMS

19 September 2022 – 16 December 2022

9 January 2023 – 31 March 2023

24 April 2023 – 09 June 2023

SEMESTER 1

19 September 2022 – 27 January 2023

SEMESTER 2

30 January 2023 – 09 June 2023

SUMMER

12 June 2023 – 22 September 2023

IMPORTANT

Swansea University and the Faculty of Science of Engineering takes any form of **academic misconduct** very seriously. In order to maintain academic integrity and ensure that the quality of an Award from Swansea University is not diminished, it is important to ensure that all students are judged on their ability. No student should have an unfair advantage over another as a result of academic misconduct - whether this is in the form of **Plagiarism**, **Collusion** or **Commissioning**.

It is important that you are aware of the **guidelines** governing Academic Misconduct within the University/Faculty of Science and Engineering and the possible implications. The Faculty of Science and Engineering will not take intent into consideration and in relation to an allegation of academic misconduct - there can be no defence that the offence was committed unintentionally or accidentally.

Please ensure that you read the University webpages covering the topic – procedural guidance <u>here</u> and further information <u>here</u>. You should also read the Faculty Part One handbook fully, in particular the pages that concern Academic Misconduct/Academic Integrity. You should also refer to the Faculty of Science and Engineering proof-reading policy and this can be found on the Community HUB on Canvas, under Course Documents.

Welcome to the Faculty of Science and Engineering!

Whether you are a new or a returning student, we could not be happier to be on this journey with you.

This has been a challenging period for everyone. The COVID-19 pandemic has prompted a huge change in society as well as how we deliver our programmes at Swansea University and the way in which you study, research, learn and collaborate. We have been working hard to make sure you will have or continue to having an excellent experience with us.

We have further developed some exciting new approaches that I know you will enjoy, both on campus and online, and we cannot wait to share these with you.

At Swansea University and in the Faculty of Science & Engineering, we believe in working in partnership with students. We work hard to break down barriers and value the contribution of everyone. Our goal is an inclusive community where everyone is respected, and everyone's contributions are valued. Always feel free to talk to academic staff, administrators, and your fellow students - I'm sure you will find many friendly helping hands ready to assist you.

We all know this period of change will continue and we will need to adapt and innovate to continue to be supportive and successful. At Swansea we are committed to making sure our students are fully involved in and informed about our response to challenges.

In the meantime, learn, create, collaborate, and most of all - enjoy yourself!

Professor Johann (Hans) Sienz Interim Pro-Vice Chancellor/Interim Executive Dean Faculty of Science and Engineering



| Faculty of Science and Engineering | | | |
|---|--|--|--|
| Interim Pro-Vice Chancellor/Interim Executive Dean | Professor Johann Sienz | | |
| Head of Operations | Mrs Ruth Bunting | | |
| Associate Dean – Student Learning and Experience (SLE) | Professor Paul Holland | | |
| School of Aerospace, Civil, Electrica | al, General and Mechanical Engineering | | |
| Head of School: | Professor Antonio Gil | | |
| School Education Lead | Professor Cris Arnold | | |
| Head of Electronic and Electrical Engineering | Professor Vincent Teng | | |
| Electronic and Electrical Engineering Programme Director | Dr Karin Ennser | | |
| Year Coordinators | Professor Amit Mehta | | |

STUDENT SUPPORT

The Faculty of Science and Engineering has two **Reception** areas - Engineering Central (Bay Campus) and Wallace 223c (Singleton Park Campus).

Standard Reception opening hours are Monday-Friday 9am-5pm.

The **Student Support Team** provides dedicated and professional support to all students in the Faculty of Science and Engineering. Should you require assistance, have any questions, be unsure what to do or are experiencing difficulties with your studies or in your personal life, our team can offer direct help and advice, plus signpost you to further sources of support within the University. There are lots of ways to get information and contact the team:

Email: studentsupport-scienceengineering@swansea.ac.uk (Monday–Friday, 9am–5pm)

Call: +44 (0) 1792 295514 and 01792 6062522 (Monday-Friday, 10am–12pm, 2–4pm).

Zoom: By appointment. Students can email, and if appropriate we will share a link to our Zoom calendar for students to select a date/time to meet.

The current student webpages also contain useful information and links to other resources:

https://myuni.swansea.ac.uk/fse/coe-student-info/

READING LISTS

Reading lists for each module are available on the course Canvas page and are also accessible via http://ifindreading.swan.ac.uk/. We've removed reading lists from the 22-23 handbooks to ensure that you have access to the most up-to-date versions. Access to print material in the library may be limited due to CV-19; your reading lists will link to on-line material whenever possible. We do not expect you to purchase textbooks, unless it is a specified key text for the course.

THE DIFFERENCE BETWEEN COMPULSORY AND CORE MODULES

Compulsory modules must be pursued by a student.

Core modules must not only be **pursued**, but also **passed** before a student can proceed to the next level of study or qualify for an award. Failures in core modules must be redeemed. Further information can be found under "Modular Terminology" on the following link - <u>https://myuni.swansea.ac.uk/academic-life/academic-regulations/taught-guidance/essential-info-taught-students/your-programme-explained/</u>

Supporting Your Studies

- Centre for Academic Success
- Faculty of Science and Engineering- Student Support

Supporting Your Professional Development

As a student studying MSc Communications Engineering at Swansea University you are continuing your educational journey which we hope will end with Engineering Council registration as a Chartered Engineer (CEng).

The Master of Science (MSc) programme Communications Engineering has been accredited by the Institution of Engineering and Technology (IET) on behalf of the Engineering Council as meeting the requirements for Further Learning for registration as a Chartered Engineer (CEng). Candidates must hold a CEng accredited BEng/BSc (Hons) undergraduate first degree to comply with full CEng registration requirements.

What this means for you is that the learning outcomes of each year of your programme of study has been carefully designed to align with Version 3 of the Engineering Council's Accreditation of Higher Education Programmes (AHEP) which forms the educational foundation for the UK Standard for Professional Engineering Competence (UK-SPEC).

The knowledge and skills you will have demonstrated by completing your programme of study are defined by achieving a set of learning outcomes distributed across the following key areas of competence:

- Science and mathematics
- Engineering analysis
- Design and innovation
- The engineer and society
- Engineering practice

To find out more about Professional Registration and what the AHEP competences are, please refer to the Engineering Council's Student Guide to Professional Registration and the Accreditation of Higher Education Programmes collated learning outcomes

The IET – Your Professional Home for Life

As a student at Swansea University, you are privileged to be associated with one of the small groups of universities that have been selected to be Academic Partners of the IET. The most tangible benefit of this is that you can register as a student member of the IET at no cost to yourself for the duration of your study. And as a student member of the IET, you can take *full advantage* of the benefits that membership of the IET offers. These include an impressive range of services supporting *Networking, Professional Development, Learning Resources* and *Membership Benefits*. A summary of these is shown on the Get more from your partnership page.

As well as these benefits, as an Academic Partner of the IET, the University can offer you access to the IET's Graduate Advantage Scheme: that is, we will pay for your first year of full Membership of the IET, and you can use the post-nominals MIET straight after graduation for no cost. This will be especially useful as you start to gain and evidence the UK-SPEC competences you will need to complete your IEng or CEng professional registration.

IET on Campus

IET On Campus is designed to support everyone in the Department of Electronic and Electrical Engineering with students at the heart of it. The IET gives you access to tailored practical, technical, and career-related resources and helps you to create links with industry and other universities, building a platform for you to demonstrate your skills and raise your profile. At Swansea, the local branch of IET on Campus is run by the Electrical & Electronic Engineering Society (E&EESoc) and is supported by the IET South Wales Local Network.

For more information, please join E&EESoc and access their social media channels.

IET Student Advisor

Dr Chris Jobling (MIET, CEng) is the *IET Student Advisor* for Swansea University. Please get in touch with him if you want to find out more about the AHEP and UKSPEC, the IET, IET student membership, IET Scholarships, Graduate Advantage, IET Communities, or opportunities to get involved with Wales Southwest Local Network as an IET young professional volunteer. He will be happy to help.

Other members of staff associated with the IET at Swansea include:

- Dr Richard Cobley (MIET)
- Dr Timothy Davies (MIET, CEng)
- Dr Augustine Egwebe (MIET)
- Dr Karin Ennser (MIET, CEng)
- Prof Lijie Li (FIET)
- Mr David Moody (MIET)

UK Electronics Skills Foundation

Swansea University is an academic partner from the UK Electronics Skills Foundation. The partnership means that you can benefit from the UKESF scholarship scheme, competitions, awards and internship programme, which connects the most capable Electronics undergraduates with leading companies in the sector.

UKESF offers opportunities for undergraduates to take advantage of an industry placement, develop their employability skills, generous financial support, and the opportunity to network with professionals in the Electronics sector. Dr Karin Ennser is the UKESF Student Advisor for Swansea University. Please contact her if you want to find out more.

Faculty prizes

The Faculty of Science and Engineering awards graduation prizes to the best MSc Communications Engineering student in each graduating year.

MSc (FHEQ Level 7) 2022/23

Communications Engineering MSc Communications Engineering

| Semester 1 Modules | Semester 2 Modules | |
|--|--|--|
| AT-M49 | AT-M79 | |
| RF and Microwaves | Optical Networks | |
| 10 Credits | 10 Credits | |
| Prof A Mehta | Dr KM Ennser | |
| CORE | CORE | |
| AT-M76 | CSCM88 | |
| Radio and Optical Wireless Communications | Network and Wireless Security | |
| 10 Credits | 15 Credits | |
| Prof L Li/Prof A Mehta | Dr P Kumar | |
| CORE | CORE | |
| AT-M80 | EG-M190 | |
| Optical Fibre Communications | Social, environmental and economic context of research | |
| 10 Credits | 10 Credits | |
| Dr KM Ennser | Dr N Wint | |
| CORE | CORE | |
| CSCM18 | EG-M191 | |
| IT-Security: Cryptography and Network Security | Communication Systems and Networks | |
| 15 Credits | 10 Credits | |
| Dr P Kumar/Dr PD James | Dr JW Jones | |
| CORE | CORE | |
| EG-M85 | EG-M47 | |
| Strategic Project Planning | Business Leadership for Engineers | |
| 10 Credits | 10 Credits | |
| Dr K Wada | Dr A Munnangi/Dr AS Walters | |
| CORE | CORE | |
| EGIM16 | | |
| Communication Skills for Research Engineers | | |
| 10 Credits | | |
| Dr SA Rolland/Dr T Lake | | |
| CORE | | |
| Dissertation | | |
| | M58 | |
| | munications Engineering | |
| 60 Credits | | |
| Prof A Mehta | | |
| CORE | | |
| Total 18 | 0 Credits | |

AT-M49 RF and Microwaves

Credits: 10 Session: 2022/23 September-January

Pre-requisite Modules:

Co-requisite Modules:

Lecturer(s): Prof A Mehta

Format: Lectures 24 hours

Course work lab demonstration 11 hours

Own directed private study 65 hours

Contact Hours will be delivered through a blend of live activities online and on-campus, and may include, for example, lectures, seminars, practical sessions and Academic Mentoring sessions.

Delivery Method: All Programmes will employ a blended approach to delivery using the Canvas Digital Learning Platform for live and self-directed online activity, with live and self-directed on-campus activities each week. Students may also have the opportunity to engage with online versions of sessions delivered on-campus

Assessment:

Examination (75 %); Coursework (25% - April)

Module Aims: Enabling students to secure strong understanding of the current microwave and RF communication technologies, both from the theoretical and experimental point of views.

Module Content:

- Modern applications of rf and microwaves
- Transmission lines
- Antennas
- Smart Antennas
- Waves

• Components (Waveguides, RF switches and RF sources)

Intended Learning Outcomes: After completing this module you should:

• Understand the application of communication technology for various modern applications, e.g. RFIDs, Satcoms, RAY Gun, and UWB Cancer detection techniques, GPS, 60 GHz radios, etc.

• Have an in-depth understanding of transmission line theory, associated equations, smith charts and line impedance transformation.

• Have a thorough understanding and analysis of different antenna types, their characteristics and their design parameters.

• Have a detailed understanding of the operation of the smart antenna (phase array antenna) and array factor.

• Understand the propagation of electromagnetic waves via various types of mediums.

• Understand various microwave components such as waveguides, mixers, switches, circulators, couplers etc.

| Assessment: | Examination 1 (75%) | | | | |
|--------------------------|-----------------------------------|------|--|---|--|
| | Coursework 1 (25%) | | | | |
| Resit Assessment: | Examination (Resit instrument) (1 | 00%) | | | |
| | | | | - | |

Assessment Description: Examination and Coursework:

Examination (75%); 2 hour examination - Answer 3 out of 4 questions

Coursework (25%): This is an individual piece of coursework. It focuses on writing a 1500 word report on the experimental investigations on single arm rectangular spiral antenna. The report should highlight the following: • Measurement of the antenna input impedance at the frequency of 3.3 GHz

- Measurement of the reflection coefficient from 3-4 GHz
- Measurement of the radiation pattern at 3.3 GHz.
- How a VNA Works
- How the Satimo Near Field Antenna Measurement facility works

This module is assessed by a combination of examination and continual assessment. In order for the continual assessment marks to count, you must achieve at least 40% in the exam component. If you achieve less than 40% in the exam, then the module mark will be just the exam mark.

Moderation approach to main assessment: Second marking as sampling or moderation

Assessment Feedback: Via internet with aid of college examination feedback system. Students are also encouraged to meet the academic for any specific feedback, if required.

Failure Redemption: If rules allow - standard University provision with marks capped. Any failure redemption of this module will be by written examination only (100%).

Additional Notes: Delivery of both teaching and assessment will be blended including live and self-directed activities online and on-campus.

• Notes, worked examples and related materials for this module can be found on Canvas.

• The Faculty of Science and Engineering has a ZERO TOLERANCE penalty policy for late submission of all coursework and continuous assessment.

This module is assessed by a combination of examination and continual assessment. In order for the continual assessment marks to count, you must achieve at least 40% in the exam component. If you achieve less than 40% in the exam, then the module mark will be just the exam mark.

AT-M58 MSc Dissertation - Communications Engineering

Credits: 60 Session: 2022/23 June-September

Pre-requisite Modules:

Co-requisite Modules:

Lecturer(s): Prof A Mehta

Format: Typically 1 hour per week i.e 10-15 hrs total contact time. Each student is to be supervised in accordance with the University's Policy on Supervision, with a minimum of three meetings held. A careful record should be kept, agreed between supervisor and student, of all such formal meetings, including dates, action agreed and deadlines set.

Delivery Method: The module is delivered primarily as an individual research project. The student is expected to liaise with the supervisor on a regular basis, with a minimum University requirement of three formal meetings for full-time students. In the case of part-time students it is recommended that a minimum of four meetings are held. Ideally, contact should be more regular, with at least one meeting a week to discuss the development and progress of the project. Depending on the project the student would be expected to carry out this research individually and to complete the necessary risk assessments and training required to work on an industrial site or within laboratory facilities of the University.

Module Aims: After passing Part One students will need to conduct a research project and write a dissertation.

The module aims to develop fundamental research skills. It comprises the development of supervised research work leading to a dissertation in the field of the Master's degree programme. The specific research topic will be chosen by the student following consultation with academic staff.

Module Content: Study for the dissertation, which may be based on practical, industrial, or literature work, or any combination of these, is primarily carried out over a period of about 12 weeks, with the dissertation being submitted at the end of September. Preparatory work on the dissertation may take place during Part One of the programme but students will only be permitted to submit their dissertation following successful completion of Part One.

In conducting the research project and dissertation the student will be exposed to all aspects of modern information retrieval processes, the organisation and resourcing of research and the organising and presentation of experimental data. The student must make inferences on conclusions, based on the evidence provided and supported by the research work. Furthermore they must assess the significance of this work in relation to the field and make suggestions about how further work could improve or clarify the research problem. The results of the project will be disseminated in a substantial dissertation demonstrating the student's ability to research a subject in depth.

The student will meet regularly with the supervisor to ensure that the project is well developed and organised. Progress will be monitored.

Intended Learning Outcomes: Technical Outcomes

On completion of this module, students should have the ability to:

- Investigate a research topic in detail.
- Formulate research aims.
- Devise and plan a research strategy to fulfil the aims.

• Carry out research work - undertake a literature search, a laboratory based or computer based investigation or a combination of these.

- Gather, organize and use evidence, data and information from a variety of primary and secondary sources.
- Critically analyse information.
- Make conclusions supported by the work and identify their relevance to the broader research area.

• Resolve or refine a research problem, with reasoned suggestions about how to improve future research efforts in the field.

• Produce a report (dissertation), with the findings presented in a well organised and reasoned manner.

Accreditation Outcomes

A comprehensive understanding of the relevant scientific principles of the specialisation (SM1fl)

A critical awareness of current problems and/or new insights most of which is at, or informed by, the forefront of the specialisation (SM2fl)

Understanding of concepts relevant to the discipline, some from outside engineering, and the ability to evaluate them critically and to apply them effectively, including in engineering projects (Sm3fl)

Ability to collect and analyse research data and to use appropriate engineering analysis tools in tackling unfamiliar problems, such as those with uncertain or incomplete data or specifications, by the appropriate innovation, use or adaptation of engineering analytical methods (EA3fl)

Knowledge, understanding and skills to work with information that may be incomplete or uncertain, quantify the effect of this on the design and, where appropriate, use theory or experimental research to mitigate deficiencies (D1fl) Knowledge and comprehensive understanding of design processes and methodologies and the ability to apply and adapt them in unfamiliar situations (D2fl)

Ability to generate an innovative design for products, systems, components or processes to fulfil new needs (D3fl) Knowledge and understanding of management and business practices, their limitations, and how these may be applied in the context of the particular specialisation (ET3fl)

Awareness of and ability to make general evaluations of risk issues in the context of the particular specialisation, including health & safety, environmental and commercial risk (ET6fl)

Advanced level knowledge and understanding of a wide range of engineering materials and components (EP1fl)Assessment:Project (100%)

Assessment Description: The research project and dissertation forms Part Two of the Masters degree.

Students should refer to:

https://www.swansea.ac.uk/academic-services/academic-guide/postgraduate-taught-awards-regulations/standard-taught-masters/

In particular, section 14 will provide further Information about dissertation preparation and submission.

The word limit is 20,000. This is for the main text and does not include appendices (if any), essential footnotes, introductory parts and statements or the bibliography and index.

Each student is to submit an electronic copy of their dissertation through the Turnitin link on Canvas by the deadline of 30th September. The online system will automatically check the similarity of the report.

The dissertation must contain:

• A statement that it is being submitted in partial fulfilment of the requirements for the degree;

• A summary of the dissertation not exceeding 300 words in length;

• A statement, signed by you, showing to what extent the work submitted is the result of your own investigation.

• Acknowledgement of other sources shall be made by footnotes giving explicit references. A full bibliography should be appended to the work;

• A declaration, signed by you, to certify that the work has not already been accepted in substance for any degree, and is not being concurrently submitted in candidature for any degree; and

• A signed statement regarding availability of the thesis.

The dissertation is marked by the supervisor and another member of staff and sent to an External Examiner for moderation. An Internal Exam Board is then held to confirm the mark. Finally, all marks are ratified at the University Postgraduate Taught Examination Board.

Moderation approach to main assessment: Universal double-blind marking

Assessment Feedback: Informal feedback will be given during regular meetings with supervisors. The supervisor will also provide an assessment of the project drafting skills during the planning of the dissertation. Work will be returned according to specified deadlines and accompanied by constructive comment.

A feedback session will be given to any student who fails their dissertation and is permitted by the Award Board to resubmit their work.

Failure Redemption: Candidates who fail the dissertation are given an opportunity to resubmit the dissertation within 3 months of the result of the examination if a full-time student or 6 months for part-time students. Such students will be given one formal feedback session, including written feedback on the reasons for failure, immediately following confirmation of the result by the University Postgraduate Taught Examination Board. The opportunity to resubmit will only be offered to students who submit a dissertation and are awarded a fail. Those candidates who do not submit a dissertation will not be offered a resubmission opportunity.

Additional Notes: Delivery of both teaching and assessment will be blended including live and self-directed activities online and on-campus.

The Faculty of Science and Engineering has a ZERO TOLERANCE penalty policy for late submission of all coursework and

continuous assessment.

If an extension is deemed appropriate a Postgraduate Taught Masters 'Application for Extension to the Submission Deadline/ Period of Candidature' Form will need to be submitted as follows:

• 30 September – deadline for Part Two students (non-resit students).

• 15 December – deadline for Part Two students (students who had resits).

AT-M76 Radio and Optical Wireless Communications

Credits: 10 Session: 2022/23 September-January

Pre-requisite Modules:

Co-requisite Modules: AT-M51; AT-M56

Lecturer(s): Prof L Li, Prof A Mehta Format: Lectures 20 hours; Direct

Lectures 20 hours; Directed private study 80 hours Contact Hours will be delivered through a blend of live activities online and on-campus, and may include, for example, lectures, seminars, practical sessions and Academic Mentoring sessions.

Delivery Method: All Programmes will employ a blended approach to delivery using the Canvas Digital Learning Platform for live and self-directed online activity, with live and self-directed on-campus activities each week. Students may also have the opportunity to engage with online versions of sessions delivered on-campus

Examination 90% and continuous assessment 10%

This module is assessed by a combination of examination and continual assessment. In order for the continual assessment marks to count, you must achieve at least 40% in the exam component. If you achieve less than 40% in the exam, then the module mark will be just the exam mark.

Module Aims: The module reviews linear modulations, channel models for radio wave propagation in wireless communications, and the receiver design principles. The transmission diversity techniques are also included. In the second part, the techniques used in optical wireless communications are explained.

Module Content:

- Point to point wireless communications and linear modulations.
- Propagation models in radio frequency and optical wireless communications.
- Receiver design principles.
- Diversity techniques.
- Performance evaluation.
- Optical wireless techniques.

Intended Learning Outcomes: Technical Outcomes

After completing the module you should be able to:

- Understand transmitter and receiver structure for linear modulations.
- Understand models of radio wave propagation, and how to design the corresponding receiver.
- Understand how to analyze point to point wireless links.
- Understand the principles of optical free-space propagation.
- Understand the components and the design of optical wireless links.

Accreditation Outcomes (AHEP)

-A comprehensive understanding of the relevant scientific principles of the specialisation (Sm1fl)

- Knowledge and comprehensive understanding of design processes and methodologies and the ability to apply and adapt them in unfamiliar situations (D7m/D2fl)

| Assessment: | Examination (90%) |
|--------------------------|---------------------------------------|
| | Coursework 1 (10%) |
| Resit Assessment: | Examination (Resit instrument) (100%) |

Assessment Description:

Coursework 1- 10% students will be divided in week 6 into three groups to survey one of the following topics: "Use of Optical Wireless as backbone in case of Natural Catastrophes" "Use of drone-based optical wireless to cover rural areas"

"Optical Satellite Links"

By week 9 each group will present their survey organizing a Powerpoint presentation of 15 minutes made by all member of the group.

Examination: 90% - Answer 3 out of 4 questions

Resit 100% Exam (coursework mark will not be used)

This module is assessed by a combination of examination and continual assessment. In order for the continual assessment marks to count, you must achieve at least 40% in the exam component. If you achieve less than 40% in the exam, then the module mark will be just the exam mark.

Moderation approach to main assessment: Universal second marking as check or audit

Assessment Feedback: During dedicated lecture, via email and during office hours.

Failure Redemption:

If rules allow - standard University provisions with marks capped. Any re-examination of this module will be by written examination only (100%).

Additional Notes: Delivery of both teaching and assessment will be blended including live and self-directed activities online and on-campus.

• AVAILABLE TO Visiting and Exchange students.

• The Faculty of Science and Engineering has a ZERO TOLERANCE penalty policy for late submission of all coursework and continuous assessment.

• Notes, worked examples and past papers for this module can be found on Canvas.

• This module is assessed by a combination of examination and continual assessment. In order for the continual assessment marks to count, you must achieve at least 40% in the exam component. If you achieve less than 40% in the exam, then the module mark will be just the exam mark.

AT-M79 Optical Networks

Credits: 10 Session: 2022/23 January-June

Pre-requisite Modules:

Co-requisite Modules:

Lecturer(s): Dr KM Ennser

Format: Lectures 20 hours; preparation for assignment 30 hours; directly private study 50 hours.

Delivery Method: All Programmes will employ a blended approach to delivery using the Canvas Digital Learning Platform for live and self-directed online activity, with live and self-directed on-campus activities each week. Students may also have the opportunity to engage with online versions of sessions delivered on-campus

A combination of lectures on campus and online teaching material.

A blended learning approach to class contact will be used in which the key concepts and readings will be introduced and understanding tested using online quizzes.

Module Aims: This module presents the essential element of modern optical networking, both in backbone and broadband access scenarios. The module evaluates WDM, the most popular, bandwidth-rich contemporary approach and also others, including optical time multiplexing and photonic packet switching. Relevant telecommunication protocol standards, client layers, and principles of networking design, network dimensioning and planning are covered. Key demonstrators and field hardened trials are presented.

Module Content:

• Client layers of optical layer.

• Network elements and topologies.

• Local, Access and Metro Networks and Data Centres: Architecture and future trends.

• Photonic Packet Switching: Optical time division multiplexing (OTDM), photonic switching node design, broadcast OTDM networks and testbeds.

• Testbed examples.

Intended Learning Outcomes: After completing the module you should be able to:

• Understand different client layers and relevant standards.

• Evaluate different WDM network elements and topologies including broadcast-and-select and wavelength routing networks.

• Understand and design of optical local, access and metro networks.

• Analyse photonic packet switching networks and time-domain optical networking approaches.

• Appraise the evolution of modern optical networks through the assessment of key network demonstrators and field implementations.

Accreditation Outcomes (AHEP):

EA2fl Ability to use fundamental knowledge to investigate new and emerging technologies.

EA3fl Ability to collect and analyse research data and to use appropriate engineering analysis tools in tackling unfamiliar problems, such as those with uncertain or incomplete data or specifications, by the appropriate innovation, use or adaptation of

engineering analytical methods.

D1m Understand and evaluate business, customer and user needs, including considerations such as the wider engineering context, public perception and aesthetics.

D2m Investigate and define the problem, identifying any constraints including environmental and sustainability limitations; ethical, health, safety, security and risk issues; intellectual property; codes of practice and standards. D1fl Knowledge, understanding and skills to work with information that may be incomplete or uncertain, quantify the effect of this on the design and, where appropriate, use theory or experimental research to mitigate deficiencies. ET2fl Awareness that engineers need to take account of the commercial and social contexts in which they operate,

ET5fl Awareness of relevant regulatory requirements governing engineering activities in the context of the particular specialisation,

EP4m Understanding of the use of technical literature and other information sources

EP2fl A thorough understanding of current practice and its limitations, and some appreciation of likely new developments

| Assessment: | Examination (60%) |
|-------------------|---------------------------------------|
| | Group Work - Presentation (20%) |
| | Assignment 1 (10%) |
| | Assignment 2 (10%) |
| Degit Aggegement. | Examination (Resit instrument) (100%) |

Assessment Description: The module is based on Examination (60%) and Continuous Assessments (40%).

The Group Work - Presentation (20%) is a group activity and it consists of delivering a short report and a presentation on a given topic on optical networking. The individual assignments consists of two online quizzes (each 10%)

Zero Tolerance Penalty for late submission of Continuous Assessment. Late submissions are given Zero (0%) mark.

• This module is assessed by a combination of examination and continual assessment. In order for the continual assessment marks to count, you must achieve at least 40% in the exam component. If you achieve less than 40% in the exam, then the module mark will be just the exam mark.

Moderation approach to main assessment: Universal second marking as check or audit

Assessment Feedback: The feedback is provided during lectures whenever possible or during office opening hours. **Failure Redemption:** If rules allow - standard University provision with marks capped. Failure Redemption of this module will be by Examination only (100%).

Additional Notes: Delivery of both teaching and assessment will be blended including live and self-directed activities online and on-campus.

• AVAILABLE TO to Visiting and Exchange students.

• Notes, worked examples and past papers for this module can be found on Canvas.

• The Faculty of Science and Engineering has a ZERO TOLERANCE penalty policy for late submission of all coursework and continuous assessment.

• This module is assessed by a combination of examination and continual assessment. In order for the continual assessment marks to count, you must achieve at least 40% in the exam component. If you achieve less than 40% in the exam, then the module mark will be just the exam mark.

AT-M80 Optical Fibre Communications

Credits: 10 Session: 2022/23 September-January

Pre-requisite Modules:

Co-requisite Modules:

Lecturer(s): Dr KM Ennser

Format: On-demand lecture materials: 20 hours; Live Discussion & Examples Classes: 10 hours; Directed Private Study: 70 hours Contact Hours will be delivered through a blend

Contact Hours will be delivered through a blend of live activities online and on-campus, and may include, for example, lectures, seminars, practical sessions and Academic Mentoring sessions.

Delivery Method: All Programmes will employ a blended approach to delivery using the Canvas Digital Learning Platform for live and self-directed online activity, with live and self-directed on-campus activities each week. Students may also have the opportunity to engage with online versions of sessions delivered on-campus

A blended learning approach to class contact will be used in which the key concepts and readings will be introduced and understanding tested using online quizzes.

The live classes will focus on discussions and examples classes (one hour per week). Live teaching sessions will be reinforced by making worked solutions available after class.

Each week will require around 2-3 hours of student engagement to review all the on-demand materials, complete the formative assessments and engage in class discussions.

Module Aims: This module is devoted to the technology underlying optical fibre communication systems. It covers the fundamental properties of optical fibres and key components, and the principles of operation of systems including WDM based high capacity transport networks. The network architecture designs and performance metrics are examined. Modern topics are introduced such as advanced modulation formats, coherent communications, spectrum efficiency and Shannon limit capacity.

Module Content:

• Introduction to optical fibre technology

• Enabling technologies: Laser sources and filters, couplers, isolators, circulators, optical multiplexers, optical amplifiers, dispersion compensators.

• Transmission systems: crosstalk, dispersion, fibre nonlinearities, noise and system sensitivity, link power budget, repeater spacing.

• Wavelength division multiplexing (WDM) systems and key components.

• WDM amplifier and system design, coherent detection and polarisation multiplexing.

Intended Learning Outcomes: After completing this module you should be able to:

- * Understand the fundamentals of optical fibre technology and their implications in optical fibre communications
- * Appraise key components and their technologies that enable modern optical networks
- * Design optical transmission systems for different architecture scenarios
- * Evaluate transmission performance and apply quantitative and qualitative metrics

The following AHEP 3 Programme Learning outcomes at Partial CEng (Further learning) (fl) and CEng (m) are partially addressed at a threshold level by this module:

* Ability to use fundamental knowledge to investigate new and emerging technologies including optical communications WDM channels digital optical signals and systems, optical propagation and waveguides (fibres), modulation and coding techniques of optical signal including phase and multilevel, organisation and operation of optical communications networks, optical network architectures and noise in amplified optical communications systems. (EA5m, EA2fl assessed by coursework and exam)

*Ability to apply a systematic approach to the analysis and design of optical communication links taking into account technical constraints such as crosstalk, dispersion, fibre nonlinearities and noises. (EA6m, EA3fl, assessed by coursework and exam)

* Ability to apply a systematic approach to the analysis and design of optical communication links taking into account health, safety and environmental issues, the cost versus performance trade-off, International Telecommunications Union (ITU) standards and social-economical issues. (D2m assessed by coursework and exam)

* Ability to apply several quantitative and qualitative metrics (eg, eye-diagram, Q factor, bit error rate, optical signalto-noise ratio, amplifier noise figure) in the analysis of network performance and design. (D3m, D1fl, assessed by coursework and exam)

*Appreciation of technology choices based on cost, capacity and demand in the context of optical fibre telecommunication. Understanding the different requirements in local access, metropolitan area, terrestrial high capacity networks and submarine links. (ET2m, ET2fl, assessed by coursework and exam).

*Knowledge of relevant legal and contractual issues (EP5m)

* A thorough understanding of current practice in the key components and their configurations in high speed optical (WDM) systems including different fibre types, amplifiers, multiplexers and compensators. (EP9m, EP2fl, assessed by coursework and exam)

*Cost and commercial constraints on system design, e.g. why amplifier spacing is maximised, access network architecture. Commercial long-distance system design and installation are presented and discussed the requirements and constraints, such as the use of solar panels to feed equipment in a desert area, positioning of the nodes due to geographic limitations (EP10m, EP2fl, assessed by coursework and exam)

| Assessment: | Exam - open book (70%) |
|-------------------|---------------------------------------|
| | Coursework 1 (5%) |
| | Coursework 2 (5%) |
| | Coursework 3 (5%) |
| | Coursework 4 (5%) |
| | Group Work - Coursework (10%) |
| Resit Assessment. | Examination (Resit instrument) (100%) |

Resit Assessment: Examination (Resit instrument) (100%)

Assessment Description: The module is assessed by an exam (70%), four pieces of coursework (20%) and a group design case study (10%). The four pieces of coursework are a mix of written assignments and online quizzes.

Zero tolerance for a late submission.

This module is assessed by a combination of examination and continual assessment. In order for the continual assessment marks to count, you must achieve at least 40% in the exam component. If you achieve less than 40% in the exam, then the module mark will be just the exam mark.

Moderation approach to main assessment: Universal second marking as check or audit

Assessment Feedback: The students receive feedback on the coursework during lectures and via Canvas. Failure Redemption: If rules allow - standard University provision with marks capped. Failure Redemption will be by Examination.

Additional Notes: Delivery of both teaching and assessment will be blended including live and self-directed activities online and on-campus.

The Faculty of Science and Engineering has a ZERO TOLERANCE penalty policy for late submission of coursework and continuous assessment.

This module is assessed by a combination of examination and continual assessment. In order for the continual assessment marks to count, you must achieve at least 40% in the exam component. If you achieve less than 40% in the exam, then the module mark will be just the exam mark.

CSCM18 IT-Security: Cryptography and Network Security

| Delivery Method: On-campus/virtual lectures and lab sessions. Module Aims: The aim of this course is to examine theoretical and practical aspects of computer and network ecurity. Module Content: Security threats and their causes. Security criteria and models. Tryptography: including basic encryption, DES, AES, hash functions. Access Control. security orbits and frameworks: including IPSec, TLS, SSL, SSH and related tools. //ulnerabilities and attacks: including port scanning, packet sniffing, SQL injection. security on the cloud. Intended Learning Outcomes: Students will have the ability to identify security threats and their causes in today's somputing infrastructures. Students will be able to explain in detail and apply techniques from Crytography and Cryptanalysis. Students will be able to apply techniques to enhance the security of existing systems, and gain a critical awareness of he limits of these techniques. Students will be able to reflect and critique on cryptographic techniques and secure systems design. Assessment: Examination 1 (70%) Coursework 1 (10%) Laboratory work (10%) Laboratory work (10%) Assessment: Examination (Resit instrument) (100%) Assessment: Examination (Resit instrument) (100%) Assessment: Examination (Resit instrument) (100%) Assessment: Examination mathemaselesson of the security of examination (70%). | CSCM18 I | T-Security: Cryptography and Network Security |
|--|-----------------------|---|
| Co-requisite Modules: cecturer(s): Dr P Kumar, Dr PD James Sormat: 30 hours lectures and labs Delivery Method: On-campus/virtual lectures and lab sessions. Module Aims: The aim of this course is to examine theoretical and practical aspects of computer and network ecurity. Module Content: Security threats and their causes. Security criteria and models. Typtography: including basic encryption, DES, AES, hash functions. Secess Control. Security tools and frameworks: including port scanning, packet sniffing, SQL injection. Security issues in wireless networks. Security on the cloud. Intended Learning Outcomes: Students will have the ability to identify security threats and their causes in today's computing infrastructures. Students will be able to explain in detail and apply techniques from Crytography and Cryptanalysis. Students will be able to apply techniques to enhance the security of existing systems, and gain a critical awareness of he limits of these techniques. Students will be able to reflect and critique on cryptographic techniques and secure systems design. Assessment: Examination 1 (70%) Coursework 1 (10%) Coursework 2 (10%) Laboradd Computer Science format unscen examination (70%). Scoursevork 3 dom in a lab. Moderation approach to main assessment: Second marking as sampling or moderation Vssessment Examination (Resit instrument) (100% | Credits: 15 Sess | ion: 2022/23 September-January |
| ecturer(s): Dr P Kumar, Dr PD James Format: 30 hours lectures and labs Pelivery Method: On-campus/virtual lectures and lab sessions. Module Aims: The aim of this course is to examine theoretical and practical aspects of computer and network ecurity. Module Content: Security threats and their causes. Security criteria and models. Typtography: including basic encryption, DES, AES, hash functions. Access Control. security criteria and models. Security criteria and models. Zuptography: including port scanning, packet sniffing, SQL injection. Security tools and frameworks: including port scanning, packet sniffing, SQL injection. security on the cloud. Security to identify security threats and their causes in today's computing infrastructures. students will be able to explain in detail and apply techniques from Crytography and Cryptanalysis. Students will be able to explain in detail and apply techniques from Crytography and Cryptanalysis. students will synthesize the concepts of design, defensive programming, as well as their application to o build robust and resilient systems. Students will be able to reflect and critique on cryptographic techniques and secure systems design. Ausessment: Examination 1 (70%) Coursework 2 (10%) Coursework 2 (10%) Laboratory work (10%) Secsent Coursework 2 (10%) Assessment: Examination (Resit instrument) (100%) Secsent Feedback: Outl | Pre-requisite M | odules: |
| Format: 30 hours lectures and labs Delivery Method: On-campus/virtual lectures and lab sessions. Module Aims: The aim of this course is to examine theoretical and practical aspects of computer and network ecurity. Module Content: Security threats and their causes. isecurity criteria and models. Cryptography: including basic encryption, DES, AES, hash functions. isecurity criteria and models. Cryptography: including basic encryption, DES, AES, hash functions. isecurity tools and frameworks: including IPSec, TLS, SSL, SSH and related tools. Vulnerabilities and attacks: including port scanning, packet sniffing, SQL injection. isecurity tools and frameworks. iecurity tools and frameworks. isecurity tools and frameworks. iecurity on the cloud. neteded Learning Outcomes: Students will have the ability to identify security threats and their causes in today's onputing infrastructures. students will synthesize the concepts of design, defensive programming, as well as their application to o build robust and resilient systems. students will be able to apply techniques to enhance the security of existing systems, and gain a critical awareness of he limits of these techniques. students will be able to reflect and critique on cryptographic techniques and secure systems design. Assessment: Examination 1 (70%) Coursework 1 (10%) Coursework 2 (10%) Laboratory work (10%) Stesessment: Examination (Resit instrument) (100%) | | |
| Delivery Method: On-campus/virtual lectures and lab sessions. Module Aims: The aim of this course is to examine theoretical and practical aspects of computer and network ecurity. Module Content: Security threats and their causes. Security criteria and models. Cryptography: including basic encryption, DES, AES, hash functions. Access Control. Security tools and frameworks: including IPSec, TLS, SSL, SSH and related tools. Vulnerabilities and attacks: including port scanning, packet sniffing, SQL injection. Security on the cloud. Intended Learning Outcomes: Students will have the ability to identify security threats and their causes in today's computing infrastructures. Students will synthesize the concepts of design, defensive programming, as well as their application to o build robust and resilient systems. Students will be able to apply techniques to enhance the security of existing systems, and gain a critical awareness of the limits of these techniques. Students will be able to reflect and critique on cryptographic techniques and secure systems design. Assessment: Examination 1 (70%) Coursework 2 (10%) Laboratory work (10%) Assessment Description: Standard Computer Science format unseen examination (70%). Courseworks done in a lab. Moderation approach to main assessment: Second marking as sampling or moderation assessment feedback: Outline solutions provided along with group and individual analytical feedback for courseworks. <tr< td=""><td>Lecturer(s): Dr</td><td>P Kumar, Dr PD James</td></tr<> | Lecturer(s): Dr | P Kumar, Dr PD James |
| Module Aims: The aim of this course is to examine theoretical and practical aspects of computer and network ecurity. Module Content: Security threats and their causes. security criteria and models. Tryptography: including basic encryption, DES, AES, hash functions. Access Control. security toris and frameworks: including IPSec, TLS, SSL, SSH and related tools. //ulnerabilities and attacks: including port scanning, packet sniffing, SQL injection. security tools and frameworks: including port scanning, packet sniffing, SQL injection. security issues in wireless networks. security up the cloud. Intended Learning Outcomes: Students will have the ability to identify security threats and their causes in today's computing infrastructures. situdents will be able to explain in detail and apply techniques from Crytography and Cryptanalysis. students will be able to apply techniques to enhance the security of existing systems, and gain a critical awareness of he limits of these techniques. students will be able to reflect and critique on cryptographic techniques and secure systems design. Assessment: Examination 1 (70%) Coursework 2 (10%) Laboratory work (10%) Coursework 2 (10%) Laboratory work (10%) Xesessment Examination 1 (70%) Courseworks and work done in a lab. Moderation approach to main assessment: Second marking as sampling or moderation Assessment Feedback: Outline solutions provided along with group and individual analytical feedback for oourseworks. </td <td>Format: 30</td> <td>hours lectures and labs</td> | Format: 30 | hours lectures and labs |
| ecurity. Module Content: Security threats and their causes. iccurity criteria and models. Eryptography: including basic encryption, DES, AES, hash functions. Access Control. Security tools and frameworks: including IPSec, TLS, SSL, SSH and related tools. Vulnerabilities and attacks: including port scanning, packet sniffing, SQL injection. Security issues in wireless networks. Security issues in wireless networks. Security issues in wireless networks. Security on the cloud. Intended Learning Outcomes: Students will have the ability to identify security threats and their causes in today's computing infrastructures. Students will be able to explain in detail and apply techniques from Crytography and Cryptanalysis. Students will be able to explain in detail and papply techniques from Crytography and Cryptanalysis. Students will be able to apply techniques to enhance the security of existing systems, and gain a critical awareness of he limits of these techniques. Students will be able to reflect and critique on cryptographic techniques and secure systems design. Assessment: Examination 1 (70%) Coursework 2 (10%) Laboratory work (10%) Resit Assessment: Examination Computer Science format unseen examination (70%). P. Courseworks and work done in a lab. Moderation approach to main assessment: Second marking as sampling or moderation Assessment Feedback: Outline solutions provided along with group and individual analytical | Delivery Metho | d: On-campus/virtual lectures and lab sessions. |
| Module Content: Security threats and their causes. Security criteria and models. Cryptography: including basic encryption, DES, AES, hash functions. Access Control. Security tools and frameworks: including port scanning, packet sniffing, SQL injection. Security such wireless networks. Security on the cloud. Intended Learning Outcomes: Students will have the ability to identify security threats and their causes in today's somputing infrastructures. Students will be able to explain in detail and apply techniques from Crytography and Cryptanalysis. Students will synthesize the concepts of design, defensive programming, as well as their application to o build robust and resilient systems. Students will be able to explain in detail und apply techniques from Crytography and Cryptanalysis. Students will be able to apply techniques to enhance the security of existing systems, and gain a critical awareness of he limits of these techniques. Students will be able to reflect and critique on cryptographic techniques and secure systems design. Assessment: Examination 1 (70%) Coursework 1 (10%) Coursework 2 (10%) Laboratory work (10%) Xessessment Description: Standard Computer Science format unseen examination (70%). Courseworks and work done in a lab. Moderation approach to main assessment: Second marking as sampling or moderation Assessment Feedback: Outline solutions provided along with group and individual analytical feedback for ourseworks. Stamination feedback | | he aim of this course is to examine theoretical and practical aspects of computer and network |
| kecurity criteria and models. Tryptography: including basic encryption, DES, AES, hash functions. Access Control. kecurity tools and frameworks: including IPSec, TLS, SSL, SSH and related tools. /ulnerabilities and attacks: including port scanning, packet sniffing, SQL injection. isecurity issues in wireless networks. isecurity on the cloud. Intended Learning Outcomes: Students will have the ability to identify security threats and their causes in today's computing infrastructures. Students will be able to explain in detail and apply techniques from Crytography and Cryptanalysis. Students will be able to explain in detail and apply techniques from Crytography and a their application to o build robust and resilient systems. Students will be able to apply techniques to enhance the security of existing systems, and gain a critical awareness of he limits of these techniques. Students will be able to reflect and critique on cryptographic techniques and secure systems design. Assessment: Examination 1 (70%) Coursework 1 (10%) Coursework 2 (10%) Laboratory work (10%) Coursework 2 (10%) Causeworks and work done in a lab. Moderation approach to main assessment: Second marking as sampling or moderation Assessment Feedback: Outline solutions provided along with group and individual analytical feedback for ourseworks. Zamination feedback summarising strengths and weaknesses of the class. Zamination Resit exam. Vaditional Notes: | <i>v</i> | |
| Cryptography: including basic encryption, DES, AES, hash functions. Access Control. Security tools and frameworks: including IPSec, TLS, SSL, SSH and related tools. Vulnerabilities and attacks: including port scanning, packet sniffing, SQL injection. Security issues in wireless networks. Security on the cloud. Intended Learning Outcomes: Students will have the ability to identify security threats and their causes in today's Somputing infrastructures. Students will be able to explain in detail and apply techniques from Crytography and Cryptanalysis. Students will synthesize the concepts of design, defensive programming, as well as their application to o build robust and resilient systems. Students will be able to apply techniques to enhance the security of existing systems, and gain a critical awareness of the limits of these techniques. Students will be able to reflect and critique on cryptographic techniques and secure systems design. Assessment: Examination 1 (70%) Coursework 1 (10%) Coursework 2 (10%) Laboratory work (10%) Coursework 2 (10%) Assessment Examination (Resit instrument) (100%) Assessment Examination (Resit instrument) (100%) Assessment Examination Resit instrument) (100%) Assessment Ecedback: Outline solutions provided along with group and individual analytical feedback for fourseworks. Zamination feedback summarising strengths and weaknesses of the class. | | |
| Access Control. Security tools and frameworks: including IPSec, TLS, SSL, SSH and related tools. /ulnerabilities and attacks: including port scanning, packet sniffing, SQL injection. Security issues in wireless networks. Security on the cloud. Intended Learning Outcomes: Students will have the ability to identify security threats and their causes in today's iomputing infrastructures. Students will be able to explain in detail and apply techniques from Crytography and Cryptanalysis. Students will be able to explain in detail and apply techniques from Crytography and Cryptanalysis. Students will be able to explain in detail and apply techniques from Crytography and Cryptanalysis. Students will be able to apply techniques to enhance the security of existing systems, and gain a critical awareness of he limits of these techniques. Students will be able to reflect and critique on cryptographic techniques and secure systems design. Assessment: Examination 1 (70%) Coursework 1 (10%) Coursework 2 (10%) Laboratory work (10%) Assessment Description: Standard Computer Science format unseen examination (70%). P. Courseworks and work done in a lab. Moderation approach to main assessment: Second marking as sampling or moderation Assessment Feedback: Outline solutions provided along with group and individual analytical feedback for iourseworks. Stamination feedback summarising strengths and weaknesses of the class. Failure Redemption: Resit exam. Miditional Notes: | • | |
| Security tools and frameworks: including IPSec, TLS, SSL, SSH and related tools. //uherabilities and attacks: including port scanning, packet sniffing, SQL injection. Security issues in wireless networks. Security on the cloud. Intended Learning Outcomes: Students will have the ability to identify security threats and their causes in today's computing infrastructures. Students will be able to explain in detail and apply techniques from Crytography and Cryptanalysis. Students will synthesize the concepts of design, defensive programming, as well as their application to o build robust and resilient systems. Students will be able to apply techniques to enhance the security of existing systems, and gain a critical awareness of the limits of these techniques. Students will be able to reflect and critique on cryptographic techniques and secure systems design. Assessment: Examination 1 (70%) Coursework 1 (10%) Coursework 2 (10%) Laboratory work (10%) Assessment: Examination (Resit instrument) (100%) Assessment: Examination Resit instrument) (100%) Assessment Feedback: Outline solutions provided along with group and individual analytical feedback for sourseworks. Science of the able solutions provided along with group and individual analytical feedback for sourseworks. Xariantation feedback summarising strengths and weaknesses of the class. *ailure Redemption: Resit exam. Viditional Notes: | | cluding basic encryption, DES, AES, hash functions. |
| Auhnerabilities and attacks: including port scanning, packet sniffing, SQL injection. Security issues in wireless networks. Security issues in wireless networks. Security on the cloud. Intended Learning Outcomes: Students will have the ability to identify security threats and their causes in today's computing infrastructures. Students will be able to explain in detail and apply techniques from Crytography and Cryptanalysis. Students will synthesize the concepts of design, defensive programming, as well as their application to o build robust and resilient systems. Students will be able to apply techniques to enhance the security of existing systems, and gain a critical awareness of he limits of these techniques. Students will be able to reflect and critique on cryptographic techniques and secure systems design. Assessment: Examination 1 (70%) Coursework 1 (10%) Coursework 2 (10%) Laboratory work (10%) Resit Assessment: Examination (Resit instrument) (100%) Assessment Description: Standard Computer Science format unseen examination (70%). 2: Courseworks and work done in a lab. Moderation approach to main assessment: Second marking as sampling or moderation Assessment Feedback: Outline solutions provided along with group and individual analytical feedback for courseworks. Standard Redemption: Resit exam. Additional Notes: Notes: <td></td> <td></td> | | |
| Security issues in wireless networks. Security on the cloud. Intended Learning Outcomes: Students will have the ability to identify security threats and their causes in today's somputing infrastructures. Students will be able to explain in detail and apply techniques from Crytography and Cryptanalysis. Students will be able to apply techniques to enhance the security of existing systems, and gain a critical awareness of he limits of these techniques. Students will be able to reflect and critique on cryptographic techniques and secure systems design. Assessment: Examination 1 (70%) Coursework 1 (10%) Coursework 2 (10%) Laboratory work (10%) Resit Assessment: Examination (Resit instrument) (100%) Assessment Texamination Resit instrument) (100%) Assessment Security and Computer Science format unseen examination (70%). Courseworks and work done in a lab. Moderation approach to main assessment: Second marking as sampling or moderation Assessment Feedback: Outline solutions provided along with group and individual analytical feedback for sourseworks. Examination feedback summarising strengths and weaknesses of the class. Failure Redemption: Resit exam. Additional Notes: Additional Notes: | • | |
| Becurity on the cloud. Intended Learning Outcomes: Students will have the ability to identify security threats and their causes in today's computing infrastructures. Students will be able to explain in detail and apply techniques from Crytography and Cryptanalysis. Students will synthesize the concepts of design, defensive programming, as well as their application to o build robust and resilient systems. Students will be able to apply techniques to enhance the security of existing systems, and gain a critical awareness of he limits of these techniques. Students will be able to reflect and critique on cryptographic techniques and secure systems design. Assessment: Examination 1 (70%) Coursework 1 (10%) Coursework 2 (10%) Laboratory work (10%) Resit Assessment: Examination (Resit instrument) (100%) Assessment Description: Standard Computer Science format unseen examination (70%). 2 Courseworks and work done in a lab. Moderation approach to main assessment: Second marking as sampling or moderation Assessment Feedback: Outline solutions provided along with group and individual analytical feedback for courseworks. Stamination feedback summarising strengths and weaknesses of the class. "alure Redemption: Resit exam. Moditional Notes: Stamination Resit exam. | | |
| ntended Learning Outcomes: Students will have the ability to identify security threats and their causes in today's computing infrastructures. Students will be able to explain in detail and apply techniques from Crytography and Cryptanalysis. Students will synthesize the concepts of design, defensive programming, as well as their application to o build robust and resilient systems. Students will be able to apply techniques to enhance the security of existing systems, and gain a critical awareness of he limits of these techniques. Students will be able to reflect and critique on cryptographic techniques and secure systems design. Assessment: Examination 1 (70%) Coursework 1 (10%) Coursework 2 (10%) Laboratory work (10%) Resit Assessment: Examination Computer Science format unseen examination (70%). P: Courseworks and work done in a lab. Moderation approach to main assessment: Second marking as sampling or moderation Assessment Feedback: Outline solutions provided along with group and individual analytical feedback for sourseworks. Examination feedback summarising strengths and weaknesses of the class. *ailure Redemption: Resit exam. Additional Notes: Xeater Science format unseen feadback summarising strengths and weaknesses of the class. | • | |
| Students will be able to explain in detail and apply techniques from Crytography and Cryptanalysis. Students will synthesize the concepts of design, defensive programming, as well as their application to o build robust and resilient systems. Students will be able to apply techniques to enhance the security of existing systems, and gain a critical awareness of he limits of these techniques. Students will be able to reflect and critique on cryptographic techniques and secure systems design. Assessment: Examination 1 (70%) Coursework 1 (10%) Coursework 2 (10%) Laboratory work (10%) Resit Assessment Examination (Resit instrument) (100%) Assessment Description: Standard Computer Science format unseen examination (70%). Courseworks and work done in a lab. Moderation approach to main assessment: Second marking as sampling or moderation Assessment Feedback: Outline solutions provided along with group and individual analytical feedback for sourseworks. Stamination feedback summarising strengths and weaknesses of the class. Failure Redemption: Resit exam. Vaditional Notes: | | |
| Students will be able to explain in detail and apply techniques from Crytography and Cryptanalysis. Students will synthesize the concepts of design, defensive programming, as well as their application to o build robust and resilient systems. Students will be able to apply techniques to enhance the security of existing systems, and gain a critical awareness of he limits of these techniques. Students will be able to reflect and critique on cryptographic techniques and secure systems design. Assessment: Examination 1 (70%) Coursework 1 (10%) Coursework 2 (10%) Laboratory work (10%) Assessment: Examination (Resit instrument) (100%) Assessment: Examination (Resit instrument) (100%) Assessment Description: Standard Computer Science format unseen examination (70%). Courseworks and work done in a lab. Moderation approach to main assessment: Second marking as sampling or moderation Assessment Feedback: Outline solutions provided along with group and individual analytical feedback for sourseworks. Zaamination feedback summarising strengths and weaknesses of the class. Failure Redemption: Resit exam. Additional Notes: Voderational Notes: | | • • • • |
| Students will synthesize the concepts of design, defensive programming, as well as their application to Students will be able to apply techniques to enhance the security of existing systems, and gain a critical awareness of Students will be able to reflect and critique on cryptographic techniques and secure systems design. Assessment: Examination 1 (70%) Coursework 1 (10%) Coursework 2 (10%) Laboratory work (10%) Coursework 2 (10%) Assessment: Examination (Resit instrument) (100%) Assessment Description: Standard Computer Science format unseen examination (70%). 2: Ourseworks and work done in a lab. Moderation approach to main assessment: Assessment Feedback: Outline solutions provided along with group and individual analytical feedback for sourseworks. Examination feedback summarising strengths and weaknesses of the class. Evaluate Redemption: Resit exam. Additional Notes: Course of the solutions residue and weaknesses of the class. | | |
| o build robust and resilient systems. Students will be able to apply techniques to enhance the security of existing systems, and gain a critical awareness of he limits of these techniques. Students will be able to reflect and critique on cryptographic techniques and secure systems design. Assessment: Examination 1 (70%) Coursework 1 (10%) Coursework 2 (10%) Laboratory work (10%) Resit Assessment: Examination (Resit instrument) (100%) Assessment Description: Standard Computer Science format unseen examination (70%). 2: Courseworks and work done in a lab. Moderation approach to main assessment: Second marking as sampling or moderation Assessment Feedback: Outline solutions provided along with group and individual analytical feedback for sourseworks. Examination feedback summarising strengths and weaknesses of the class. Failure Redemption: Resit exam. Additional Notes: | | |
| Students will be able to apply techniques to enhance the security of existing systems, and gain a critical awareness of he limits of these techniques. Students will be able to reflect and critique on cryptographic techniques and secure systems design. Assessment: Examination 1 (70%) Coursework 1 (10%) Coursework 2 (10%) Laboratory work (10%) Resit Assessment: Examination (Resit instrument) (100%) Assessment Description: Standard Computer Science format unseen examination (70%). 2 Courseworks and work done in a lab. Moderation approach to main assessment: Second marking as sampling or moderation Assessment Feedback: Outline solutions provided along with group and individual analytical feedback for courseworks. Examination feedback summarising strengths and weaknesses of the class. Failure Redemption: Resit exam. Additional Notes: Examination Resit exam. | • | |
| he limits of these techniques. Students will be able to reflect and critique on cryptographic techniques and secure systems design. Assessment: Examination 1 (70%) Coursework 1 (10%) Coursework 2 (10%) Laboratory work (10%) Resit Assessment: Examination (Resit instrument) (100%) Assessment Description: Standard Computer Science format unseen examination (70%). 2: Courseworks and work done in a lab. Moderation Moderation approach to main assessment: Second marking as sampling or moderation Assessment Feedback: Outline solutions provided along with group and individual analytical feedback for courseworks. Examination feedback summarising strengths and weaknesses of the class. Failure Redemption: Resit exam. Additional Notes: Additional Notes: | | • |
| Students will be able to reflect and critique on cryptographic techniques and secure systems design. Assessment: Examination 1 (70%) Coursework 1 (10%) Coursework 2 (10%) Laboratory work (10%) Resit Assessment: Examination (Resit instrument) (100%) Assessment Description: Standard Computer Science format unseen examination (70%). P. Courseworks and work done in a lab. Moderation approach to main assessment: Moderation approach to main assessment: Second marking as sampling or moderation Assessment Feedback: Outline solutions provided along with group and individual analytical feedback for courseworks. Examination feedback summarising strengths and weaknesses of the class. Failure Redemption: Resit exam. Additional Notes: Additional Notes: | | |
| Assessment: Examination 1 (70%) Coursework 1 (10%) Coursework 2 (10%) Laboratory work (10%) Resit Assessment: Examination (Resit instrument) (100%) Assessment Description: Standard Computer Science format unseen examination (70%). 2 Courseworks and work done in a lab. Moderation approach to main assessment: Second marking as sampling or moderation Assessment Feedback: Outline solutions provided along with group and individual analytical feedback for rourseworks. Examination feedback summarising strengths and weaknesses of the class. Failure Redemption: Resit exam. Additional Notes: | | * |
| Coursework 1 (10%) Coursework 2 (10%) Laboratory work (10%) Resit Assessment: Examination (Resit instrument) (100%) Assessment Description: Standard Computer Science format unseen examination (70%). Courseworks and work done in a lab. Moderation approach to main assessment: Second marking as sampling or moderation Assessment Feedback: Outline solutions provided along with group and individual analytical feedback for courseworks. Examination feedback summarising strengths and weaknesses of the class. Failure Redemption: Resit exam. | Students will be | able to reflect and critique on cryptographic techniques and secure systems design. |
| Coursework 1 (10%) Coursework 2 (10%) Laboratory work (10%) Resit Assessment: Examination (Resit instrument) (100%) Assessment Description: Standard Computer Science format unseen examination (70%). Courseworks and work done in a lab. Moderation approach to main assessment: Second marking as sampling or moderation Assessment Feedback: Outline solutions provided along with group and individual analytical feedback for courseworks. Examination feedback summarising strengths and weaknesses of the class. Failure Redemption: Resit exam. | | |
| Coursework 1 (10%) Coursework 2 (10%) Laboratory work (10%) Resit Assessment: Examination (Resit instrument) (100%) Assessment Description: Standard Computer Science format unseen examination (70%). Courseworks and work done in a lab. Moderation approach to main assessment: Second marking as sampling or moderation Assessment Feedback: Outline solutions provided along with group and individual analytical feedback for courseworks. Examination feedback summarising strengths and weaknesses of the class. Failure Redemption: Resit exam. | | |
| Coursework 1 (10%) Coursework 2 (10%) Laboratory work (10%) Resit Assessment: Examination (Resit instrument) (100%) Assessment Description: Standard Computer Science format unseen examination (70%). Courseworks and work done in a lab. Moderation approach to main assessment: Second marking as sampling or moderation Assessment Feedback: Outline solutions provided along with group and individual analytical feedback for courseworks. Examination feedback summarising strengths and weaknesses of the class. Failure Redemption: Resit exam. | | |
| Coursework 1 (10%) Coursework 2 (10%) Laboratory work (10%) Resit Assessment: Examination (Resit instrument) (100%) Assessment Description: Standard Computer Science format unseen examination (70%). Courseworks and work done in a lab. Moderation approach to main assessment: Second marking as sampling or moderation Assessment Feedback: Outline solutions provided along with group and individual analytical feedback for courseworks. Examination feedback summarising strengths and weaknesses of the class. Failure Redemption: Resit exam. | Assessment: | Examination 1 (70%) |
| Coursework 2 (10%) Laboratory work (10%) Resit Assessment: Examination (Resit instrument) (100%) Assessment Description: Standard Computer Science format unseen examination (70%). Courseworks and work done in a lab. Moderation approach to main assessment: Second marking as sampling or moderation Assessment Feedback: Outline solutions provided along with group and individual analytical feedback for courseworks. Examination feedback summarising strengths and weaknesses of the class. Failure Redemption: Resit exam. Additional Notes: | | |
| Laboratory work (10%) Resit Assessment: Examination (Resit instrument) (100%) Assessment Description: Standard Computer Science format unseen examination (70%). Courseworks and work done in a lab. Moderation approach to main assessment: Second marking as sampling or moderation Assessment Feedback: Outline solutions provided along with group and individual analytical feedback for courseworks. Examination feedback summarising strengths and weaknesses of the class. Failure Redemption: Resit exam. Additional Notes: | | |
| Resit Assessment: Examination (Resit instrument) (100%) Assessment Description: Standard Computer Science format unseen examination (70%). Courseworks and work done in a lab. Moderation approach to main assessment: Second marking as sampling or moderation Assessment Feedback: Outline solutions provided along with group and individual analytical feedback for courseworks. Examination feedback summarising strengths and weaknesses of the class. Failure Redemption: Resit exam. Additional Notes: | | |
| Assessment Description: Standard Computer Science format unseen examination (70%). 2 Courseworks and work done in a lab. Moderation approach to main assessment: Second marking as sampling or moderation Assessment Feedback: Outline solutions provided along with group and individual analytical feedback for courseworks. Examination feedback summarising strengths and weaknesses of the class. Failure Redemption: Resit exam. Additional Notes: | | |
| Courseworks and work done in a lab. Moderation approach to main assessment: Second marking as sampling or moderation Assessment Feedback: Outline solutions provided along with group and individual analytical feedback for courseworks. Examination feedback summarising strengths and weaknesses of the class. Failure Redemption: Resit exam. Additional Notes: | | |
| Moderation approach to main assessment: Second marking as sampling or moderation Assessment Feedback: Outline solutions provided along with group and individual analytical feedback for courseworks. Examination feedback summarising strengths and weaknesses of the class. Failure Redemption: Resit exam. Additional Notes: | | - |
| Assessment Feedback: Outline solutions provided along with group and individual analytical feedback for courseworks. Examination feedback summarising strengths and weaknesses of the class. Failure Redemption: Resit exam. Additional Notes: | | |
| courseworks. Examination feedback summarising strengths and weaknesses of the class. Failure Redemption: Resit exam. Additional Notes: | | |
| Examination feedback summarising strengths and weaknesses of the class. Failure Redemption: Resit exam. Additional Notes: | courseworks. | |
| Failure Redemption: Resit exam. Additional Notes: | | back summarising strengths and weaknesses of the class. |
| Additional Notes: | | |
| | - | |
| verilelle to visiting and eveloped at deute | | ~- |
| a valiance to visuing and exchange suidents | Available to visit | ing and exchange students |

CSCM88 Network and Wireless Security

Credits: 15 Session: 2022/23 January-June

Pre-requisite Modules:

Co-requisite Modules:

Lecturer(s): Dr P Kumar

Format: 30 hours lectures and labs

Delivery Method: On campus lectures and labs.

Module Aims: Low cost networked computers add eyes and ears (or sensors) and arms, legs and voices (or actuators) to the Internet – called the Internet of Things (IoT) connected smart objects. Networking technologies play a critical role in almost all modern software-based systems, whether the fixed networks of computers, or the growing pervasive devices which have increasingly diverse profiles of network connectivity. As a result, they provide a potential vector for many forms of attack and are an ideal location for many threat mitigations and isolation technologies.

Module Content: Overview of Cryptography -- Basic encryption and decryption: terminology, substitution, stream, and block ciphers; characteristics of good ciphers. Symmetric and asymmetric encryption. Encryption algorithms: DES, RSA, AES, etc. Hashing.

Network fundamentals -- TCP/IP, SSL/TLS review, tools for network analysis, routing algorithms, threat modelling, network attachment protections: RADIUS, EAP, 802.1x, etc.

Network defense -- Form of firewalls, behaviours and design, and layered protections

Intrusion detection -- Techniques for detecting abnormal patterns of behaviours.

Mobile Network systems -- Security complexities introduced by mobility, security architecture and protocols.

Security in wireless sensor networks (WSN) -- WSN architectures and protocols, security threats, cryptographic primitives, key establishment and distribution, security of ZigBee WSNs, security of Industrial-IoT devices (as a case study), formal verification, and future trends.

Case Studies -- AKA (Authentication and Key Agreement): 4/5G security; IoT security – 6LowPAN and CoAP IETF standards.

Intended Learning Outcomes: 1) Students will have the ability to identify security vulnerabilities and their causes in modern networking infrastructures.

2) Students will be able to explain and apply techniques from networking protocols.

3) Students will be able to apply skills learned to designing and developing secure emerging wireless networks.

4) Students will be able to apply techniques to enhance the security of existing networks and gain a critical awareness of the limits of these techniques.

Assessment: Examination 1 (70%)

Laboratory work (30%)

Resit Assessment: Examination (Resit instrument) (100%)

Assessment Description: Standard Computer Science format unseen examination.

Project based lab.

Moderation approach to main assessment: Second marking as sampling or moderation

Assessment Feedback: Outline solutions provided along with group and individual analytical feedback for courseworks.

Examination feedback summarising strengths and weaknesses of the class.

Failure Redemption: Resit exam.

Additional Notes:

Available to students on Specialist Master programmes.

| EG-M190 Social, environmental and economic context of research |
|---|
| Credits: 10 Session: 2022/23 January-June |
| Pre-requisite Modules: |
| Co-requisite Modules: |
| Lecturer(s): Dr N Wint |
| Format:30 formal contact hours |
| 10 x 1 hour lectures |
| 10 x 2 hour interactive workshops |
| Delivery Method: All Programmes will employ a blended approach to delivery using the Canvas Digital Learning Platform for live and self-directed online activity, with live and self-directed on-campus activities each week. Student may also have the opportunity to engage with online versions of sessions delivered on-campus |
| Lecture and workshops |
| Module Aims: There is an increasing need for engineers to work towards complex, so called 'wicked problems', for |
| example the secure supply of energy. This necessitates a holistic approach and involves making decisions based on a range of different factors, and consideration for economic, ethical, social, political and environmental, as well as technical limitations. |
| Obtaining and making sense of such information involves types of knowledge and the use of tools and techniques that have not always been traditionally used within engineering disciplines. For example, ethical issues concerning negative impacts on environment or society may raise questions of value, duty or morality and requires the application of moral reasoning rather than scientific reasoning. |
| During this module we will make use of a variety of engineering case studies which exemplify the need to consider non-technical aspects of engineering projects. We will use qualitative research approaches and ethical frameworks to help in our engineering decision making. We will also consider the role of the engineer in policy making. Module Content: Different types of knowledge and research approaches used to obtain different types of knowledge |
| and information |
| The use of moral reasoning and ethical frameworks |
| Policy process and the role of the engineer in informing policy |
| Intended Learning Outcomes: Technical Outcomes |
| By the end of this module students should be able to: |
| Knowledge of the stages of a research project and how to select appropriate research methods. |
| Accreditation Outcomes (AHEP) |
| Awareness of the need for a high level of professional and ethical conduct in engineering (EL8M / ET1fl) |
| Awareness that engineers need to take account of the commercial and social contexts in which they operate (EL9M/ ET2fl) |
| Awareness that engineering activities should promote sustainable development (EL11M / ET4fl) |
| Assessment: Coursework 1 (60%) Coursework 2 (40%) |
| Participation Exercise (0%) |
| Resit Assessment: Coursework reassessment instrument (100%) |
| Assessment Description: Assessment One: Selection of a contemporary engineering topic/project. Outline of the role of different types of knowledge and information needed to inform project. Ethical, economic, social and environmental evaluations of the engineering issues involved. Assessment Two: A policy brief (choice of contemporary engineering topic) |
| r |

PASS/FAIL COMPONENT Minimum attendance and contribution to workshop sessions

Note, that this module cannot be passed if this pass/fail element is not passed. If you do not meet the requirements of the Pass/Fail component, you will receive a QF outcome. This means that you will be required to repeat the failed component(s), even if your module mark is above 50%

Moderation approach to main assessment: Universal second marking as check or audit

Assessment Feedback: Formative and peer feedback will be given in group/workshop sessions

Feedback during Q&As in lecture and example classes.

Lecturer available for ad-hoc feedback during office hours.

Written feedback on all coursework submitted

Failure Redemption: Students will be provided with the opportunity to resubmit failed components.

If engagement in group project activities is below required level, no supplementary will be possible and module will have to be resat in the following year.

Additional Notes: Delivery of both teaching and assessment will be blended including live and self-directed activities online and on-campus.

EG-M191 Communication Systems and Networks

Credits: 10 Session: 2022/23 January-June

Pre-requisite Modules:

Co-requisite Modules:

Lecturer(s): Dr JW Jones Format: Lectures 20 hours

Directed private study 80 hours

Contact Hours will be delivered through a blend of live activities online and on-campus, and may include, for example, lectures, seminars, practical sessions and Academic Mentoring sessions.

Delivery Method: All Programmes will employ a blended approach to delivery using the Canvas Digital Learning Platform for live and self-directed online activity, with live and self-directed on-campus activities each week. Students may also have the opportunity to engage with online versions of sessions delivered on-campus

Coursework 25% as 5 Canvas test, each carrying 5 marks. Standard 75% exam to answer 3 out of 4 questions.

Lectures: 20 hours

Directed private study: 80 hours

Module Aims: The principles of the Internet are explained including protocols, services and functions of its 6 out of 7 OSI layers from the application layer down to the link layer. Emphasis is on understanding the TCP/IP protocol stack. Such knowledge of the Internet is then extended to cover the principles of wireless and mobile networks, multimedia networking, security in computer networks, and telecommunication networks management.

Module Content: The principles of the Internet are explained including the protocols, services and functions of its 6 out of 7 OSI layers from the application layer down to the link layer. Emphasis is on understanding of the TCP/IP protocol stack. Such knowledge of the Internet is then extended to cover principles and problems of wireless and mobile networks, multimedia networking, security in computer networks, and telecommunication networks management.

Intended Learning Outcomes: Technical Outcomes

After completing this module you should be able to:

• Understand how the Internet works and what are its components.

- Understand what protocols are employed in the Internet, and their operations, functions and services provided.
- Understand the important issues in the current developments of the Internet.
- Understand the technical literature about the Internet.

Accreditation Outcomes (AHEP)

- A comprehensive understanding of the relevant scientific principles of the specialisation (SM1fl)

- Understanding of concepts relevant to the discipline, some from outside engineering, and the ability to evaluate them critically and to apply them effectively, including in engineering projects (SM3fl)

- Ability both to apply appropriate engineering analysis methods for solving complex problems in engineering and to assess their limitations (EA1fl)

Assessment: Examination 1 (75%) Coursework 1 (25%)

Resit Assessment: Examination (Resit instrument) (100%)

Assessment Description: The coursework 25% is assessed via 5 individual tests on Canvas.

The standard exam 75% has the choice of 3 out of 4 questions.

This module is assessed by a combination of examination and continual assessment. In order for the continual assessment marks to count, you must achieve at least 40% in the exam component. If you achieve less than 40% in the exam, then the module mark will be just the exam mark.

Moderation approach to main assessment: Universal second marking as check or audit

Assessment Feedback: Continuous feedback during lectures and by Canvas.

Failure Redemption: If rules allow - standard University provision with marks capped. Failure Redemption will be by 100% Examination

Additional Notes: Delivery of both teaching and assessment will be blended including live and self-directed activities online and on-campus.

• AVAILABLE TO Visiting and Exchange students.

• The Faculty of Science and Engineering has a ZERO TOLERANCE penalty policy for late submission of all coursework and continuous assessment.

• Notes, worked examples and past exam papers for this module can be found on Canvas.

• This module is assessed by a combination of examination and continual assessment. In order for the continual assessment marks to count, you must achieve at least 40% in the exam component. If you achieve less than 40% in the exam, then the module mark will be just the exam mark.

EC MAT D a Taradanah ing Cara T

| | 17 Business Leadership for Engineers D Session: 2022/23 January-June |
|---------------|--|
| | ite Modules: |
| A | ite Modules: |
| | a): Dr A Munnangi, Dr AS Walters |
| | · · · · · · · · · · · · · · · · · · · |
| Format: | Lectures/Workshops - 22 hours |
| | Open door tutorials/workshops - 8 hours |
| | Directed private study 70 hours |
| | Contact Hours will be delivered through a blend of live activities online and on-campus, and may |
| | include, for example, lectures, seminars, practical sessions and Academic Mentoring sessions. |
| - | fethod: All Programmes will employ a blended approach to delivery using the Canvas Digital Learning |
| | or live and self-directed online activity, with live and self-directed on-campus activities each week. Studen |
| may also h | ave the opportunity to engage with online versions of sessions delivered on-campus |
| Combinatio | on of interactive lectures/workshops/case studies and self-study. |
| | ims: At the end of this course students will be able to recognise and understand key characteristics of |
| | as well as a wide range of strategic business skills, ideas and theories with emphasis on innovation and |
| - | eurial thinking" which is essential for the current multidisciplinary engineering environment. The course |
| - | tegrates practical project work and academic rigour. |
| • | ontent: Workshop 1 – Introduction & Leadership Part 1 |
| | 2 – Leadership Part 2 |
| - | 3 – Team Formation, Development and Communication |
| | 4 - Entrepreneurial Thinking |
| - | 5 – Change Management |
| - | 6 – Strategic Management |
| - | 7 – Innovation and Business Thinking, Group Assignment Part 1 |
| - | 8 – Innovation and Business Thinking, Group Assignment Part 2 |
| - | 9 – Group Assignment Workshop |
| - | 10 – Group Assignment Workshop |
| - | Learning Outcomes: |
| Technical (| |
| | ful completion of this module students will be expected, at threshold level, to be: |
| | rate an understanding of current leadership issues. Critically appraise theories and approaches to leadership |
| | same time reflect on personal leadership aspects. |
| | ge to assess the basic factors that must be considered for a business formation. Use of basic level strategy |
| | tion methods in order for an organisation to gain competitive advantage. Critically evaluate the rationale |
| | g methods for idea generation/innovation. |
| - | ireness of theoretical perspectives and approaches to change management in organisational environments. |
| | the relationship between the external context of an organisation and its internal context and their impact o |
| its strategic | |
| - | ate and appraise, entrepreneurial way of working, team development and communication skills |
| | are and appraise, entrepreneuriar way or working, team development and communication skills |
| Accreditati | on Outcomes (AHEP) |
| - Investigat | te and define the problem, identifying any constraints including environmental and sustainability |
| - | ; ethical, health, safety, security and risk issues; intellectual property; codes of practice and standards (D2) |

limitations; ethical, health, safety, security and risk issues; intellectual property; codes of practice and standards (D2) - Demonstrate the ability to generate an innovative design for products, systems, components or processes to fulfil new needs (D8m)

- Knowledge and understanding of management and business practices, their limitations, and how these may be applied in the context of the particular specialisation, (ET3fl)

- Awareness that engineering activities should promote sustainable development and ability to apply quantitative techniques where appropriate, (ET4fl)

- Awareness of and ability to make general evaluations of risk issues in the context of the particular specialisation, including health & safety, environmental and commercial risk. (ET6fl)

- Understanding of the key drivers for business success, including innovation, calculated commercial risks and customer satisfaction. (ET7m)

| Assessment: | Group Work - Coursework (80%) |
|-----------------------------------|--|
| | Online Class Test (10%) |
| | Online Class Test (10%) |
| Resit Assessmer | nt: Coursework reassessment instrument (100%) |
| Assessment Des | cription: Online Test 1 Assessment level marking - PGTM March 10% |
| Online Test 2 As | sessment level marking - PGTM March 10% |
| Group Work Cor | ursework Assessment level marking - PGTM April 80% |
| • • • | assignment will require application of the "key skills" and innovation development tools to generate -world scenarios – report (40 pages) and development of Business Canvas. |
| exam, the marks | ssessed by a combination of group-based and individual assignments (quiz-1 and quiz-2). In the mair students get in quiz -1 and quiz-2 will add to the marks the individual gets in the group assignment esit exam, the quiz-1 and quiz-2 marks will not add to the project. |
| | proach to main assessment: Partial second marking |
| Assessment Fee | dback: |
| Continuous grou | p feedback on "out-comes" of workshops, after submission of coursework 1 at request during open- |
| tutorials. | |
| Failure Redemp | |
| | rding to University regulations. |
| 100% coursewor | |
| Additional Note activities online | s: Delivery of both teaching and assessment will be blended including live and self-directed and on-campus. |
| • | cience and Engineering has a ZERO TOLERANCE penalty policy for late submission of all continuous assessment |
| Related assignme | ents are used to assess this module. |
| This module is a | ssessed by a combination of group-based and individual assignments. In order for the individual |

This module is assessed by a combination of group-based and individual assignments. In order for the individual assessment marks to count, you must achieve at least 40% in the group-based assignment. If you achieve less than 40% in the group-based assignment, then the module mark will be just the group-based assignment mark.

EG-M85 Strategic Project Planning

Credits: 10 Session: 2022/23 September-January

Pre-requisite Modules:

Co-requisite Modules:

Lecturer(s): Dr K Wada

Format: Lectures and Case Studies 13-15 hours; Project Monitoring 7 hours (project briefing, project update and presentations); Private Study 78-80 hours (reading, group work, exam preparation) Contact Hours will be delivered through a blend of live activities online and on-campus, and may

include, for example, lectures, seminars, practical sessions and Academic Mentoring sessions.

Delivery Method: All Programmes will employ a blended approach to delivery using the Canvas Digital Learning Platform for live and self-directed online activity, with live and self-directed on-campus activities each week. Students may also have the opportunity to engage with online versions of sessions delivered on-campus

Series of lectures and combination of case study, project briefing/update and group work sessions.

Practical group work sessions (50%) will be arranged in order to grasp the project management techniques and effectively apply them to form a 'High Performance Team'. This coursework assessment (CA) is comprised of a group project and group presentation.

Examination - Closed Book (50%) at the end of the semester.

Module Aims: This module has been accredited by the professional body - the Association for Project Management (APM). At the end of this course students will be able to recognise and define the key characteristics and components of a project, understand the advantages/disadvantages associated with the management of both small and large projects, and have an appreciation of the strategic tools and techniques available to enable effective or efficient project management leading to a 'High Performance Team'. The acquired skills will be reinforced by the completion of a group project to produce an initial feasibility report (e.g. a business case/project management plan document) for a major regional project.

Module Content: 1) Lectures: series of lectures will be conducted and/or recorded to cover the fundamentals of strategy and project management. Various tools and techniques used by a project manager at large in the industry will be demonstrated with figures/diagrams/tables/videos and further elaborated through relevant examples.

Intended coverage of syllabus (as recommended by APM):

- 1. Structure of organisations and projects
- 2. Project life cycle
- 3. Project contexts and environments
- 4. Governance and structured methodologies
- 5. Communication
- 6. Leadership and teamwork
- 7. Planning for success
- 8. Scope management
- 9. Schedule and resource management
- 10. Procurement
- 11. Project risk management and issue management
- 12. Project quality management

2) Case study/Webinar: internal/external guest speaker(s) will be invited to give talks on some of the topics on project management, an hour session each.

3) Project briefing and update: information on CA (including but not limited to project titles, group allocation, project manager/assistant manager nominations, marking scheme, report format, and presentation arrangement) will be announced during these sessions. Frequently asked questions (FAQs) will be answered in the meantime.

4) Group work and Presentation: dedicated hours will be provided for the group work (i.e. dealing with CA task). No lectures during these sessions. With regard to CA, dedicated time slots will be arranged for the final presentation.

Intended Learning Outcomes: Technical Outcomes

On successful completion of this module students will be expected, at threshold level, to be able to:

- Demonstrate a comprehensive knowledge and understanding of project management - the nature of both small and large projects, the issues and constraints such as environmental and sustainability limitations; ethical, legal, health, safety, security and risk issues; the tools available to manage the project - and critically evaluate them and apply the tools effectively in projects to communicate the outputs to technical and non-technical audiences. (Assessed by Coursework report, Presentation and Exam; or Resit Exam)

- Use fundamental knowledge to investigate new and emerging technologies via application of strategy such as PESTLE analysis, SWOT analysis and Porter's generic strategies as a means not only to understand the key drivers for business success pertaining to the commercial, economic and social context of engineering processes, but also to identify, compare and evaluate competitive advantage, cost leadership, differentiated product/services, or niche markets. (Assessed by Coursework report, Presentation and Exam; or Resit Exam)

- Have awareness of relevant legal and contractual issues, as well as quality issues and their application to continuous improvement (i.e. quality planning, quality assurance, quality control and continuous improvement). This requires the demonstration of knowledge, interpretation and application of project management theory and practice. (Assessed by Coursework report, Presentation and Exam; or Resit Exam)

- Demonstrate a comprehensive knowledge and understanding of the role of a project manager - an ability to exercise initiative and personal responsibility: i) understand the team members' characteristic and their needs; ii) delegate project activities and find ways to resolve conflicts through effective communication to build a 'High Performance Team'; and iii) understand and evaluate business, customer and user needs. (Assessed by Coursework report, Presentation and/or Resit Exam)

Accreditation Outcomes (AHEP)

Investigate and define the problem, identifying any constraints including environmental and sustainability limitations; ethical, health, safety, security and risk issues; intellectual property; codes of practice and standards (D2)
Communicate their work to technical and non-technical audiences (D6)

- Awareness that engineers need to take account of the commercial and social contexts in which they operate (ET2fl)

- Knowledge and understanding of management and business practices, their limitations, and how these may be applied in the context of the particular specialisation (ET3fl)

- Awareness that engineering activities should promote sustainable development and ability to apply quantitative techniques where appropriate (ET4fl)

- A thorough understanding of current practice and its limitations, and some appreciation of likely new developments (EP2fl)

Ability to apply engineering techniques, taking account of a range of commercial and industrial constraints (EP3fl)
Understanding of different roles within an engineering team and the ability to exercise initiative and personal responsibility, which may be as a team member or leader (EP4fl)

| Assessment: | Examination 1 (50%) |
|-------------|---------------------|
| | Coursework 1 (50%) |

Assessment Description: Coursework 1 is a group project allocated during the lecture series. Examination 1 is a standard closed book examination.

The pass mark for a module at Year 4/M is 50%. In addition to this, students must also achieve at least 40% in both components to pass this module.

If you do not meet the component level requirements for the module you will receive a QF outcome. This means that you will be required to repeat the failed component(s), even if your module mark is above 50%.

Moderation approach to main assessment: Universal second marking as check or audit

Assessment Feedback: Informal feedback is given during lectures, project briefing/update sessions, group presentations, and at group work meetings. Formal feedback is given via standard College of Engineering feedback protocols.

Failure Redemption: Failure Redemption of this module will be by repeating an equivalent coursework and/or exam to any component in which a pass mark was not achieved.

Marks achieved in assessment component passed during the first attempt will automatically be transferred to the equivalent component in the resit.

No opportunity to resit the passed component.

Additional Notes: Delivery of both teaching and assessment will be blended including live and self-directed activities online and on-campus.

Penalty for late submission of work: ZERO TOLERANCE.

Available to visiting and exchange students wishing to enhance project management skills.

The pass mark for a module at Year 4/M is 50%. In addition to this, students must also achieve at least 40% in both components to pass this module.

Office hours, lecture notes and other teaching materials and notifications will be posted on Canvas.

EGIM16 Communication Skills for Research Engineers

Credits: 10 Session: 2022/23 September-January

Pre-requisite Modules:

Co-requisite Modules:

Lecturer(s): Dr SA Rolland, Dr T Lake

Format: Lectures (10h), Exercises (20h), Reading / Private Study (30h), Preparation for Assessment (40h) **Delivery Method:** The module will be delivered on campus and partially online.

Module Aims: Communication at a research level differs from that at the undergraduate level in that it is usually driven by an output or result rather than the requirement to show knowledge or understanding. The skill of a good communicator at research level lies in efficiently and rigorously conveying the ideas behind the theory and proof of the research output. Verbal, written, visual and group communication will be explored through a series of lectures and formative exercises.

Module Content:

Written Communication: [6 hours]

- The usual layout of reports, theses, journal & conference papers.
- How to write a good abstract for a research output.
- What should be in the introduction
- Contents of the main body of a research output.
- Effective conclusions
- Writing style
- Cross-referencing, captions, references
- Critical review of self and others
- Design concepts for research posters

Oral Communication: [6 hours]

- The usual layout of a research presentation
- Slide design for a research presentation
- Delivery of a presentation, do's and don'ts
- Maintaining the audience's interest.

Other topics: [3 hours]

- Attending & chairing meetings
- Conferences submissions and attendance
- Submission of papers and peer review.

Intended Learning Outcomes: Technical Outcomes:

By the end of this module the student will be able to:

• Write a paper or equivalent employing the structure and rigour required at research level (assessed by assignments 1 and 4)

• Efficiently communicate the concepts associated with complex ideas (assessed by the first written assignment and the oral presentation)

• Critically evaluate a written output (assessed within the second assessment component)

• Verbally present a complex idea using the presentation structure, slide content and delivery techniques expected of a research engineer (assessed through the oral presentation)

• Demonstrate an awareness of the other modes of communication of ideas at a research level such as posters and group discussions (assessed in the second assessment component)

Accreditation Outcomes (AHEP)

- Awareness of the need for a high level of professional and ethical conduct in engineering (EL8M / ET1fl)

- Awareness that engineers need to take account of the commercial and social contexts in which they operate (EL9M / ET2fl)

- Awareness that engineering activities should promote sustainable development and ability to apply quantitative techniques where appropriate (EL11M / ET4fl)

- A thorough understanding of current practice and its limitations, and some appreciation of likely new developments (P9M / EP2fl)

| Assessment: | Assignment 1 (10%) |
|-------------|------------------------|
| | Assignment 2 (10%) |
| | Oral Examination (40%) |
| | Writing (40%) |
| | |

Assessment Description:

The first sit assessment will consist of 4 assignments.

The first assessment component will be a short written piece, up to two pages long, which will test the students understanding of the concepts with respect to the written work and to allow feedback to the participants in the module prior to the final assessment. This is an individual piece of coursework.

The second component will feature a small number of tasks which are aimed to evaluate the students understanding of the other ideas, beyond the written word and oral presentations, which are covered in the module. This will include the critical review of a written output. Other possible tasks include group meetings and the creation of a poster. The coursework may be done individually or in groups, this will be confirmed at the time of setting the work.

The oral examination will involve the students presenting an example of the work they have undertaken in the past, typically a project, through an oral presentation. The target duration of the oral presentation will usually be between 8 to 10 minutes. The exact duration will be specified in the assignment descriptor. This is an individual piece of coursework.

The final, fourth, component will require the student to write a paper or equivalent. This paper will be between four to five pages in length and will be written to a format described in the assignment descriptor. This is an individual piece of coursework.

The pass mark for a module at Level 4/M is 50%. In addition to this Students must achieve at least 40% in the Oral Examination AND 40% in the Writing assessment to pass the module.

The reassessment will consist of 2 assignments, details of which are provided in a later section.

Moderation approach to main assessment: Second marking as sampling or moderation

Assessment Feedback: CANVAS will be used to provide individual feedback to the students on all the components that contribute to the final mark. For the first assessment component a class feedback document is also generally included on CANVAS.

As part of the practical sessions the students will receive verbal feedback on their performance. These sessions do not contribute to the final mark.

Failure Redemption: Candidates shall be given one opportunity to redeem a failure in the module during the summer supplementary period.

All components are redeemable individually in the event of failure across the module.

In addition, the 40 % oral and written assignments of the first must be passed individually to pass the module, and will have to be redeemed even if a pass mark is achieved for the module overall on first sit. A pass mark on both main assessment components will be required to pass the module.

Additional Notes: Delivery of both teaching and assessment will be blended including live and self-directed activities online and on-campus.

All lectures and course material will be provided on CANVAS.

The pass mark for a module at Level 4/M is 50%. In addition to this Students must achieve at least 40% in the Oral Examination AND 40% in the Writing assessment to pass the module.

The Faculty of Science and Engineering has a ZERO TOLERANCE penalty policy for late submission of all coursework and continuous assessment.