Faculty of Sciences
Department of Computer Science

UNIVERSITY of York

Professional Development and Training in System Safety Engineering

Contents

Introduction

As technology advances into every part of our lives, the safety and security of goods and services becomes more important and challenging. The need for safety and security is all around us, whether this is the safety of systems in industries, such as aerospace, nuclear, automotive or medicine, or the threat of viruses and hackers to a company's data.

System safety engineering is concerned with the analysis and assessment of 'systems of systems', platforms and systems to identify and evaluate safety risks, and influence design and operation to reduce risks.

Classical hazard and safety analysis techniques have historically dealt poorly with computers and software, particularly as modern systems are highly integrated, and often networked. Current trends towards the 'internet of things', autonomy and cyber-physical systems are exacerbating this situation. Addressing these issues is a sub-discipline of Safety Critical Systems Engineering.

Our courses provide a comprehensive grounding in the principles of system safety engineering and safety critical system engineering, to refresh, renew and extend your skills in this area. The modules will give you knowledge of safety engineering using examples from a range of domains including the railway, automotive, aerospace, health and marine industries.



Why York?

- Learn from internationally respected experts in the field
- Choose to study for a recognised postgraduate award
- Learn core principles that are transferable across industry domains
- Study is broken into manageable one-week blocks
- Refresh your knowledge to enhance job performance
- Keep up to date with the latest trends

Learn from the experts

You will be taught by world-leading experts in the field of system safety engineering, who have worked extensively in industry and undertaken research into the discipline. This experience, coupled with up-to-date training materials and real-life industrial case studies, will help you to place learning in context.

Our research has helped to shape what is done in system safety today. One example is the Goal Structuring Notation (GSN) developed at York to improve industrial practice in developing and presenting safety case arguments. This has become an embedded and established international approach to safety case development. GSN now appears in a number of national and international safety standards as a recommended approach to safety case development.

With this combination of relevant research and industry experience we are able to develop our teaching in response to new advances, the requirements of industry, and to keep your skills and knowledge up to date.

Our experience and expertise

Our short courses provide a comprehensive grounding in the principles of system safety engineering such as hazard identification and analysis, risk assessment and management, system safety justification and certification, through life safety, and safety management systems.

These principles are put into an industrial context through examples from our extensive portfolio of collaboration in the UK and worldwide. Our courses are well respected by industry, and we have provided training for delegates from many different domains.

We have provided training for:

- Military: BAE Systems, Qinetiq, Syntell
- Civil Aerospace: Rolls Royce, Airbus, GE Aviation Systems, Thales
- Automotive: Jaguar Land Rover
- Railway: Beijing Jiaotong University, Inspectie Leefomgeving en Transport (ILT)
- Nuclear: Office for Nuclear Regulation
- Marine: Royal Hydrographic Office
- Medical: Connecting for Health
- Energy: British Energy

Learning outcomes

Our modules will provide you with a thorough grounding and practical experience in the use of state-of-the-art techniques for development of safety critical systems. We place an emphasis on the use of software, together with an understanding of the principles behind techniques so that you can make sound engineering judgements during the design and deployment of such a system.

A pleasure to be taught by highly qualified lecturers who are clearly passionate about the subject matter."

MODULES AT A GLANCE

We offer eleven short course modules in System Safety Engineering, which are delivered over five days, enabling you to learn alongside your work, ensuring your skills are fully up to date.

1

FOUNDATIONS OF SYSTEM SAFETY ENGINEERING (FSSE)

2

SYSTEMS ENGINEERING FOR SAFETY (SEFS)

3

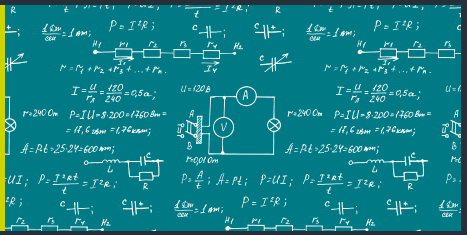
HAZARD AND RISK ASSESSMENT (HRAS)

4

SOFTWARE REQUIREMENTS (SWRE)

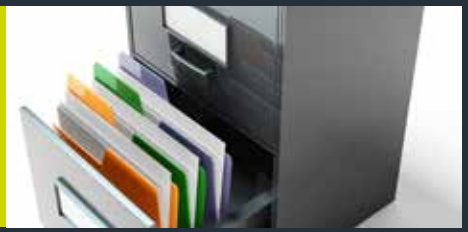
5

SYSTEM SAFETY ASSESSMENT (SSAS)



6 SAFETY MANAGEMENT SYSTEMS (SMSY)

7 SAFETY CASE DEVELOPMENT AND REVIEW (SCDR)



8 HUMAN FACTORS FOR SAFETY (HUFS)

9 COMPUTERS AND SAFETY (CASA)

10 THROUGH LIFE SAFETY (TLSA)

11 SECURITY FOR SAFETY CRITICAL SYSTEMS (SESA)

1 Foundations of System Safety Engineering (FSSE)

Automotive safety can be divided into active safety and passive safety. Passive safety refers to systems such as PRS, ARS, brakes and windscreens. Active safety refers to systems such as ACC, ABS, driver assistance systems and so on. Most of the active safety features come in the form of Electronic Control Units (ECUs) which are being increasingly used for the control of systems.

This module is an introduction to the principles of system safety, including risk, basic terminology, and the main types of hazard and safety assessment techniques. You will receive a brief overview of material which will be covered in greater depth in later modules, such as legal issues, management of safety critical projects, and human factors.

> ***"The case studies were very good, showing how various safety methods and analyses are used in real life."***

By the end of this course you will be able to:

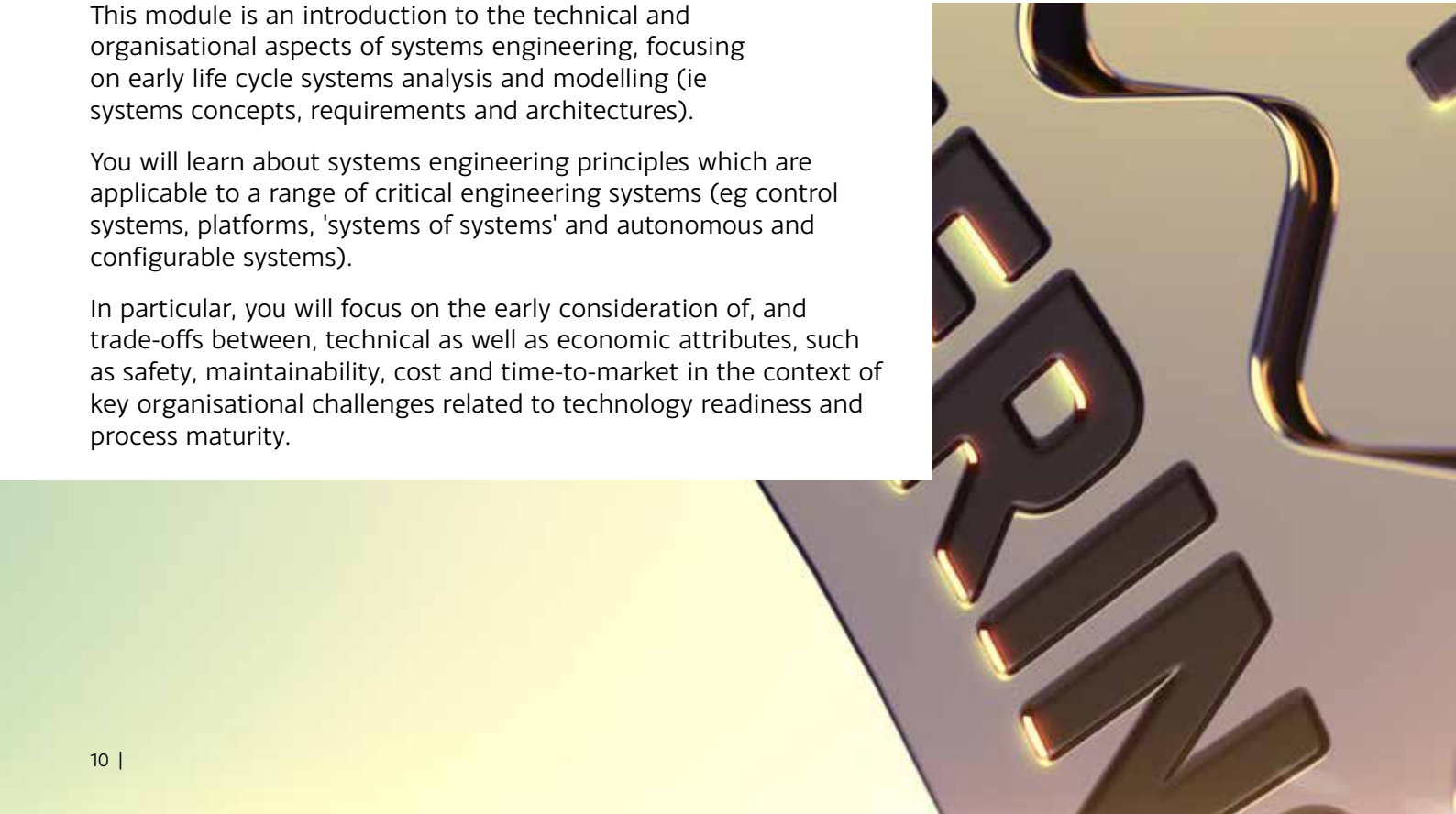
- Understand risk, and factors influencing perception and acceptability of risk
- Give definitions of safety-related terminology, and discuss how the use of terminology varies between countries and industrial sectors
- Understand the ISO 26262 safety-critical systems life cycle, and the roles of the major groups of techniques within it.

2 Systems Engineering for Safety (SEFS)

This module is an introduction to the technical and organisational aspects of systems engineering, focusing on early life cycle systems analysis and modelling (ie systems concepts, requirements and architectures).

You will learn about systems engineering principles which are applicable to a range of critical engineering systems (eg control systems, platforms, 'systems of systems' and autonomous and configurable systems).

In particular, you will focus on the early consideration of, and trade-offs between, technical as well as economic attributes, such as safety, maintainability, cost and time-to-market in the context of key organisational challenges related to technology readiness and process maturity.

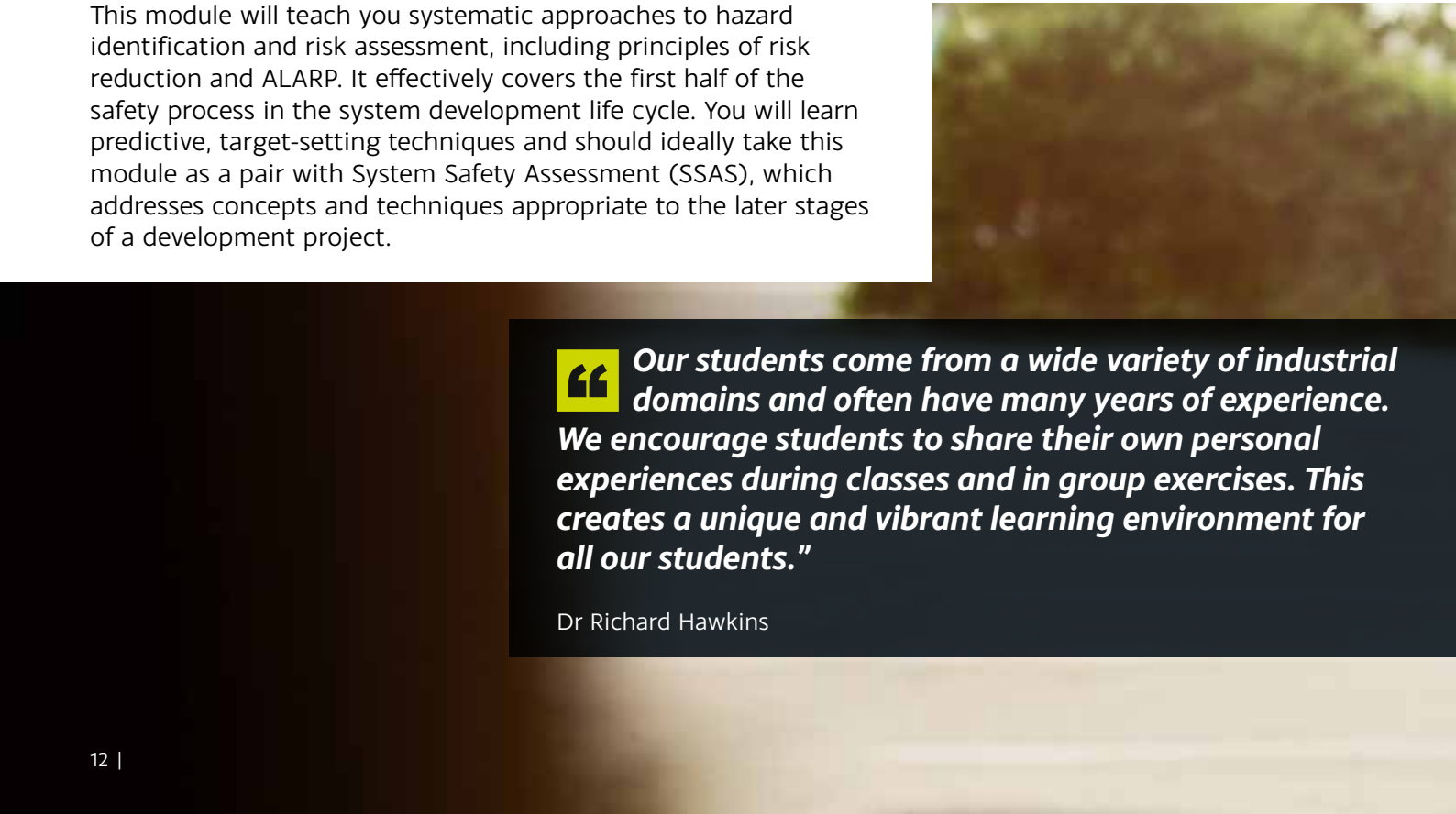


By the end of this course you will be able to:

- Explain the scope and nature of systems engineering in the context of high safety risk industries
- Identify and assess the interaction between systems engineering and economics
- Describe the role and importance of organisational aspects of systems engineering in the development life cycle in the context of high safety risk industries
- Participate in requirements definition, architecture design, trade-off analysis and system modelling.

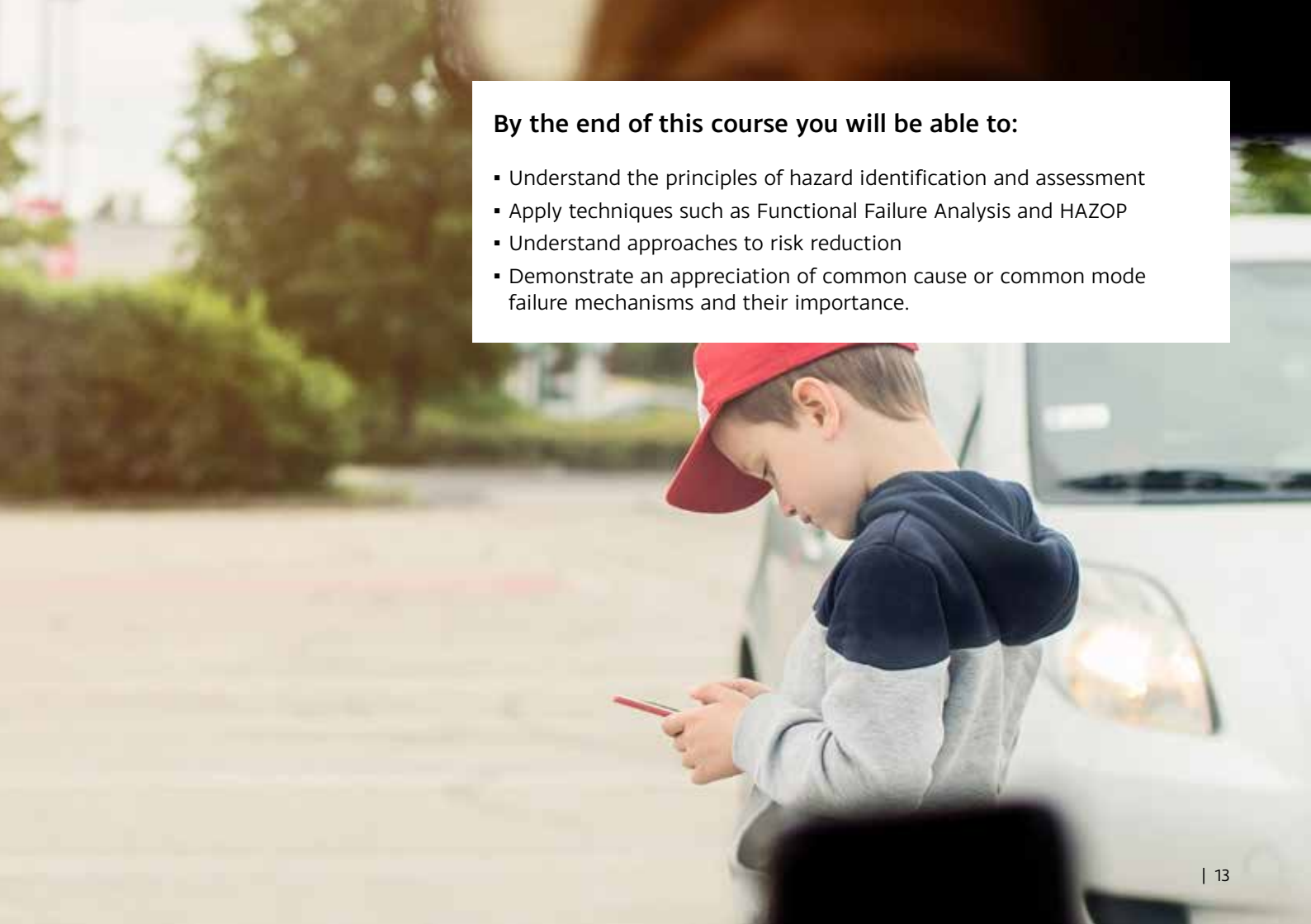
3 Hazard and Risk Assessment (HRAS)

This module will teach you systematic approaches to hazard identification and risk assessment, including principles of risk reduction and ALARP. It effectively covers the first half of the safety process in the system development life cycle. You will learn predictive, target-setting techniques and should ideally take this module as a pair with System Safety Assessment (SSAS), which addresses concepts and techniques appropriate to the later stages of a development project.



“Our students come from a wide variety of industrial domains and often have many years of experience. We encourage students to share their own personal experiences during classes and in group exercises. This creates a unique and vibrant learning environment for all our students.”

Dr Richard Hawkins

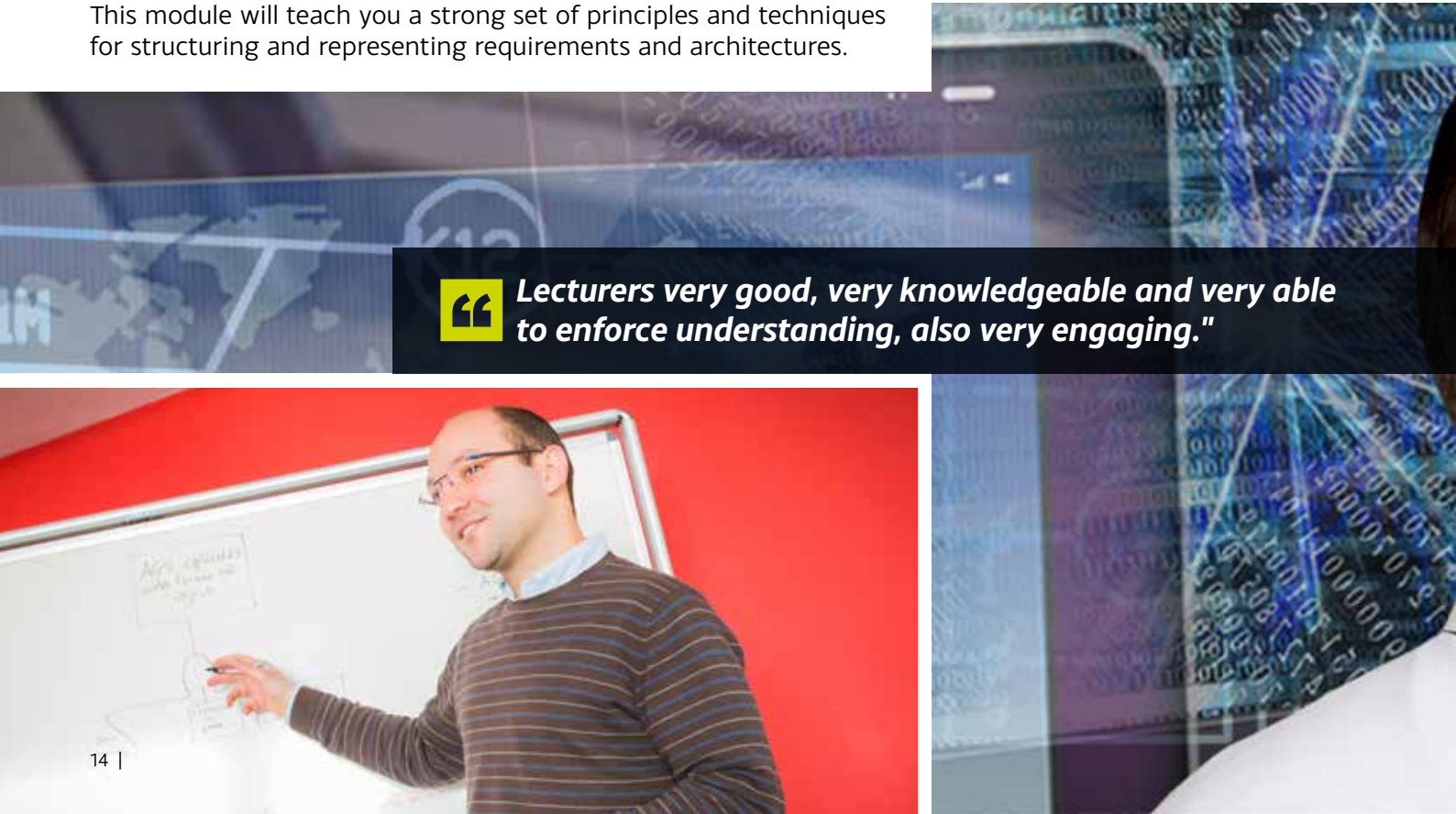


By the end of this course you will be able to:

- Understand the principles of hazard identification and assessment
- Apply techniques such as Functional Failure Analysis and HAZOP
- Understand approaches to risk reduction
- Demonstrate an appreciation of common cause or common mode failure mechanisms and their importance.

4 Software Requirements (SWRE)

This module will teach you a strong set of principles and techniques for structuring and representing requirements and architectures.



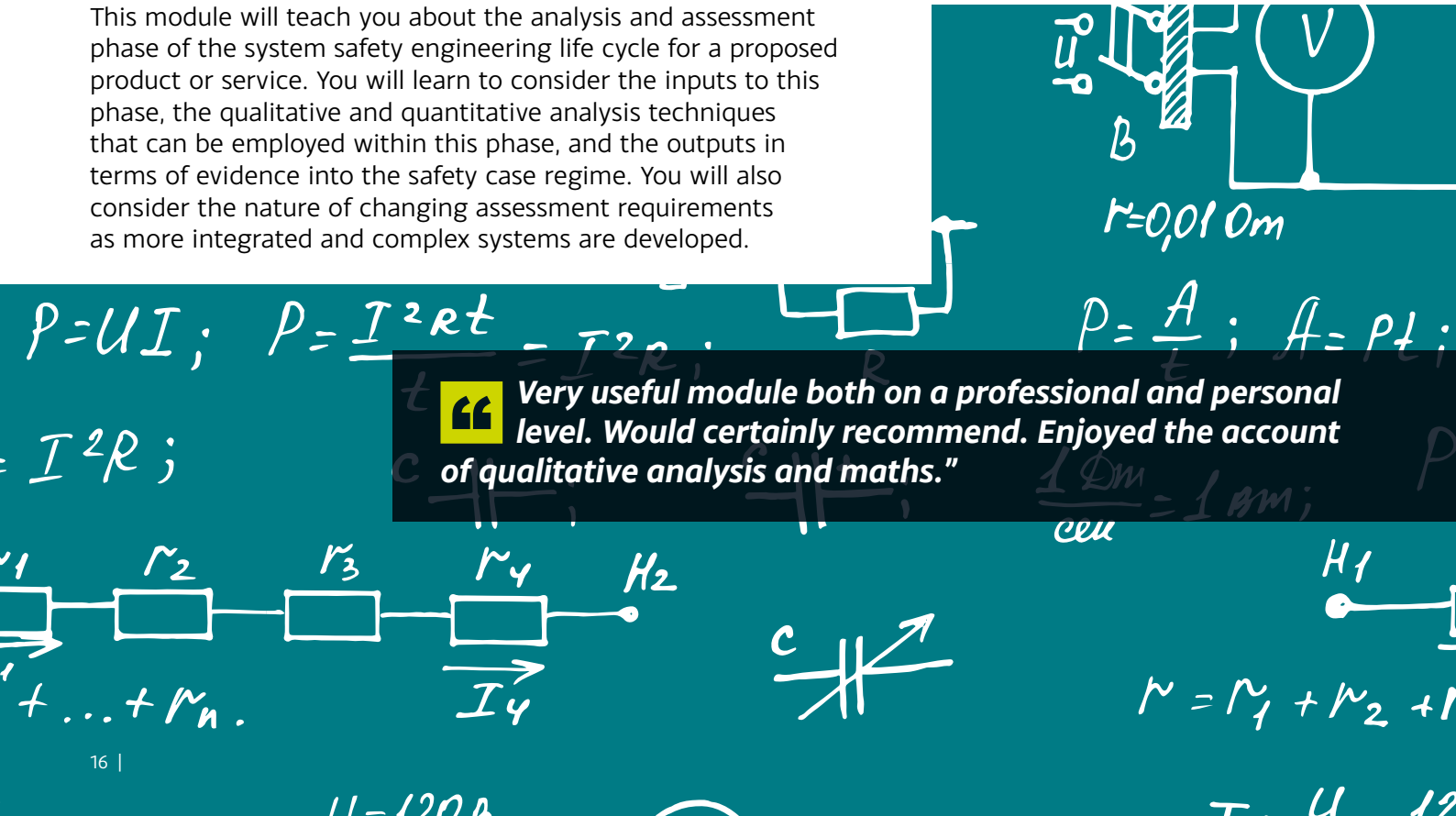
> ***Lecturers very good, very knowledgeable and very able to enforce understanding, also very engaging."***

By the end of this course you will be able to:

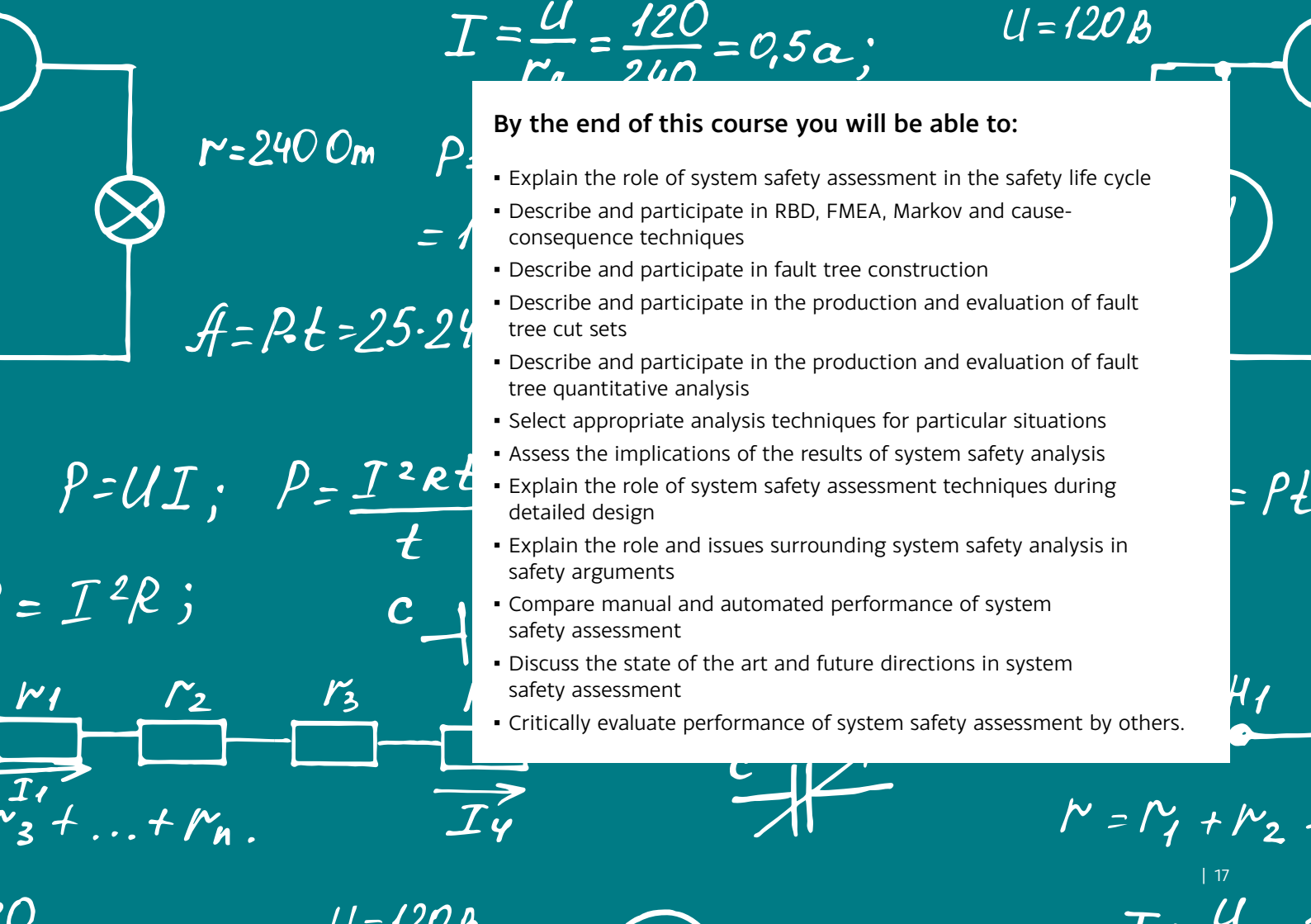
- Describe the role of requirements engineering and architecture design and assessment for the development of critical systems
- Explain different types of requirements
- Perform a quality review of requirements
- Explain the desirable attributes of a requirements set
- Describe and participate in techniques for requirements elicitation, representation validation, re-use and traceability
- Select and apply software architectural strategies to address requirements
- Assess the selection and application of software architectural strategies
- Apply appropriate notations for software architecture representation
- Discuss the state of the art and future directions in software architecture modelling.

5 System Safety Assessment (SSAS)

This module will teach you about the analysis and assessment phase of the system safety engineering life cycle for a proposed product or service. You will learn to consider the inputs to this phase, the qualitative and quantitative analysis techniques that can be employed within this phase, and the outputs in terms of evidence into the safety case regime. You will also consider the nature of changing assessment requirements as more integrated and complex systems are developed.



> ***"Very useful module both on a professional and personal level. Would certainly recommend. Enjoyed the account of qualitative analysis and maths."***



By the end of this course you will be able to:

- Explain the role of system safety assessment in the safety life cycle
- Describe and participate in RBD, FMEA, Markov and cause-consequence techniques
- Describe and participate in fault tree construction
- Describe and participate in the production and evaluation of fault tree cut sets
- Describe and participate in the production and evaluation of fault tree quantitative analysis
- Select appropriate analysis techniques for particular situations
- Assess the implications of the results of system safety analysis
- Explain the role of system safety assessment techniques during detailed design
- Explain the role and issues surrounding system safety analysis in safety arguments
- Compare manual and automated performance of system safety assessment
- Discuss the state of the art and future directions in system safety assessment
- Critically evaluate performance of system safety assessment by others.

6 Safety Management Systems (SMSY)

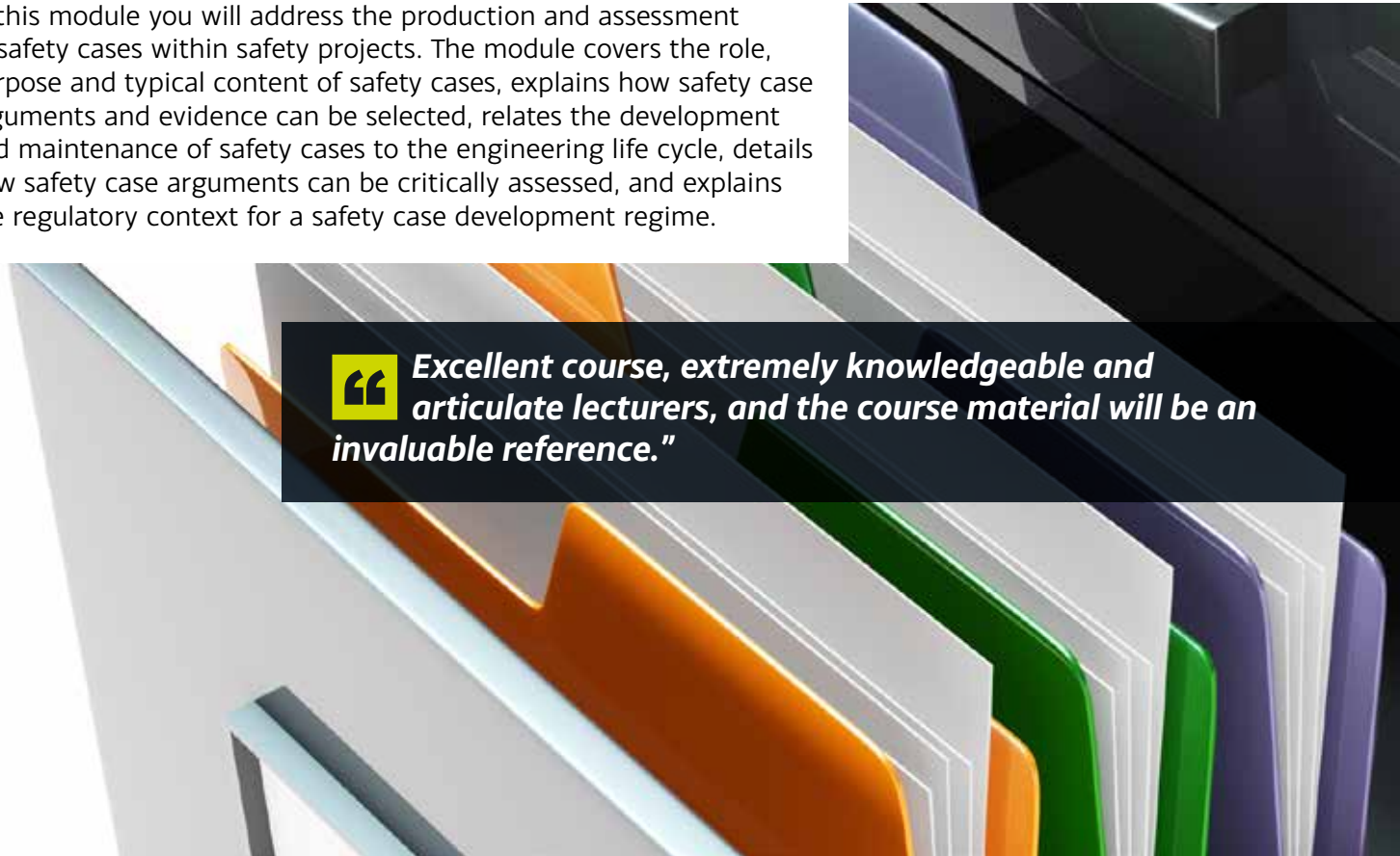
This module will provide you with an awareness of the issues associated with conducting technical safety activities within an organisational and regulatory environment and enable you to develop skills in applying theoretical safety engineering knowledge in situations constrained by available education, resources and organisational culture.

By the end of this course you will be able to:

- Discuss the evolution of regulatory and legal contexts for safety
- Discuss the relationship between business and safety risk management
- Evaluate the role of organisational structure in safety performance
- Differentiate between safety management system documentation and safety management systems
- List the key activities covered by a safety management system
- Discuss the role of philosophy, policy, procedure and practice in safety management systems
- Characterise the safety culture of an organisation
- Prepare a work breakdown structure for a safety programme
- Estimate cost and time for safety activities
- Appraise a safety management proposal for practicality
- Describe the requirements for safety competency management
- Explain the relationship between safety competency and engineering ethics
- Design a suite of metrics for a safety programme
- Differentiate between proactive and reactive safety activities
- Discuss the state of the art and future directions in safety management systems.

7 Safety Case Development and Review (SCDR)

In this module you will address the production and assessment of safety cases within safety projects. The module covers the role, purpose and typical content of safety cases, explains how safety case arguments and evidence can be selected, relates the development and maintenance of safety cases to the engineering life cycle, details how safety case arguments can be critically assessed, and explains the regulatory context for a safety case development regime.



“Excellent course, extremely knowledgeable and articulate lecturers, and the course material will be an invaluable reference.”

By the end of this course you will be able to:

- Comprehend the role, purpose and typical content of a safety case
- Devise and present clear safety arguments using both text and graphical notations (particularly the Goal Structuring Notation)
- Understand the risks, strengths and weaknesses of safety cases
- Recognise and distinguish common forms of safety arguments
- Understand how to review and evaluate a safety case
- Understand how to undertake safety case maintenance throughout the life cycle
- Understand the emerging concepts in safety cases.

8 Human Factors for Safety (HUFS)

On this course you will be introduced to concepts and techniques that can be used to support the design and evaluation of complex interactive systems with a particular emphasis on safety critical systems. These techniques include work analysis (including task analysis and scenario analysis), human error assessment, design and evaluation of interactive systems, and human reliability assessment.

> ***"It is great to work with students actively engaged in so many safety-critical domains. Their engagement with, and reflection on, the challenges of safety-critical systems is a perfect complement to our research-led teaching. It's a great learning environment, for everyone."***
>
> Dr Katrina Attwood

By the end of this course you will have an understanding of:

- Usability and its relation to error
- User requirements elicitation and analysis
- Work representation and hierarchical task analysis
- Principles of design and prototyping
- Evaluation of interactive systems
- Errors and principles relating to human reliability
- Human reliability analysis
- Human error analysis.

9 Computers and Safety (CASA)

On this course you will be introduced to the issues of using computers in safety-critical or safety-related applications. The course highlights areas of concern to safety engineers, including an in-depth examination of the software development process, consideration of requirement specifications, and design and analysis. These features are critical to the deployment of computers in safety-critical applications.

"Enjoyed the mix of theory with industrial anecdotes, enhanced by academic lecturers with good practical experience."

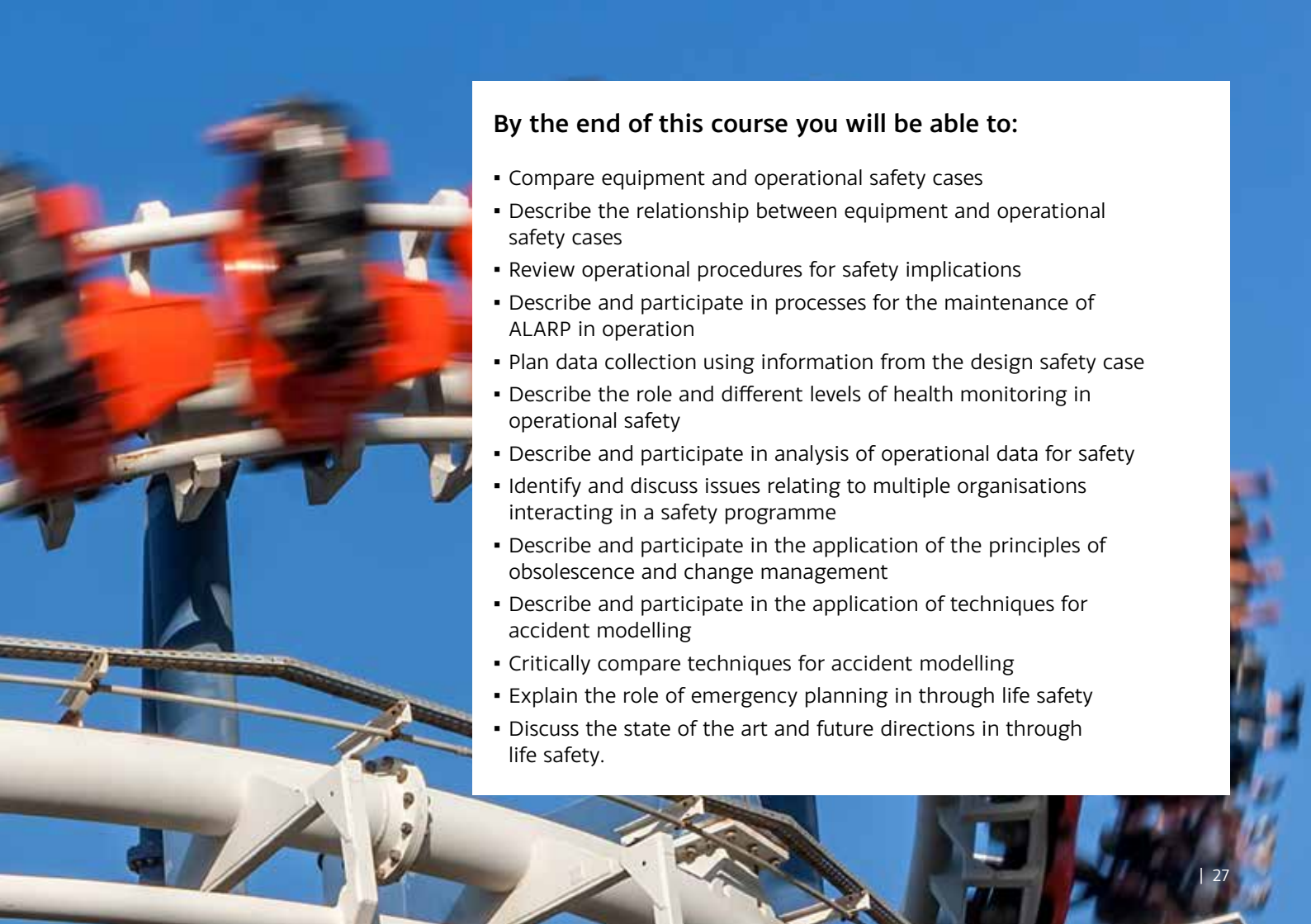
By the end of this course you will be able to:

- Explain the issues relating to the use of software in safety-critical systems
- Evaluate software development life cycle models for safety
- Describe the basic elements of a computer
- Discuss the relationship between system and software requirements
- Differentiate between 'bottom-up' and 'top-down' views of software assurance
- Discuss the issues in communicating requirements from one discipline to another
- Select and participate in the application of appropriate software safety analysis techniques
- Describe the role and principles of software architecture in the design process
- Identify the decisions relevant for safety in a software development process
- Compare the approaches taken by software standards
- Assess the appropriateness of software verification and analysis in a system safety argument
- Describe the issues and potential approaches to incorporating software COTS into a safety-critical system
- Discuss the state of the art and future directions in software safety.

10 Through Life Safety (TLSA)

This module addresses the safety issues that arise after system deployment including:

- Safe management of operational systems
- Procedures required to maintain the safety of systems when maintenance or modification is required
- Safety monitoring and advanced safety monitoring.



By the end of this course you will be able to:

- Compare equipment and operational safety cases
- Describe the relationship between equipment and operational safety cases
- Review operational procedures for safety implications
- Describe and participate in processes for the maintenance of ALARP in operation
- Plan data collection using information from the design safety case
- Describe the role and different levels of health monitoring in operational safety
- Describe and participate in analysis of operational data for safety
- Identify and discuss issues relating to multiple organisations interacting in a safety programme
- Describe and participate in the application of the principles of obsolescence and change management
- Describe and participate in the application of techniques for accident modelling
- Critically compare techniques for accident modelling
- Explain the role of emergency planning in through life safety
- Discuss the state of the art and future directions in through life safety.

11 Security for Safety Critical Systems (SESA)

This module will provide you with a broad awareness of security principles, measures and techniques in order to provide a critical understanding of the relationships between safety and security and how security threats can develop into hazardous events.

> ***"As a practitioner of system/functional safety in the automotive industry I cannot recommend the MSc in Safety Critical Systems Engineering highly enough. The course structure and the mandatory modules cover the fundamentals of system safety in such depth and breadth as to be applicable to any safety standard. Unlike previous degree courses I refer to my York notes a great deal, since they are extremely relevant to my day-to-day safety activities."***
>
> Robert Palin
> Jaguar Land Rover

By the end of this course you will be able to:

- Differentiate between confidentiality, integrity and availability
- Define and explain security definitions and concepts
- Summarise the differences between types of security (physical, information, data network)
- Define and explain information security risk management activities throughout the system life cycle (development, monitoring and change)
- Identify information security methods and considerations
- Describe architectural approaches to mitigating security risk
- Describe current approaches to security regulation for safety-critical systems
- Explain the content and differences between different security standards eg ED-202, ED-203, ED-204, ISO 27005:2011
- Assess the interdependencies between safety and security
- Participate in a security-safety risk assessment
- Describe the current limitations of the engineering of safe and secure systems
- Describe the concept of assurance cases for safety and security.

Converting to a postgraduate award

You can choose to study our modules as individual one-week courses, or use them to count towards a recognised postgraduate award.

We offer an MSc/Diploma in Safety Critical Systems Engineering and a Postgraduate Certificate in Systems Safety Engineering.

These courses aim to provide you with a thorough grounding and practical experience in the use of state-of-the-art techniques for development and operation of safety critical systems, together with an understanding of the principles behind these techniques so that you can make sound engineering judgements during the design, deployment and operation of such a system. On completing the course, you will be equipped to play a leading role in safety-critical systems engineering.

All our postgraduate programmes are suitable for both full-time and part-time students.

The part-time MSc course is typically taken over three years.

For further details on the courses, including how to apply, please see: ***cs.york.ac.uk/postgraduate/taught-courses***

Our courses in System Safety Engineering are accredited by both the Institute of Engineering and Technology (IET) and the Chartered Institute for IT (BCS).

Bespoke courses

We can tailor individual courses to your specific requirements, ensuring they are just right for your business needs.

We offer a range of professional development services which includes working with individuals to design and develop bespoke courses. These courses can vary in length from one day to two weeks and can be delivered either on-site, at a location of your choice, or at the University of York. You can choose from one of the existing one-week short course modules detailed in this booklet, or, if you have a specific area of interest, we are more than happy to discuss your requirements.

We have developed and delivered bespoke courses for major defence and transport companies (automotive, rail, aerospace), military and public bodies, academic departments and independent safety assessment organisations, (BAE Systems, Airbus, Syntell, Rolls-Royce and Invensys) in locations all over the world, including Australia, Singapore, China, Europe and the UK. Courses can be tailored to suit audiences ranging from systems engineers, software engineers, service developers or programme managers - requiring an initial introduction to safety issues - to experienced safety engineers who want to investigate the latest topics and methods in systems and software safety.

Research and consultancy

We welcome collaboration with organisations on research projects and we offer a consultancy service to maximise your business and employees' potential.

We are currently working with several companies on projects to help them take their business forward. Many of our staff undertake consultancy work and have experience of working within a wide-range of organisations to help them to innovate and keep ahead of their competitors.

If you would like us to help you, either through research or a on consultancy basis, please contact the External Programmes Manager to discuss your requirements.

Tel: +44 (0)1904 325415
Email: cs-postgraduate@york.ac.uk

Book your place

To book on any of the courses or to find out about registering for a postgraduate degree, please contact:

Professional Development and Training Administrator

Email: cs-postgraduate@york.ac.uk
Telephone: +44 (0)1904 325536

You can also find more information and book short course modules online at:
york.ac.uk/cs/professional

Contact Us

Professional Development and
Training Administrator

Email: cs-postgraduate@york.ac.uk
Telephone: +44 (0)1904 325536

You can also find more information at
york.ac.uk/cs/professional

cs.york.ac.uk/professional