

# Centre for High Integrity Systems Engineering: Professional Development and Training

[www.cs.york.ac.uk/chise](http://www.cs.york.ac.uk/chise)





## Introduction

The discipline of System Safety Engineering has developed over the last half of the twentieth century. It is concerned with the systematic analysis of systems to identify and evaluate risks, with the aim of influencing design in order to reduce risks.

In mature industries, such as aerospace and nuclear power, the discipline has been remarkably successful, although there have been notable exceptions to the generally good safety record, eg the Chernobyl and Ariane 5 accidents.

The short courses we offer provide a comprehensive grounding in the principles of system safety engineering, such as hazard identification, hazard analysis, risk assessment, through life risk management and system safety justification and certification. In addition, we address advanced topics such as assessment of human factors and software safety analysis and justification.

Various trends pose challenges for traditional approaches to system safety engineering. For example, classical hazard and safety analysis techniques deal poorly with computers and software where the dominant failure causes are errors and

oversights in requirements or design. Thus these techniques need extending and revising in order to deal effectively with modern systems. Also, in our experience, investigation of issues to do with safety of computer systems have given some useful insights into traditional system safety engineering, eg into the meaning of important concepts such as the term hazard. This is the sub-discipline of Safety Critical Systems Engineering for computer based control systems.

The short courses we provide may be used as part of a Continuing Professional Development programme for the Institute of Engineering and Technology (IET), or the British Computer Society (BCS). As part of this, our courses meet the IET Position Statement on Safety Critical Systems, released in October 2009. You can find out how at our website [www.cs.york.ac.uk/cpd/iet-principles](http://www.cs.york.ac.uk/cpd/iet-principles).

You can choose to attend single modules to develop your understanding in a particular area, or attend multiple modules as part of your professional development. These modules can then be used to register for an MSc, Postgraduate Diploma or Certificate.

*"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 LandRover, MSc in Safety-Critical Systems Engineering**

## Our expertise

You will be taught by world-leading experts in the field of system safety.

Our team is made up of academics who have worked extensively in industry as well as undertaken research into the discipline. This research has helped to shape some of what is done in system safety today. An example of this is the Goal Structuring Notation (GSN) developed at York to improve industrial practice in developing and presenting safety case arguments, which 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 overview of both relevant research and industry experience, we are able to develop our teaching in response to new advances and the requirements of industry, to keep your skills and knowledge up to date.

## Modules

Each module lasts for one week, and takes place in York. Visit [www.cs.york.ac.uk/chise](http://www.cs.york.ac.uk/chise) for the latest dates.

If you're thinking of taking our MSc, Postgraduate Diploma or Certificate programme, the modules are a great way of experiencing our teaching and starting in the discipline. If you pass the optional assessment, the module can be counted towards a relevant award if you register within two years.

However, you can choose to take any modules one by one as you wish - you may simply be looking to update your knowledge in a particular area or find out about something new. The flexibility of this approach means that you can just choose to study what areas interest you the most.

We recommend that you take Foundations of System Safety Engineering first, followed by Hazard and Risk Assessment. However, modules can be taken in any order provided learning prerequisites have been met. You can find out more details about each of the modules at [www.cs.york.ac.uk/chise](http://www.cs.york.ac.uk/chise).

### Foundations of System Safety Engineering

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. It also provides 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.

### Hazard and Risk Assessment

This module addresses hazard identification, the application of hazard analysis techniques, and the management and tracking of safety-related risks throughout the life of a system.

### Systems Engineering 1

This module is an introduction to the technical aspects of systems engineering, for embedded control systems. It is influenced by the requirements of gas turbine control, but is intended to present general principles which are applicable to a range of similar embedded safety-critical control systems.

### Software Requirements and Architectures

It is important to treat requirements and architecture together, as requirements can rarely be truly design independent, and it is necessary to have strong links between these two representations in order to establish and maintain product lines. The aim of this module is to provide software engineers with a strong set of principles and techniques for structuring and representing requirements and architectures.

### Electrical Systems and Design

This module provides an introduction to electrical machines and power electronics, and an appreciation of applications and systems issues. It covers operating principles and operational characteristics, competing technologies and design considerations.

### System Safety Assessment

This module is the partner to the Hazard and Risk Assessment module. It covers classical system safety analysis techniques, with an emphasis on fault trees (FTA) and Failure Modes and Effects Analysis (FMEA).

### Introduction to Control Theory

You will learn the fundamentals of classical and modern control in this module. The focus is on providing you with current techniques to design controllers for linear systems, and this is supported by a series of case studies.

### Human Factors for Safety Critical Systems

This module introduces 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. There will also be introductions to the ergonomic, psychological and socio-technical factors that are relevant to an understanding of safety critical systems.

### Safety Case Development and Review

This module addresses the production and assessment of safety cases within safety projects. You will cover the role, purpose and typical content of a safety case; identify how safety case arguments can be selected and critically assessed; explore the development and maintenance of safety cases into the engineering lifecycle; and understand the regulatory context for a safety case development regime.

### Software Testing Analysis and Review

This module is an introduction to systematic methods of verification. It covers a range of static and dynamic techniques and considers their use within the development process. Although many of the techniques covered can be applied to a wide range of software projects, we shall study them from the point of view of safety critical systems. All too often software is designed and *then* tested. The real aim must be to take a more holistic view, where design is carried out with verification in mind to achieve overall goals. We take a view of testing, including various automated and manual static analysis techniques. In addition, we show how increased rigour at the specification stage can significantly help lower-level testing.

### Safety Management Systems

In this module you will gain an awareness of the issues associated with conducting technical safety activities within an organisational and regulatory environment. The aim is to develop skills to apply theoretical safety engineering knowledge in situations constrained by available education, resources and organisational culture.

### Through Life Safety

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; and safety monitoring and advanced safety monitoring techniques.

### Computers and Safety

This is primarily intended to give system safety engineers an introduction to the issues that must be considered when computers are used in safety critical or safety-related applications. The module starts with an overview of how computer systems work, from hardware up to application software. The emphasis throughout is on highlighting areas that are of potential concern to safety engineers. This is followed by a more in-depth examination of the software development process. In particular, we describe aspects of requirements specification, design and analysis that are critical to deployment of computers in safety critical applications. You will also consider the structuring and collection of evidence for a software safety case.

### Aircraft Control Systems

This module provides an introduction to the systems architecture of modern civil and military aircraft. It provides an introduction to the principles underpinning the design of aircraft flight guidance and control systems, particularly the integration of fault tolerant systems and the certification of guidance systems.



### Control Architecture

This module covers the principles applied in the architecture design of the control systems and the functionalities for different gas turbine applications. In addition, the module explores the future directions of control architectures.

### Sensors and Effectors

This module addresses sensors and effectors from a control perspective, including software for controlling and managing sensors and effectors. It also addresses developments in sensor technology.

### Software Implementation

This module considers the theory, methods and techniques behind software implementation, emphasising the needs of safety critical systems development. You will be introduced to the principles of software implementation, and will develop an understanding of the software development process, with a specific focus on implementation; the theory, techniques and tools which relate to the development of software; and the most significant issues affecting the construction of reliable and timely software.

## Systems Engineering 2

This module complements Systems Engineering 1, focusing on systems engineering processes and management. It addresses the issues of risk and obsolescence in systems engineering management as well as the wider aspects of engineering management, including organisations and competencies. It therefore aims to provide sufficient awareness of systems engineering structural issues to provide an understanding of approaches to the managerial aspects of systems engineering projects.

## Timings and locations of modules

All modules are taught in one week blocks at the University of York. Further details on each of the modules and when they are taking place can be found at [www.cs.york.ac.uk/chise](http://www.cs.york.ac.uk/chise).

## Converting to a postgraduate award

### MSc/Diploma in Safety Critical Systems Engineering Postgraduate Certificate in System Safety Engineering

We also offer flexible postgraduate programmes suitable for part-time students. The MSc and Diploma in Safety Critical Systems Engineering emphasises the issues involved in the construction of safety critical systems, incorporating software.

This MSc is made up of six compulsory modules and three optional specialist subject modules. The six compulsory modules are:

- ▶ Foundations of System Safety Engineering
- ▶ Hazard and Risk Assessment
- ▶ System Safety Assessment
- ▶ Safety Case Development and Review
- ▶ Safety Management Systems
- ▶ Critical Evaluation.

You will gain a thorough grounding and practical experience in the use of state-of-the-art techniques for the development of safety critical systems. You will also gain an understanding of the principles behind these techniques to enable you to make sound engineering judgements during the design and deployment of such a system, particularly when software is involved.

When you have completed the programme, you will be equipped to play a leading and professional role in safety critical systems engineering related aspects of industry and commerce.



Visit [www.cs.york.ac.uk/postgraduate/taught-courses](http://www.cs.york.ac.uk/postgraduate/taught-courses) for more details.

## Bespoke courses

In addition to the modules described above, we can provide a range of courses tailored to your specific requirements, either on-site or at the University of York. You can choose any of the modules in this leaflet, or, if you have a specific area of interest in system safety, we are happy to discuss your requirements.

We have delivered bespoke courses for major defence and transport sector companies, military and public bodies, academic departments and independent safety assessment organisations, including BAE Systems, Airbus, Syntell, Rolls-Royce and Invensys, in locations all over the world, including Australia, Europe and the UK.

Courses can be tailored to suit audiences ranging from systems or software engineers requiring an initial introduction to safety issues, up to experienced safety engineers who want to investigate the latest topics and methods in systems and software safety.

If you would like to discuss your requirements, please contact Louise Earnshaw on +44 (0)1904 325414 or email [postgraduate@cs.york.ac.uk](mailto:postgraduate@cs.york.ac.uk)

## Why choose to study at York?

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

## Modules in Large Scale Complex IT Systems

We also offer modules from our Engineering Doctorate in Large Scale Complex IT Systems (LSCITS) as professional development and training.

These include:

- ▶ Systems Engineering for LSCITS
- ▶ Empirical Methods for LSCITS
- ▶ Socio-Technical Systems
- ▶ Predictable Software Systems
- ▶ High-Integrity Systems Engineering
- ▶ Technology Innovation.

Further information on all these modules is available at [www.cs.york.ac.uk/engd/-Core-Modules-](http://www.cs.york.ac.uk/engd/-Core-Modules-)

*“As a clinician working for the Department of Health Informatics Directorate (the organisation responsible for delivering the NHS National Programme for IT) supporting software architects, engineers and project managers to deliver safe technology to the NHS, I have found the MSc in Safety Critical Systems Engineering to be absolutely essential. The quality of the lectures, teaching materials and content delivered is second to none. I have not undertaken any training or education since qualifying as a clinician that has been so relevant, useful and practical for my daily job.*

*I would recommend that anyone working in healthcare with an interest in patient safety should take the Foundations of System Safety Engineering module at the very least. For those who have a more focused safety role, particularly in healthcare technology, the University offers a number of modules to choose from, working up to the MSc in Safety Critical Systems Engineering.”*

**Beverley Scott, Clinical Safety Advisor,  
Department of Health Informatics Directorate**

## Book your place

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

Professional Development and Training Administrator  
**Email:** [postgraduate@cs.york.ac.uk](mailto:postgraduate@cs.york.ac.uk)  
**Telephone:** +44 (0)1904 325402

You can also find more information and book online at [www.cs.york.ac.uk/chise](http://www.cs.york.ac.uk/chise)

