Jaguar Land Rover
Technical Accreditation Scheme
Developing your future in the workplace
Contents

Introduction to the TAS Scheme 1
Introduction to York modules 2
Why York? 3
Learn from the experts 3
Modules at a glance 4
Foundations of Systems Safety Engineering (FSSE) 6
Systems Engineering for Safety (SEFS) 8

Hazard and Risk Assessment (HRAS) 10
Software Requirements (SWRE) 12
System Safety Assessment (SSAS) 14
Safety Management Systems (SMSY) 16
Safety Case Development and Review (SCDR) 18

Human Factors for Safety (HUFS) 20
Computers and Safety (CASA) 22
Through Life Safety (TLSA) 24
MSc Options 28
Book your place 29
Introduction to the TAS Scheme

The Technical Accreditation Scheme (TAS) is part of the Jaguar Land Rover Learning Academy. It provides an innovative and progressive approach to skills growth; making the most of the academic excellence of all the University partners involved in the delivery of this cutting edge education.

Jaguar Land Rover (JLR) launched the TAS Scheme to deliver skills development in specific key technical disciplines. All partner Universities deliver masters level and accredited modules as part of the scheme and modules can be all taken separately or combined to form a qualification, up to and including an MSc or EngD from one of the partner universities.

As part of the TAS Scheme, the University of York offer 11 modules in the area of Systems Safety Engineering. This brochure will detail what York can offer you as part of this innovative scheme.

"Personal development is business critical to JLR ensuring continued innovation and technical excellence in the design, manufacture and delivery of premium cars and auto engines, The Technical Accreditation Scheme is our innovative and progressive approach to skills growth making the most of the excellence of our university partners in delivering cutting edge education."

Jo Lopes
Head of Technical Excellence, JLR
Introduction to York modules

Technology advances into every part of our lives, safety and security of goods and services becomes more important and challenging. Whether that be 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, the need for safety and security is all around us.

System safety engineering is concerned with the systematic 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 dealt poorly with computers and software, particularly as modern systems are highly integrated, and often networked to form “systems of systems”. Addressing these issues is the sub-discipline of safety critical systems engineering for computer-based systems.

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 give you knowledge of safety engineering using examples from a range of domains including automotive safety standards.
Why 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 blocks
- Choose to study for a recognised postgraduate award
- 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 as well as undertaken research into the discipline. This experience, coupled with up-to-date training materials and real-life industrial case studies, will help you to learn in the context you need.

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 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.
We offer eleven short course modules in System Safety Engineering, which are delivered over 5 days, enabling you to learn alongside your work, ensuring your skills are fully up to date.
Automotive safety can be divided into active safety and passive safety. Passive safety refers to systems such as PRS, ARS, brakes, windscreens, and so on. 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 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. 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.

"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 lifecycle, and the roles of the major groups of techniques within it.
This module is an introduction to the technical and organisational aspects of systems engineering, focusing on early life cycle systems analysis and modelling (i.e., systems concepts, requirements and architectures).

It intends to present systems engineering principles which are applicable to a range of critical engineering systems (e.g., control systems, platforms, systems of systems and autonomous and configurable systems).

In particular, it focuses 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.
Hazard and Risk Assessment (HRAS)

This module teaches 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 lifecycle. It encompasses predictive, target-setting techniques and should ideally be taken as a pair with System Safety Assessment, which addresses concepts and techniques appropriate to the later stages of a development project.

“The University of York System Safety TAS modules continue to be the best source of learning for both functional safety and the wider system safety. The relevance of this training increases more and more as the control of the vehicle transitions more and more from the driver to the machine.”

Roger Rivett
Functional Safety Technical Specialist
By the end of this course you will be able to:

- An understanding of the principles of hazard identification and assessment
- The ability to apply techniques such as Functional Failure Analysis and HAZOP
- An understanding of approaches to risk reduction
- An appreciation of common cause or common mode failure mechanisms and their importance.
4 Software Requirements (SWRE)

The aim of this module is to provide 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 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.
This module aims to cover the analysis and assessment phase of the system safety engineering life cycle for a proposed product or service. It does so by considering the inputs to this phase, the qualitative and quantitative analysis techniques that can be employed within this phase, and the outputs from this phase in terms of evidence into the safety case regime. It also considers the 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 lifecycle
- 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.
This module aims to provide students with an awareness of the issues associated with conducting technical safety activities within an organisational and regulatory environment and to develop skills at 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.
This module addresses the production and assessment of safety cases within safety projects. The module covers the role, purpose and typical content of safety case; explains how safety case arguments and evidence can be selected; relates the development and maintenance of safety cases to the engineering lifecycle; details how safety case arguments can be critically assessed; and explains the regulatory context for a safety case development regime.
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.
This course introduces you 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.
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.
Computers and Safety (CASA)

This course aims to introduce you to the issues of using computers in safety-critical or safety-related applications. The course highlights areas of potential concern to safety engineers, including an in-depth examination of the software development process, considering aspects of requirement specifications, design and analysis that are critical to the deployment of computers in safety-critical applications.

“A pleasure to be taught by highly qualified lectures who are clearly passionate about the subject matter.”
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.
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
- Identifying 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.

This module aims to provide a broad awareness of security principles, measures and techniques; to provide a critical understanding of the interrelationships between safety and security and how security threats can develop into hazardous events; to address the elements identified in this figure.

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 lifecycle (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 e.g. ED-202, ED-203, ED-204, ISO27005:2011
- 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 in System Safety Engineering with Automotive Applications and an MSc Safety Critical Systems Engineering.

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

MSc in System Safety Engineering with Automotive Applications

This MSc course has been developed for the Jaguar Land Rover Technical Accreditation Scheme and is designed to prepare you for work in the demanding field of Safety Systems Engineering (SSE) by exposing you to the latest science and technology within this field.

In the core module phase, the course focuses on the principles and practices in SSE across a range of domains, including automotive. In the optional module phase, the course focuses on specialist SSE and automotive topics. The projects are also designed to consider SSE topics within an automotive context.

The course is available on a part-time basis, taking typically four years to complete. You will take 12 assessed modules over three years, five of which are Core (C) and seven Optional (O), plus a project on a SSE topic within the automotive domain (in the final year). Modules are taken at York and other TAS (Technical Accreditation Scheme) providers.
MSc in Safety Critical Systems Engineering

This course aims 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, students will be equipped to play a leading role in safety-critical systems engineering. This course is available on both a full time and part time basis. The part time course is typically taken over three years.

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

---

Book your place

All York TAS scheme modules take place in one week blocks delivered at the University of Warwick or the University of York. Course dates can be found on both SuccessFactors and online at www.cs.york.ac.uk/professional/JLRTAS

JLR employees should complete the required TAS registration form for each module they wish to register for. This can be found on SuccessFactors. Once you have registered via SuccessFactors you will be contacted by York and asked to also register with them.

To find out about registering for a postgraduate degree, please contact:

Professional Development and Training Administrator
Email: postgraduate@cs.york.ac.uk
Telephone: +44 (0)1904 325536

You can also find more information and book online at: www.cs.york.ac.uk/postgraduate
Contact Us

Professional Development and Training Administrator

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

You can also find more information and book online at
www.cs.york.ac.uk/professional/JLRTAS