BURGE HUGHES WALSH

SYSTEMS ENGINEERING

3-day Workshop on Designing Safe Systems

Workshop Description

Systems are unsafe because we design them or manufacture them to be so. Current approaches to product safety miss an opportunity to "design-in safety" because they don't consider safety until a solution exists. At this point the design solution is analysed to see how it can be, or become, unsafe, with any issues addressed through a re-design. While this is obviously a sensible approach, safety can be, and should be addressed much earlier during the requirements phase.

The application of a systems approach during the requirements phase allows us to understand how the "problem" can made unsafe. At this point no solution exists but we understand the engineering problem as a set of interconnected functions. The design phase is concerned with selecting the best technological solution to each function that are integrated through an architecture. Clearly how those technological solutions perform and interact dictate the product safety. Poor choices could lead to an unsafe system: we design in unsafety! However, if we understand how the problem could become unsafe by investigating the potential functional failures and how unsafe behaviour can emerge through the interaction between those functions, we have an opportunity to design in safety by selecting technology that make the failures impossible or at least less likely.

The systems approach to designing safe systems aligns with the classic approaches with the analyses feeding the classic Hazard Analysis, Hazard Logs and Safety Cases. It does require, however, for safety to be integral task of system design and thereby the remit of the design engineer.

This 3-day course is aimed providing attendees with an awareness, understanding, specific knowledge and the application of System Safety concepts, principles and practice that can be employed to design inherently safe systems.

Who Should Attend?

This course can be taken by anybody who is involved in the design of systems.

Benefits to the Individual and Business

During an intensive three days of teaching and practical 'hands on' exercises, participants will be challenged to develop the skills and mindset that can be applied to any design situation irrespective of context.

At the end of the course participants will:

- be aware of, and understand, the concepts and principles of a systems approach to product safety
- understand the safety engineering process and how it aligns with systems engineering.
- have been given an overview of the system safety engineering tool set.
- have had an opportunity to practise the use of key safety tools, particularly those related to design
- understand how the safety engineering process and tool output contributes the classic Hazard Analysis and generation of Safety Cases.

Learning Approach

The learning approach is based on the Kolb learning cycle with a significant proportion of the course set aside for exercises to reinforce the learning. Indeed, the course employs a number of small group exercises involving a case study to provide a practical focus for the course which enables the delegates to practise the methodology and tools.

Course Content

Day 1

- Introduction and Delegate expectations
- What is safe?
- Types of safety
  - Product
  - Health and Safety at Work
- Why systems safety?
  - Perception and risk
  - Legal reasons: The Law and "duty of care"
- Safety Thinking
  - Risk based approaches
  - Systems approaches
- Classic Safety Engineering
  - Hazards, accidents and risk
  - Heinrich's Triangle
  - Hazard identification and assessment
  - Causes: Faults and failures – active and latent conditions
  - "Swiss Cheese" model
  - Measuring safety
  - ALARP
  - Risk management – dealing with un-safety
- Safety Engineering
- Purpose of safety engineering
  - The basic safety engineering process:
  - Lifecycle Management, systems Engineering and Safety engineering
  - Opportunities with the extended V model for safety engineering
  - The Safety Case
  - Purpose of a safety case
  - Issues with safety cases
  - Basic Safety Case content
  - Constructing safety arguments
  - Presenting clear arguments
  - Typical safety argument structure
  - Types of safety evidence
  - Hints and tips when developing safety cases

Day 2

- Day 1 Review
- A Systems Approach to Safety Engineering
- A Systems view of Safety
  - Emergence – desirable and undesirable
  - System Purpose and Function
  - Context and constraints
  - Behaviour – event, patterns and structure
- System Unsafety Causes
  - Element failure
  - Dysfunctional Interactions
  - Variation and Noise
- System Safety, Hazards and Risk
- Hazard Analysis
  - How to do it | Practise Examples
- Hazards and Lifecycle Management
  - V-Diagram
  - Lifecycles and Design Reviews
- Designing in Safety
  - Traditional vs Systems approach to design and safety
  - Understanding the Systems problem (fully) through functionality
  - Functionality and safety
- Understanding unsafety due to Failure
  - Functional Failure Mode and Effects Analysis
    - How to do it | Practise Examples
- Root Cause Analysis
  - Cause and Effects Analysis
    - How to do it | Practise Examples
  - Multiple Cause Analysis
    - How to do it | Practise Examples
  - Fault Tree Analysis
    - How to do it | Practise Examples

Day 3

- Day 1 and 2 Review
- Understanding unsafety due to Noise
- Noise and safety
  - Parameter- Diagrams
    - How to do it
    - Practise Examples
  - What-Why Matrix
    - How to do it
    - Practise Examples
- Understanding unsafety due to Dysfunctional Interactions
  - Linked Parameter- Diagrams
  - Functional Modelling and Sensitivity Analysis
    - How to do it
    - Practise Examples
- Designing in Safety
- Functions in Designs
  - Function Means Analysis
    - How to do it
    - Practise Examples
- Summary and Close

Course Delivery

The course has been designed for minimum numbers of 8 and maximum of 16 and can be delivered on site or at a suitable venue.

Workshop Costs

The cost of delivering the 3-day workshop, excluding delivery tutor accommodation and expenses, but including all courseware is £6,500. VAT will apply at the prevailing rate.

The course can be tailored to suit individual customer's operations.

BURGE HUGHES WALSH

QAS INTERNATIONAL ISO 9001:2015 REGISTERED FIRM

ENDORSED TRAINING PROVIDER

BURGE HUGHES WALSH LIMITED

First Floor, 6 Allerton Road, Rugby, Warwickshire CV23 0PA

enquiries@burgehugheswalsh.co.uk

www.burgehugheswalsh.co.uk

01788 550015