

Developing a Safety Case - An Introduction

Overview

This one-day course is designed to impart a basic understanding of the concepts underlying safety analysis, and of the structure and rationale of the safety documentation required by the Ministry of Defence procurement process. The course describes the methods and procedures for preparing clear, concise and comprehensive documents in accordance with specific standards, notably Defence Standard 00-56 and JSP454.

Target Audience

The course is designed for defence industry personnel such as:

- Engineers and designers who make decisions affecting the safety of new or modified military systems.
- Project Managers who require an overview of safety case development for budgetary purposes.
- Operations Managers who need an awareness of the risks associated with the equipment and the ways in which they are controlled.

Objectives and Utility

On completing this course, delegates will take away a basic understanding of safety analysis. This knowledge will benefit them directly in a professional sense and benefit their sponsoring organisation through their increased perception of the risks associated with defence equipment and the ways of avoiding them throughout the CADMID cycle.

The Training Process

The course consists of eight complementary modules. Its presentation is largely audiovisual - interspersed with a number of short practical exercises to encourage delegate participation and reinforce the key principles.

All delegates are issued with comprehensive course notes and a certificate of attendance.

Developing a Safety Case - An Introduction

Course Programme

Day 01 - AM

083 What is a Safety Case

The first module provides delegates with the definition of a safety case used by the UK Ministry of Defence. It describes the role of the safety case in the defence procurement process, and its evolution through the phases of the CADMID cycle from Concept to Disposal. Examples are provided of the purposes of a safety case and the advantages it brings.

084 Fundamental Concepts

Delegates will learn the meaning and application of safety-related concepts such as:

- Scope of safety case, safety targets
- Hazard, hazard event, hazard event frequency, frequency time base, hazard controls
- Accident, accident trigger, accident trigger probability, accident frequency, accident severity, accident consequences (for personnel, equipment and environment), accident controls
- Risk, risk tolerability criteria, risk matrix, risk class, risk anchor point, unmitigated risk, mitigated risk, control failure risk
- As low as reasonably practicable (ALARP), the ALARP triangle, the ALARP statement

085 Analyses

This module discusses the following processes and systems and their role in the development of the safety case:

- Safety Management System (SMS)
- Project Safety Panel (PSP)
- Human Factors Analysis (HFA)
- Fault tree analysis (FTA)
- Event Tree Analysis (ETA)
- Failure Modes Effects and Criticality Analysis (FMECA)
- Preliminary hazard analysis (PHI)
- Data recording, analysis and corrective action system (DRACAS)
- Independent Safety Assessor (ISA)

086 Documentation

This module provides an overview of the safety documentation required by the MoD:

- Target Audience Description
- System Requirements Document
- System Specification Document
- System Safety Plan
- Hazard Log
- Safety Case Report
- Component-level data and documents
- Minutes of HAZOP meetings

087 Standards and Legislation

There is a proliferation of standards and legislation in the field of safety. This module describes the following documents, and the hierarchy in which they are placed by the Defence Standards Organisation, [DStan].

- Def Stan 00-56 Issue 2 and 3, Parts 1 and 2 (Safety Management Requirements)
- Def Stan 00-55 (Safety related software)
- Acquisition Safety and Environmental Management System: POSMS, POEMS
- Def Stan 00-27 Issue 2 (Impulse Noise measurement)
- Control of Noise at Work Regulations 2005
- Def Stan 00-25 (Human Factors)
- JSP 430 (Sea systems safety)
- JSP 454 (Land systems safety)
- JSP 520 (Ordnance, Munitions and Explosives)
- ISO 14001: Environmental Management Systems

Day 01 - PM

088 Human Reliability

The importance of human error to overall system safety has grown as the equipment used has become more reliable. So an understanding of human reliability issues is essential for safety case developers.

This module begins by exploring the types and contexts of human error, and then examines the techniques available for identifying and quantifying it. The following human reliability analysis techniques are covered: Human HAZOP, THERP, HEART, SHERPA and QHRA. The modifying role of performance shaping factors on error likelihood is explained. The role of Human Performance Limiting Values in providing a limit on the estimation of human reliability is described.

The module concludes by examining a range of approaches for controlling and therefore reducing human error.

089 Practical Session

Working in groups, delegates will be set the task of analysing the safety of a simple but hazardous military system. The output will be a list of hazards with estimates of their frequencies. The session will conclude with a comparison and discussion of the findings.

090 Software Tools

Considering the complexity of the calculations and the need for meticulous audit trails, it is not surprising that computer packages are commonly used for managing the hazard data for the safety case. The merits and demerits of the following tools are discussed:

- Cassandra (HVR)
- HARMS (BMT)
- Access, Excel, Word (Microsoft)

500-R Recapitulation

The course is summarised. This is also a final opportunity for questions and answers.