Principles of Engineering Safety Management

Ian Spalding
Praxis Critical Systems Ltd
20 Manvers Street, Bath, England, BA1 1PX

Abstract

Praxis Critical Systems has been involved over many years in helping companies across a wide range of industries introduce, and successfully run, effective Safety Management Systems. This paper is a distillation of our experience and provides a grounding in the principles of Engineering Safety Management.

An effective Safety Management System should combine the principles of the latest standards with practical experience of safety management and safety case approval. The paper provides a background to safety management by describing the legislative framework and relevant safety standards to which a Safety Management System must conform. The paper provides an understanding of the key concepts of safety management and defines the essential safety terminology, the concept of the safety lifecycle, and covers the responsibilities and roles undertaken by staff. A Safety Management System also depends on effective planning and documentation and the paper describes the essential safety documents.

A central part of the paper introduces the main techniques of Hazard Identification and Hazard Analysis which lead to Risk Assessment and the setting of Safety Requirements. A key part of managing safety is to provide assurance that both the processes and the engineering being applied will yield satisfactory results and an outline of safety assurance is provided. Finally, the concepts of the Safety Case and Safety Certification are covered.

Introduction

Every organisation has an obligation and responsibility to understand the safety implications of the services and products being provided and to manage these implications effectively. It is now widely recognised within many industries, and within various international standards, that to ensure best practice and the highest standards, safety-related activities must be carried out within the framework of a Safety Management System. Such a system can assist in making sure that all the necessary safety activities are carried out at the right time and in a cost effective manner, so increasing confidence in the safety of the services and products.
This paper sets out the principles of a Safety Management System and describes how these might be applied. The context of the Safety Management System described is that of an engineering environment which is principally concerned with the development and implementation of systems involving programmable electronic systems (PES).

**Legislative Context**

As engineers working on safety-related projects, we must be aware of regulations and legislation relating to the safety of products and services. In the UK, the primary legislation in this area comprises the Health and Safety at Work Act (HSWA) 1974 and the Consumer Protection Act (CPA) 1987.

The HSWA provides a legislative framework for promoting high standards of health and safety at work. The HSWA is administered by the Health and Safety Executive (HSE) which is, in turn, supervised by the Health and Safety Commission (HSC). The HSE assumes overall responsibility for a number of industries and sectors including the Nuclear and Offshore industries and the Railways. From time to time, legally-binding Regulations applying to those industries and sectors are issued under the HSWA. Recent regulations issued under the HSWA, eg The Management of Health and Safety at Work Regulations 1992 [HSC 92] and the Construction (Design and Management) Regulations 1994 [HSCb 94], have a wider influence. These Regulations require employers to make suitable and sufficient assessment of the risks to the health and safety of employees and the general public who may be affected by their undertaking. The HSC Approved Code of Practice [HSC 92] outlines the principles of risk assessment for this purpose.

The Consumer Protection Act (CPA) 1987 enables members of the general public who are injured by defective products to gain redress from the producers of those goods. Under the CPA, the injured party need show only that the product is not as safe as people are entitled to expect. This places a far greater responsibility on the producer who previously was required to show only that they had taken reasonable care. Defences allowed under the CPA include the ‘development risks defence’ in which a producer will not be liable for injuries caused by a defective product if he or she can prove that the defect could not have been expected to be discovered given the state of scientific and technical knowledge when the product was released.

The CPA enacts, in the UK, the European Product Liability Directive of 1985. The European Union is becoming increasingly influential in setting safety standards for manufacturers of products and suppliers of services via the publication of European Directives which are reflected in national law or used as the basis for action in the European Court.

As engineers assigned to safety-related projects, we must take our responsibilities for safety seriously. Whilst recognising that absolute safety is unattainable, and that the decision on what is economically justifiable is a matter for judgment, we must take all reasonably practicable measures to ensure the safety of the systems we develop.