

# Preface

The core of safety engineering is a systematic approach to identifying the hazards and hazardous events that could happen, and then eliminating or controlling the risk. All this must be done until the risk is tolerable, and then it must be recorded, demonstrated and sustained over time. In step with this, there is a duty to assure yourself and demonstrate to others that your system, project, process or piece of equipment is tolerably safe, not only to the people who come into direct contact with it, but also members of the public and the environment at large. Corporate image and survivability is at stake, when considering what safety related actions to take. It really can be the difference between life and death, if it is applied correctly, the benefits to the organisation are truly amazing – lower lost time, fewer workplace incidents, improved staff loyalty and a better bottom line.

The major tools for accomplishing all of this is the concept of a safety case and safety report. The parallels with a legal case are useful – they equally scare corporate managers. The main difference with the safety case is that you have the opportunity to construct the case in your own time and whilst you are developing the system. You do not have to be called to court to have to start to prepare your case, you can do it now while you have all the information around you and full control over it.

The key elements of this text are based around identifying the meaning and measurement of safety and risk; the motivation behind the need to construct a safety case; the management of the task of generating and presenting one; and how to maintain it once it has been produced. Explicit guidance is given on developing risk matrices, safety targets, demonstrating ALARP, the value of preventing a fatality and tools and techniques for safety assessments. Coupled with these, are specific chapters on human factors, software factors and management factors and how they influence safety performance and safety cultures. All these areas need to be considered in a robust, consistent and complete safety case.

The text takes a world view of safety engineering across all the hazardous industries – nuclear, rail, chemical, defence and construction, citing historical and not-so-historical incidents to provide real examples of the textural points being made. Some you will probably be familiar with, others show classic traits of poor safety practice and worse safety management.

The importance of the safety case cannot be understated, it has become integral to UK industry, with statutes mandating its use in certain high risk industry. Knowledge of it is required to operate at any level in any of the industries noted above. Additionally, risk and safety have become political issues, the UK Government has expressly said that safety management – getting the right

balance between innovation and change on one hand, and avoidance of shocks and crisis on the other – is now central to the business of good government.<sup>1</sup> Within the US, the safety case concept has yet to take real hold. It is certainly known about, even as long ago as 1998, an influential paper on maintaining US leadership in aeronautics directly recommended safety arguments systematically presented in the form of a safety case. This document also cited that this would provide the aircraft industry with an approach to certification that is rapid, repeatable and accurate.<sup>2</sup>

Around the rest of the world, the safety case concepts are being employed with great effect. From European air-traffic control to Australian petroleum facilities, the safety case is in essential use recording risks, the controls in place and the safety management system in place to ensure that the controls are competently and steadily applied.

This book will provide an introduction to and discussion on the contemporary techniques for developing and assessing safety cases and safety reports. It gives an understanding of the principles behind the techniques so that readers can start to make judgements about safety and risk during their studies and work. The text also seeks to enhance the reader's appreciation of the importance of the role of safety engineering within the team, the organisation and the societal community.

Finally, whilst this book offers a full and wide ranging consideration of system safety engineering, it is guidance and discussion only, and is in no way a replacement for full safety assurance. Safety concerns should be addressed by a team of competent professionals, using their experience and judgement in combination with best practice, techniques and other applicable processes.

Richard Maguire  
September 2006

---

<sup>1</sup> “Risk: Improving government’s capability to handle risk and uncertainty”, The Cabinet Strategy Office, 2002.

<sup>2</sup> “Maintaining US Leadership in Aeronautics: Breakthrough Technologies to Meet Future Air and Space Transportation Needs and Goals”, The National Academy Press, 1998.