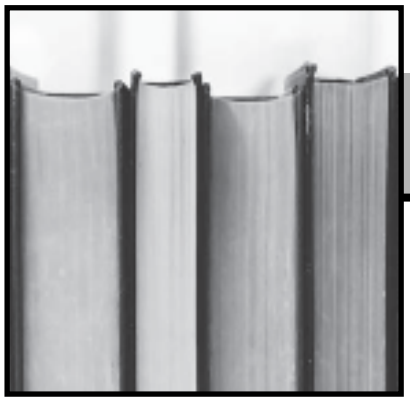


System Safety Bookshelf

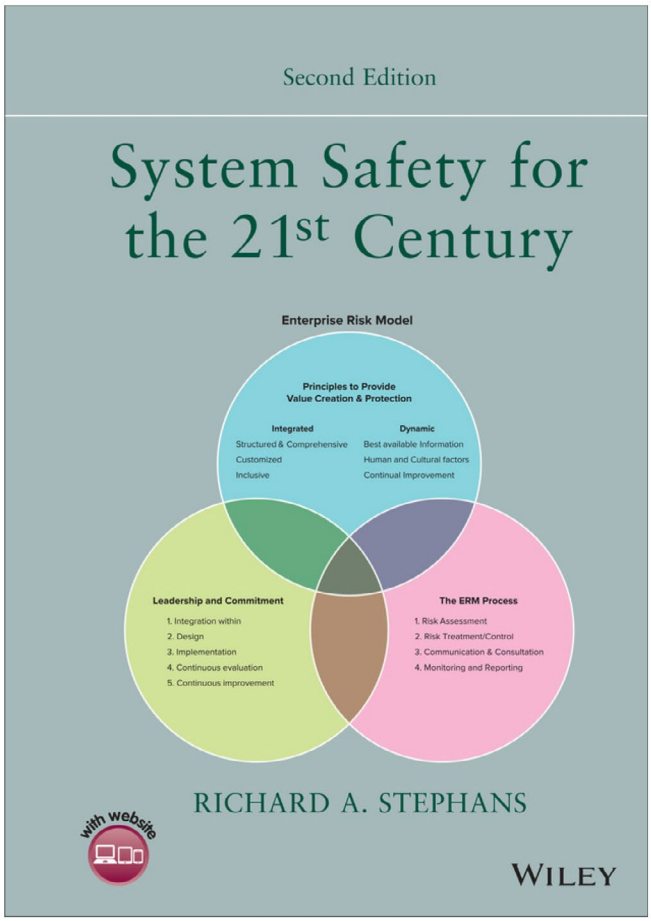
by Malcolm Jones

System Safety for the 21st Century

2nd Edition

Activities, processes and products are undertaken for a reason and that is for an overall benefit. However, all are subject to hazards and risk and there must be a constant process of looking for the correct benefit/risk balance – of course no activity, process or product is completely free from risk – or the concept zero risk. The comprehensive approach to achieving this desired balance sits under the heading of System Safety. So, what is it? It is the process and the set of support tools which enable one to minimise the hazards and detriments associated with the relevant activities. In order to accomplish this one must define the system and its boundaries and then to both identify the hazardous conditions that can arise within the boundary together with the threats that impinge on the system from outside of the boundary, and in addition, the threats to the environment emanating from inside of the boundary. In the former case they can arise from quality failures, including human reliability, and logic failures arising from 'as yet' not understood fault sequences. In the 'external case' they arise from failures such as poor training, environmental uncertainties and in the setting of incorrect policy and strategy. Over many decades System Safety has evolved from a more re-active nature - learning from failures and improving – not really suitable for high consequence enterprises - to today's more pro-active form. This is now based on better fundamental understanding, better assessment processes, better standards, more comprehensive analysis tools with better audit and regulation procedures. However, unlike 'set educational subjects' such as engineering, science, technology and mathematics, there are less opportunities for formal System Safety education and training in academia and elsewhere, even though system safety impacts on all aspects of life. One hopes that this will continue to be rectified.

This leads us directly to the importance and value of this book, which gives a complete insight into the nature of what System Safety is all about, including its approaches, methodologies and tools, and which provides guidance on the successful application of a comprehensive, pro-active approach for ensuring safe system design.



Richard A. Stephans
ISBN: 978-1-119-63475-1
Print | September 2022 | 416 Pages

This is a book that will prove valuable to all practitioners in System Safety, ranging from the experienced proponents who need reminding of the range of procedures and techniques available for tackling the challenges that lie in front of them, to the new practitioners who are about to embark on new and fruitful careers in this exciting and valuable field. The essential guide to start them soundly on their way. The book is written in a form whose preface directs the reader to the appropriated parts of the book to satisfy each category of interested recipient, whether safety manager, student or dedicated safety professionals. The original Edition of 2004 has now been updated to include important System Safety developments that have evolved since that time and as such, brings the subject up to date.

It is not the purpose of the book to delve into detail in all specific areas, follow on detail can be found from the supporting reference list, but rather it identifies in a comprehensive fashion the range of where and how System Safety can be applied. As such, it acts as the launching points for further detailed practitioner application on an as-needed custom basis.

Not only should System Safety be valued for its moral dimension, but a successful and well-structured safety culture is invaluable within the competitive environment which enterprises inhabit. For well-understood reasons, good safety represents a major attribute for enterprise brand and commercial success. At the extreme end lie enterprises where safety failure can be catastrophic and where the application of System Safety should be paramount. The author's valuable experience in these areas is reflected in the contents of the book.

The book also ventures into Artificial Intelligence aspects of System Safety, but this is restricted to health aspects. Of course, we are now seeing a burgeoning of AI in many other areas of System Safety, coupled with associated concerns about its probabilistic rather than deterministic relationship between cause and effect, when applied to high consequence enterprises.

The author has many decades of experience in hands-on successful application of System Safety in a wide range of areas and is a member of a cadre of pioneers in the US who established the concept of the System Safety profession, and which eventually founded what has become the International System Safety Society. He was a prominent member of that evolution and has continued to play a significant role in its subsequent developments, both in leadership and educator roles. He is a Co-Editor of the Society's "System Safety Analysis Handbook". The author was very familiar with the System Safety challenges that engineers faced in those early days and his direct involvement and experience has enabled him to clearly highlight the System Safety development history in the book. This 2nd edition brings us up to date with modern approaches. The author has also capitalised on this experience in relation to his role as an educator, and this is again reflected in the style of the book and of course in its associated Instructor Manual, which forms part of this review. The Manual gives comprehensive advice on how an Educator can best develop teaching courses by way of best structuring and ordering of chapter coverage. Each chapter in turn has an associated set of questions to best support student learning through enabling a deeper and more reflective

> "The book covers the whole range of System Safety from system concept through to disposal and along the way covering all aspects of risk management, control processes, accident analysis and sound design principles."

Photo: Pexels

understanding of contents of each chapter.

The author's System Safety fund of knowledge and experience is founded in his extensive career in US DOD, DOE and environmental restoration programmes. For this reason, the book inevitably has a strong US slant, for example with its references to US aviation, DOE, DOD, NASA, EPA, OSHA and the US nuclear industries. As such, its contents may not be immediately familiar to an international audience. For example, in the UK, where system safety activities are based around Relevant Good Practice, Joint Service Publications and the Ministry of Defence requirements for an enveloping Formal Safety Case, with its emphasis on demonstrating that the risk is As Low as Reasonably Practicable (ALARP). The latter being a legal requirement in the UK. Nevertheless, from a general perspective, the book's contents will be familiar, understood and applicable internationally. After all, the processes of System Safety including its problems, techniques, procedures and requirements are somewhat common the world over. For this reason, the book will not suffer from this national bias base.

The book covers the whole range of System Safety from system concept through to disposal and along the way covering all aspects of risk management, control processes, accident analysis and sound design principles. This is complemented with a comprehensive range of risk analysis tools and procedures, with examples of application given to set the reader in the right direction. Perhaps one approach that is not covered is the Systems -Theoretic Accident Model and Processes (STAMP) methodology advocated by Nancy Leveson of MIT.

This revised edition now includes a section on the value of System Safety in hospital health care and management, together with the general medical field, reminding the reader of how wide-ranging is the application of System Safety. We are all now very well aware of its value in the field of infection control given the recent/current Corona virus pandemic.

The book contains an extensive list of references, again mainly of a US nature, for those who require to delve in more depth into the various processes and tools of System Safety. One to note is the 1997 Edition of the System Safety Analysis Handbook, Second Edition, St Pauls MN, Published by the International System Safety Society.

In summary, System Safety practitioners within whatever areas and level of business they occupy; technical, management, medical, educational, would surely benefit from having this on their bookshelf and the associated Instructor Manual a must for the latter category.

Reviewed by - Malcolm Jones, BSc, PhD, C. Eng, C. Phys, F. int P, MBE, a long time Fellow of the International System Safety Society. He is a Physicist by training and has more than 50 years of experience in safety in the UK's nuclear Industry, within which he still plays an active role. During his career he has gained a number of National and International awards, including the International Systems Safety Society's development award for lifetime contributions to the development of the System Safety process.