Preface

In the past two decades, industry—particularly the process industry—has witnessed the development of several large 'super-projects', most in excess of a billion dollars. These large super-projects include the exploitation of mineral resources such as alumina, copper, iron, nickel, uranium and zinc, through the construction of huge complex industrial process plants. Although these super-projects create many thousands of jobs resulting in a significant decrease in unemployment, especially during construction, as well as projected increases in the wealth and growth of the economy, they bear a high risk in achieving their forecast profitability through maintaining budgeted costs. Most of the super-projects have either exceeded their budgeted establishment costs or have experienced operational costs far in excess of what was originally estimated in their feasibility prospectus scope. This has been the case not only with projects in the process industry but also with the development of infrastructure and high-technology projects in the petroleum and defence industries. The more significant contributors to the cost 'blow-outs' experienced by these projects can be attributed to the *complexity of their engineering design*, both in technology and in the complex integration of systems. These systems on their own are usually adequately designed and constructed, often on the basis of previous similar, though smaller designs.

It is the critical combination and complex integration of many such systems that give rise to *design complexity* and consequent frequent failure, where high risks of the integrity of engineering design are encountered. Research into this problem has indicated that large, expensive engineering projects may have quite superficial *design reviews*. As an essential control activity of engineering design, design review practices can take many forms. At the lowest level, they consist merely of an examination of engineering drawings and specifications before construction begins. At the highest level, they consist of comprehensive evaluations to ensure *due diligence*. Design reviews are included at different phases of the engineering design process, such as conceptual design, preliminary or schematic design, and final detail design. In most cases, though, a structured basis of measure is rarely used against which designs, or design alternatives, should be reviewed. It is obvious from many

examples of engineered installations that most of the problems stem from a lack of proper evaluation of their *engineering integrity*.

In determining the complexity and consequent frequent failure of the critical combination and complex integration of large engineering processes and systems, both in their level of technology as well as in their integration, the integrity of their design needs to be determined. This includes *reliability*, *availability*, *maintainability* and *safety* of the inherent process and system functions and their related equipment. Determining engineering design integrity implies determining reliability, availability, maintainability and safety *design criteria* of the design's inherent systems and related equipment. The tools that most design engineers resort to in determining integrity of design are techniques such as hazardous operations (HazOp) studies, and simulation. Less frequently used techniques include hazards analysis (HazAn), fault-tree analysis, failure modes and effects analysis (FMEA) and failure modes effects and criticality analysis (FMECA). Despite the vast amount of research already conducted, many of these techniques are either misunderstood or conducted incorrectly, or not even conducted at all, with the result that many high-cost super-projects eventually reach the construction phase without having been subjected to a rigorous and correct evaluation of the integrity of their designs.

Much consideration is being given to general engineering design, based on the theoretical expertise and practical experience of chemical, civil, electrical, electronic, industrial, mechanical and process engineers, from the point of view of '*what should be achieved*' to meet the design criteria. Unfortunately, it is apparent that not enough consideration is being given to '*what should be assured*' in the event the design criteria are not met. It is thus on this basis that many high-cost super-projects eventually reach the construction phase without having been subjected to a proper rigorous evaluation of the integrity of their designs. Consequently, research into a methodology for determining the integrity of engineering design has been initiated by the contention that not enough consideration is being given, in engineering design and design reviews, to *what should be assured* in the event of design criteria not being met. Many of the methods covered in this handbook have already been thoroughly explored by other researchers in the fields of reliability, availability, maintainability and safety analyses. What makes this compilation unique, though, is the combination of these methods and techniques in probability and possibility modelling, mathematical algorithmic modelling, evolutionary algorithmic modelling, symbolic logic modelling, artificial intelligence modelling, and object oriented computer modelling, in a logically structured approach to determining the integrity of engineering design.

This endeavour has encompassed not only a *depth of research* into the various methods and techniques—ranging from quantitative probability theory and expert judgement in Bayesian analysis, to qualitative possibility theory, fuzzy logic and uncertainty in Markov analysis, and from reliability block diagrams, fault trees, event trees and cause-consequence diagrams, to Petri nets, genetic algorithms and artificial neural networks—but also a *breadth of research* into the concept of integrity

in engineering design. Such breadth is represented by the topics of reliability and performance, availability and maintainability, and safety and risk, in an overall concept of *designing for integrity* during the engineering design process. These topics cover the integrity of engineering design not only for complex industrial processes and engineered installations but also for a wide range of engineering systems, from mobile to installed equipment.

This handbook is therefore written in the best way possible to appeal to:

1. Engineering design lecturers, for a comprehensive coverage of the subject theory and application examples, sufficient for addition to university graduate and postgraduate award courses.
2. Design engineering students, for sufficient theoretical coverage of the different topics with insightful examples and exercises.
3. Postgraduate research candidates, for use of the handbook as overall guidance and reference to other material.
4. Practicing engineers who want an easy readable reference to both theoretical and practical applications of the various topics.
5. Corporate organisations and companies (manufacturing, mining, engineering and process industries) requiring standard approaches to be understood and adopted throughout by their technical staff.
6. Design engineers, design organisations and consultant groups who require a 'best practice' handbook on the integrity of engineering design practice.

The topics covered in this handbook have proven to be much more of a research challenge than initially expected. The concept of design is both complex and complicated—even more so with engineering design, especially the design of engineering systems and processes that encompass all of the engineering disciplines. The challenge has been further compounded by focusing on applied and current methodology for determining the *integrity* of engineering design. Acknowledgement is thus gratefully given to those numerous authors whose techniques are presented in this handbook and also to those academics whose theoretical insight and critique made this handbook possible. The proof of the challenge, however, was not only to find solutions to the integrity problem in engineering design but also to be able to deliver some means of implementing these solutions in a practical computational format. This demanded an in-depth application of very many subjects ranging from mathematical and statistical modelling to symbolic and computational modelling, resulting in the need for research beyond the basic engineering sciences. Additionally, the solution models had to be tested in those very same engineering environments in which design integrity problems were highlighted. No one looks kindly upon criticism, especially with regard to allegations of shortcomings in their profession, where a high level of resistance to change is inevitable in respect of implementing new design tools such as AI-based blackboard models incorporating collaborative expert systems. Acknowledgement is therefore also gratefully given to those captains of industry who allowed this research to be

conducted in their companies, including all those design engineers who offered so much of their valuable time. Last but by no means least was the support and encouragement from my wife and family over the many years during which the topics in this handbook were researched and accumulated from a lifetime career in consulting engineering.

Rudolph Frederick Stapelberg

http://www.springer.com/978-1-84800-174-9

Handbook of Reliability, Availability, Maintainability and Safety in Engineering Design

Stapelberg, R.F.

2009, XXIV, 827 p. 281 illus., Hardcover
ISBN: 978-1-84800-174-9