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

Rudolph Frederick Stapelberg

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

Springer

Rudolph Frederick Stapelberg, BScEng, MBA, PhD, DBA, PrEng
Adjunct Professor
Centre for Infrastructure and Engineering Management
Griffith University
Gold Coast Campus
Queensland
Australia

ISBN 978-1-84800-174-9 e-ISBN 978-1-84800-175-6

DOI 10.1007/978-1-84800-175-6

British Library Cataloguing in Publication Data
Stapelberg, Rudolph Frederick
Handbook of reliability, availability, maintainability and
safety in engineering design
1. Reliability (Engineering) 2. Maintainability
(Engineering) 3. Industrial safety
I. Title
620'.0045
ISBN-13: 9781848001749

Library of Congress Control Number: 2009921445

Cover design: eStudio Calamar S.L., Girona, Spain

Printed on acid-free paper

9 8 7 6 5 4 3 2 1

springer.com

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

Contents

List of Figures

List of Tables

Part I
Engineering Design Integrity Overview

Chapter 1
Design Integrity Methodology

Abstract In the design of critical combinations and complex integrations of large engineering systems, their *engineering integrity* needs to be determined. Engineering integrity includes *reliability*, *availability*, *maintainability* and *safety* of inherent systems functions and their related equipment. The *integrity of engineering design* therefore includes the *design criteria* of reliability, availability, maintainability and safety of systems and equipment. The overall combination of these four topics constitutes a methodology that ensures good engineering design with the desired engineering integrity. This methodology provides the means by which complex engineering designs can be properly analysed and reviewed, and is termed a RAMS analysis. The concept of RAMS analysis is not new and has been progressively developed, predominantly in the field of product assurance. Much consideration is being given to engineering design based on the theoretical expertise and practical experiences of chemical, civil, electrical, electronic, industrial, mechanical and process engineers, particularly from the point of view of '*what should be achieved*' to meet design criteria. Unfortunately, not enough consideration is being given to '*what should be assured*' in the event design criteria are not met. Most of the problems encountered in engineered installations stem from the lack of a proper evaluation of their *design integrity*. This chapter gives an overview of methodology for determining the integrity of engineering design to ensure that consideration is given to '*what should be assured*' through appropriate design review techniques. Such design review techniques have been developed into automated continual design reviews through intelligent computer automated methodology for determining the integrity of engineering design. This chapter thus also introduces the application of artificial intelligence (AI) in engineering design and gives an overview of artificial intelligence-based (AIB) modelling in designing for reliability, availability, maintainability and safety to provide a means for continual design reviews throughout the engineering design process. These models include a RAM analysis model, a dynamic systems simulation blackboard model, and an artificial intelligence-based (AIB) blackboard model.

R.F. Stapelberg, *Handbook of Reliability, Availability, Maintainability and Safety in Engineering Design*, © Springer 2009

1.1 Designing for Integrity

In the past two decades, industry, and particularly the process industry, has witnessed the development of large super-projects, most in excess of a billion dollars. Although these super-projects create many thousands of jobs resulting in significant decreases 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. Because of the *complexity of design* of these projects, and the fact that most of the problems encountered in the projects stem from a lack of proper evaluation of their *integrity of design*, it is expected that research in this field should arouse significant interest within most engineering-based industries in general. Most of the super-projects researched by the author 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. The poor performances of these projects are given in the following points that summarise the findings of this research:

- In all of the projects studied, additional funding had to be obtained for cost overruns and to cover shortfalls in working capital due to extended construction and commissioning periods. Final capital costs far exceeded initial feasibility estimates. Additional costs were incurred mainly for rectification of insufficiently designed system circuits and equipment, and increased engineering and maintenance costs. Actual construction completion schedule overruns averaged 6 months, and commissioning completion schedule overruns averaged 11 months. Actual start-up commenced $+1$ year after forecast with all the projects.
- Estimated cash operating costs were over-optimistic and, in some cases, no further cash operating costs were estimated due to project schedule overruns as well as over-extended ramp-up periods in attempts to obtain design forecast output.
- Technology and engineering problems were numerous in all the projects studied, especially in the various process areas, which indicated insufficient design and/or specifications to meet the inherent process problems of corrosion, scaling and erosion.
- Procurement and construction problems were experienced by all the projects studied, especially relating to the lack of design data sheets, incomplete equipment lists, inadequate process control and instrumentation, incorrect spare parts lists, lack of proper identification of spares and facilities equipment such as manual valves and piping both on design drawings and on site, and basic quality 'corner cutting' resulting from cost and project overruns. Actual project schedule overruns averaged $+1$ year after forecast.
- Pre-commissioning as well as commissioning schedules were over-optimistic in most cases where actual commissioning completion schedule overruns averaged 11 months. Inadequate references to equipment data sheets and design specifications resulted in it later becoming an exercise of identifying as-built equipment, rather than of confirming equipment installation with design specifications.

- The need to rectify processes and controls occurred in all the projects because of detrimental erosion and corrosion effects on all the equipment with design and specification inadequacies, resulting in cost and time overruns. Difficulties with start-ups after resulting forced stoppages, and poor systems performance with regard to availability and utilisation resulted in longer ramp-up periods and shortfalls of operating capital to ensure proper project handover.
- In all the projects studied, schedules were over-optimistic with less than optimum performance being able to be reached only much later than forecast. Production was much lower than envisaged, ranging from 10 to 60% of design capacity 12 months after the forecast date that design capacity would be reached. Problems with regard to achieving design throughput occurred in all the projects. This was due mainly to low plant utilisation because of poor process and equipment design reliability, and short operating periods.
- Project management and control problems relating to construction, commissioning, start-up and ramp-up were proliferate as a result of an inadequate assessment of design complexity and project volume with regard to the many integrated systems and equipment.

It is obvious from the previous points, made available in the public domain through published annual reports of real-world examples of recently constructed engineering projects, that most of the problems stem from a lack of proper evaluation of their *engineering integrity*. The important question to be considered therefore is:

What does integrity of engineering design actually imply?

Engineering Integrity

In determining the complexity and consequent frequent failure of the critical combination and complex integration of large engineering processes, both in technology as well as in the integration of systems, their *engineering integrity* needs to be determined. This engineering integrity includes *reliability*, *availability*, *maintainability* and *safety* of the inherent process systems functions and their related equipment. Integrity of *engineering design* therefore includes the *design criteria* of *reliability*, *availability*, *maintainability* and *safety* of these systems and equipment.

Reliability can be regarded as the probability of successful operation or *performance* of systems and their related equipment, with minimum risk of loss or disaster or of *system failure*. Designing for reliability requires an evaluation of the *effects of failure* of the inherent systems and equipment.

Availability is that aspect of system reliability that takes equipment *maintainability* into account. Designing for availability requires an evaluation of the *consequences of unsuccessful operation or performance* of the integrated systems, and the critical requirements necessary to restore operation or performance to design expectations.

Maintainability is that aspect of maintenance that takes *downtime* of the systems into account. Designing for maintainability requires an evaluation of the *accessi-*

bility and '*repairability*' of the inherent systems and their related equipment in the event of failure, as well as of integrated systems shutdown during planned maintenance.

Safety can be classified into three categories, one relating to *personal protection*, another relating to *equipment protection*, and yet another relating to *environmental protection*. Safety in this context may be defined as "not involving risk", where risk is defined as "the chance of loss or disaster". Designing for safety is inherent in the development of designing for reliability and maintainability of systems and their related equipment. *Environmental protection* in engineering design, particularly in industrial process design, relates to the prevention of failure of the inherent process systems resulting in environmental problems associated predominantly with the treatment of wastes and emissions from chemical processing operations, high-temperature processes, hydrometallurgical and mineral processes, and processing operations from which by-products are treated.

The overall combination of these four topics constitutes a methodology that ensures good engineering design with the desired engineering integrity. This methodology provides the means by which complex engineering designs can be properly analysed and reviewed. Such an analysis and review is conducted not only with a focus upon individual inherent systems but also with a perspective of the critical combination and complex integration of all the systems and related equipment, in order to achieve the required reliability, availability, maintainability and safety (i.e. integrity).

This analysis is often termed a *RAMS analysis*. The concept of RAMS analysis is not new and has been progressively developed over the past two decades, predominantly in the field of *product assurance*. Those industries applying product assurance methods have unquestionably witnessed astounding revolutions of knowledge and techniques to match the equally astounding progress in technology, particularly in the electronic, micro-electronic and computer industries. Many technologies have already originated, attained peak development, and even become obsolete within the past two decades. In fact, most systems of products built today will be long since obsolete by the time they wear out. So, too, must the development of ideas, knowledge and techniques to adequately manage the application and maintenance of newly developed systems be compatible *and* adaptable, or similarly become obsolete and fall into disuse. This applies to the concept of engineering integrity, particularly to the integrity of engineering design.

Engineering knowledge and techniques in the design and development of complex systems either must become part of a new information revolution in which compatible and, in many cases, more stringent methods of design reviews and evaluations are adopted, especially in the application of *intelligent computer automated methodology*, or must be relegated to the archives of obsolete practices.

However, the phenomenal progress in technology over the past few decades has also confused the language of the engineering profession and, between engineering disciplines, engineers still have trouble *speaking the same language*, especially with regard to understanding the intricacies of concepts such as *integrity*, *reliability*,

availability, *maintainability* and *safety* not only of components, assemblies, subsystems or systems but also of their integration into larger complex installations.

Some of the more significant contributors to cost 'blow-outs' experienced by most engineering projects can be attributed to the complexity of their engineering design, both in technology and in the complex integration of their systems, as well as a lack of meticulous engineering design project management. The individual process systems on their own are adequately designed and constructed, often on the basis of previous similar, although smaller designs.

> *It is the critical combination and complex integration of many such process systems that gives rise to design complexity and consequent frequent failure, where high risks of the integrity of engineering design are encountered.*

Research by the author into this problem has indicated that large, expensive engineering projects may often have superficial *design reviews*. As an essential control activity of engineering design, design review practices can take many forms. At the lowest level, they consist of an examination of engineering drawings and specifications before construction begins. At the highest level, they consist of comprehensive *due diligence* evaluations. Comprehensive 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, a predefined and structured basis of measure is rarely used against which the design, or design alternatives, should be reviewed.*

This situation inevitably prompts the question *how can the integrity of design be determined prior to any data being accumulated on the results of the operation and performance of the design*? In fact, how can the reliability of engineering plant and equipment be determined prior to the accumulation of any statistically meaningful failure data of the plant and its equipment? To further complicate matters, *how will plant and equipment perform in large integrated systems, even if nominal reliability values of individual items of equipment are known*? This is the dilemma that most design engineers are confronted with. 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).

This is evident by scrutiny of a typical Design Engineer's Definitive Scope of Work given in Appendix A. Despite the vast amount of research already conducted in the field of reliability analysis, many of these techniques seem to be 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. Verification of this statement is given in the extract below in which comment is delivered in part on an evaluation of the intended application of *HazOp* studies in conducting a preliminary design review for a recent laterite–nickel process design.

The engineer's definitive scope of work for a project includes the need for conducting preliminary design HazOp reviews as part of design verification. Reference to determining equipment criticality for mechanical engineering as well as for electrical engineering input can be achieved only through the establishment of failure modes and effects analysis (FMEA). There are, however, some concerns with the approach, as indicated in the following points.

Comment on intended HazOp studies for use in preliminary design reviews of a new engineering project:

- In HazOp studies, the differentiation between analyses at higher and at lower systems levels in assessing either hazardous operational failure consequences or system failure effects is extremely important from the point of view of determining *process criticality*, or of determining *equipment criticality*.
- The determination of *process criticality* can be seen as a preliminary HazOp, or a higher systems-level determination of process *failure consequences*, based upon *process function definition* in relation to the classical HazOp 'guide words', and obtained off the *schematic design* process flow diagrams (PFDs).
- The determination of *equipment criticality* can be seen as a detailed HazOp (or HazAn), or determination of system *failure effects*, which is based upon *equipment function definition*.
- The extent of analysis is very different between a preliminary HazOp and a detailed HazOp (or HazAn). Both are, however, essential for the determination of integrity of design, the one at a higher process level, and the other at a lower equipment level.
- A preliminary HazOp study is essential for the determination of integrity of design at process level, and should include *process reliability* that can be quantified from *process design criteria*.
- *The engineer's definitive scope of work for the project does not include a determination of process reliability, although process reliability can be quantified from process design criteria.*
- A detailed HazOp (or HazAn) is essential for the determination of integrity of design at a lower equipment level, and should include estimations of critical *equipment reliability* that can be quantified from *equipment design criteria*.
- *The engineer's definitive scope of work does not include a determination of equipment reliability, although equipment reliability is quantified from detail equipment design criteria.*
- Failure modes and effects analysis (FMEA) is dependent upon equipment function definition at assembly and component level in the systems breakdown structure (SBS), which is considered in equipment specification development during *schematic* and *detail design*. Furthermore, FMEA is strictly dependent upon a correctly structured SBS at the lower systems levels, usually obtained off the *detail design* pipe and instrument drawings (P&IDs).

It is obvious from the above comments that a severe lack of insight exists in the essential activities required to establish a proper evaluation of the *integrity* of engineering design, with the consequence that many 'good intentions' inevitably result

in superficial design reviews, especially with large, complex and expensive process designs.

Based on hands-on experience, as well as in-depth analysis of the potential causes of the cost 'blow-outs' of several super-projects, an inevitable conclusion can be derived that insufficient research has been conducted in determining the integrity of process engineering design, as well as in design review techniques. Much consideration is being given to engineering design based on the theoretical expertise and practical experience of process, chemical, civil, mechanical, electrical, electronic and industrial engineers, particularly 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. Thus, many high-cost super-projects eventually reach the construction phase without having been subjected to a rigorous evaluation of the integrity of their designs.

The contention that not enough consideration is being given in engineering design, as well as in design review techniques, to '*what should be assured*' in the event of design criteria not being met has therefore initiated the research presented in this handbook into a methodology for determining the integrity of engineering design. This is especially of concern with respect to the critical combinations and complex integrations of large engineering systems and their related equipment. Furthermore, an essential need has been identified in most engineering-based industries for a practical intelligent computer automated methodology to be applied in engineering design reviews as a structured basis of measure in determining the integrity of engineering design to achieve the required reliability, availability, maintainability and safety.

The objectives of this handbook are thus to:

1. Present concise theoretical formulation of conceptual and mathematical models of engineering design integrity in design synthesis, which includes design for reliability, availability, maintainability and safety during the conceptual, schematic or preliminary, and detail design phases.
2. Consider critical development criteria for intelligent computer automated methodology whereby the conceptual and mathematical models can be used practically in the mining, process and construction industries, as well as in most other engineering-based industries, to establish a structured basis of measure in determining the integrity of engineering design.

Several target platforms for evaluating and optimising the practical contribution of research in the field of engineering design integrity that is addressed in this handbook are focused on the design of large industrial processes that consist of many systems that give rise to design complexity and consequent high risk of design integrity. These industrial process engineering design 'super-projects' are insightful in that they incorporate almost all the different basic engineering disciplines, from chemical, civil, electrical, industrial, instrumentation and mechanical to process engineering. Furthermore, the increasing worldwide activity in the mining, process and construction industries makes such research and development very timely. The

following models have been developed, each for a specific purpose and with specific expected results, either to validate the developed theory on engineering design integrity or to evaluate and verify the design integrity of critical combinations and complex integrations of systems and equipment.

RAMS analysis modelling This was applied to validate the developed theory on the determination of the integrity of engineering design. This computer model was applied to a recently constructed engineering design of an environmental plant for the recovery of sulphur dioxide emissions from a nickel smelter to produce sulphuric acid.

Eighteen months after the plant was commissioned and placed into operation, failure data were obtained from the plant's distributed control system (DCS), and analysed with a view to matching the developed theory with real operational data after plant start-up. The comparative analysis included determination of systems and equipment criticality and reliability.

Dynamic systems simulation modelling This was applied with individually developed process equipment models (PEMs) based on *Petri net* constructs, to initially determine mass-flow balances for preliminary engineering designs of large integrated process systems. The models were used to evaluate and verify the process design integrity of critical combinations and complex integrations of systems and related equipment, for schematic and detail engineering designs. The process equipment models have been verified for correctness, and the relevant results validated, by applying the PEMs in a large dynamic simulation of a complex integration of systems.

Simulation modelling for design verification is common to most engineering designs, particularly in the application of simulating outcomes during the preliminary design phase. Dynamic simulation models are also used for design verification during the detail design phase but not to the extent of determining outcomes, as the level of complexity of the simulation models (and, therefore, the extent of data analysis of the simulation results) varies in accordance with the level of detail of the design.

At the higher systems level, typical of preliminary designs, dynamic simulation of the behaviour of exogenous, endogenous and status variables is both feasible and applicable. However, at the lower, more detailed equipment level, typical of detail designs, dynamic continuous and/or discrete event simulation is applicable, together with the appropriate verification and validation analysis of results, their sensitivity to changes in primary or base variables, and the essential need for adequate simulation run periods determined from statistical experimental design. Simulation analysis should not be based on model development time.

Mathematical modelling Modelling in the form of developed optimisation algorithms (OAs) of process design integrity was applied in predicting, assessing and evaluating reliability, availability, maintainability and safety requirements for the complex integration of process systems. These models were programmed into the PEM's script so that each individual process equipment model inherently has the facility for simplified data input, and the ability to determine its design integrity with