Chapter 2
Design Integrity and Automation

Abstract The overall combination of the topics of reliability and performance, availability and maintainability, and safety and risk in engineering design constitutes a methodology that 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 on individual inherent systems but also with a perspective of the critical combination and complex integration of all of the design's systems and related equipment, in order to achieve the required *design integrity*. A basic and fundamental understanding of the concepts of reliability, availability and maintainability and, to a large extent, an empirical understanding of safety have in the main dealt with statistical techniques for the measure and/or estimation of various parameters related to each of these concepts that are *based on obtained data*. However, in *designing* for reliability, availability, maintainability and safety, it is more often the case that the measures and/or estimations of various parameters related to each of these concepts are *not based on obtained data*. Furthermore, the complexity arising from an integration of engineering systems and their interactions makes it somewhat impossible to gather meaningful statistical data that could allow for the use of objective probabilities in the analysis of the integrity of engineering design. Other acceptable methods must therefore be sought to determine the integrity of engineering design in the situation where data are not available or not meaningful. Methodology in which the technical uncertainty of inadequately defined design problems may be formulated in order to achieve maximum design integrity has thus been developed to accommodate its use in conceptual and preliminary engineering design in which most of the design's systems and components have not yet been precisely defined. This chapter gives an overview of *design automation* methodology in which the technical uncertainty of inadequately defined design problems may be formulated through the application of intelligent design systems that can be used in creating or altering conceptual and preliminary engineering designs in which most of the design's systems and components still need to be defined, as well as *evaluate a design* through the use of evaluation design automation (EDA) tools.

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

2.1 Industry Perception and Related Research

It is obvious that most of the problems of recently constructed super-projects stem from the lack of a proper evaluation of the *integrity* of their design. Furthermore, it is obvious 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 engineering design projects are subject to relatively superficial design reviews, especially with large, complex and expensive process plants.

Based on the results of cost 'blow-outs' of these super-projects, the conclusion reached is that insufficient research has been conducted in the determination of the integrity of engineering design, its application in design procedure, as well as in the severe shortcomings of current design review techniques.

2.1.1 Industry Perception

It remains a fact that, in most engineering design organisations, the designs of large engineering projects are based upon the theoretical expertise and practical experiences pertaining to chemical, civil, electrical, industrial, mechanical and process engineering, from the point of view of '*what should be achieved*' to meet the demands of various design criteria. It is apparent, though, that not enough consideration is being given to the point of view of '*what should be assured*' in the event that the demands of design criteria are not met.

As previously indicated, the tools that most design engineers resort to in determining integrity of design are techniques such as *hazardous operations (HazOp)* and *simulation*, whereas less frequently used techniques include *hazards analysis (HazAn)*, *fault-tree analysis (FTA)*, *failure modes and effects analysis (FMEA)* and *failure modes effects and criticality analysis (FMECA)*.

It unfortunately also remains a fact that most of these techniques are either misunderstood or conducted incorrectly, or not even conducted at all, with the result that many high-cost engineering 'super-projects' eventually reach the construction phase without having been subjected to a rigorous evaluation of the integrity of their designs. One of the outcomes of the research presented in this handbook has been the development of an *artificial intelligence-based (AIB)* model in which *AI* modelling techniques, such as the inclusion of *knowledge-based expert systems* within a *blackboard model*, have been applied in the development of intelligent computer automated methodology for determining the integrity of engineering design. The model fundamentally provides a capability for *automated continual design reviews* throughout the engineering design process, whereby groups of design engineers collaboratively input specific design data and schematics into their relevant knowledge-based expert systems, which are then concurrently evaluated for integrity of the design. The overall perception in industry of the benefits of such a methodology is still in its infant stages, particularly the concept of having a diverse team of experts or multidisciplinary groups of design engineers available at all stages of a design,

as represented by their knowledge-based expert systems. The potential savings in avoiding cost 'blow-outs' during engineering project construction are still not properly appreciated, and the practical implementation of a collaborative *AIB blackboard model* from conceptual design through to construction still needs further evaluation.

2.1.2 Related Research

As indicated previously, many of the methods and techniques applied in the fields of reliability, availability, maintainability and safety have been thoroughly explored by many other researchers. Some of the more significant findings of these researchers are grouped into the various topics of 'reliability and performance', 'availability and maintainability', and 'safety and risk' that are included in the theoretical overview and analytic development chapters in this handbook. Further research in the application of artificial intelligence in engineering design can be found in the comprehensive three-volume set of multidisciplinary research papers on 'Design representation and models of routine design'; 'Models of innovative design, reasoning about physical systems, and reasoning about geometry'; and 'Knowledge acquisition, commercial systems, and integrated environments' (Tong and Sriram 1992).

Research in the application of artificial intelligence in engineering design has also been conducted by authorities such as the US Department of Defence (DoD), the US National Aeronautics and Space Administration (NASA) and the US Nuclear Regulatory Commission (NUREG).

Under the topics of *reliability and performance*, some of the more recent researchers whose works are closely related to the integrity of engineering design, particularly *designing for reliability*, covered in this handbook are S.M. Batill, J.E. Renaud and Xiaoyu Gu in their simulation modelling of uncertainty in multidisciplinary design optimisation (Batill et al. 2000); B.S. Dhillon in his fundamental research into reliability engineering in systems design and design reliability (Dhillon 1999a); G. Thompson, J.S. Liu et al. in their practical methodology to designing for reliability (Thompson et al. 1999); W. Kerscher, J. Booker et al. in their use of fuzzy control methods in information integration technology (IIT) for process design (Kerscher et al. 1998); J.S. Liu and G. Thompson again, in their approach to multi-factor design evaluation through parameter profile analysis (Liu and Thompson 1996); D.D. Boettner and A.C. Ward in their use of artificial intelligence (AI) in engineering design and the application of labelled interval calculus in multi-factor design evaluation (Boettner and Ward 1992); and N.R. Ortiz, T.A. Wheeler et al. in their use of expert judgment in nuclear engineering process design (Ortiz et al. 1991). Note that all these data sources are included in the References list of Chapter 3.

Under the topics of *availability and maintainability*, some of the researchers whose works are related to the integrity of engineering design, particularly *designing for availability* and *designing for maintainability*, covered in this handbook are V. Tang and V. Salminen in their unique theory of complicatedness as a framework

for complex systems analysis and engineering design (Tang and Salminen 2001); X. Du and W. Chen in their extensive modelling of robustness in engineering design (Du and Chen 1999a); X. Du and W. Chen also consider a methodology for managing the effect of uncertainty in simulation-based design and simulation-based collaborative systems design (Du and Chen 1999b,c); N.P. Suh in his research into the theory of complexity and periodicity in design (Suh 1999); G. Thompson, J. Geominne and J.R. Williams in their method of plant design evaluation featuring maintainability and reliability (Thompson et al. 1998); A. Parkinson, C. Sorensen and N. Pourhassan in their approach to determining robust optimal engineering design (Parkinson et al. 1993); and J.L. Peterson in his research into Petri net (PN) theory and its specific application in the design of engineering systems (Peterson 1981). Note that all these data sources are included in the References list of Chapter 4.

Similarly, under the topics of *safety and risk*, some of the researchers whose works are also related to the integrity of engineering design and covered in this handbook are A. Blandford, B. Butterworth et al. in their modelling applications incorporating human safety factors into the design of complex engineering systems (Blandford et al. 1999); R.L. Pattison and J.D. Andrews in their use of genetic algorithms in safety systems design (Pattison and Andrews 1999); D. Cvetkovic and I.C. Parmee in their multi-objective optimisation of preliminary and evolutionary design (Cvetkovic and Parmee 1998); M. Tang in his knowledge-based architecture for intelligent design support (Tang 1997); J.D. Andrews in his determination of optimal safety system design using fault-tree analysis (Andrews 1994); D.W. Coit and A.E. Smith for their research into the use of genetic algorithms for optimising combinatorial design problems (Coit and Smith 1994); H. Zarefar and J.R. Goulding in their research into neural networks for intelligent design (Zarefar and Goulding 1992); S. Ben Brahim and A. Smith in their estimation of engineering design performance using neural networks (Ben Brahim and Smith 1992), as well as G. Chryssolouris and M. Lee in their use of neural networks for systems design (Chryssolouris and Lee 1989), and J.W. McManus of NASA Langley Research Center in his pioneering work on the analysis of concurrent blackboard systems (McManus 1991). Note that all these data sources are included in the References list of Chapter 5.

Recently published material incorporating integrity in engineering design are few and either focus on a single topic, predominantly reliability, safety and risk, or are intended for specific engineering disciplines, especially electrical and/or electronic engineering. Some of the more recent publications on the application of reliability, maintainability, safety and risk in industry, rather than in engineering design include N.W. Sachs' 'Practical plant failure analysis: a guide to understanding machinery deterioration and improving equipment reliability' (Sachs 2006), which explains how and why machinery fails and how basic failure mechanisms occur; D.J. Smith's 'Reliability, maintainability and risk: practical methods for engineers' (Smith 2005), which considers the integrity of safety-related systems as well as the latest approaches to reliability modelling; and P.D.T. O'Connor's 'Practical reliability engineering' (O'Connor 2002), which gives a comprehensive, up-to-date description of all the important methods for the design, development, manufacture

and maintenance of engineering products and systems. Recent publications relating specifically to design integrity include E. Nikolaidis' 'Engineering design reliability handbook' (Nikolaidis et al. 2005), which considers reliability-based design and modelling of uncertainty when data are limited.

2.2 Intelligent Design Systems

Methodology in which the technical uncertainty of inadequately defined design problems may be formulated in order to achieve maximum design integrity has been developed in this research to accommodate its use in conceptual and preliminary engineering design in which most of the design's systems and components have not yet been precisely defined. Furthermore, intelligent computer automated methodology has been developed through artificial intelligence-based (AIB) modelling to provide a means for continual design reviews throughout the engineering design process. This is progressively becoming acknowledged as a necessity, not only for use in future large process super-projects but for engineering design projects in general, particularly construction projects that incorporate various engineering disciplines dealing with, e.g. high-rise buildings and complex infrastructure projects.

2.2.1 The Future of Intelligent Design Systems

Starting from current methods in the engineering design process, and projecting our vision further to new methodologies such as AIB modelling to provide a means for continual design reviews throughout the engineering design process, it becomes apparent that there can and should be a rapid evolution of the application of intelligent computer automated methodology to future engineering designs. Currently, three generations of design tools and approaches can be enumerated: The first generation is what we currently have—a variety of tools for representing designs and design information, in many cases not integrated nor well catalogued, with the following features:

- Information flows consume much time of personnel involved.
- Engineers spend much of their time on managerial, rather than technical tasks.
- Constraints from downstream are rarely considered.

Widespread use of knowledge-based systems will rapidly be adopted, marking a second generation in which techniques become available that allow first-generation tools to be integrated, networked and coordinated.

Most companies are already fully networked and integrated. The following projections can be made for this second generation of knowledge-based systems and tools:

- Knowledge-based tools are developed to complement and replace first-generation *shells*. These are targeted for *design assistance*, rather than for general design applications, especially tools for design evaluation, selection and review problems that can be enhanced and expanded for a wide range of different engineering applications.
- Various design strategies are built into *expert system shells*, so that knowledge from new areas of engineering design can be utilised appropriately.

Projecting even further, the third generation will arise as there is widespread automation of the application of knowledge-based tools such as *design automation*, which will require advances in the application of machine learning and knowledge acquisition techniques, and the automation of new innovations in design verification and validation such as *evaluation design automation*.

The third generation will also have automated the process of applying these tools in design organisations. With each generation, the key aspects of the previous generations become ever more widespread as technology moves out of the research and development phase and into commercial products and tools.

The above projections and trends are expected in the following areas:

- Degree of integration and networking of intelligent design tools;
- Degree of automation of the application of design tool technology;
- Sophistication of general-purpose tools (shells);
- Degree of usage in engineering design organisations;
- Degree of understanding of the design process of complex systems.

2.2.2 Design Automation and Evaluation Design Automation

Research work on *design automation (DA)* has concentrated on programs that play an active role in the design process, in that they actually create or alter the design. A design automation environment typically contains a design representation or design database through which the design is controlled. Such a design automation environment usually interacts with a predetermined set of resident *computer-aided design (CAD)* tools, and will attempt to act as a manager of the *CAD* tools by handling input/output requirements and possibly automatically sequencing these *CAD* tools. Furthermore, it provides a design platform acting as a framework that, in effect, shields the designer from cumbersome details and allows for design work at a high level of abstraction during the earlier phases of the engineering design process (Schwarz et al. 2001).

Evaluation design automation (EDA) tools, on the other hand, are passive in that they *evaluate a design* in order to determine how well it performs. Evaluation design automation uses a '*frame-based*' knowledge representation to store and process expert knowledge. Frames provide a means of grouping packages of knowledge that are related to each other in some manner, where each knowledge package may have widely differing representations. The packages of knowledge are referred to

as '*slots*' in the frame. The various slots could contain knowledge such as symbolic data indicating performance values, heuristic rules indicating likely failure modes, or procedures for design review routines. The knowledge contained in these slots can be grouped according to a systems hierarchy, and the frames as such can be grouped to form a hierarchy of contexts.

Another important aspect to *EDA* is *constraint propagation*, for it is through constraint propagation that design criteria are aligned with implementation constraints. Usually, constraint propagation is achievable through *data-directed invocation*. Data-directed invocation is the mechanism that allows the design to incrementally progress as the objectives and needs of the design become apparent. In this fashion, the design constraints will change and propagate with each modification to the partial design. This is important, since the design requirements typically cannot be determined a priori (Lee et al. 1993).

The construct of Chapters 3, 4 and 5 in Part II is based upon the prediction, assessment and evaluation of reliability, availability, maintainability and safety, according to the particular engineering design phases of conceptual design, preliminary design and detail design respectively. Besides an initial introduction into engineering design integrity, the chapters are further subdivided into the related topics of theory, analysis and practical application of each of these concepts. Thus, Chapters 3, 4 and 5 include a *theoretical overview*, which gives a certain *breadth* of research into the theory covering each concept in engineering design; an insight into *analytic development*, which gives a certain *depth* of research into up-to-date analytical techniques and methods that have been developed and are currently being developed for analysis of each concept in engineering design; and an exposition of *application modelling*, whereby specific computational models have been developed and applied to the different concepts, particularly *AIB modelling* in which *expert systems* within a networked *blackboard model* are applied to determine engineering design integrity.

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