

**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

© 2009 Springer-Verlag London Limited

Apart from any fair dealing for the purposes of research or private study, or criticism or review, as permitted under the Copyright, Designs and Patents Act 1988, this publication may only be reproduced, stored or transmitted, in any form or by any means, with the prior permission in writing of the publishers, or in the case of reprographic reproduction in accordance with the terms of licences issued by the Copyright Licensing Agency. Enquiries concerning reproduction outside those terms should be sent to the publishers.

The use of registered names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant laws and regulations and therefore free for general use.

The publisher makes no representation, express or implied, with regard to the accuracy of the information contained in this book and cannot accept any legal responsibility or liability for any errors or omissions that may be made.

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

Part I Engineering Design Integrity Overview

1	Design Integrity Methodology	3
1.1	Designing for Integrity	4
1.1.1	Development and Scope of Design Integrity Theory	12
1.1.2	Designing for Reliability, Availability, Maintainability and Safety	14
1.2	Artificial Intelligence in Design	21
1.2.1	Development of Models and AIB Methodology	22
1.2.2	Artificial Intelligence in Engineering Design	25
2	Design Integrity and Automation	33
2.1	Industry Perception and Related Research	34
2.1.1	Industry Perception	34
2.1.2	Related Research	35
2.2	Intelligent Design Systems	37
2.2.1	The Future of Intelligent Design Systems	37
2.2.2	Design Automation and Evaluation Design Automation	38

Part II Engineering Design Integrity Application

3	Reliability and Performance in Engineering Design	43
3.1	Introduction	43
3.2	Theoretical Overview of Reliability and Performance in Engineering Design	45
3.2.1	Theoretical Overview of Reliability and Performance Prediction in Conceptual Design	60
3.2.2	Theoretical Overview of Reliability Assessment in Preliminary Design	72
3.2.3	Theoretical Overview of Reliability Evaluation in Detail Design	90

3.3	Analytic Development of Reliability and Performance in Engineering Design	107
3.3.1	Analytic Development of Reliability and Performance Prediction in Conceptual Design	107
3.3.2	Analytic Development of Reliability Assessment in Preliminary Design	133
3.3.3	Analytic Development of Reliability Evaluation in Detail Design	190
3.4	Application Modelling of Reliability and Performance in Engineering Design	241
3.4.1	The RAMS Analysis Application Model	242
3.4.2	Evaluation of Modelling Results	271
3.4.3	Application Modelling Outcome	285
3.5	Review Exercises and References	288
4	Availability and Maintainability in Engineering Design	295
4.1	Introduction	296
4.2	Theoretical Overview of Availability and Maintainability in Engineering Design	302
4.2.1	Theoretical Overview of Availability and Maintainability Prediction in Conceptual Design	308
4.2.2	Theoretical Overview of Availability and Maintainability Assessment in Preliminary Design	349
4.2.3	Theoretical Overview of Availability and Maintainability Evaluation in Detail Design	385
4.3	Analytic Development of Availability and Maintainability in Engineering Design	415
4.3.1	Analytic Development of Availability and Maintainability Prediction in Conceptual Design	416
4.3.2	Analytic Development of Availability and Maintainability Assessment in Preliminary Design	436
4.3.3	Analytic Development of Availability and Maintainability Evaluation in Detail Design	456
4.4	Application Modelling of Availability and Maintainability in Engineering Design	486
4.4.1	Process Equipment Models (PEMs)	486
4.4.2	Evaluation of Modelling Results	500
4.4.3	Application Modelling Outcome	518
4.5	Review Exercises and References	520

5	Safety and Risk in Engineering Design	529
5.1	Introduction	530
5.2	Theoretical Overview of Safety and Risk in Engineering Design	537
5.2.1	Forward Search Techniques for Safety in Engineering Design	541
5.2.2	Theoretical Overview of Safety and Risk Prediction in Conceptual Design	588
5.2.3	Theoretical Overview of Safety and Risk Assessment in Preliminary Design	607
5.2.4	Theoretical Overview of Safety and Risk Evaluation in Detail Design	627
5.3	Analytic Development of Safety and Risk in Engineering Design	676
5.3.1	Analytic Development of Safety and Risk Prediction in Conceptual Design	678
5.3.2	Analytic Development of Safety and Risk Assessment in Preliminary Design	687
5.3.3	Analytic Development of Safety and Risk Evaluation in Detail Design	702
5.4	Application Modelling of Safety and Risk in Engineering Design	725
5.4.1	Artificial Intelligence-Based (AIB) Blackboard Model	726
5.4.2	Evaluation of Modelling Results	776
5.4.3	Application Modelling Outcome	790
5.5	Review Exercises and References	791
A	Design Engineer’s Scope of Work	799
B	Bibliography of Selected Literature	807
Index		811

List of Figures

1.1	Layout of the RAM analysis model	24
1.2	Layout of part of the OOP simulation model	25
1.3	Layout of the AIB blackboard model	26
3.1	Reliability block diagram of two components in series	48
3.2	Reliability of a high-speed self-lubricated reducer	49
3.3	Reliability block diagram of two components in parallel	50
3.4	Combination of series and parallel configuration	51
3.5	Reduction of combination system configuration	51
3.6	Power train system reliability of a haul truck (Komatsu Corp., Japan)	53
3.7	Power train system diagram of a haul truck	53
3.8	Reliability of groups of series components	55
3.9	Example of two parallel components	56
3.10	Reliability of groups of parallel components	57
3.11	Slurry mill engineered installation	57
3.12	Total cost versus design reliability	61
3.13	Stress/strength diagram	66
3.14	Interaction of load and strength distributions (Carter 1986)	68
3.15	System transition diagram	74
3.16	Risk as a function of time and stress	77
3.17	Criticality matrix (Dhillon 1999)	83
3.18	Simple fault tree of cooling water system	87
3.19	Failure hazard curve (life characteristic curve or risk profile)	92
3.20	Shape of the Weibull density function, $F(t)$, for different values of β	100
3.21	The Weibull graph chart for different percentage values of the failure distribution	101
3.22	Parameter profile matrix	108
3.23	Determination of a data point: two limits	109
3.24	Determination of a data point: one upper limit	109
3.25	Determination of a data point: one lower limit	110
3.26	Two-variable parameter profile matrix	112

3.27	Possibility distribution of <i>young</i>	152
3.28	Possibility distribution of <i>somewhat young</i>	152
3.29	Values of linguistic variable <i>pressure</i>	160
3.30	Simple crisp inference	167
3.31	a Basic property $A' = A$. b Basic property $B' = B$	168
3.32	a, b Total indeterminance	169
3.33	a, b Subset property	169
3.34	Effects of λ on the probability density function	199
3.35	Effects of λ on the reliability function	199
3.36	Example exponential probability graph	203
3.37	Weibull p.d.f. with $0 < \beta < 1$, $\beta = 1$, $\beta > 1$ and a fixed μ (ReliaSoft Corp.)	205
3.38	Weibull c.d.f. or unreliability vs. time (ReliaSoft Corp.)	206
3.39	Weibull 1–c.d.f. or reliability vs. time (ReliaSoft Corp.)	206
3.40	Weibull failure rate vs. time (ReliaSoft Corp.)	207
3.41	Weibull p.d.f. with $\mu = 50$, $\mu = 100$, $\mu = 200$ (ReliaSoft Corp.)	208
3.42	Plot of the Weibull density function, $F(t)$, for different values of β	210
3.43	Minimum life parameter and true MTBF	212
3.44	Revised Weibull chart	213
3.45	Theories for representing uncertainty distributions (Booker et al. 2000)	217
3.46	Methodology of combining available information	225
3.47	Baselines of an engineering design project	230
3.48	Tracking reliability uncertainty (Booker et al. 2000)	239
3.49	Component condition sets for membership functions	240
3.50	Performance-level sets for membership functions	240
3.51	Database structuring of SBS into dynasets	245
3.52	Initial structuring of plant/operation/section	247
3.53	Front-end selection of plant/operation/section: RAMS analysis model spreadsheet, process flow, and treeview	248
3.54	Global grid list (spreadsheet) of systems breakdown structuring	249
3.55	Graphics of selected section PFD	251
3.56	Graphics of selected section treeview (cascaded systems structure)	252
3.57	Development list options for selected PFD system	253
3.58	Overview of selected equipment specifications	254
3.59	Overview of the selected equipment technical data worksheet	255
3.60	Overview of the selected equipment technical specification document	256
3.61	Analysis of development tasks for the selected system	257
3.62	Analysis of selected systems functions	258
3.63	Functions analysis worksheet of selected component	259
3.64	Specifications of selected major development tasks	260
3.65	Specifications worksheet of selected equipment	261
3.66	Diagnostics of selected major development tasks	262
3.67	Hazards criticality analysis assembly condition	263

3.68	Hazards criticality analysis component condition	264
3.69	Hazards criticality analysis condition diagnostic worksheet	265
3.70	Hazards criticality analysis condition spreadsheet	266
3.71	Hazards criticality analysis criticality worksheet	267
3.72	Hazards criticality analysis criticality spreadsheet	268
3.73	Hazards criticality analysis strategy worksheet	269
3.74	Hazards criticality analysis strategy spreadsheet	270
3.75	Hazards criticality analysis costs worksheet	271
3.76	Hazards criticality analysis costs spreadsheet	272
3.77	Hazards criticality analysis logistics worksheet	273
3.78	Hazards criticality analysis logistics spreadsheet	274
3.79	Typical data accumulated by the installation's DCS	275
3.80	Design specification FMECA—drying tower	280
3.81	Design specification FMECA—hot gas feed	281
3.82	Design specification FMECA—reverse jet scrubber	282
3.83	Design specification FMECA—final absorption tower	283
3.84	Weibull distribution chart for failure data	285
3.85	Monte Carlo simulation spreadsheet results for a gamma distribution best fit of TBF data	287
4.1	Breakdown of total system's equipment time (DoD 3235.1-H 1982) where UP TIME = operable time, DOWN TIME = inoperable time, OT = operating time, ST = standby time, ALDT = administrative and logistics downtime, TPM = total preventive maintenance and TCM = total corrective maintenance . . .	297
4.2	Regression equation of predicted repair time in nomograph form . . .	308
4.3	Three-system parallel configuration system	311
4.4	Life-cycle costs structure	318
4.5	Cost minimisation curve for non-recurring and recurring LCC	321
4.6	Design effectiveness and life-cycle costs (Barringer 1998)	327
4.7	Markov model state space diagram	350
4.8	Multi-state system transition	352
4.9	Operational availability time-line model—generalised format (DoD 3235.1-H 1982)	389
4.10	Operational availability time-line model—recovery time format (DoD 3235.1-H 1982)	390
4.11	A comparison of downtime and repair time (Smith 1981)	404
4.12	Example of a simple power-generating plant	411
4.13	Parameter profile matrix	418
4.14	Simulation-based design model from two different disciplines (Du et al. 1999c)	430
4.15	Flowchart for the extreme condition approach for uncertainty analysis (Du et al. 1999c)	431
4.16	Flowchart of the Monte Carlo simulation procedure (Law et al. 1991)	433

4.17	Propagation and mitigation strategy of the effect of uncertainties (Parkinson et al. 1993)	436
4.18	Translation of a flowchart to a Petri net (Peterson 1981)	438
4.19	Typical graphical representation of a Petri net (Lindemann et al. 1999)	440
4.20	Illustrative example of an MSPN for a fault-tolerant process system (Ajmone Marsan et al. 1995)	444
4.21	MSPN for a process system based on a queuing client-server paradigm (Ajmone Marsan et al. 1995)	446
4.22	Extended reachability graph generated from the MSPN model (Ajmone Marsan et al. 1995)	446
4.23	Reduced reachability graph generated from the MSPN model	448
4.24	MRSPN model for availability with preventive maintenance (Bobbio et al. 1997)	453
4.25	MRSPN model results for availability with preventive maintenance	455
4.26	Models of closed and open systems	462
4.27	Coal gas production and clarifying plant schematic block diagram	464
4.28	a Series reliability block diagram. b Series reliability graph	467
4.29	a Parallel reliability block diagram. b Parallel reliability graph	467
4.30	Process flow block diagram	468
4.31	Availability block diagram (ABD)	469
4.32	Simple power plant schematic process flow diagram	469
4.33	Power plant process flow diagram systems cross connections	470
4.34	Power plant process flow diagram sub-system grouping	471
4.35	Simple power plant subgroup capacities	472
4.36	Process block diagram of a turbine/generator system	479
4.37	Availability block diagram of a turbine/generator system, where A = availability, MTBF = mean time between failure (h), MTTR = mean time to repair (h)	479
4.38	Example of defined computer automated complexity (Tang et al. 2001)	483
4.39	Logistic function of complexity vs. complicatedness (Tang et al. 2001)	484
4.40	Blackboard model and the process simulation model	488
4.41	Systems selection in the blackboard model	489
4.42	Design equipment list data in the blackboard model	490
4.43	Systems hierarchy in the blackboard model context	491
4.44	User interface in the blackboard model	492
4.45	Dynamic systems simulation in the blackboard model	493
4.46	General configuration of process simulation model	495
4.47	Composition of systems of process simulation model	496
4.48	PEM library and selection for simulation modelling	497
4.49	Running the simulation model	499
4.50	Simulation model output results	500
4.51	Process flow diagram for simulation model sector 1	504

4.52	Design details for simulation model sector 1: logical flow initiation	505
4.53	Design details for simulation model sector 1: logical flow storage PEMs	506
4.54	Design details for simulation model sector 1: output performance results	507
4.55	Simulation output for simulation model sector 1	508
4.56	Process flow diagram for simulation model sector 2	510
4.57	Design details for simulation model sector 2: holding tank process design specifications	511
4.58	Design details for simulation model sector 2: output performance results	512
4.59	Simulation output for simulation model sector 2	514
4.60	Process flow diagram for simulation model sector 3	517
4.61	Design details for simulation model sector 3: process design specifications	518
4.62	Design details for simulation model sector 3: output performance results	519
4.63	Simulation output for simulation model sector 3	520
5.1	Fault-tree analysis	542
5.2	Event tree	543
5.3	Cause-consequence diagram	544
5.4	Logic and event symbols used in FTA	546
5.5	Safety control of cooling water system	548
5.6	Outage cause investigation logic tree expanded to potential root cause areas	554
5.7	Root cause factors for the systems and equipment design area	554
5.8	Factor tree for origin of design criteria	555
5.9	Event tree for a dust explosion (IEC 60300-3-9)	558
5.10	Event tree branching for reactor safety study	562
5.11	Event tree with boundary conditions	563
5.12	Event tree with fault-tree linking	564
5.13	Function event tree for loss of coolant accident in nuclear reactor (NUREG 75/014 1975)	566
5.14	Example cause-consequence diagram	568
5.15	Structure of the cause-consequence diagram	569
5.16	Redundant decision box	570
5.17	Example fault tree indicating system failure causes	571
5.18	Cause-consequence diagram for a three-component system	572
5.19	Reduced cause-consequence diagram	573
5.20	BDD with variable ordering $A < B < C$	573
5.21	Example of part of a cooling water system	602
5.22	Fault tree of dormant failure of a high-integrity protection system (HIPS; Andrews 1994)	620

5.23	Schematic of a simplified high-pressure protection system	625
5.24	Typical logic event tree for nuclear reactor safety (NUREG-751014 1975)	630
5.25	Risk curves from nuclear safety study (NUREG 1150 1989) Appendix VI WASH 1400: c.d.f. for early fatalities	631
5.26	Simple RBD construction	636
5.27	Layout of a complex RBD (NASA 1359 1994)	637
5.28	Example RBD	638
5.29	RBD to fault tree transformation	639
5.30	Fault tree to RBD transformation	640
5.31	Cut sets and path sets from a complex RBD	641
5.32	Transform of an event tree into an RBD	641
5.33	Transform of an RBD to a fault tree	642
5.34	High-integrity protection system (HIPS)	644
5.35	Cause-consequence diagram for HIPS system (Ridley et al. 1996) . .	645
5.36	Combination fault trees for cause-consequence diagram	646
5.37	Modified cause-consequence diagram for HIPS system (Ridley et al. 1996)	647
5.38	Combination fault trees for modified cause-consequence diagram . .	648
5.39	Final cause-consequence diagram for HIPS system (Ridley et al. 1996)	649
5.40	Combination fault trees for the final cause-consequence diagram (Ridley et al. 1996)	650
5.41	a Kaplan–Meier survival curve for rotating equipment, b estimated hazard curve for rotating equipment	655
5.42	a Risk exposure pattern for rotating equipment, b risk-based maintenance patterns for rotating equipment	656
5.43	Typical cost optimisation curve	657
5.44	Probability distribution definition with @RISK (Palisade Corp., Newfield, NY)	675
5.45	Schema of a conceptual design space	679
5.46	Selecting design objects in the design knowledge base	682
5.47	Conceptual design solution of the layout of a gas cleaning plant . . .	683
5.48	Schematic design model of the layout of a gas cleaning plant	683
5.49	Detail design model of the scrubber in the layout of a gas cleaning plant	684
5.50	Fault-tree structure for safety valve selection (Pattison et al. 1999) . .	695
5.51	Binary decision diagram (BDD) for safety valve selection	696
5.52	High-integrity protection system (HIPS): example of BDD application	697
5.53	Schematic layout of a complex artificial neural network (Valluru 1995)	705
5.54	The building blocks of artificial neural networks, where σ is the non-linearity, x_i the output of unit i , x_j the input to unit j , and w_{ij} are the weights that connect unit i to unit j	705

5.55	Detailed view of a processing element (PE)	705
5.56	A fully connected ANN, and its weight matrix	706
5.57	Multi-layer perceptron structure	706
5.58	Weight matrix structure for the multi-layer perceptron	707
5.59	Basic structure of an artificial neural network	707
5.60	Input connections of the artificial perceptron (a_n, b_1)	708
5.61	The binary step-function threshold logic unit (TLU)	708
5.62	The non-binary sigmoid-function threshold logic unit (TLU)	709
5.63	Boolean-function input connections of the artificial perceptron (a_n, o_0)	710
5.64	Boolean-function pattern space and TLU of the artificial perceptron (a_n, o_0)	710
5.65	The gradient descent technique	711
5.66	Basic structure of an artificial neural network: back propagation	712
5.67	Graph of membership function transformation of a fuzzy ANN	714
5.68	A fuzzy artificial perceptron (AP)	715
5.69	Three-dimensional plots generated from a neural network model illustrating the relationship between speed, load, and wear rate (Fusaro 1998)	716
5.70	Comparison of actual data to those of an ANN model approximation (Fusaro 1998)	716
5.71	Example failure data using cusum analysis (Ilott et al. 1997)	718
5.72	Topology of the example ANN (Ilott et al. 1997)	719
5.73	a) An example fuzzy membership functions for pump motor current (Ilott et al. 1995), b) example fuzzy membership functions for pump pressure (Ilott et al. 1995)	720
5.74	Convergence rate of ANN iterations	721
5.75	Standard back-propagation ANN architecture (Schocken 1994)	723
5.76	Jump connection back-propagation ANN architecture (Schocken 1994)	723
5.77	Recurrent back-propagation with dampened feedback ANN architecture (Schocken 1994)	723
5.78	Ward back propagation ANN architecture (Schocken 1994)	724
5.79	Probabilistic (PNN) ANN architecture (Schocken 1994)	724
5.80	General regression (GRNN) ANN architecture (Schocken 1994)	724
5.81	Kohonen self-organising map ANN architecture (Schocken 1994) ..	724
5.82	AIB blackboard model for engineering design integrity (ICS 2003) .	728
5.83	AIB blackboard model with systems modelling option	729
5.84	Designing for safety using systems modelling: system and assembly selection	730
5.85	Designing for safety using systems modelling	731
5.86	Treeview of systems hierarchical structure	732
5.87	Technical data sheets for modelling safety	733
5.88	Monte Carlo simulation of RBD and FTA models	734
5.89	FTA modelling in designing for safety	736

5.90	Weibull cumulative failure probability graph of HIPS	737
5.91	Profile modelling in designing for safety	738
5.92	AIB blackboard model with system simulation option	739
5.93	PFD for simulation modelling	740
5.94	PEMs for simulation modelling	741
5.95	PEM simulation model performance variables for process information	742
5.96	PEM simulation model graphical display of process information	743
5.97	Petri net-based optimisation algorithms in system simulation	744
5.98	AIB blackboard model with CAD data browser option	745
5.99	Three-dimensional CAD integrated model for process information ..	746
5.100	CAD integrated models for process information	747
5.101	ANN computation option in the AIB blackboard	748
5.102	ANN NeuralExpert problem selection	749
5.103	ANN NeuralExpert example input data attributes	750
5.104	ANN NeuralExpert sampling and prediction	751
5.105	ANN NeuralExpert sampling and testing	752
5.106	ANN NeuralExpert genetic optimisation	753
5.107	ANN NeuralExpert network complexity	754
5.108	Expert systems functional overview in the AIB blackboard knowledge base	755
5.109	Determining the conditions of a process	756
5.110	Determining the failure effect on a process	757
5.111	Determining the risk of failure on a process	758
5.112	Determining the criticality of consequences of failure	759
5.113	Assessment of design problem decision logic	760
5.114	AIB blackboard knowledge-based expert systems	761
5.115	Knowledge base facts frame in the AIB blackboard	762
5.116	Knowledge base conditions frame slot	763
5.117	Knowledge base hierarchical data frame	764
5.118	The Expert System blackboard and goals	765
5.119	Expert System questions factor—temperature	766
5.120	Expert System multiple-choice question editor	767
5.121	Expert System branched decision tree	768
5.122	Expert System branched decision tree: nodes	769
5.123	Expert System rules of the knowledge base	770
5.124	Expert System rule editor	771
5.125	Testing and validating Expert System rules	772
5.126	Fuzzy logic for managing uncertain data	774
5.127	AIB blackboard model with plant analysis overview option	775
5.128	Automated continual design review: component SBS	776
5.129	Automated continual design review: component criticality	777

List of Tables

3.1	Reliability of a high-speed self-lubricated reducer	49
3.2	Power train system reliability of a haul truck	54
3.3	Component and assembly reliabilities and system reliability of slurry mill engineered installation	58
3.4	Failure detection ranking	81
3.5	Failure mode occurrence probability	81
3.6	Severity of the failure mode effect	82
3.7	Failure mode effect severity classifications	83
3.8	Qualitative failure probability levels	83
3.9	Failure effect probability guideline values	84
3.10	Labelled intervals for specific performance parameters	131
3.11	Parameter interval matrix	131
3.12	Fuzzy term <i>young</i>	151
3.13	Modifiers (hedges) and linguistic expressions	152
3.14	Truth table applied to propositions	163
3.15	Extract from FMECA worksheet of quantitative RAM analysis field study: RJS pump no. 1 assembly	181
3.16	Extract from FMECA worksheet of quantitative RAM analysis field study: motor RJS pump no. 1 component	183
3.17	Extract from FMECA worksheet of quantitative RAM analysis field study: MCC RJS pump no. 1 component	185
3.18	Extract from FMECA worksheet of quantitative RAM analysis field study: RJS pump no. 1 control valve component	186
3.19	Extract from FMECA worksheet of quantitative RAM analysis field study: RJS pump no. 1 instrument loop (pressure) assembly	187
3.20	Uncertainty in the FMECA of a critical control valve	188
3.21	Uncertainty in the FMECA of critical pressure instruments	189
3.22	Median rank table for failure test results	200
3.23	Median rank table for Bernard's approximation	202
3.24	Acid plant failure modes and effects analysis (ranking on criticality) .	276
3.25	Acid plant failure modes and effects criticality analysis	279

3.26	Acid plant failure data (repair time RT and time before failure TBF) ..	284
3.27	Total downtime of the environmental plant critical systems	286
3.28	Values of distribution models for time between failure	286
3.29	Values of distribution models for repair time	287
4.1	Double turbine/boiler generating plant state matrix	412
4.2	Double turbine/boiler generating plant partial state matrix	413
4.3	Distribution of the tokens in the reachable markings	447
4.4	Power plant partitioning into sub-system grouping	471
4.5	Process capacities per subgroup	473
4.6	Remaining capacity versus unavailable subgroups	474
4.7	Flow capacities and state definitions of unavailable subgroups	474
4.8	Flow capacities of unavailable sub-systems per sub-system group ...	475
4.9	Unavailable sub-systems and flow capacities per sub-system group ..	475
4.10	Unavailable sub-systems and flow capacities per sub-system group: final summary	475
4.11	Unavailable subgroups and flow capacities incidence matrix	477
4.12	Probability of incidence of unavailable systems and flow capacities ..	477
4.13	Sub-system/assembly integrity values of a turbine/generator system ..	480
4.14	Preliminary design data for simulation model sector 1	503
4.15	Comparative analysis of preliminary design data and simulation output data for simulation model sector 1	507
4.16	Acceptance criteria of simulation output data, with preliminary design data for simulation model sector 1	508
4.17	Preliminary design data for simulation model sector 2	509
4.18	Comparative analysis of preliminary design data and simulation output data for simulation model sector 2	513
4.19	Acceptance criteria of simulation output data, with preliminary design data for simulation model sector 2	515
4.20	Preliminary design data for simulation model sector 3	516
4.21	Comparative analysis of preliminary design data and simulation output data for simulation model sector 3	516
4.22	Acceptance criteria of simulation output data, with preliminary design data for simulation model sector 3	521
5.1	Hazard severity ranking (MIL-STD-882C 1993)	539
5.2	Sample HAZID worksheet	540
5.3	Categories of hazards relative to various classifications of failure ...	540
5.4	Cause-consequence diagram symbols and functions	569
5.5	Standard interpretations for process/chemical industry guidewords ...	578
5.6	Matrix of attributes and guideword interpretations for mechanical systems	579
5.7	Risk assessment scale	585
5.8	Initial failure rate estimates	586
5.9	Operational primary keywords	600

5.10	Operational secondary keywords: standard HazOp guidewords	601
5.11	Values of the Q-matrix	612
5.12	Upper levels of systems unreliability due to CCF	623
5.13	Analysis of valve data to determine CCF beta factor	626
5.14	Sub-system component reliability bands	638
5.15	Component functions for HIPS system	644
5.16	Typical FMECA for process criticality	658
5.17	FMECA with preventive maintenance activities	659
5.18	FMECA for cost criticality	663
5.19	FMECA for process and cost criticality	665
5.20	Risk assessment scale	667
5.21	Qualitative risk-based FMSE for process criticality, where (1)=likelihood of occurrence (%), (2)=severity of the consequence (rating), (3)=risk (probability×severity), (4)=failure rate (1/MTBF), (5)=criticality (risk×failure rate).	668
5.22	FMSE for process criticality using residual life	674
5.23	Fuzzy and induced preference predicates	680
5.24	Required design criteria and variables	697
5.25	GA design criteria and variables results	701
5.26	Boolean-function input values of the artificial perceptron (a_n, o_0)	710
5.27	Simple 2-out-of-4 vote arrangement truth table	735
5.28	The AIB blackboard data object construct	785
5.29	Computation of $\Gamma_{j,k}$ and $\theta_{j,k}$ for blackboard B1	787
5.30	Computation of non-zero $\Omega_{j,k}$, $\Sigma_{j,k}$ and $\Pi_{j,k}$ for blackboard B1	787
5.31	Computation of $\Gamma_{j,k}$ and $\theta_{j,k}$ for blackboard B2	789
5.32	Computation of non-zero $\Omega_{j,k}$, $\Sigma_{j,k}$ and $\Pi_{j,k}$ for blackboard B2	789

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.

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, sub-systems 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