STELLINGEN

behorende bij het proefschrift

DEVELOPMENTS IN THE USE OF FAILURE RATE DATA AND RELIABILITY PREDICTION METHODS FOR HARDWARE

David J Smith

Delft, 29 mei 2000

1. Het is noodzakelijk om tijdens de ontwerpfase door meting te verifiëren of aan de verwachte bedrijfszekerheid en veiligheid eisen wordt voldaan. Daarom zijn hiervoor geschikte modellering technieken nodig welke gebruik kunnen maken van beperkte storingsgegevens.

2. Er zijn veldgegevens over storingsgraad en storingsvormen vereist om de potentiële bedrijfszekerheid van het technisch systeem, of van de ontwerpalternatieven, voor specifieke storingsvormen te kunnen voorspellen. Daartoe dienen eenduidig gedefinieerde gegevenselementen te worden verzameld met behulp van computer ondersteunde onderhoudsinformatie systemen, om consistente gegevens te kunnen verschaffen.

3. Als gevolg van de talloze toepassingen van technische systemen en de onderscheiden wijze van vastlegging van gegevens, vertonen deze grote toleranties. Daarom dienen de resultaten van de toegepaste modellering technieken te worden uitgedrukt met betrouwbaarheidsintervallen.

4. Er staat veelal maar een beperkte hoeveelheid storingsgegevens ter beschikking, Daarom dient bij analyses gebruik te worden gemaakt van betrouwbaarheidsintervallen om realistische interpretaties te kunnen uitvoeren.

5. De huidige methoden voor modellering van de te voorspellen bedrijfszekerheid overschrijden vaak de nauwkeurigheid van de beschikbare data. Daarom wordt het gebruik van eenvoudige voorspellingsmethoden aanbevolen.

6. Als gevolg van verschillende afhankelijkheden bij storingen met een gemeenschappelijke oorzaak (Common Cause Failures CCF), domineren deze vaak de bedrijfsonzekerheid van systemen en beïnvloeden de voordelen van redundantie in negatieve zin.

7. Methoden voor het beoordelen van bedrijfszekerheid zullen voortdurend verder worden ontwikkeld onder invloed van toenemende complexiteit. Daarom dienen deze mede de menselijke en software factoren en de interactie daarvan met het technische systeem, mede te beschouwen.

8. Storingsregistratie en methoden voor modellering van de bedrijfszekerheid zijn toepasbaar daar waar gevolgen van storingen kunnen worden waargenomen en gekwantificeerd. Het gebruik hiervan moet daarom op meer gebieden worden aangemoedigd, zoals bijvoorbeeld in de medische- en in de gedragswetenschappen, zoals de psychologie en de criminologie.

9. Een belangrijk voordeel in het schrijven van een proefschrift dat is gebaseerd op bijdragen die de auteur gedurende een 20-jarige beroepspraktijk op dit gebied heeft ontwikkeld, is de mogelijkheid om de kloof tussen theorie en praktijk beter te overbruggen. Dit heeft het mogelijk gemaakt om modellen en gegevens in een beter perspectief te plaatsen met betrekking tot de nauwkeurigheid van de resultaten uit de modeltoepassingen.

10. Ervaring leidt gewoonlijk tot modificatie. Daarom ligt de weg naar verbetering in de studie van storingen.

11. Gemakkelijker toegang tot informatie en een betere presentatie daarvan leidt niet tot hogere kwaliteit van de informatie.

1. During the design phase it is necessary to verify, by measurement, conformance to reliability and safety targets. Appropriate modelling techniques are therefore required which can make use of limited failure data.

2. Field failure rate and failure mode data are needed, in order to predict the potential system reliability of proposed designs for specific failure modes. To this end unambiguously defined data elements must be collected. Computerised maintenance management provides an opportunity to generate more consistent failure data.

3. Generic failure rate data are subject to wide tolerances due to the numerous applications of hardware systems, and to differing practices in recording data fields. Modelling techniques therefore need to express results using confidence limits.

4. There are often only small quantities of failure data. Analysis therefore needs to make use of statistical significance measures in order to make realistic interpretations.

5. Present reliability modelling methods often exceed the accuracy of the data available to quantify them. Thus simplified prediction methods are justified.

6. Due to various dependencies, common cause failures (CCF) often dominate system unreliability by defeating the benefits of redundancy. Therefore the modelling of CCF (and its identification in field data) should continue to be developed.

7. Reliability assessment methods will continue to develop as systems become more complex. There is therefore an increasing need to take account of human and software factors and their interaction with the hardware system.

8. Failure data collection and reliability modelling methods are applicable wherever failure consequences can be observed and quantified. Their use should therefore be encouraged in more fields as, for example, in medical treatments and in behavioral processes such as psychology and criminology.

9. A major benefit to preparing a doctoral thesis, based on contributions developed during twenty years work in the field, is that it has been possible for the author to bridge the gap between theory and practice. This has enabled models and data to be put into perspective, having regard to the limits of accuracy from the models.

10. Experience usually leads to modification. Therefore the route to improvement lies in the study of failures.

11. Improved access to information, and its better presentation, do not improve its quality.

DEVELOPMENTS IN THE USE OF FAILURE RATE DATA AND RELIABILITY PREDICTION METHODS FOR HARDWARE

DAVID J SMITH

DEVELOPMENTS IN THE USE OF FAILURE RATE DATA AND RELIABILITY PREDICTION METHODS FOR HARDWARE

PROEFSCHRIFT

ter verkrijging van de graad van doctor
aan de Technische Universiteit Delft,
op gezag van de Rector Magnificus prof ir K F Wakker,
in het openbaar te verdedigen ten overstaan van een commissie,
door het College voor Promoties aangewezen,
op maandag 29 mei 2000 te 10.30 uur

door

DAVID J SMITH
Bachelor of Science (Hons)
Council for National Academic Awards (UK)

geboren te Purley, Engeland

Dit proefschrift is goedgekeurd door de promotor:

Prof ir K Smit.

Samenstelling promotiecommissie:

1. Rector Magnificus	Technische Universiteit Delft
2. Prof ir K Smit	Technische Universiteit Delft
3. Prof dr R M Cooke	Technische Universiteit Delft
4. Prof dr A R Hale	Technische Universiteit Delft
5. Prof ir W L Kling	Technische Universiteit Delft
6. Prof dr A D McGettrick	University of Strathclyde
7. Prof ir J L Spoormaker	Technische Universiteit Delft
8. Dr ir A Bossche	Technische Universiteit Delft

ISBN: 09516562 6 0

Printed in England

"Plurality is not to be posited without necessity."

This saying by William of Occam, a 14th century philosopher, is known as Occam's Razor and means "The simplest explanation is best so do not use more parameters than necessary in a model". I believe this to be an important principle for the Reliability and Risk profession.

Dedicated to Gladys and Frank

ABSTRACT

DEVELOPMENTS IN THE USE OF FAILURE RATE DATA AND RELIABILITY PREDICTION METHODS FOR HARDWARE

During design, meaningful reliability predictions are needed for showing if minimum life cycle costs are likely to be achieved and for establishing specified reliability, availability and safety-integrity of systems. Therefore, safety and life-cycle cost targets are set (chapter 2) and these are reflected in target reliability, availability and maintainability parameters for the design.

RAMS (Reliability/ Availability/ Maintainability/ Safety) design assessments consist of quantified failure predictions at system, sub-system or component level and are best carried out early in the design-cycle.

There are two major problems (described in chapter 1) associated with this assessment activity:

a) Accuracy of the available failure rate data
b) Adequacy of the reliability prediction methods

This thesis outlines a reliability prediction method (outlined in chapter 2) which provides contributions to existing reliability technology and extends the state of the art as follows:

1) A method of comparing predicted RAMS with the targets by expressing predictions using confidence limits (ie maximum/minimum predicted values). Traditionally, single predicted values are used (chapters 3 & 4).

2) The use of single parts failure rates, chosen from any one data source, results in a single predicted system failure rate value. This thesis makes use of the author's collection of failure rate data to provide part failure rates expressed as maximum/minimum ranges. Forty four reliability prediction cases have been correlated against subsequently achieved operational field data and a statistical relationship established. This enables a reliability or availability prediction to be expressed as a range subject to confidence limits (chapter 3).

3) Markov models are frequently used for reliability/availability prediction of multi-state situations. A set of simplified Markov equations has been developed and their accuracy compared with the unsimplified equations (in

chapter 5). This comparison justifies the use of the simplified models in view of the inaccuracies of the failure rate data.

4) Unrevealed (hidden) failures are currently modelled by treating them as revealed failures where the unit down time is generally half of the proof-test interval. A set of expressions for modelling random coincident unrevealed failures has been developed (chapter 5).

5) The existing common cause failure models involve estimating the proportion of such failures by a subjective assessment of design features (eg segregation, diversity). Further development of common cause failure modelling is presented here. It provides objective scoring of design features and takes account of proof-test intervals. The model has been calibrated against field data (chapter 6).

6) Traditionally, times to failure of component parts were modelled by graphical probability plotting of the Weibull function and, more recently, by the use of software models. The author provides a method (software tool) which gives three separate measures of significance of the Weibull parameters. It also allows an optimum discard period to be calculated for the component part in question, based on given planned maintenance costs and unplanned penalty costs of failure (chapters 7 - 8).

The author's book (Smith D J, 1997) contains a significant amount of the material submitted for this thesis. Relevant portions of the book have therefore been included in this text. The author's software packages FARADIP, COMPARE and BETAPLUS also form a part of this thesis. The FARADIP and COMPARE user manuals are reproduced as Appendices 2 and 4 and the BETAPLUS material is included in chapter 6. Appendix 3 contains the details of the author's study of the correlation between predicted reliability and subsequent field data.

In a subject requiring continuous improvement it is intended to continue collecting and analysing data, beyond this thesis, in order to extend and further calibrate the models shown.

Companies and organisations are urged to collect and analyse their own failure data in order to enhance the accuracy of their RAMS predictions and to enable the models and correlations described in this thesis to be developed further.

David J Smith
29 May 2000

SAMENVATTING

ONTWIKKELINGEN IN HET GEBRUIK VAN STORINGSGRAAD GEGEVENS EN BEDRIJFSZEKERHEID VOORSPELLINGSMETHODEN VOOR TECHNISCHE SYSTEMEN.

Voor het realiseren van opgelegde veiligheid- en beschikbaarheidseisen en het minimaliseren van levenscycluskosten van technische systemen is het wenselijk tijdens het ontwerp bedrijfszekerheidsvoorspellingen uit te voeren.

Daarom dienen veiligheid en levensduurkosten gespecificeerd (hoofdstuk 2) en vertaald te worden naar bedrijfszekerheid, beschikbaarheid en onderhoudbaarheid doelen voor het ontwerp van een technisch systeem.

Evaluatie van ontwerp alternatieven bestaat uit gekwantificeerde voorspellingen van het storingsgedrag op systeem-, subsysteem en component-niveau en kunnen het beste worden uitgevoerd in een zo vroeg mogelijk stadium van het ontwerp.

Er zijn twee belangrijke problemen (beschreven in hoofdstuk 1) met betrekking tot voornoemde evaluatie activiteit:
a) Betrouwbaarheid van de beschikbare storingsgevens
b) Geschiktheid van de bedrijfszekerheid voorspellingsmethoden

Dit proefschrift beschrijft een bedrijfszekerheid voorspellingsmethode (in hoofdstuk 2) die een bijdrage levert aan de verdere ontwikkeling van de huidige stand van zaken en wel als volgt:

1) Een methode voor het vergelijken van RAMS (Reliability, Availability, Maintainability and Safety) voorspellingen met de specificaties en de toepassing van betrouwbaarheid intervallen (minimum en maximum van de voorspelling). Gebruikelijk is enkelvoudige voorspelde waarde (hoofdstuk 3 en 4).

2) Het gebruik van een storingsgraad voor afzonderlijke onderdelen, ontleend aan een bepaalde gegevensbron, met als resultaat een voorspelling van de storingsgraad van het systeem als enkelvoudige voorspelde waarde. In dit proefschrift wordt gebruik gemaakt van door de auteur verzamelde storingsgraad gegevens, waarmee het mogelijk is storingsgraad van onderdelen uit te drukken als minimum en maximum waarden. Er zijn 44

bedrijfszekerheid voorspellingen van systemen in de ontwerpfase gecorreleerd met de later gerealiseerde bedrijfszekerheid gedurende de operationele fase en een statistische relatie is vastgesteld. Dit maakt het mogelijk om een bedrijfszekerheid of beschikbaarheid voorspelling uit te drukken als een waarde met een betrouwbaarheidsinterval (hoofsdstuk 3).

3) Vaak worden Markov modellen gebruikt voor bedrijfszekerheid/ beschikbaarheid voorspelling. Een set van vereenvoudigde Markov -vergelijkingen (hoofdstuk 5). Deze vergelijking rechtvaardigt het gebruik van vereenvoudigde modellen, met het oog op de onnauwkeurigheden in de storingsgraadgegevens.

4) Verborgen storingen worden veelal gemodelleerd door deze te behandelen als evidente storingen, waarbij de niet-beschikbaarheid in het algemeen de helft is van het interval voor de functionele test. Een set van uitdrukkingen voor het modelleren van random co-incident verborgen storingen, is ontwikkeld (hoofdstuk 5) en de nauwkeurigheid van de uitkomsten is vergeleken met die van niet-vereenvoudigde vergelijkingen.

5) De bestaande modellen voor storingen met gemeenschappelijke oorzaak, maken gebruik van schattingen voor het aandeel daarvan, door een subjectieve beoordeling van ontwerpkarakteristieken zoals bijvoobeeld afscheiding en diversiteit van componenten. Verdere ontwikkeling van de modellering van storingen met een gemeenschappelijke oorzaak wordt gepresenteerd. Het voorziet in het toekennen van objectieve waarderingen voor ontwerpkarakteristieken en betrekt hierin de intervallen voor functionele tests. Het model is gekalibreerd met behulp van praktijk gegevens (hoofdstuk 6).

6) Het is gebruikelijk om de storingssintervallen van componenten en onderdelen te modelleren met behulp van het grafisch uitzetten daarvan met een Weibull functie en, meer recent, met behulp van computers. De auteur verschaft een methode in de vorm van een computermodel waarmee drie afzonderlijke waarden voor de significantie van de Weibull parameters kunnen worden vastgesteld. Het model kan ook voor de betreffende componenten een optimaal verwissel interval berekenen, gebaseerd op gegeven geplande en ongeplande kosten (hoofdstuk 7 en 8).

Een publicatie, in de vorm van een boek van de hand van de auteur (Smith, 1997) bevat een substantieel deel van het materiaal dat onderdeel vormt van dit proefschrift. Daarom zijn relevante delen van bovengenoemde publicatie in het proefschrift opgenomen. De software modellen "Faradip", "Compare" en "Betaplus", ontwikkeld door de auteur, vormen eveneens een onderdeel van dit proefschrift. Daartoe zijn de gebruikershandleidingen van "Faradip" en "Compare," opgenomen als bijlagen 2 en 4 en het materiaal dat betrekking heeft op "Betaplus" in hoofdstuk 6 is de studie door de auteur over de correlatie tussen voorspelde bedrijfszekerheid en de gerealiseerde bedrijfszekerheid op basis van veldgegevens.

Voor een onderwerp, dat onderhevig is aan continue verbetering, is het de bedoeling om het verzamelen en analyseren van gegevens voort te zetten, om daarmee de gepresenteerde modellen beter te kunnen kalibreren.

Bedrijven en organisaties worden aangemoedigd om de eigen storingsgegevens te verzamelen en te analyseren, ten einde de nauwkeurigheid van de RAMS voorspellingen te verhogen en daardoor in staat te zijn om de modellen en verbanden, beschreven in dit proefschrift, verder te ontwikkelen.

David J Smith
29 mei 2000

ACKNOWLEDGEMENTS

I wish to express my sincere thanks to Professor Klaas Smith for inviting me to Delft to undertake this PhD thesis. His constructive comments and critique have helped me to improve and refine this study since its original conception.

I would also like to thank the committee members for their encouragement and for constructive comments on the various drafts during the development of this work and also Professors Andrew Hale (Delft), Andrew McGettrick (Strathclyde) and Ron Allan (UMIST) for earlier encouragement.

I would like to thank Mr Robert Winchurch of HR Strategies, Mr Andy Cross of UK AEA, Dr Paul Banks of TRANSCO, and Mr John Coupland of the IEE for much assistance in locating relevant material for drawing comparisons during this study.

Many thanks also to Mr "Sam" Samuel for considerable help with my software packages.

I am very grateful to Ken Simpson for many hours of "in depth" review, which resulted in numerous enhancements and corrections to the final manuscript.

Throughout the development of this thesis I have been fortunate to receive a great deal of encouragement from Dr Ian Jutting and Dr Phil Dixon. I value their interest highly, without which I might not have succeeded.

My special thanks, also, to Susan for all her encouragement.

CONTENTS

NOTATIONS, ABBREVIATIONS AND DEFINITIONS

SYMBOLS

λ	LAMBDA used for failure rate
β	BETA (used in both Weibull and common cause failure topics)
η	ETA used in the Weibull expression
γ	GAMMA used in the Weibull expression
Σ	SIGMA (sum of)
T	Proof-test or auto-test interval
$>$	Greater than
$>>$	many times greater than

ABBREVIATIONS

ALARP	As low as reasonably practicable
CCF	Common cause failure
CMF	Common mode failure
CPL	Cost per life saved
CPU	Central processing unit
EMC	Electro-magnetic compatibility
exp	exponential
FMEA	Failure mode and effect analysis
FMECA	Failure mode, effect & criticality analysis
HAZOP	Hazard and operability study
HSE	Health & Safety Executive
H_2S	Hydrogen sulphide
IEE	Institution of Electrical Engineers
IEEE	Institution of Electrical and Electronic Engineers
LCC	Life-cycle costs
ln	exponential logarithm
MDT	Mean down time
MTBF	Mean time between failures
MTTF	Mean time to fail
MTTR	Mean time to repair
PFD	Probability of failure on demand
PMH	Per million hours
QRCM	Quantified reliability centred maintenance
RAMS	Reliability, availability, maintainability, safety-integrity
RCM	Reliability centred maintenance
STD	Standard deviation

DEFINITIONS

ACTIVE REDUNDANCY: Configuration of operating items whereby system failure requires the failure of more than one individual item.

AS LOW AS REASONABLY PRACTICABLE: A parameter (usually PFD) which has been reduced to a point whereby further improvement would be at a cost deemed to be grossly disproportional to the benefit predicted.

AUTO-TEST: A form of proof-test (usually provided by software) which is either continuous or initiated automatically at a defined interval.

COINCIDENT RANDOM FAILURES: Failures which occur independently of each other, and at random, and within a specified interval.

COMMON CAUSE FAILURES (CCF): Failures which are linked, due to some dependency, and arise from a single cause.

COMMON MODE FAILURES (CMF): Failures which are linked, due to some dependency, and exhibit a single mechanism.

DOWN TIME: The total time for which an item (or system) is in the failed state.

DEGRADATION/DRIFT FAILURES: Component level faults whereby a gradual change of one or more of its parameters eventually causes it to fail.

LIFE-CYCLE COSTS: Costs arising from corrective and preventive maintenance, and from the consequences of failures, during the total life of a system.

PROBABILITY OF FAILURE ON DEMAND: The probability that an item will be in the failed state at any instant (numerically equal to the unavailability for that failure mode).

PROOF-TEST: A test for unrevealed failures at some defined interval and usually carried out by personnel.

REPAIR RATE: The reciprocal of the down time of the item in question.

REVEALED FAILURES: Failures which are evident by their mode.

SAFETY: The feature of a system whereby specific failure modes lead to hazardous scenarios.

STANDBY REDUNDANCY: Configuration of items whereby one or more items is available to replace a failed item and system failure requires the failure of more than one such item.

UNAVAILABILITY: The proportion of time during which any item (or system) is in the state which has been defined as failure.

UNREVEALED FAILURES: Failures which are not evident by their mode and which are therefore only revealed as a result of a proof test.

PART 1 - JUSTIFICATION

CHAPTER 1

A NEED FOR REALISTIC RELIABILITY PREDICTION METHODS

1.1 SUMMARY

This chapter emphasises the need for risk, reliability and availability prediction during the phases of functional design. It also addresses the need to establish those maintenance parameters (eg discard intervals, spares quantities, preventive maintenance regimes) which are relevant to the predictions.

Problems associated with the accuracy of failure rate data, and hence the accuracy of reliability prediction, are explained. The requirements for a realistic method, which takes account of imprecise failure rate data, are outlined.

A "RAMS-cycle" model is introduced as a means of illustrating where and how the prediction methods are applied during design and field use. In this thesis the abbreviation RAMS is used for ease of reference to reliability, availability, maintainability and safety-integrity.

Furthermore, the assessment of safety also involves the use of RAMS parameters which are applied to the hazardous failure modes. Maintainability is not ignored since it affects availability. Nevertheless, the parameters of primary interest in this thesis are reliability and availability.

Current practice, such as is called for in IEC 61508, 1999, involves RAMS prediction using failure rate data but without taking into account the confidence limits of that data.

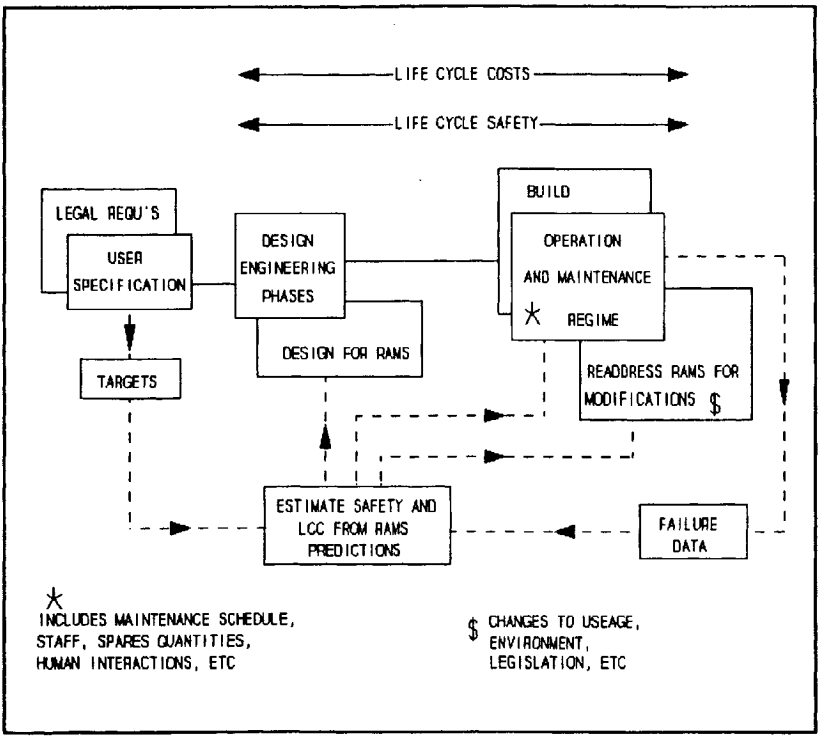
This thesis concerns the interpretation of data and the subsequent reliability modelling of random hardware failures. In addition to these random hardware failures, although not the subject of this thesis, it is necessary to address system failures arising from systematic failures (eg software errors) and those caused by human factors. These are mentioned briefly in chapter 5.

1.2 THE FOCUS OF RELIABILITY/AVAILABILITY PREDICTION

Explicit RAMS targets, followed by RAMS predictions, are needed in order to make comparisons between design options both for new equipment and when proposing modifications. As well as being determined by equipment design and by the parts failure rates, RAMS is also affected by operating, and environmental factors and by maintenance parameters (eg spares levels, discard intervals).

Predictions should be repeated for each proposed change of design, or change of maintenance strategy, to enable trade offs to be made between those factors which effect RAMS. Figure 1.1 addresses the extent of the design and operating life of equipment and shows where RAMS predictions are applied.

Figure 1.1 - The focus of RAMS prediction



There are two main drivers which impose a requirement for RAMS predictions to be carried out by equipment designers and owners. They are; a) the need to optimise safety by reducing the frequency of hazardous failure modes and; b) the desire to minimise life-cycle costs.

a) SAFETY: This is currently the main motivator for applying RAMS studies, as manufacturers are often required to prove that their product satisfies safety requirements. The steadily increasing requirements of COMAH, CE, and IEC 61508 call for quantified safety evaluation. As a result HAZOPs (Hazard and Operability Studies), FMECAs (Failure Mode, Effects and Criticality Analyses) and other RAMS assessment techniques are being applied to safety-related systems. Thus, it is now commonplace to engineer products and systems whilst attempting to minimise the probability of hazardous failures despite containing costs within credible bounds.

b) LIFE CYCLE COSTS: There is an opportunity to extend the use of these RAMS techniques to minimise life cycle-costs. During the design-cycle (Figure 1.2) there is a need, at feasibility, conceptual and detailed design stages, to compare the effect of different design options on reliability and availability. Maintenance parameters (which include discard intervals, spares levels, etc) as well as the functional design itself have a pronounced effect on the operating costs of equipment and systems. Large financial benefits, in operations and maintenance, can be achieved as a result of small (but cost effective) changes to the design, the maintenance strategy, spares holding, human factors, etc. Calculating this benefit is addressed in chapter 4 of this thesis.

There is therefore a need for adequate RAMS assessment methods which take account of the imprecision of failure rate data as well as addressing all the relevant parameters (for example common cause failures).

1.3 CREDIBILITY OF RELIABILITY/AVAILABILITY PREDICTION

RAMS (which includes safety-integrity) prediction suffers from poor credibility, particularly amongst engineers who are not themselves RAMS specialists. This stems from three fundamental reasons:

a) The major limitation in RAMS prediction is that it requires parts failure rate data in order to predict system reliability/safety. The repeatability of data between its SOURCE and the SUBJECT of the prediction (usually a proposed design or modification) is poor due to the large number of parameters which influence the failure rate. Components of like description exhibit failure rates differing by as much as two orders of magnitude. This is addressed in chapter 3 and a paper by the author (Smith D J, 1986).

b) System RAMS modelling, whereby the failure/success logical combinations of its sub-systems are described, is not well understood outside the RAMS profession. There is incidentally a need to educate engineers in basic RAMS techniques (Appendix 8). As a result, the techniques are often used in such a way as to suggest a precision which is not supported by the data (chapter 3).

c) Engineers are educated to understand deterministic models. However, in the past, probability and statistics have not been well taught and thus non-RAMS engineers frequently have difficulty understanding RAMS concepts.

1.4 THE RAMS-CYCLE MODEL

The purpose of the RAMS-cycle model in Figure 1.2 is to expand on Figure 1.1 to provide a visual link between the RAMS activities and a typical design-cycle. The top portion shows the specification and feasibility stages of design leading to conceptual engineering and then to detailed design.

RAMS targets should be included in the requirements specification as a project or contractual requirement which can include both assessment of the design and demonstration of performance. This is particularly important since RAMS targets may otherwise be perceived as adding to time and budget and there will be little other incentive, within the project, to specify them.

Since different system failure modes will be caused by different parts failures it is important to realise the need for separate targets for each undesired system failure mode. This is explained further in paragraph 2.3 of chapter 2.

Because one purpose of the feasibility stage is to decide if the proposed design is viable (given the current state-of-the-art) then the RAMS targets may be modified

during the feasibility engineering stage if initial predictions show them to be unrealistic. Subsequent versions of the requirements specification would then contain revised targets, for which revised RAMS predictions will be required, as described by the deliverables listed below against the review loops shown in Figure 1.2.

These loops represent RAMS prediction inputs to the design review process. This is sometimes called technical review as, for example, in MIL 499B, 1992. Note that loops [1], [2] and [3] correspond to the RAMS prediction activity shown in Figure 1.1. In more detail, the loops are:

- A review of the system RAMS feasibility calculations against the initial RAMS targets (Figure 1.2 - loop [1]).

- A formal (documented) review of the conceptual design RAMS predictions against the RAMS targets (Figure 1.2 - loop [2]).

- A formal (documented) review, of the detailed design, against the RAMS targets (Figure 1.2 - loop [3]).

- A formal (documented) design review of the RAMS tests, at the end of design and development, against the requirements (Figure 1.2 - loop [4]). This is the first opportunity (usually somewhat limited) for some level of real demonstration of the project/contractual requirements.

- A formal review of the acceptance demonstration which involves RAMS tests against the requirements (Figure 1.2 - loop [5]). These are frequently carried out before delivery but would preferably be extended into, or even totally conducted, in the field (Figure 1.2 - loop [6]).

- An ongoing review of field RAMS performance against the targets (Figure 1.2 - loops [7,8,9]) including subsequent improvements.

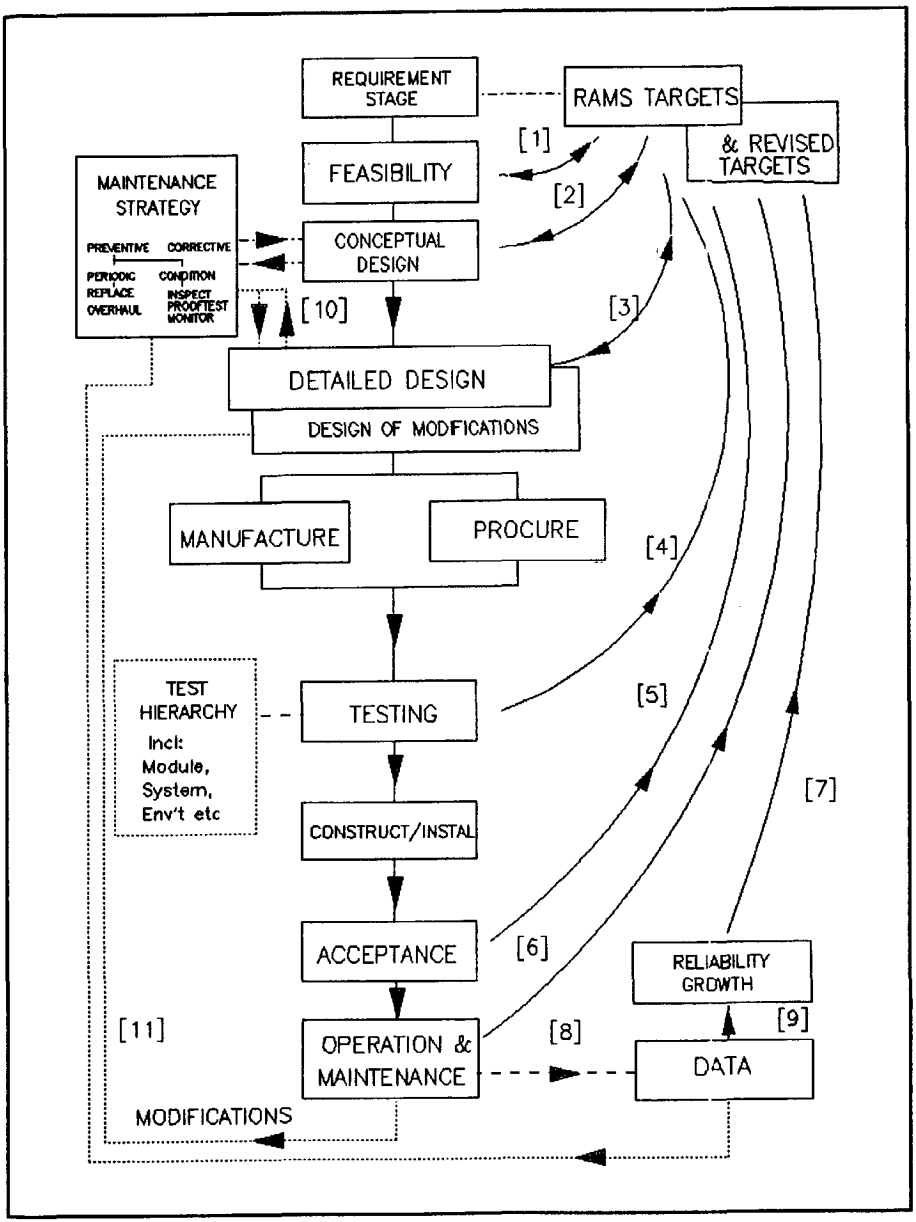
Not every one of the above review loops will be applied to each contract. The extent of review will depend on the size and type of project.

Test, although shown as a single box in this simple RAMS-cycle model, will usually involve a test hierarchy consisting of component, module, sub-system and system tests. These must be described in the project documentation.

The maintenance strategy (ie programme) is relevant to RAMS since both preventive and corrective maintenance affect reliability and availability. Repair times influence unavailability as do preventive maintenance parameters. (Figure 1.2 - the loops [10]) show that maintenance is considered at the design stage where it will impact on the RAMS predictions. At this point the RAMS predictions can begin to influence the planning of maintenance strategy (eg periodic replacements/overhauls, proof-test inspections, auto-test intervals, spares levels, number of repair crews).

For completeness, the RAMS-cycle model also shows the feedback of field data into a reliability growth programme and into the maintenance strategy (Figure 1.2 - loops [8] [9] & [11]). Sometimes the growth programme is a contractual requirement and it may involve targets beyond those in the original design specification.

Figure 1.2 - RAMS-Cycle model



1.5 COMPATIBILITY OF FAILURE RATE DATA AND RELIABILITY MODELS

Simple prediction techniques (eg fault tree analysis, reliability block diagrams) sometimes involve little more than establishing the series and redundant features in a system. System failure probability is then calculated from the underlying mathematics (often making the assumption of independent random failures).

More complex modelling techniques allow more varied assumptions to be made (eg non-random distributions applied to failure rates and down times, different failure rates for different system states and modes of operation). Because these models require more sophisticated mathematical solutions, simulation is sometimes used to quantify the system RAMS. Complex modelling provides a more precise description of the system under analysis.

However, the additional precision of the more complex methods may be wasted due to the lack of precision of the failure rate data sources (chapters 3 & 4). In any case, it is the relative results of predictions, comparing design and maintenance options, which are of far greater importance than absolute values.

Easily applied and cost effective methods are therefore required which can provide the benefits of RAMS evaluation whilst also allowing for imprecise failure rates. This thesis addresses that need.

1.6 THE NEED FOR A METHOD

The previous paragraphs establish the need for RAMS assessment methods (this is introduced in chapter 2, Figure 2.1). These methods must:

a) Use modelling which is not unjustifiably over-detailed, and is thus consistent with having to make use of wide tolerance failure rate and failure mode data. It must permit ranges of predicted values to be addressed and provide meaningful assessments without wasting resources on unjustified sophistication.

b) Facilitate optimum decisions about design and maintenance which lead to overall life-cycle cost savings. The designer will make these decisions as a result of the RAMS requirements placed on him. Comparison of options is

possible despite the wide tolerance range in the calculations. As a result, it should encourage non-RAMS specialists to carry out RAMS studies.

c) Be seen to be cost effective to implement so that the cost of its use is visibly small compared with the potential life-cycle cost savings being addressed. This is illustrated in paragraphs 4.4 and 4.5 of chapter 4. RAMS assessments must be given suitable resources so that they do not increase project lead times.

d) Take account of the fact that both common cause failures (chapter 6 shows how to cater for this) and human error (see chapter 5.5) can dominate the unavailability. Even simple models therefore need to be sufficiently realistic as to take account of these factors in the modelling.

e) Be useable, as a design review tool, by professional engineers who are not RAMS specialists, following training that involves days rather than weeks of study. A brief syllabus of essential topics and study times, for this purpose, is provided in Appendix 8. The syllabus would enable these non-RAMS specialists to make use of the author's supporting software tools described in the user manuals (FARADIP.THREE, 1997; COMPARE, 1997; BETAPLUS, 1997) provided as parts of this thesis. Thus, the method will be suitable for use within small design teams such as in concurrent engineering (O'Connor P D T, 1994).

f) Evolve to take account of continually increasing system complexities which, in turn, lead to new types of failure mode arising from the greater number of hardware and software interconnections within a system. The model needs to be able to identify and evaluate them with appropriate data and models and, also, to apply suitable RCM.

CHAPTER 2

RAMS PREDICTION AND THE SYSTEM LIFE-CYCLE

2.1 SUMMARY

In this chapter a comparison is made between the current "state of the art" of RAMS prediction methods and the contributions of the author.

The method to be described (Figure 2.1) brings together a number of techniques, developed by the author, into a cohesive process. It specifically addresses the problems outlined in chapter 1 and is designed to provide RAMS predictions which take account of imprecise failure rate data.

Figure 2.1 outlines the RAMS prediction method and shows the point of application of each of the remaining chapters in the thesis.

Figure 2.1 expands on the prediction review loops [1], [2] and [3] and the data loops [8] and [9] which were shown in Figure 1.2.

2.2 CHOOSING FAILURE RATE AND FAILURE MODE DATA (Covered in Chapter 3)

Reliability prediction models require hardware failure rate and percentage failure mode data, and also human error rate data, in order to be quantified.

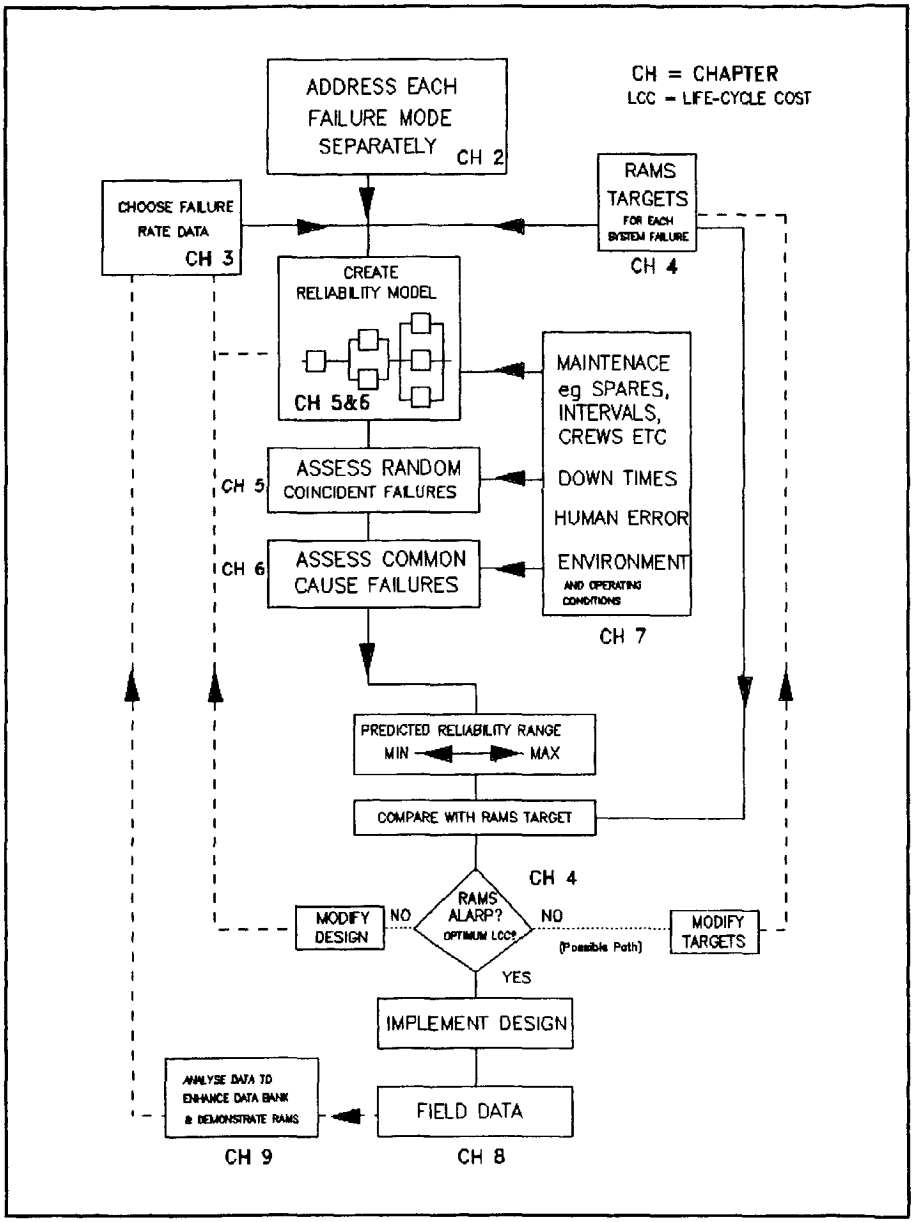
Traditionally, a single parts failure rate data source is chosen by the RAMS engineer. As a result, the predicted system RAMS is expressed as a single absolute number. The major proportion of these sources are listed in Appendix 5. They cover 20 years of data collection and thus combine new and old data. In general there tends to be a trend of gradually increasing reliability (Appendix 9) which renders the older sources less applicable. Nevertheless, due to the shortage of failure rate data, they are retained for comparison and to swell the overall amount of data.

In this thesis, the author's data (listed in Appendix 5) have been used to calculate a distribution of achieved versus predicted RAMS parameters enabling confidence limits, whose variances are related to the data source, to be applied to the predicted RAMS (chapter 3). Thus optimistic and pessimistic RAMS limits can be established.

Also, this work demonstrates that there is a relationship between the source of the data and the confidence limits. Site specific (eg natural gas compressor station), industry specific (eg offshore oil and gas platforms) and generic data (developed in chapter 3) are compared with the predictions and found to result in different accuracies.

Because site specific data are often not available, the author's comprehensive data bank known as FARADIP.THREE, 1997, has been developed which combines the failure rates from the sources in Appendix 5 and shows ranges of failure rates for each part. The data sources which make up the author's overall data bank are listed in Appendix 5 and include his gas industry data as well as published sources. Some of the published sources are not recent but are nevertheless useful for comparison purposes when constructing the FARADIP ranges.

Figure 2.1 - An outline of the RAMS prediction method



2.3 COMPARING PREDICTED RAMS WITH THE TARGETS (Covered in Chapter 4)

RAMS targets (eg failure rate, unavailability) will have been set, either as a result of quantified safety assessments or because of the cost of plant unavailability. There must be targets for each individual system level (top level) failure mode (eg fail to shut down, spurious shut down). This is essential since each particular system failure will be the result of particular combinations of specific parts failures. For example, spurious shutdown may result from EITHER of 2 sensors failing to a high output if they are voted on a "one out of two" basis. On the other hand BOTH sensors failing low would result in a failure to shutdown the system. Thus, both the part failure rate and the failure logic (EITHER vis a vis BOTH) are affected by the system failure mode.

These targets will have been set taking account of historical data from comparable systems, results of benchmark studies, and of technology progress.

Current practice is to compute a single predicted RAMS value for comparison with each target. In this thesis a method is proposed for comparing the predicted confidence range with the target in order to quantify the degree of uncertainty.

Assessing the cost of using the prediction method is also described, in order to show that it is small compared with the potential savings involved, having regard to the system life cycle costs.

2.4 RAMS MODELLING (Covered in Chapter 5)

In order to evaluate the redundant elements of systems MARKOV analysis is often used since it models systems which can have several states. This is fully described, including the criteria for the applicability of modelling techniques, in chapter 5.

However, the precision offered by use of the full MARKOV equations is rarely justified (except for large values of failure rate multiplied by down time) as is demonstrated in chapter 5.

Equations of system failure rate and unavailability are developed in chapter 5, and in Smith D J, 1997. These provide models for random coincident failures taking account of a number of repair regimes (eg one or more repair crews available for

each sub-system failure). They are based on MARKOV models and make use of the condition (usually a realistic approximation) that mean time between failures is large (order of 10^n years) compared with mean down time (order of hours/days).

In the separate case of hidden (ie unrevealed) failures in redundant systems, current practice is to treat them as revealed failures having a down time equal to half the proof-test interval. Equations are also developed for this case (see chapter 5).

RAMS models often require the quantification of human error (eg failures arising from omission of a task or commission of an incorrect action), of software error and of repair times. Although not a main theme in this thesis, for completeness, chapter 5 references existing methods.

2.5 COMMON CAUSE EFFECTS (Covered in Chapter 6)

The models described in chapter 5 do not take account of common cause failures (CCF) where redundancy is defeated by a single cause. In many cases these common cause failures dominate the unreliability by having frequencies orders greater than the coincident random failures described in paragraph 2.4.

The accuracy of CCF modelling is therefore of greater importance than that used for coincident random failures.

The current state of the art is reviewed in Wray A M, 1996 and the most commonly accepted method in use is the "BETA model" method described by Smith D J, 1997 and UKAEA, UPM 3.1, 1996.

This thesis develops and calibrates a more advanced "BETA factor" model whose enhancements are described in chapter 6.

2.6 QUANTIFIED RELIABILITY CENTRED MAINTENANCE (Covered in Chapter 7)

Reliability centred maintenance involves determining a maintenance programme based on a knowledge of reliability parameters. A software program, containing a number of improvements (COMPARE User manual, 1997), has been developed:

a) To assist in optimising discard and replacement intervals where a component failure rate is significantly increasing and where the unplanned failure costs exceed the planned overhaul or renewal costs. Times to failure are needed for the analysis and significance measures are used in the technique. Figure 2.1 shows where this software model is applied to analysing field data (chapter 7).

b) To assist condition-based maintenance by optimising inspection or proof-test intervals for unrevealed failures in redundant systems. Here the cost of an unplanned failure needs to exceed the cost of the proof-test. Figure 2.1 shows where this technique is applied during the RAMS prediction modelling (chapter 7).

c) To assist condition-based maintenance by optimising spares levels by calculating their effect on unavailability. The program computes availability predictions for different spares levels, failure rates, repair times and procurement times. Figure 2.1 shows where this technique is applied during RAMS prediction modelling (chapter 7).

In order to calculate optimum intervals, the program requires the user to input the assumed planned maintenance costs (ie preventive maintenance) and unplanned costs (ie corrective maintenance and failure penalties).

Current practice offered by Moubray J, 1991 involves both subjective assessment and some quantification.

2.7 FIELD DATA FEEDBACK AND ANALYSIS (Covered in Chapter 8)

RAMS predictions rely on the collection of failure data. Based on experience of field data recording, the essential parameters for field data reporting are specified in order that:

a) predictions can be validated at a later date in order to demonstrate reliability.

b) data for future predictions can be enhanced in order to improve the accuracy of predictions.

c) data can be adequately recorded so as to extract:

- times to failure for Weibull analysis (chapters 7 & 8).
- failure modes to permit reliability modelling (chapter 3).
- maintenance times and costs for RCM calculations (chapter 7).

d) data can be screened, to some extent, to distinguish between intrinsic failures and induced failures (eg operator and maintenance induced). This is not easy since the underlying causes of failure are often no longer available at the time of data collection or to the data analyst. Nevertheless some screening is possible (chapter 8.2) and is important since the derived failure rates will vary according to which incidents are included or omitted by the screening. This can be an important consideration where reliability is being formally demonstrated.

Currently, data collection methods often fail to preserve the individual times to failure of the component items or to distinguish between calendar and operating time. This thesis advocates recording individual times to failure and provides the above RCM software tool (COMPARE User manual, 1997) to establish the distribution of the times to failure (ie Weibull analysis).

PART 2 - THE RAMS PREDICTION METHOD

CHAPTER 3

USING FAILURE RATE DATA

3.1 SUMMARY

The relative values from RAMS predictions have greater validity as comparisons of alternatives than as absolute predictions of reliability. Nevertheless, absolute values are generally used for comparison against targets. There is therefore a need to improve on the use of a single (inaccurate) predicted reliability figure.

This chapter describes a method of expressing RAMS predictions as a range having confidence limits, as opposed to the current practice of stating a single figure. Findings of other authors are offered for comparison. Figure 2.1 shows where this chapter fits into the thesis.

Although the ranges are symmetrical the variances are influenced by the source of the failure rate data and this is dealt with here.

The FARADIP User Manual, 1997 is included as Appendix 2 and the author's study "Correlation between predicted reliability and subsequent field data" is provided as Appendix 3.

3.2 VARIABILITY OF FAILURE DATA

Observed failure rates vary widely for different parts and equipments, despite their having the same physical description. The reasons for this are outlined in chapter 4 of Smith D J, 1997 and are:

- Some failure rate data include items replaced during preventive maintenance whereas others do not. These items should, ideally, be excluded from the data but, in practice, it is not always possible to identify them. This can affect rates by an order of magnitude.

- Failure rates are affected by the tolerance of a design and this will cause a variation in the values. Because definitions of failure vary, a given parametric drift may be included in one data base as a failure, but ignored in another.

- Although nominal environmental and quality assurance levels are described in some databases, the range of parameters covered by these broad descriptions is large. They represent, therefore, another source of variability.

- Component parts are often only described by reference to their broad type (e.g. signal transformer). Data are therefore combined for a range of similar devices rather than being separately grouped, thus widening the range of values. Furthermore, different failure modes are often mixed together in the data.

- The degree of data screening will affect the relative numbers of intrinsic and induced failures in the quoted failure rate (chapter 8.2h).

- Reliability growth occurs where field experience is used to enhance reliability as a result of modifications. This will influence the failure rate data.

- Trial and error replacement, as a means of diagnosis, and maintenance reports listed as "no fault found" can artificially inflate failure rate data.

- Some data records undiagnosed incidents and "no fault found" visits. If these are included in the statistics as faults, then failure rates can be inflated. Quoted failure rates are therefore influenced by the way they are interpreted by an analyst.

Failure rate values can span one or two orders of magnitude as a result of different combinations of these factors. In general, data sources (Appendix 5) quote failure rates as a single figure although IEEE standard 500, 1994 does provide ranges of likely failure rate.

3.3 CORRELATION BETWEEN PREDICTIONS AND FIELD DATA

Appendix 3 compares forty four RAMS predictions with the field data subsequently obtained from the equipment during operation. It lists the predictions and field data values with references to the underlying documents which contain them.

The ratio of predicted failure rate (or system unavailability) to field failure rate (or system unavailability) was calculated for each of the forty four examples and the results were classified in three categories:

a) Predictions using site specific data: These are predictions based on failure rate data which have been collected from similar equipment being used on very similar sites (eg two or more UK gas compression sites where environment, operating methods, maintenance strategy and equipment are largely the same). Another example would be the use of failure rate data from a gas flow meter corrector circuit used throughout the natural gas distribution network. This data might be applied to the RAMS prediction for a new design of circuitry for the same application. Appendix 3 provides details showing that the distribution of predicted versus field reliability has a mean ratio of slightly better then 2:1 (better or worse).

b) Predictions using industry specific data: An example would be the use of the OREDA offshore failure rate data book (Appendix 5) for a RAMS prediction of a proposed offshore gas compression package. Appendix 3 provides details showing that the distribution of predicted versus field reliability has a mean ratio of slightly better then 3:1 (better or worse).

c) Predictions using generic data: These are predictions for which neither of the above two categories of data are available. Generic data sources (listed in Appendix 5) are used. FARADIP.THREE (described in Appendix 2) is also a generic data source in that it combines a large number of sources. Appendix 3 provides details showing that the distribution of predicted versus field reliability has a mean ratio of slightly better then 3½:1 (better or worse).

Appendix 3 lists the forty four ratios of predicted RAMS to subsequent field RAMS with each ratio grouped into one of the three data source categories described above.

The distribution of these ratios was assumed to be Gaussian and a statistical significance (Chi-square) test was applied which showed approximately 75% goodness of fit. The Gaussian distribution was then applied to provide confidence limits whereby predicted RAMS values can be expressed in confidence ranges. A brief summary of the confidence ranges, established in Appendix 3, is:

FOR A PREDICTION USING SITE SPECIFIC DATA

There is 95% confidence that the field failure rate (or unavailability) will be better than 3½ times the predicted value and 90% confidence that the field failure rate (or unavailability) will be better than 2½ times the predicted value.

There is 90% confidence that the field failure rate will be in a range: 3½:1 to 1:3½

FOR A PREDICTION USING INDUSTRY SPECIFIC DATA

There is 95% confidence that the field failure rate (or unavailability) will be better than 5 times the predicted value and 90% confidence that the field failure rate (or unavailability) will be better than 4 times the predicted value.

There is 90% confidence that the field failure rate will be in a range: 5:1 to 1/5

FOR A PREDICTION USING GENERIC DATA

There is 95% confidence that the field failure rate (or unavailability) will be better than 8 times the predicted value and 90% confidence that the field failure rate (or unavailability) will be better than 6 times the predicted value.

There is 90% confidence that the field failure rate will be in a range: 8:1 to 1/8

In section 3.4 additional evidence in support of the 8:1 range is provided from the FARADIP data bank which suggests 7:1.

Useful comparisons are provided by the following studies.

Earlier work of Snaith E R, 1981 covering similar industry specific equipment. A similar study of 130 pairs of predictions and field data showed:

95% confidence that the field failure rate (or unavailability) will be better than 4 times the predicted value. Snaith is 90% confident that the field failure rate (or unavailability) will be better than 3 times the predicted value. He shows 90% confidence that the eventual field failure rate will be in a range: 3:1 to 1/4.

Snaith E R, 1981 also states that 50% of predictions are pessimistic and 50% optimistic. Although he does not subdivide the data pairs, as above, it can be inferred, from his paper, that they are largely industry specific with some site specific data sources.

Pirovano et al, 1988 observe at the component level only a 3.5:1 ratio of predicted to observed failure rate. Majeske et al, 1998 compare bench test data with predicted failure rates for vehicle modifications and show a generalised relationship of 2:1.

At the electronic PCB level Wood et al, 1994 found predictions to be conservative between 2:1 and 10:1. A Quantum Inc corporate paper anon, 1996 shows a 4:1 optimistic prediction for disc drives.

The above comparisons suggest ranges between 2:1 and 10:1 which is supportive of the author's results 3.5:1, 5:1, 8:1. Snaith E R, 1981 (3.5:1) and Quantum Inc, 1996 (4:1) agree closely with the author (5:1) for industry specific data.

3.4 USING GENERIC DATA

There are a number of generic data banks, the majority of which are listed in Appendix 5. The author has collated all of the component failure rates in these published sources, together with his own gas industry failure rate data, which spans 15 years. This data bank consists of 7,500 lines of failure rates and the sources are listed in Appendix 5. A sample page of this data bank is shown in Appendix 6, page 160. Each line of failure rate data consists of 11 fields (which can include the failure mode and rate, mean time to repair, data source, date, probability of failure on demand, environment).

The author's FARADIP.THREE User manual, 1997 provides nested menus of failure rate ranges and provides failure mode percentages (see Appendix 2). The nested menus cover the following items shown in Table 3.1.

Table 3.1 - FARADIP.THREE Nested menus

Discrete	
	Diodes
	Opto-electronics
	Lamps and displays
	Crystals
	Tubes
Passive	
	Capacitors
	Resistors
	Inductive
	Microwave
Instruments and Analysers	
	Analysers
	Fire and Gas detection
	Meters
	Flow instruments
	Pressure instruments
	Level instruments
	Temperature instruments
Connection	
	Connections and connectors
	Switches and breakers
	PCBs cables and leads
Electro-mechanical	
	Relays and solenoids
	Rotating machinery (fans, motors, engines)
Power	
	Cells and chargers
	Supplies and transformers
Mechanical	
	Pumps
	Valves and parts
	Bearings
	Miscellaneous
Pneumatics	
Hydraulics	
Computers, data processing and communications	
Alarms, fire protection, arresters and fuses	

The ranges are expressed by the use of 3 columns (as shown in Table 3.2) which enable high and low failure rates to be shown, together with an indication of the modal value. A few data sources were omitted by virtue of age or outlying values and the ranges represent approximately 90% of the data. The way in which the columns are used to indicate spread and mode are fully described in Appendix 2.

In general the lower failure rate figure in the FARADIP range, if used in a prediction, is likely to yield a RAMS prediction which might reasonably be anticipated after some field burn-in and assuming that the type of equipment has been subject to realistic reliability growth. The failure rate of recently designed equipment might well be an order of magnitude greater than this figure.

The author's data bank has been examined to ascertain if failure rate is related to the age of the data. The comparison is described in Appendix 9 and reveals a 40% improvement in failure rate between the 1980s and 1990s.

The "centre column" figure (in Table 3.2) indicates a failure rate which is more frequently indicated by the various data sources. It is therefore a matter of judgement as to whether it should be used in place of the lower figure.

The higher failure rate figure in the FARADIP range (Table 3.2), will include a proportion of defects and failures which have not lead to system failure BUT have been revealed during preventive maintenance. In some data sources (eg OREDA, Appendix 5) it is clear which rates apply to critical vis a vis degraded conditions. In other sources (eg MIL 217, Appendix 5) only a single failure rate is offered and it is not clear which modes of failure are included. Because failure rate data collection schemes vary in their interpretation of events this explains the existence of wide ranges of quoted values, especially with generic figures.

A typical "screen" from FARADIP.THREE is shown in Table 3.2 and another (for Diodes) is shown in Appendix 2.

Table 3.2 - Sample from FARADIP.THREE - (Fire & gas detectors screen)

	Failure rates, per million hours		
Gas pellister (fail .003)	5.00	10	30
Detector smoke ionization	1.00	6.00	40
Detector ultraviolet	5.00	8.00	20
Det'r infra red (fail .003)	2.00	7.00	50
Detector rate of rise	1.00	4.00	12
Detector temperature	0.10	2.00	.
Firewire/rod + psu	25	.	.
Detector flame failure	1.00	10	200
Detector gas IR (fail .003)	1.50	5.00	80
Failure modes (proportion):			
Rate of rise	Spurious 0.6	Fail 0.4	
Temp, firewire/rod	Spurious 0.5	Fail 0.5	
Gas pellister	Spurious 0.3	Fail 0.7	
Infra red	Spurious 0.5	Fail 0.5	
Smoke (ionize) & UV	Spurious 0.6	Fail 0.4	

The ranges of failure rate, seen in the FARADIP columns, vary according to the component part. Overall, the range is 50:1 (ie between 1 and 2 orders of magnitude). Table 3.3 shows the extent of these ranges by each component group.

Quoted failure rate ranges are also observed for memory chips of 20:1 by Neswadba et al, 1988.

Talmor et al, 1997 and Denson et al, 1996 refer to the Bayesian merging of generic data with field experience whereby the data are adjusted, in a weighted manner, as field data becomes available.

Table 3.3 - FARADIP Data Ranges

COMPONENT	RATIO OF MAX/MIN FAILURE RATE SHOWN ACROSS THE RANGES	
Microelectronics	11	
Microelectronics < 40°C	4	
Diodes	38	
Transistors	19	
Opto-electronics	19	
Lamps	21	
Crystals	25	
Tubes	6	
ELECTRONICS OVERALL		**18**
Capacitors	223	
Resistors	31	
Inductors	8	
Microwave	2	
DISCRETE OVERALL		**66**
Analysers	4	
Fire&Gas detection	55	
Meters		
Flow measurement	20	
Pressure measurement	35	
Level measurement	24	
Temperature measurement	45	
INSTRUMENTATION OVERALL		**31**
Connections	54	
Switches	81	
PCBs/cable	8	
Relays	59	
Rotating components	12	
Cells/chargers	16	
Generators/transformers	53	
Bearings	21	
Mechanical items	52	
Pneumatics/hydraulics	16	
Pumps	27	
Valves	42	
Computers	18	
Communications	7	
Alarms/fuses/protection	30	
OVERALL FARADIP DATA BASE		**50**

Since drift and degradation related failures are likely to be the main reason for the higher FARADIP figure they will probably have been revealed during preventive maintenance and are thus less likely to lead to the "system failure" which is being addressed in a RAMS prediction.

Thus, RAMS predictions which use the lower half of the FARADIP component failure rate range will therefore indicate the reliability most likely to be ultimately achieved by a design. That is to say, after burn-in and some reliability growth and excluding non-critical degradation failures which would be revealed during preventive maintenance.

Therefore, the most credible range of failure rates achieved in practice (if the drift and degradation defects mentioned above are to be excluded) is thought to be from the FARADIP lower failure rate to the midpoint of the FARADIP range.

Because the arithmetic mean of two widely spaced failure rates favours the higher value, the midpoint of a failure rate range is best expressed by use of the geometric mean as explained in chapter 4 of Smith D J, 1997. The square root (ie geometric mean) of the FARADIP range thus provides the most credible range of failure rates relating to the eventual predicted field reliability.

Thus, from Table 3.3, the square root of 50 suggests a **range of 7:1**. This lends additional significance to the 90% confidence range for generic data calculated as **8:1** in section 3.3 above.

3.5 USING MIXED DATA SOURCES

It often occurs that mixed data sources are used for a RAMS prediction such that, for example, site specific data are available for a few component parts but generic data are used for the other parts. The confidence range would then be assessed as follows:

If $Range_s$ and $Range_g$ are the confidence ranges for the site specific and generic data expressed as a multiplier in 3.3 above and in Appendix 3. Then:

THE RANGE FOR A GIVEN PREDICTION USING MIXED DATA SOURCES

$$= \frac{(\Sigma\lambda_s \times \text{Range}_s) + (\Sigma\lambda_g \times \text{Range}_g)}{\Sigma\lambda_s + \Sigma\lambda_g}$$

where $\Sigma\lambda_s$ and $\Sigma\lambda_g$ are the total failure rates of the site specific and generic items respectively.

For example, using the 3½:1 and 8:1 ranges (90% confidence) given in section 3.3 then if $\Sigma\lambda_s = 20$ per million hrs (pmh) and $\Sigma\lambda_g = 100$ pmh, the range for the prediction (at 90% confidence) would be:

$$\frac{(20 \times 3.5) + (100 \times 8)}{120} = 7.25:1$$

3.6 CONCLUSIONS AND RECOMMENDATIONS

From 3.3 it can be seen that site specific data should be used in preference to industry specific data which, in turn, should be used in preference to generic data. The predictions based on this data should be expressed as confidence ranges as described in this chapter and using the correlations provided from Appendix 3.

Since there is a general trend of increasing reliability (Appendix 9) then, if a number of data sources are available (for the same application), the failure rate used should be weighted in favour of the more recent data.

Where mixed data sources are used the confidence range should be adjusted using the method shown in 3.5.

If generic data is the only source for a prediction then the midpoint of the FARADIP lower range should be used as described in 3.4.

The author's correlation work, shown in Appendix 3, is not commonly carried out by other authors (except Snaith E R, 1981) but should be encouraged since it is the only empirical method of providing confidence ranges for reliability predictions.

CHAPTER 4

COMPARING RAMS PREDICTIONS WITH TARGETS

4.1 SUMMARY

Building on the predicted confidence ranges described in chapter 3, this chapter offers criteria for comparing each target RAMS parameter with the range of values explained in chapter 3. Figure 2.1 shows where this chapter fits into the overall thesis.

A criterion for meeting or not meeting the target is provided, based on the predicted confidence range rather than a single value.

A cost justification, based on examples of the author's experience, is provided for carrying out RAMS assessment against the targets.

4.2 SAFETY-RELATED TARGETS

The use of availability and failure rate to set safety targets is described in detail in IEC 61508, 1999 and in I GAS E IGE/SR/15, 1998.

A typical example would be a low demand rate scenario involving an Emergency Shut Down System. The risk reduction provided by the shutdown equipment is expressed as a PROBABILITY OF FAILURE ON DEMAND which is numerically equal to its unavailability. Thus "add-on" safety systems are generally given a target UNAVAILABILITY. This unavailability target is calculated as follows:

> Assume a maximum tolerable risk target for an involuntary risk scenario (eg death by explosion) is given as 10^{-5} per annum for a single death (A).
> Assume that 10^{-1} of the hazardous events (B), in the assessment, lead to death.
> The target maximum failure rate for the hazardous event is therefore C = A/B = 10^{-4} pa.
> Assume that a fault tree or other evaluation suggests that the unprotected process achieves a hazardous failure rate of 5×10^{-2} pa (D).
> The target maximum FAILURE ON DEMAND (and thus the maximum tolerable UNAVAILABILITY) for the safety system would need to be E = C/D = $\underline{2 \times 10^{-3}}$.

Current practice favours establishing two RAMS safety targets (each based on the target fatality rates). The "Maximum Tolerable" target (A, in the above example) means that one would not tolerate greater than that associated level of risk frequency. A lower "Broadly Acceptable" target is taken to mean that one accepts the associated probability of death as reasonable in the circumstances, and would not seek to expend much effort in reducing it further. A "Tolerable" region exists in between which implies that, whilst one is prepared to live with that particular frequency of the risk, one would review its causes and possible defences with a view to reducing it further. Cost enters the assessment in that any potential reduction in risk frequency would have to be compared with the cost needed to achieve it.

This cost principle is described in chapter 9 of Smith D J, 1997 as the concept of ALARP (As Low as Reasonably Practicable) which describes the way in which risk is treated by the UK HSE (Health and Safety Executive) and in Europe in general. It is also described in HSE, 1992, The Tolerability of Risk from Nuclear Power Stations. The concept is that all reasonable measures will be taken in respect of risks which lie in this "Tolerable" zone, to reduce them until the cost of further risk reduction is grossly disproportionate to the benefit. In this context grossly disproportionate implies a "cost per life saved" which is in excess of whatever is currently accepted as reasonable within a particular industry.

A process for comparing predictions with targets (illustrated in Figure 4.1) is recommended as follows:

* Decide on an acceptable confidence level for the RAMS prediction. Decide (from section 3.3 and Appendix 3) on the range applicable to that confidence level. For example section 3.3 shows a range of 5:1 to 1/5:1 at 90% confidence when industry specific data is being used. If a mixture of data sources is being used then section 3.5 shows how to modify the range.

* As shown in Figure 4.1, compare the predicted unavailability x range (or failure rate x range) with the "Broadly Acceptable" target. If this is better than the target then the design is accepted.

* If the predicted unavailability x range (or failure rate x range) is worse than the "Broadly Acceptable" target but better than the "Maximum Tolerable" target then the design is acceptable, subject to ALARP.

* If the unavailability x range or (failure rate x range) is worse than the "Maximum Tolerable" target then the design is rejected.

To test for ALARP, using the Cost per Life saved principle, consider a potential design improvement whose cost is $£_{improvement}$ and compute:

CPL (Cost per Life Saved) =

$£_{improvement}$ / [Change of failure rate (pa) x Number of lives saved x 40 years]

(Note: the use of 40 years is a common benchmark based on typical system life). If this cost per life saved exceeds the currently accepted figure then the improvement is not justified. If it is less than or equal to the cost per life saved then the improvement is justified. Other improvements should be similarly tested.

The ethical question arises as to the value of cost per life saved to be used. Organisations are reluctant to state grossly disproportionate levels of CPL. Currently figures in the range £500,000 to £2,000,000 are common. Where a risk has the potential for multiple fatalities then higher sums may be used.

However a value must be chosen, by the operator, for each assessment. The value selected must take account of any uncertainty inherent in the assessment and may have to take account of any company specific issues such as the number of similar installations. The greater the potential number of lives lost and the greater the aversion to the scenario then the larger is the choice of the cost per life saved criteria. Values which have been quoted include:

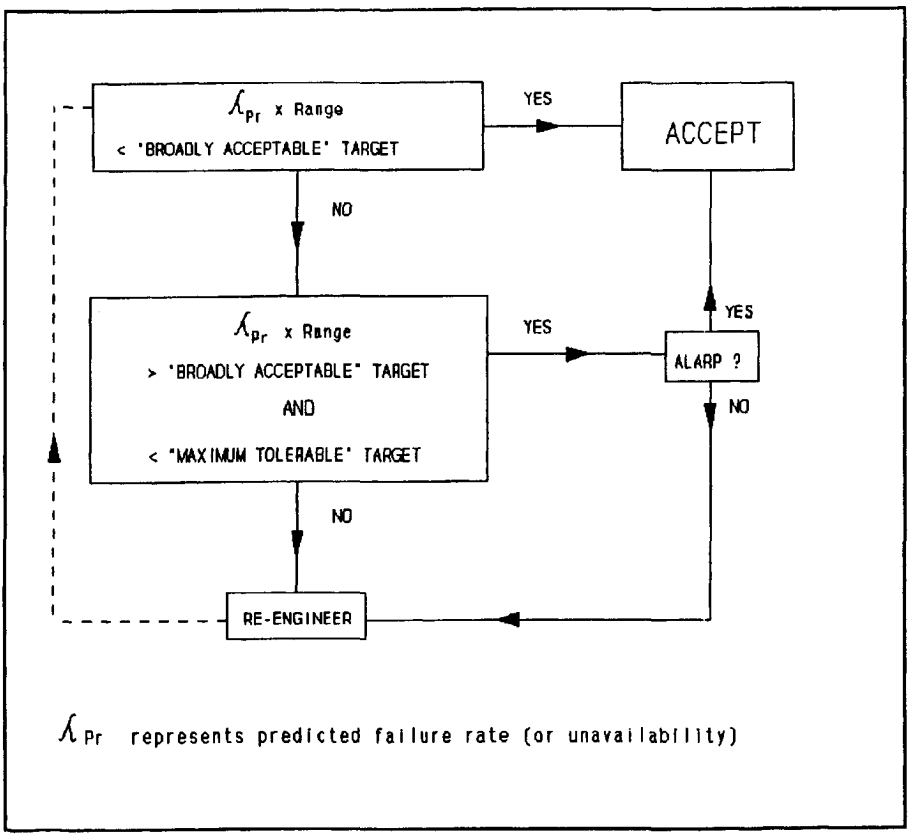
Approximately £1,000,000 by HSE, 1999 where there is a recognised scenario, a voluntary aspect to the exposure, a sense of having personal control, small numbers of casualties per incident. An example would be PASSENGER ROAD TRANSPORT.

Approximately £2,000,000-£4,000,000 by the HSE, 1991 where the risk is not under personal control and therefore an involuntary risk. An example would be TRANSPORT OF DANGEROUS GOODS.

Approximately £5,000,000-£15,000,000, mooted in the press, where there are large numbers of fatalities, there is uncertainty as to the frequency and no personal control by the victim. An example would be MULTIPLE RAIL PASSENGER FATALITIES.

This is a controversial area and figures can be subject to rapid revision in the light of catastrophic incidents and subsequent media publicity. A recent example, of the demand for automatic train protection in the UK, involves approximately £14,000,000 per life saved. This is despite the earlier rail industry practice of regarding £2,000,000 as an appropriate figure (Hale et al, 1998).

Figure 4.1 - Comparison of predicted RAMS ranges with targets



As an example let the "Broadly Acceptable" target be a probability of failure on demand of 2×10^{-3} and the "Maximum Tolerable" level be 2×10^{-2}.

If the predicted unavailability, using industry specific data, is 1.0×10^{-3} then, from Appendix 3 and section 3.3, the 90% confidence range is 5:1. Therefore, we are 90% confident that the eventual unavailability will be between $5 \times 1.0 \times 10^{-3} = 5.0 \times 10^{-3}$ and $1/5 \times 1.0 \times 10^{-3} = 2.0 \times 10^{-4}$. The pessimistic limit does not satisfy the initial acceptance criteria (2×10^{-3}) but, on the other hand, it does not fall outside the "Maximum Tolerable" limit (2×10^{-2}). Thus, the design would be acceptable subject to satisfying the requirements of ALARP.

4.3 COST RELATED TARGETS

On the other hand, a RAM target may be the result of considering life-cycle costs, as opposed to safety. In these cases the target is usually stated as a single figure rather than the ALARP range described above.

However, a similar comparison to Figure 4.1 can be performed to assess the RAM prediction against the target.

Use the pessimistic availability (or failure rate) to test the effect of any potential design alternative whose cost is $£_{change}$. Compute the cost of the enhanced or reduced RAM per annum.

Then compare the capital cost of the proposed design alternative ($£_{change}$) with the discounted annual savings to determine its justification.

4.4 THE COSTS OF APPLYING THE RAMS PREDICTION METHOD

The cost of carrying out RAMS-cycle prediction activities, in particular reliability prediction, will usually be small compared with the potential safety or life-cycle cost savings addressed in the previous two sections. The following examples are based on the author's experience.

A cost justification may be requested for carrying out these RAMS prediction activities. In which case the costs of the following activities should be estimated, for comparison with the predicted savings. RAMS prediction costs (ie resources) will depend upon the complexity of the equipment. The following two budgetary

examples, expressing RAMS prediction costs as a percentage of the total development and procurement costs, are given:

> **Example A)** A simple safety sub-system consisting of a duplicated "shut down" or "fire detection" system with up to 100 inputs and outputs, including power supplies, annunciation and operator interfaces.
>
> **Example B)** A single stream plant process (eg chain of gas compression, chain of H_2S removal reactors and vessels) and associated pumps and valves (up to 20) and the associated instrumentation (up to 50 pressure, flow and temperature transmitters).

The following resource budgets are based on the author's personal records of 40 RAMS prediction tasks in the gas industry, in the 1990s.

	Mandays for **A)**	Mandays for **B)**
Figure 1.2 loop [1]: Feasibility RAMS prediction. This will consist of a simple block diagram prediction with the vessels or electronic controllers treated as units.	4	6
Figure 1.2 loop [2]: Conceptual design prediction. Similar to [1] but with more precise input/output quantities.	10	13
Figure 1.2 loop [3]: Detailed prediction Includes FMECA at circuit level for 75% of the units, attention to common cause, human error and proof-test intervals.	6	18

	Mandays for **A)**	Mandays for **B)**
Figure 1.2 loop [4]: RAMS testing. This refers to preparing sub-system and system test plans and analysis of test data rather then the actual test effort.	2	10
Figure 1.2 loop [5]: Acceptance testing This refers to preparing test plans and analysis of test data rather then the actual test effort.	2	6
Figure 1.2 loop [6]: First year, reliability growth reviews. This is a form of design review using field data.	1	2
Figure 1.2 loop [7]: Subsequent reliability growth, data analysis.	2	3
Figure 1.2 loop [9]: First year, field data analysis. Not including effort for field data recording but analysis of field returns.	2	8
Figure 1.2 loop [10]: RCM planning This includes identification of major components, establishing RAMS data for them, calculation of optimum discard, spares and proof-test intervals (chapter 7).	3	8

	Mandays for A)	Mandays for B)
OVERALL TOTALS	32	74
COST @ £250/manday	£8K	£18.5K
TYPICAL PROJECT COST (DESIGN AND PROCURE)	£150K	£600K
RAMS cost as % of TOTAL PROJECT COST	5.3%	3.1%

4.5 CONCLUSIONS AND RECOMMENDATIONS

Life-cycle costs (for both safety and unavailability) can be orders greater than the above quoted project costs. Thus, even relatively small enhancements in MTBF/ Availability will easily lead to costs far in excess of the example expenditures quoted above.

The use of confidence ranges (from chapter 3) provides a more realistic method of comparing predicted reliability and or safety with the targets set. The method should be used for expressing RAMS predictions and can be adapted, by use of Appendix 3, to accommodate confidence levels required by the user.

The cost of carrying out RAMS prediction activities is in the order of 3% to 5% of total project cost. Although definitive records are not readily available it is credible that the assessment process, with its associated comparison of alternatives and proposed modifications, will lead to savings which exceed this outlay. In the above examples, credible results of the RAM studies might be:

A) ESD System:
The unavailability might typically be improved from 0.001 to 0.0005 as a result of the RAM study. Spurious shutdown, resulting from failure of the ESD, might typically be £500,000 per day for a small gas production platform. Thus, the **£8,000** expenditure on RAM saves:

£500,000 x (0.001-0.0005) x 365 = **£91,000 per annum**

B) H_2S System:
The availability might typically be improved from 0.95 to 0.98 as a result of the RAM study. Loss of throughput, resulting from failure, might typically cost £5,000 per day. Thus, the **£18,500** expenditure on RAM saves:

£5,000 x (0.98-0.95) x 365 = **£55,000 per annum**

Non RAMS-specialist engineers should receive training (outlined in Appendix 8) in RAMS techniques in order that they acquire sufficient competence to understand the benefits of those activities. The IEE competency guidelines document, 1999 offers a framework for assessing such competencies.

CHAPTER 5

RELIABILITY/AVAILABILITY MODELLING

5.1 SUMMARY

In view of the accuracy limitations discussed in chapter 3, there is a need for simple RAMS modelling equations. To evaluate redundant systems with repair, existing practice uses MARKOV models which provide equations for availability of systems with repair. Figure 2.1 shows where this chapter fits into the overall thesis.

This chapter develops simplified MARKOV solutions for redundancy with revealed failures and verifies the adequacy of their accuracy. It also provides similar models for redundancy involving unrevealed failures.

5.2 SIMPLIFIED MARKOV MODELS (REVEALED FAILURES)

This chapter addresses coincident independent failures, for redundant systems with repair. Coincident independent failures refers to any redundant configuration whereby it is assumed that more than one independent failure is needed for the failure of that configuration. Common cause (ie dependent) failures which defeat the benefit of redundancy are addressed in chapter 6.

Coincident independent failure modelling can be carried out in 2 ways:

- Markov modelling based on system state diagrams (Figure 5.1).
- Simulation models.

Simulation is a useful technique when the limitations of constant failure rate and repair rate (the distribution of repair times is often logNormal) cannot be enjoyed and where complex modelling allows for operational factors such as make-up of lost throughput within a specified time. However, the majority of RAMS predictions involve the assumption of constant failure rate and repair time, often because data are sufficiently limited to make this the only realistic assumption. In these cases simulation can be unnecessarily sophisticated and simple Markov models will suffice.

Markov modelling involves evaluating system state diagrams such as are shown in Figure 5.1. Typical system states would be "no subsystems failed", "one subsystem failed" etc. The resulting availability equations contain several terms and are developed in chapter 8 of Smith D J, 1997 and shown in Appendix 7 of this thesis.

Given the realistic and frequent assumption that failure rate is much less than repair rate [ie the reciprocal of mean down time], then many of the terms in the MARKOV equation are insignificant, particularly in the RAMS application where failure rate data are, as already discussed, imprecise.

This chapter summarises a set of simplified Markov models from Smith D J, 1997 for modelling random coincident failures where down time is small compared with MTBF.

Simplification of the models is justified for two reasons:

- The inaccuracy of the approximation is small having regard to the imprecision of the failure data. This is demonstrated later in this chapter.

- The rate of common cause failures (CCF) is considerably greater than that of coincident independent failures because a proportion of CCF (typically 10% as addressed in chapter 6) is likely to be far greater than the random coincidence predicted by the MARKOV models. Unnecessarily precise MARKOV models are therefore not justified.

System state diagrams (Figure 5.1) are constructed to model systems having redundant units and subject to various repair times and numbers of repair crews. The number of repair crews available to react to a unit failure will affect the result. Both scenarios can be found in practice although it is more common to find only a single crew being available.

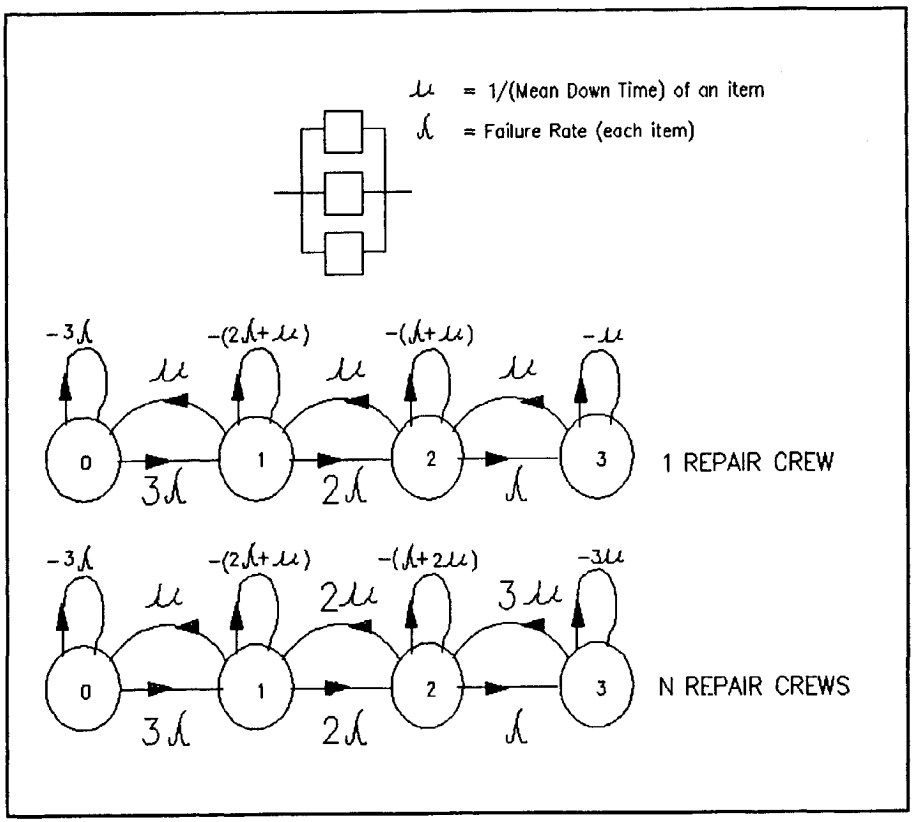
The state diagrams are algebraically evaluated to provide equations which are used to calculate system RAMS, based on the constant failure rates and fixed down times of its sub-systems.

Two state diagrams for a triplicated system are shown in Figure 5.1. The states, modelled from left to right, are 'no units failed' (0), 'one unit failed' (1), 'two units failed' (2) and 'three units failed' (3). In the case of full redundancy [1 out of 3] then the 3 left hand states (0,1,2) represent "system success". For [2 out of 3 redundancy] then the 2 left hand states (0,1) represent "system success". The first diagram assumes a single repair crew to be shared amongst the unit failures. The second [lower diagram] allows for sufficient repair crews so that all unit failures receive immediate attention.

The Tables of equations (Tables 5.2.1 to 5.2.4) cover the redundant configurations of the most widely used system architectures. Single and multiple repair crew scenarios are addressed, and the approximation that MTBF > > Mean Down Time is used. These equations are also shown in chapter 8 of Smith D J, 1997.

Appendix 7 shows that the first order MARKOV process for modelling redundant systems, with repair of revealed failures, gives $2\lambda^2/ (3\lambda + 1/MDT)$ as the system failure rate of a duplicated system whose units have λ failure rate and MDT down time. This simplifies to $2 \lambda^2$ MDT if $\lambda << 1/MDT$.

Figure 5.1 - State diagrams for a triplicated system



The following Tables of simplified equations are from Smith D J, 1997. Each unit is assumed to have a failure rate λ and a Mean Down Time MDT.

Table 5.2.1 - System failure rates with 1 repair crew

Number of Units				
1	λ			
2	$2\lambda^2$ MDT	2λ		
3	$6\lambda^3MDT^2$	$6\lambda^2MDT$	3λ	
4	$24\lambda^4MDT^3$	$24\lambda^3MDT^2$	$12\lambda^2MDT$	4λ
	1	2	3	4
	Number	Required	to	Operate

Table 5.2.2 - System unavailabilities with 1 repair crew

Number of Units				
1	λMDT			
2	$2\lambda^2$ MDT^2	$2\lambda MDT$		
3	$6\lambda^3MDT^3$	$6\lambda^2MDT^2$	$3\lambda MDT$	
4	$24\lambda^4MDT^4$	$24\lambda^3MDT^3$	$12\lambda^2MDT^2$	$4\lambda MDT$
	1	2	3	4
	Number	Required	to	Operate

Table 5.2.3 - System failure rates with n repair crews

Number of Units				
1	λ			
2	$2\lambda^2$ MDT	2λ		
3	$3\lambda^3MDT^2$	$6\lambda^2MDT$	3λ	
4	$4\lambda^4MDT^3$	$12\lambda^3MDT^2$	$12\lambda^2MDT$	4λ
	1	2	3	4
	Number	Required	to	Operate

Table 5.2.4 - System unavailabilities with n repair crews

Number of Units				
1	λMDT			
2	λ^2 MDT^2	$2\lambda MDT$		
3	λ^3MDT^3	$3\lambda^2MDT^2$	$3\lambda MDT$	
4	λ^4MDT^4	$4\lambda^3MDT^3$	$6\lambda^2MDT^2$	$4\lambda MDT$
	1	2	3	4
	Number	Required	to	Operate

Each of the expressions in the above tables has been compared with the full (unsimplified) algebraic MARKOV expressions. The ratios are expressed in Table 5.2.5 which shows the inaccuracies (calculated as ratios of the simplified to the unsimplified equations) up to "3 out of 4" redundancy (ie quadruplication) and for values of λ MDT (ie probability of failure on demand) from 0.00001 - 0.1.

Considering "1 out of 2" redundancy for example, the inaccuracy of the simple equation $2\lambda^2$ MDT is $[2\lambda^2 \text{ MDT}] / [2\lambda^2/ (3\lambda + 1/\text{MDT})] = 3\lambda \text{ MDT} + 1$. Expressed in percentage terms this inaccuracy is $100(3\lambda \text{ MDT})$. So, for a λ MDT of 0.1 the inaccuracy is 3%.

Looking at the graphs, in Figure 5.2, it can be seen that, for both repair scenarios, an inaccuracy of better than 30% applies for all cases where λ MDT is less than about 0.02.

In other words, for a failure rate of 100 per million hours the down time could be as high as 200 hours. Alternatively for a down time of 4000 hours the failure rate could be as great as 5 per million hours. Hence, having regard to the accuracy limitations outlined in chapter 3, use of the simplified expressions is justified.

It should be noted that where λ MDT is small it approximates to the unavailability which is $[\lambda \text{ MDT}]/[1+ \lambda \text{ MDT}]$.

Table 5.2.5 - Inaccuracies for λ and unavailability

% Inaccuracy of the "1 crew" models

λxMDT	"1 oo 2"	"1 oo 3"	"1 oo 4"	"2 oo 3"	"2 oo 4"	"3 oo 4"
0.00001	0.003	0.004	0.005	0.005	0.006	0.007
0.0001	0.03	0.04	0.05	0.05	0.06	0.07
0.001	0.3	0.4	0.5	0.5	0.6	0.7
0.01	3	4	5	5	6	7
0.1	30	50	70	50	90	70

% Inaccuracy of the "n crews" models

λxMDT	"1 oo 2"	"1 oo 3"	"1 oo 4"	"2 oo 3"	"2 oo 4"	"3 oo 4"
0.00001	0.003	0.0035	0.0043	0.005	0.005	0.007
0.0001	0.03	0.035	0.043	0.05	0.05	0.07
0.001	0.3	0.35	0.43	0.5	0.5	0.7
0.01	3	4	4	5	5	7
0.1	30	40	50	50	60	70

Figures 5.2(i) and (ii) present these results in graphical form.

Figure 5.2(i) - Inaccuracy, 1 repair crew

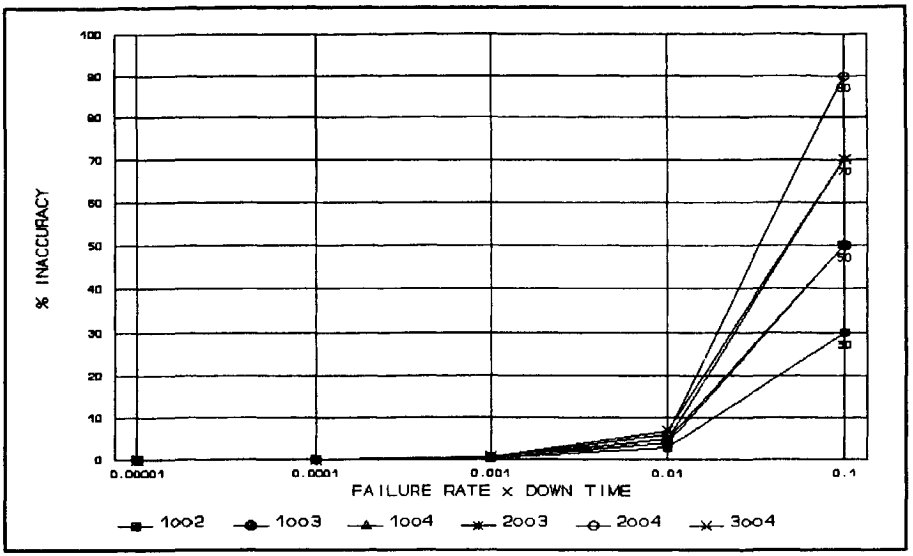
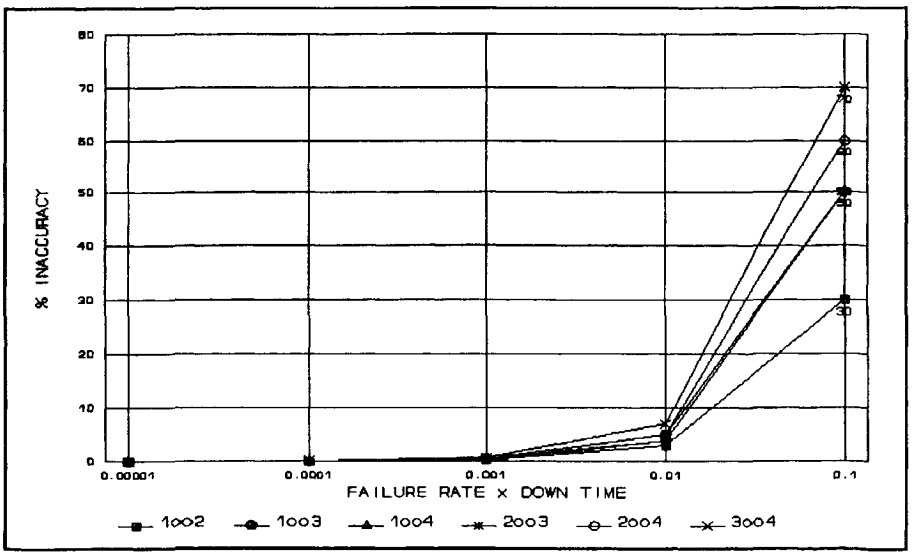


Figure 5.2(ii) - Inaccuracy, n repair crews



5.3 RAMS PREDICTION MODELS FOR UNREVEALED FAILURES

Unrevealed failures will eventually be revealed by some form of auto-test or proof-test. Whether manually scheduled or automatically initiated (eg auto-test using programmable logic) there will be a proof-test interval, T.

In chapter 8 of Smith D J, 1997 it is shown how the actual time during which a redundant unit remains failed is related, according to the level of redundancy, to the proof-test interval T. This issue is also addressed in O'Connor P D T, 1991. A single repair crew scenario is assumed to be the most applicable in this case since proof-test is usually carried out on one redundant item at a time. In any case it is assumed that only one crew would be available to rectify any defects found. The following expressions are developed in chapter 8 of Smith D J, 1997.

Table 5.3.1 provides equations of failure rates for different redundancy options.

Table 5.3.2 provides the (more useful) equations of unavailability.

Table 5.3.1 - Failure rates

Number of units			
2	λ^2T		
3	λ^3T^2	$3\lambda^2T$	
4	λ^4T^3	$4\lambda^3T^2$	$6\lambda^2T$
	1	2	3
	Number	Required to	Operate

Table 5.3.2 - Unavailabilities

Number of units			
2	$\lambda^2T^2/3$		
3	$\lambda^3T^3/4$	λ^2T^2	
4	$\lambda^4T^4/5$	λ^3T^3	$2\lambda^2T^2$
	1	2	3
	Number	Required to	Operate

In the following example, assume that one unit is required to operate in a redundant architecture involving two units. The failures are unrevealed and subject to a proof-test interval of one year. If the failure rate of each unit is 10 per million hours then the unavailability is calculated as:

$$\lambda^2T^2/3 = (10 \times 10^{-6})^2 \times (8760)^2 \ / \ 3$$
$$= 2.6 \times 10^{-3}$$

5.4 MEAN DOWN TIME OF SYSTEMS

For revealed failures the MDT consists of the active mean time to repair (MTTR) + any logistic delays (eg travel, site access, spares procurement, administration).

For unrevealed failures the MDT is related to the proof-test interval (referred to as T in 5.3 above) + the active MTTR + any logistic delays. The way in which failure is defined determines, to some extent, what is included in the down time. If the unavailability of a process is confined to failures whilst production is in progress then outage due to scheduled preventive maintenance is not included in the definition of failure. However the definition of dormant failures of redundant units affects the overall unavailability (as calculated by the equations in section 5.3).

Although not within the scope of this thesis, the need arises to estimate the active repair time when quantifying a RAMS prediction model. If empirical repair time data is not available then the estimation method known as "Procedure 3" in US MIL HANDBOOK 472, 1966 is recommended. This is described in detail in chapter 14 of Smith D J, 1997 and consists of a checklist scoring methodology with a regression model to estimate the active MTTR.

5.5 QUANTIFICATION OF HUMAN ERROR

In addition to the random coincident hardware failures (chapter 5), and their associated dependent failures (chapter 6), it is frequently necessary to include human error in a RAMS prediction model (eg fault tree).

It can be argued that the majority of well-known major incidents, such as Three Mile Island, Bhopal, Chernobyl, Zeebrugge, Clapham and Paddington are related to the interaction of complex systems with human beings. In short, the implication is that human error was involved, to a greater or lesser extent, in these and similar incidents. For some years there has been an interest in modelling these factors so that quantified reliability and risk assessments can take account of the contribution of human error to the system failure.

Although not within the scope of this thesis, which is based on work relating to hardware failures, the topic is sufficiently important to be briefly addressed here. As technical systems are becoming more and more reliable, the relative contribution of human factors related failures is growing.

Estimation methods derived from other publications are briefly described, by the author, in chapter 8 of Smith D J, 1997 and by UKAEA SRDA-R11, 1995. Work continues in this area as outlined in Busse D, 1998 PhD report.

Human error rate data for various forms of activity, particularly in operations and maintenance, are needed. In the early 1960s there were attempts, by UKAEA, to develop a database of human error rates and these led to models of human error whereby rates could be estimated by assessing relevant factors such as stress, training and complexity. These human error probabilities include not only simple failure to carry out a given task, but diagnostic tasks where errors in reasoning, as well as action, are involved. There is not a great deal of data available due to the following problems:

- Low probabilities require large amounts of experience in order for meaningful statistics to emerge.
- Data collection concentrates on recording the event rather than analysing the causes.
- Many large organizations have not been prepared to commit the necessary resources to collect data.

More recently, interest has developed in exploring the underlying reasons, as well as probabilities, of human error. As a result there are currently several models, each developed by separate groups of analysts working in this field.

The better known are HEART (Human Error Assessment and Reduction Technique), THERP (Technique for Human Error Rate Prediction) and TESEO (Empirical Technique To Estimate Operator Errors) and these are described in UKAEA SRDA-R11, 1995.

5.6 SOFTWARE ERRORS

This thesis addresses the quantification of hardware related failures. However, RAMS assessment must also address software faults which might propagate to become system failures.

This requires a quantitative approach to the control of software design and is addressed elsewhere. The author has developed software quality assessment checklists in Smith D J, 1995 (Achieving Quality Software).

5.7 CONCLUSIONS AND RECOMMENDATIONS

Use of the simplified Markov expressions, summarised in this chapter, is justified having regard to the relationship between predicted and achieved reliability as discussed in chapter 3.

The prediction models for unrevealed failures provide similar expressions for modelling those applications where repair of failed redundant units is subject to a regular proof-test.

Human factors are becoming more dominant in system reliability and should be the subject of further study.

CHAPTER 6

COMMON CAUSE (DEPENDENT) FAILURE

6.1 SUMMARY

This chapter describes the current approach to the modelling and quantification of common cause failures. It then describes a more advanced model which takes account of diagnostic intervals (mooted by Walls et al, 1989) and addressed in IEC standard 61508, 1999. The author's model has been calibrated against field data to a far greater extent than previous models. Figure 2.1 shows where this chapter fits into the overall thesis.

Common cause failures often dominate the unreliability of redundant systems by virtue of defeating the random coincident failure feature of redundant protection.

This sensitivity of system failure to CCF places emphasis on the credibility of CCF estimation and thus justifies efforts to improve the models.

6.2 TYPES OF CCF MODEL

Whereas simple models of redundancy (as developed in chapter 5) assume that failures are both random and independent, common cause failure (CCF) modelling takes account of failures which are linked, due to some dependency, and therefore occur simultaneously or, at least, within a sufficiently short interval as to be perceived as simultaneous.

Two examples are:

a) the presence of water vapour in gas causing both valves in twin streams to seize due to icing. In this case the interval between the two failures might be in the order of days. However, if the proof-test interval for this dormant failure is two weeks then the two failures will, to all intents and purposes, be simultaneous.

b) inadequately rated rectifying diodes on identical twin printed circuit boards failing simultaneously due to a voltage transient.

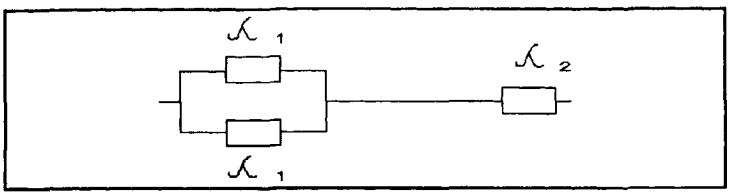
The term common mode failure (CMF) is also frequently used and a brief explanation of the difference between CMF and CCF is therefore necessary. CMF refers to coincident failures of the same mode, in other words failures which have an identical

appearance or effect. On the other hand, the term CCF implies that the failures have the same underlying cause. It is possible (although infrequent) for two CMFs not to have a common cause and, conversely, for two CCFs not to manifest themselves in the same mode. In practice the difference is slight and unlikely to affect the data, which rarely contain sufficient detail to justify any difference in the modelling. Since the models addressed in this chapter involve assessing defences against the CAUSES of coincident failure CCF will be used throughout. Early work on CCF modelling is described by Edwards et al, 1979. Summaries of methods and their development are given by Wray A M, 1996 and Hanks B J, 1998.

The current approaches to modelling this phenomenon are described with references to their sources as follows:

a) The simple BETA (β) model, which assumes that a fixed proportion (β) of the failures arise from a common cause. The estimation of (β) is assessed according to the system. The method is based on very limited historical data.

Figure 6.1 - Reliability block diagrams for CCF



In Figure 6.1 (λ_1) is the failure rate of a single redundant unit and (λ_2) is the common cause failure rate such that (λ_2) = $\beta(\lambda_1)$ for the simple BETA model and also the Partial BETA model, in b) below.

b) The PARTIAL BETA (β) model, also assumes that a fixed proportion (β) of the failures arise from a common cause. It is more sophisticated than the simple BETA model in that the contributions to (β) are split into groups of design and operating features which are believed to influence the degree of CCF. Thus the BETA factor is made up by adding together the contributions from each of a number of factors within each group. In traditional Partial Beta models the following groups of factors can be found in UKAEA UPM 3.1, 1996; Edwards et al, 1979; Wray A M, 1996; Rutledge et al, 1995 and others.

These factors are further developed in this thesis and are generally listed as:

- Similarity (Diversity between redundant units reduces CCF)
- Separation (Physical distance and barriers reduce CCF)
- Complexity (Simpler equipment is less prone to CCF)
- Analysis (Previous FMEA and field data analysis will have reduced CCF)
- Procedures (Control of modifications and of maintenance activities can reduce CCF)
- Training (Designers and maintainers can help to reduce CCF by understanding root causes)
- Control (Environmental controls can reduce susceptibility to CCF, eg weather proofing of duplicated instruments)
- Tests (Environmental tests can remove CCF prone features of the design, eg emc testing)

The PARTIAL BETA model can also be represented by the reliability block diagram shown in Figure 6.1. The UKAEA UPM 3.1 approach is the most widely used method at present and was developed from an earlier model Humphries R, 1987. β is assumed to be made up of a number of partial β's, each contributed to by the various groups of causes of CCF. β is then estimated by reviewing and scoring each of the contributing factors (eg diversity, separation).

c) The System Cut-off model, described by Wray A M, 1996 offers a single failure rate for all failures (independent and dependent both combined). It argues that the dependent failure rate dominates the coincident failures. Again, the choice is affected by system features such as diversity and separation. It is the least sophisticated of the models in that it does not base the estimate of system failure rate on the failure rate of the redundant units.

d) The Boundary model, also described by Wray A M, 1996, uses two limits of failure rate. Namely, limit A which assumes all failures are common cause (λ_u) and limit B which assumes all failures are random (λ_l). The system failure rate is computed using a model of the following type:

$$\lambda = (\lambda_l^n \times \lambda_u)^{1/(n+1)}$$

where the value of n is chosen according to the degree of diversity between the redundant units. n is an integer, normally from 0-4, which increases with the level of diversity between redundant units. It is chosen in an arbitrary and subjective way. This method is a mathematical device, having no foundation in empirical data, which relies on a subjective assessment of the value of n. It provides no traceable link (as does the Partial BETA method) between the assessment of n and the perceived causes of CCF.

e) The Multiple Greek Letter model (Wray A M, 1996) is similar to the BETA model but assumes that the BETA ratio varies according to the number of coincident failures. Thus two coincident failures and three coincident failures would have different BETA's. However, in view of the inaccuracy inherent in the approximate nature of these models it is considered to be too sophisticated and cannot therefore be supported by field data until more detailed information is available.

Further comparison of these models is offered by Edwards et al, 1979 and Wray A M, 1996. All the models are, in their nature, approximate but, because CCF failure rates (which are in the order of $\beta \times \lambda$) are much greater than the coincident independent failures (in the order of λ^n), then greater precision in estimating CCF is needed than for the redundant coincident models provided in (chapter 5). Balbir et al, 1988 provide theoretical comparisons of CCF models for different redundant architectures.

6.3 THE BETAPLUS MODEL

The Partial BETA model is chosen for further development in this thesis because:

- it is objective and maximises traceability in the estimation of BETA. In other words the choice of checklist scores (shown in the next section of this chapter) when assessing the design, can be recorded and reviewed.
- it is possible for any user of the model to develop the checklists further to take account of any relevant failure causal factors that may be perceived.
- it is possible to calibrate the model against actual failure rates, albeit with very limited data.
- there is a credible relationship between the checklists and the system features being analysed. The method is thus likely to be acceptable to the non-specialist.
- the additive scoring method allows the partial contributors to β to be weighted separately.
- the β method acknowledges a direct relationship between (λ_2) and (λ_1) as depicted in Figure 6.1.
- it permits an assumed "non-linearity" between the value of β and the scoring over the range of β. The reasoning for this is developed throughout this chapter.

The earlier Partial BETA model, described in 6.2b above, is further developed by the author to include the following enhancements:

a) CATEGORIES OF FACTORS:
Whereas existing methods rely on a single subjective judgement of score in each category, the BETAPLUS method provides specific design and operational related questions to be answered in each category. These were developed by the author in Smith D J, 1997 in consultation with the UK HSE for the then draft IEC 61508 standard. Specific questions are individually scored, in each category (ie separation, diversity, complexity, assessment, procedures, competence, environmental control, environmental test) thereby permitting an assessment of the design and its operating and environmental factors. Current BETA methods (eg UPM 3.1, 1996) only involve a single scoring of each category (eg a single subjective score for diversity).

b) SCORING:
The maximum score for each question has been weighted by calibrating the results of assessments against known field operational data - see section 6.5. Programmable and non-programmable equipment have been accorded slightly different checklists in order to reflect the equipment types (see section 6.3.1).

c) TAKING ACCOUNT OF DIAGNOSTIC COVERAGE:
Walls et al, 1989 also note that CCF are not always simultaneous and Young-Ju, 1997 postulates a load sharing underlying cause. However, data suggest that CCF is more dependent on external influences as is reflected in the checklists. Since CCF are not simultaneous, an increase in auto-test or proof-test frequency will reduce CCF since they may not occur at precisely the same moment. Thus, more frequent testing will prevent some CCF. This is shown to be true during the calibration of the method, described in section 6.5. Some defences will protect against the type of failure which increased proof-test might identify (for example failures in parallel channels where diversity would be beneficial). Other defences will protect against the type of failure which increased proof-test is unlikely to identify (for example failures prevented as a result of long term experience with the type of equipment). This needs to be reflected in the model.

d) SUB-DIVIDING THE CHECKLISTS ACCORDING TO THE EFFECT OF DIAGNOSTICS:
Two columns are used for the checklist scores. Column (A) contains the scores for those features of CCF protection which are perceived as being enhanced by an increase of diagnostic frequency (either proof-test or auto-test). Column (B), however, contains the scores for those features thought not to be enhanced by an improvement in diagnostic frequency. In some cases the score has been split between the two columns, where it is thought that some, but not all, aspects of the feature are affected. This split is intuitive and was made in conjunction with the HSE during the development of Smith D J, 1997 (T076).

e) ESTABLISHING A MODEL:
It is necessary to propose a model in such a way as to allow the scoring to be modified by the frequency and coverage of diagnostic test. The (A) column scores are modified by multiplying by a factor (C) derived from diagnostic related considerations (6.3.2). This (C) score is based on the diagnostic frequency and coverage. (C) is in the range 1 to 3. BETA is then estimated from the following RAW SCORE total:

$$S = \text{RAW SCORE} = (\Sigma A \times C) + \Sigma B$$

It is assumed that the effect of the diagnostic score (C) on the effectiveness of the (A) features is linear. In other words each failure mode is assumed to be equally likely to be revealed by the diagnostics. Only more detailed data can establish if this is not a valid assumption.

f) NON-LINEARITY:
There are currently no CCF data to justify departing from the assumption (UKAEA UPM 3.1, 1996) that, as BETA decreases (ie improves), then successive improvements become proportionately harder to achieve. Thus the relationship of the BETA factor to the raw score [(ΣAxC) + ΣB] is assumed to be exponential and this non-linearity is reflected in the equation (in section 6.4) which translates the raw score into a BETA factor.

g) EQUIPMENT TYPE:
The scoring has been developed separately for programmable and non-programmable equipment, in order to reflect the slightly different criteria which apply to each type of equipment.

i) CALIBRATION:
The model is then calibrated against the author's field data (see section 6.5)

6.3.1 Checklists and scoring of the (A) and (B) factors in the model

The following scoring criteria have been developed as described above. To cover each of the categories (ie separation, diversity, complexity, assessment, procedures, competence, environmental control, environmental test) checklist questions have been assembled to reflect the likely features which defend against CCF. Initially, the maximum score for each question was allocated in such proportions as to reflect subjective judgements of their relative importance. The scores were then adjusted, as described in 6.5, to take account of the relative contributions to CCF in each area, as shown in the author's data and summarised in Tables 6.5.1 & 2. The score values have been weighted to calibrate the model against the data.

When addressing each question a score, less than the maximum of 100% may be entered. For example, in the first question, if the judgement is that only 50% of the cables are separated then 50% of the maximum scores (15 and 52) may be entered in each of the (A) and (B) columns (7.5 and 26).

The checklists are presented in two forms (6.3.1.1 and 6.3.1.2). The reason for this is that the questions applicable to programmable based equipments will be slightly different to those necessary for non-programmable items (eg field devices and instrumentation). The data against which this model is calibrated are similarly sub-divided in Table 6.5.2.

6.3.1.1 CHECKLIST AND SCORING for Equipment containing Programmable Electronics

(1) SEPARATION/SEGREGATION	A MAX SCORE	B MAX SCORE
Are all signal cables separated at all positions?	15	52
Are the programmable channels on separate printed circuit boards?	85	55
OR are the programmable channels in separate racks?	90	60
OR in separate rooms or buildings?	95	65
MAXIMUM SCORE	110	117

(2) DIVERSITY/REDUNDANCY	A MAX SCORE	B MAX SCORE
Do the channels employ diverse technologies?; 1 electronic + 1 mechanical/pneumatic	100	25
OR 1 electronic or CPU + 1 relay based	90	25
OR 1 CPU + 1 electronic hardwired	70	25
OR do identical channels employ enhanced voting? ie "M out of N" where N>M+1	40	25
OR N=M+1	30	20
Were the diverse channels developed from separate requirements from separate people with no communication between them?	20	-

Were the 2 design specifications separately audited against known hazards by separate people and were separate test methods and maintenance applied by separate people?	12	25
MAXIMUM SCORE	132	50

(3) COMPLEXITY/DESIGN/APPLICATION /MATURITY/EXPERIENCE	A MAX SCORE	B MAX SCORE
Does cross-connection between CPUs preclude the exchange of any information other than the diagnostics?	30	-
Is there > 5 years experience of the equipment in the particular environment?	-	10
Is the equipment simple < 5 PCBs per channel? **OR** < 100 lines of code **OR** < 5 ladder logic rungs **OR** < 50 I/O and < 5 safety functions?	-	20
Are I/O protected from over-voltage and over-current and rated > 2:1?	30	-
MAXIMUM SCORE	60	30

(4) ASSESSMENT/ANALYSIS and FEEDBACK of DATA	A MAX SCORE	B MAX SCORE
Has a combination of detailed FMEA, Fault Tree analysis and design review established potential CCFs in the electronics?	-	140
Is there documentary evidence that field failures are fully analysed with feedback to design?	-	70
MAXIMUM SCORE	-	210

(5) PROCEDURES/HUMAN INTERFACE	A MAX SCORE	B MAX SCORE
Is there a written system of work on site to ensure that failures are investigated and checked in other channels? (including degraded items which have not yet failed)	30	20
Is maintenance of diverse/redundant channels staggered at such an interval as to ensure that any proof-tests and cross-checks operate satisfactorily between the maintenance?	60	-
Do written maintenance procedures ensure that redundant separations as, for example, signal cables are separated from each other and from power cables and must not be re-routed?	15	25
Are modifications forbidden without full design analysis of CCF?	-	20
Is diverse equipment maintained by different staff?	15	20
MAXIMUM SCORE	120	85

(6) COMPETENCE/TRAINING/SAFETY CULTURE	A MAX SCORE	B MAX SCORE
Have designers been trained to understand CCF?	-	100
Have installers been trained to understand CCF?	-	50
Have maintainers been trained to understand CCF?	-	60
MAXIMUM SCORE	-	210

(7) ENVIRONMENTAL CONTROL	A MAX SCORE	B MAX SCORE
Is there limited personnel access?	40	50
Is there appropriate environmental control? (eg temperature, humidity)	40	50
MAXIMUM SCORE	80	100

(8) ENVIRONMENTAL TESTING	A MAX SCORE	B MAX SCORE
Has full EMC immunity or equivalent mechanical testing been conducted on prototypes and production units (using recognised standards)?	-	316
MAXIMUM SCORE	-	316

	A MAX SCORE	B MAX SCORE
TOTAL MAXIMUM SCORE	**502**	**1118**

6.3.1.2 CHECKLIST AND SCORING for non-Programmable Equipment

Only the first three categories have different questions as follows:

(1) SEPARATION/SEGREGATION	A MAX SCORE	B MAX SCORE
Are the sensors or actuators physically separated and at least 1 metre apart?	15	52
If the sensor/actuator has some intermediate electronics or pneumatics, are the channels on separate PCBs and screened?	65	35
OR if the sensor/actuator has some intermediate electronics or pneumatics, are the channels indoors in separate racks or rooms?	95	65
MAXIMUM SCORE	110	117

(2) DIVERSITY/REDUNDANCY	A MAX SCORE	B MAX SCORE
Do the redundant units employ different technologies?; eg 1 electronic or programmable + 1 mechanical/pneumatic	100	25
OR 1 electronic, 1 relay based	90	25

OR 1 PE, 1 electronic hardwired	70	25
OR do the devices employ "M out of N" voting where; N > M+1	40	25
OR N=M+1	30	20
Were separate test methods and maintenance applied by separate people?	32	52
MAXIMUM SCORE	132	50

(3) COMPLEXITY/DESIGN/APPLICATION /MATURITY/EXPERIENCE	A MAX SCORE	B MAX SCORE
Does cross-connection preclude the exchange of any information other than the diagnostics?	30	-
Is there > 5 years experience of the equipment in the particular environment?	-	10
Is the equipment simple eg non programmable type sensor or single actuator field device?	-	20
Are devices protected from over-voltage and over-current and rated > 2:1 or mechanical equivalent?	30	-
MAXIMUM SCORE	60	30

(4) ASSESSMENT/ANALYSIS and FEEDBACK OF DATA

As for Programmable Electronics (see 6.3.1.1)

(5) PROCEDURES/HUMAN INTERFACE

As for Programmable Electronics (see 6.3.1.1)

(6) COMPETENCE/TRAINING/SAFETY CULTURE

As for Programmable Electronics (see 6.3.1.1)

(7) ENVIRONMENTAL CONTROL

As for Programmable Electronics (see 6.3.1.1)

(8) ENVIRONMENTAL TESTING

As for Programmable Electronics (see 6.3.1.1)

	A MAX SCORE	B MAX SCORE
TOTAL MAXIMUM RAW SCORE (Both programmable and non-programmable lists)	**502**	**1118**

6.3.2 Assessment of the diagnostic interval factor (C)

In order to establish the (C) score it is necessary to address the effect of the frequency and coverage of proof-test or auto-test. In the following table the diagnostic coverage, expressed as a percentage, is an estimate of the proportion of failures which would be detected by the proof-test or auto-test. This can be estimated by judgement or, more formally, by applying FMEA at the component level to decide whether each failure would be revealed by the diagnostics.

The diagnostic interval is shown for each of the two (programmable and non-programmable) assessment lists. The (C) values have been chosen to cover the range 1-3 in order to construct a model which caters for the known range of BETA values.

For Programmable Electronics

	Interval < 1 min	Interval 1-5 mins	Interval 5-10 mins	Interval > 10 mins
Diagnostic Coverage				
98%	3	2.5	2	1
90%	2.5	2	1.5	1
60%	2	1.5	1	1

For Sensors & Actuators

	Interval < 2 hrs	Interval 2hrs - 2days	Interval 2days-1week	Interval > 1 week
Diagnostic Coverage				
98%	3	2.5	2	1
90%	2.5	2	1.5	1
60%	2	1.5	1	1

A score of C > 1 may only be proposed if the resulting action, initiated by the diagnostics, has the effect of preventing or invalidating the effect of the subsequent CCF failure. For example, in some process industry equipment, even though the first of the CCF failures was diagnosed before the subsequent failure, there would nevertheless be insufficient time to take action to maintain the process. The subsequent (second) CCF failure would thus occur before effective action could be taken. Therefore, in such a case, the diagnostics would not help in defending against CCF and a C > 1 score cannot be proposed in the assessment.

6.3.3 Total RAW SCORE

Taking the proposed model given in 6.3e) on page 55 then, from the above scores, the maximum possible TOTAL RAW SCORE is:

$$\text{RAW SCORE} = S = (3 \times 502) + 1118 = 2624$$

6.4 THE PROPOSED MODEL

6.4.1 The exponential model

An exponential model is proposed to reflect the increasing difficulty in further reducing BETA as the score increases (as discussed in paragraph 6.3.f). This is reflected in the following equation:

$$\beta = 0.3 \exp(-3.4S/2624)$$

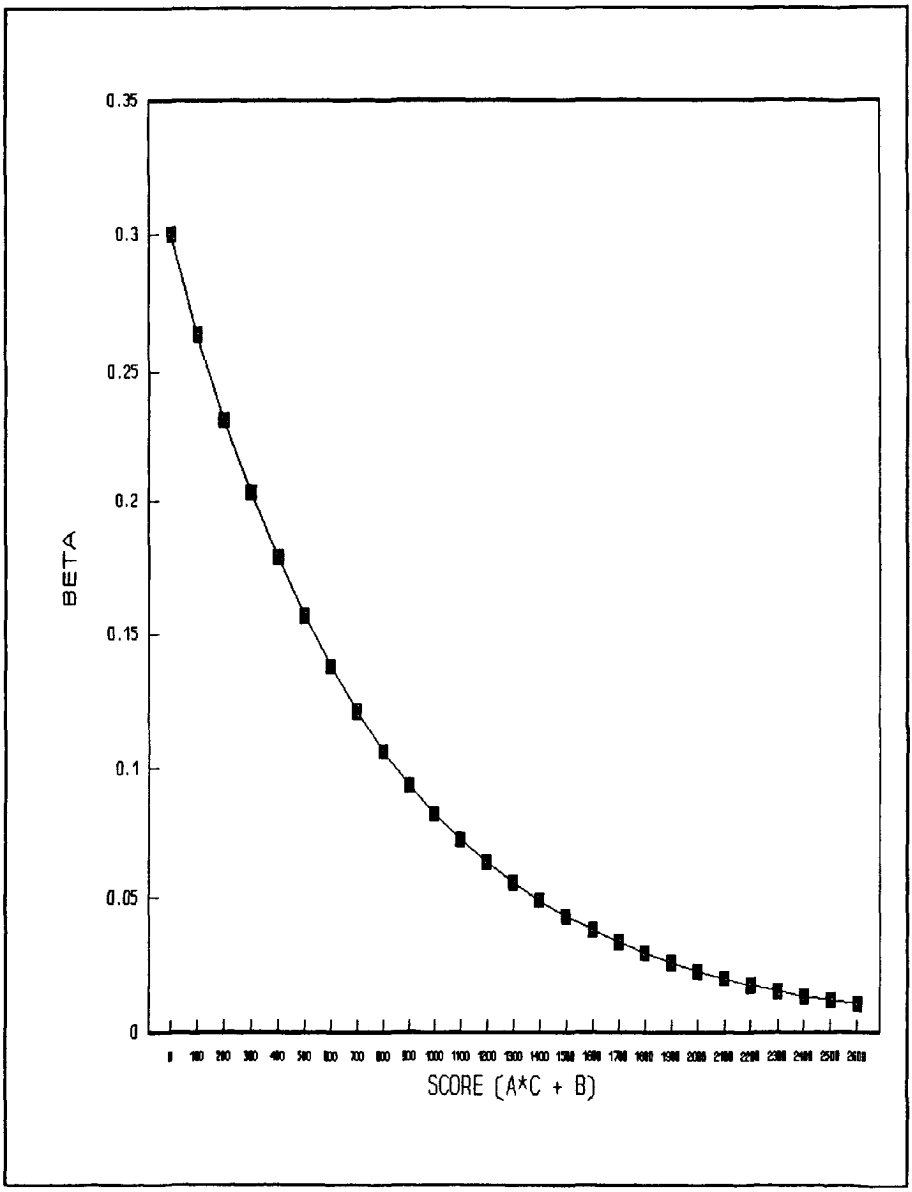
Since the value 2624 is the maximum possible score total (previous section) it is the denominator of the exponent in order for the maximum and minimum BETA values to correspond to the minimum and maximum scores.

The model is required to provide a maximum BETA of 0.3 and a minimum of 0.01, as explained in section 6.5, to fit the data available (section 6.5 & UKAEA UPM 3.1, 1996).

The value 3.4 in the numerator of the exponent, and the 0.3 coefficient, enable the model to satisfy the maximum and minimum limits of β=0.01 and β=0.3 corresponding to the maximum and minimum scores of 2624 and zero.

Figure 6.2 illustrates this exponential relationship between BETA and the TOTAL RAW SCORE.

Figure 6.2 - Beta against raw score



6.4.2 Some limiting scores

The following examples of limiting scores, which arise from the model, are of interest. They feature diversity and separation since these are often the most relevant design factors under consideration. Using the "programmable equipment" checklist,

Given a zero score for diversity (for identical redundancy with only "1 out of 2" voting) then the minimum achievable BETA is **1.9%.** (A=360; B=1058; C=3)

Given a zero score for diversity AND also given minimal auto-test then the minimum achievable BETA is **4.8%**.(A=360; B=1058; C=1)

Given a zero score for diversity AND a zero score for separation the minimum achievable BETA is **3.2%**. (A=260; B=951; C=3)

Given a zero score for diversity AND a zero score for separation AND minimal auto-test the minimum achievable BETA is **6.2%**. (A=260; B=951; C=1)

Given a C=1 score then the minimum achievable BETA is **3.7%**. (A=502; B=1118; C=1)

6.5 CALIBRATION OF THE MODEL

There are very few failure rate data which identify CCF. The small amount of earlier data are described in Edwards et al, 1979; Wray A M, 1996 and Rutledge et al, 1995. The author has liaised with UK Atomic Energy Reliability, UKHSE, Norwegian SINTEF, British Telecommunication and RAMS specialist colleagues in the UK (in aerospace, telecommunications, process industries). It is believed that no significant other data, currently available, apart from the author's data.

In order to calibrate the model the following are required :

- A maximum and a minimum limit for β: The currently accepted range is 1%-30% described in UKAEA UPM 3.1, 1996. This is based on USA Pressurised Water Reactor data. The author's gas industry data support this assumption (Table 6.5.2).

- A weighted contribution, from each factor, to the overall β: This was achieved by taking account of the relative proportion of each partial BETA factor used in UKAEA UPM 3.1, 1996 also modified by the author's gas industry data and shown in Table 6.5.1.

- An assumption on the modifying effect of the (C) factor: This is given a range from 1:1 to 3:1 in order to fit the scores to the maximum and minimum BETA values.

- Some calibration against actual field data: The author has derived common cause failure data from his research of failure data in the UK gas distribution industry. This has been used to calibrate the BETA factor, against 12 groups of equipment which are summarised into 5 groups in Table 6.5.2.

6.5.1 Weighting the categories using the field data

The weighted contribution of CCF, attributable to each of the categories of defence (diversity, separation etc), is assessed as follows. Table 6.5.1 compares the percentage obtained from UKAEA UPM 3.1, 1996 with the author's gas industry data. A compromise between the UPM 3.1 proportions and those indicated by the author's data has been made in weighting the (A) and (B) scores in the above model. The maximum scores in each category have been weighted by the figures shown in the right hand column of Table 6.5.1.

Table 6.5.1 - Table of % contributions to CCF

	UPM3.1 (0)	DJS1 (1)	DJS2 (2)	DJS3 (3)	β+ (4)
SEPARATION	16%	10%	7%	17%	17%
DIVERSITY	11.5%	10%	7%	17%	17%
COMPLEXITY	11.5%	-	7%	7%	8%
ASSESSMENT	11.5%	-	7%	7%	8%
PROCEDURES	20%	9%	7%	16%	17%
COMPETENCE	10%	-	7%	7%	8%
EN'CONTROL	11.5%	7.5%	7%	14.5%	13%
ENV'T TEST	8%	7.5%	7%	14.5%	12%

Columns (0) to (4)

(0) UKAEA, 1996, UPM 3.1.
(1) These percentages are derived by studying the author's gas industry data and assigning the failures to the most likely category in terms of cause.
(2) 56% of the author's data did not contain sufficient information to permit modes/causes to be identified. Therefore, this residual 56% has been distributed evenly across the categories (7% per category).
(3) Is the total of columns (1) & (2).
(4) The BETAPLUS model provides a compromise between the UKAEA (0) and column (3) data. Column (3) was compared with the UKAEA percentages and a judgement/ compromise made in order to propose this BETAPLUS model.

6.5.2 Calibrating the model against field data

Since the majority of available field data is for non-programmable equipment the version of the checklist (6.3.1.2), has been calibrated against the author's data and compared with UKAEA, 1996, UPM 3.1 and tabulated in Table 6.5.2.

In Table 6.5.2, the assessed BETA is shown for values of C=1 and C=3. The C=1 column implies little diagnostic coverage and can be compared with the DJS(i) column which is the author's data but omitting failures which could be detected by diagnostics. The C=3 column implies considerable diagnostic coverage (ie 98%) and is to be compared with the DJS(ii) column which is the author's data making use of only failures likely to be detected by diagnostics.

It should be noted that, whilst it is relatively easy to demonstrate, by FMEA or by test, that 60% diagnostic coverage is achieved it is an onerous undertaking to demonstrate 98% coverage.

Table 6.5.2 - Table of % BETA values comparing data with the model

	DJS(i) DATA	DJS (ii) DATA	β+ C=1	β+ C=3	UPM 3.1
75 BAR Control Valves, Pressure Regulators	19%	13.5%	17%	13%	9.3%
Gas reception terminal, amine pumps	10.8%	6.2%	12%	6.7%	11.8%
Offshore pressure switches	10.5%	7%	10.1%	5.2%	6.1%
PLCs, non-diverse, no auto-test, offshore	<4% >0.2% @ 80% C Int	<4% >0.2% @ 80% C Int	7.6%	4.4%	9.4%
PLCs, non-diverse, no auto-test, onshore	<16% >2.2% @ 80% C Int	<16% >2.2% @ 80% C Int	7.6%	4.4%	9.4%

(C Int signifies confidence interval). The 75 Bar control valve values compare well with the 10%-19% quoted by Hanks B J, 1998.

6.6 FUTURE DEVELOPMENT OF THE MODEL

Because of the nature of this model, additional features (as perceived by any user) can be proposed in each of the categories. The model can then be modified by applying the following process:

- Add the perceived factor to the checklist by adding a new question to the appropriate category in the checklist.
- Make a judgement of the (A) and (B) scores having regard to the other existing maximum score values and to the relative importance of the new feature, as a CCF defence.
- Adjust all the scores in that category in proportion to each other such that the total maximum raw score ([ΣA x 3] + ΣB) remains as before (ie [502 x 3] + 1118).

If subsequent field data indicate a change of relative importance between the categories (significantly different to the right hand column (4) of Table 6.5.1) then adjust the scores in each category so that the category totals reflect the new proportions, also ensuring that the total possible raw score (S=2624) remains unaltered.

Establishing the occurrence of CCF, from field data, is not easily achieved without appropriate planning of the data recording format (see chapter 8). Traditional data collection methods seldom provide sufficient information to identify that CCFs have occurred, let alone the means of identifying the underlying causes as described by the above checklists. Therefore conscious effort is required when planning data collection in order to take account of these needs (see chapters 7 and 8).

Although the relative importance of the scoring factors was developed by the author Smith D J, 1997 (T076) in consultation with the UK HSE, there is scope for further development of the checklist criteria. Hale et al, 1999 describe the use of paired comparisons (method described in UKAEA, 1995, SRDA R-11) for relating maintenance factors to failure. The BETAPLUS model will benefit from further modification based on expert opinion used to rank the effectiveness of the checklist criteria in defending against CCF.

6.7 USING THE MODEL TO EVALUATE PROPOSED DESIGN MODIFICATIONS

The model can best be used iteratively to test the effect of design, operating and maintenance proposals where these would alter the scoring. A BETA value can be assessed for a proposed equipment. Proposed changes can be reflected by altering the scores and recalculating BETA. The increased design or maintenance cost can be reviewed against the costs and/or savings in unavailability by re-running the RAMS predictions using the improved BETA. As with all RAMS predictions the proportional comparison of values rather than the absolute value is of primary value.

6.8 CONCLUSIONS AND RECOMMENDATIONS

The partial BETA approach to CCF modelling offers the greatest flexibility of all the existing models in that it allows any perceived feature of defence against CCF to be included.

The BETAPLUS model offers an advance on existing models by taking account of diagnostic intervals and diagnostic coverage.

The BETAPLUS model has been subject to a degree of calibration beyond the existing models which are only calibrated at the two extremes of the exponential (1% and 30%).

As with most developments of models, the BETAPLUS model is based on a limited amount of data. Further data collection aimed specifically at identifying the time intervals between CCF failures and at identifying the underlying causes is highly desirable for its future development.

CHAPTER 7

QUANTIFIED RELIABILITY CENTRED MAINTENANCE (QRCM)

7.1 SUMMARY

Chapters 3,4,5 & 6 have dealt with design RAMS prediction and its comparison with RAMS targets. This chapter deals with three specific methods for optimising the maintenance strategy, which should be initially developed during the design phase and adjusted during operations. These three methods include optimum discard intervals, optimum spares quantities and optimum proof-test intervals.

Figure 2.1 shows where this chapter fits into the overall thesis. It shows where maintenance related parameters such as spares quantities and maintenance intervals have an effect on reliability and availability. RAMS predictions are thus relevant to developing and adjusting the maintenance programme.

Although RAMS modelling usually quantifies the beneficial effects of proof-test and discard on reliability, it must also be acknowledged that maintenance activity, as a result of human error, can induce failures.

A number of methods are in use for deciding on optimum maintenance strategies as outlined by Moubray J, 1991 and based on earlier work by Nowlan and Heap, 1978 and Bazovsky, 1961. This chapter concentrates on the author's COMPARE software tool (User manual, 1997) which provides algorithms for QRCM in the areas of optimising spares levels, discard/overhaul intervals and proof-test intervals.

The COMPARE User Manual, 1997 is part of this thesis and is reproduced as Appendix 4. The Manual shows the structure of the package and also the author's QRCM algorithm (Figure 2 of Appendix 4 on page 141) which shows where each of the techniques are applicable.

The purpose of this chapter is to encourage the use of the three simple quantified RCM techniques.

7.2 OPTIMUM DISCARD/REPLACEMENT/OVERHAUL

Maintenance is often classified into three areas. These are, as outlined by Ling-Yau, 1997, period (ie time based) preventive maintenance, condition-based maintenance and breakdown repair. This section deals with preventive replacement which requires increasing failure rate as well as planned costs being less then unplanned costs.

Given that significantly increasing failure rate (eg Weibull shape parameter > 1) has been established and provided that planned (preventive) costs are less than unplanned (corrective and penalty due to unavailability) costs, then optimum overhaul/discard periods can be calculated.

These can be applied to individual items as an AGE related replacement strategy or to multiple items as BLOCK replacement strategies, described in Appendix 4.

In order to make realistic use of this technique, statistically significant wearout distributions need to be established from the times to failure of a significant sample of items. The mere fitting of an algorithm to the data (eg Weibull probability plotting) is not sufficient since the implied wearout characteristic may not be significantly different to the constant failure rate assumption.

Wearout can be described by the 3 parameter Weibull expression as applied by Jiang et al, 1997 who used 100 times to failure. Since this quantity of data is seldom available in the process industry, the author's COMPARE method (Appendix 4) initially utilises the 2 parameter Weibull equation and provides for iteration to a 3 parameter version if adequate data should be available. Holmes et al, 1995 provide a simple non-parametric test of data which provides an initial "feel" for the distribution but does not lead to an optimum discard decision.

Appendix 4, the COMPARE User Manual, explains the application of the Weibull expression $R(t) = \exp -([t-\gamma]/\eta)^{\beta}$ to the analysis of times to failure. In chapter 6 of Smith D J, 1997 the author outlines the basic theory behind the Weibull function as do most authors in the field.

A feature of the COMPARE technique is the measures by which significance of the inferred Weibull parameters can be assessed.

- The loglog against log probability plot, showing the data points, is displayed giving an initial "feel" for the data fit.

- The Least Squares regression line is calculated as an initial means of calculation of the parameters and to remove subjectivity from creating a line through the data points.

- As pointed out by Lawson et al, 1997 least squares regression can suffer from the additional weighting of points furthest from the line. Thus, in COMPARE, the least squares estimate is used as the first point of iteration for the Maximum Likelihood estimation of the Weibull parameters. Mudholkar et al, 1993 also advocate the maximum likelihood and address the need to establish goodness of fit. Farnum et al, 1997 also address the use of maximum likelihood.

- Also, in COMPARE, a simple Gnedenko significance test (described in Appendix 4) is applied to the data to determine the likelihood that the estimated BETA is significantly different to the value $\beta=1$.

If the result of this Weibull analysis is a shape parameter, significantly in excess of $\beta=1$, then the question of optimum discard can be addressed.

Equations for the cost per unit time of both preventive maintenance (replacement or complete overhaul) and unplanned corrective maintenance failure costs (including the cost of down time) are developed, in Appendix 4, for both AGE and BLOCK replacement strategies. The equations form the basis of the algorithms in the COMPARE tool. Examples of tables of unit cost per time against replacement interval are then shown in section 3.6.3 of Appendix 4 in the form that the software tool presents them to the user. These tables can be recalculated over smaller ranges to provide enhanced precision.

As shown in Appendix 4 the cost per unit time (for Age Replacement) is given by:

$$\frac{[£_u \times (1-R(T))] + [£_p \times R(T)]}{\int_0^T R(t)dt}$$

where $£_u$ is the cost of unplanned outage (ie failure) and $£_p$ is the cost of a planned replacement.

The optimum replacement interval facility may then be accessed if the user is satisfied with the significance of the Weibull inference from the data.

In the author's experience only a limited number of components show a significantly increasing failure rate. This is often due to the phenomenum (known as Drenick's law) whereby a mixture of 3 or more different failure modes will show a random failure distribution irrespective of the β's of the individual modes.

7.3 OPTIMUM SPARES LEVEL

In order to propose an optimum spares level it is necessary to consider the cost of spares, to estimate the cost of unavailability and to calculate the unavailability which will occur, taking account of the following parameters:

- Number of spares
- Failure rate of the item
- Number of identical items
- Degree of redundancy within those items
- Lead time of procurement (added to the replacement time if no spare is available)
- Replacement time (unit down time) when an item fails and a spare is available

Optimum spares levels can then be assessed for stated levels of the above parameters. Appendix 4 describes how a Markov process is used, by COMPARE, to evaluate each of the options.

Having specified the above parameters, system unavailability can be calculated and compared with the incremental cost of each spare.

The MARKOV technique assumes the existence of constant failure rate.

The question may arise of spares levels where a significant wearout has been established. Given that preventive discard (as treated in 7.2 above) has been carried out then assume that there is a discard interval T which has been established for a particular item. It is possible to utilise the above MARKOV method under two conditions:

- That there is a number of the items in use and that sufficient time has elapsed for the population failure rate to have stabilised and become pseudo random as described in chapter 6.4 of Smith D J, 1997. In this case the failure rate may be estimated as the reciprocal of the maximum likelihood MTBF, calculated by COMPARE.

- That the replacement interval T is short compared with the mission time in question, in which case the failure rate is taken as above.

7.4 OPTIMUM PROOF-TEST INTERVAL

Optimum proof-test intervals can be assessed, for both active and standby redundant systems, assuming constant failure rate and for given planned and unplanned costs.

The equations for the algorithm are described in Appendix 4. The COMPARE software package also displays tables (similar to 3.6.3 in Appendix 4) of cost per unit time, from which the optimum proof-test interval can be established. These tables can be recalculated over smaller ranges to provide enhanced precision.

The minimum cost can be found by tabulating the cost against the proof-test interval (T). In the general case the total cost per unit time is:

$$\frac{[£_u \times (1-R(T))] + [£_p \times R(T)]}{\int^{T}_{0} R(t)dt}$$

7.5 NEGATIVE ASPECTS OF MAINTENANCE

Human factors studies (addressed in section 5.5) show that maintenance activities can induce failures. In sections 7.2 and 7.4 the improvements in availability, deriving from maintenance, were addressed. However, the reliability model (eg fault tree) could equally include an allowance for maintenance human error leading to failure.

The effect on the model would be dependent upon the frequency of the maintenance task and the rate of human error involved.

Human error rates in the order of 10^{-2} and greater are not uncommon as is recorded in Comer et al, 1986 and Smith D J, 1997.

7.6 CONCLUSIONS AND RECOMMENDATIONS

These QRCM techniques should be applied at the design stage since the parameters involved impact directly on system reliability. The design RAMS assessment thus requires that maintenance strategy is addressed at this early stage.

During operational use, field data should be used on an ongoing basis to adjust the RCM calculations described in this chapter.

The COMPARE package offers enhanced significance in the estimation of Weibull parameters, a fast and comprehensive evaluation of unavailability versus spares and an automated tool for calculating optimum proof-test intervals.

PART 3 - VALIDATION

CHAPTER 8

FIELD DATA COLLECTION AND ANALYSIS

8.1 SUMMARY

Field failure data are the inputs to the failure rate/mode data banks needed to support RAMS prediction methods. In the first instance data are collected as part of a company data collection scheme. Multiple data sources (eg multi-company data such as OREDA, 1997) may be aggregated into a data bank such as that collected by the author. It is therefore vital that data collection and screening methods are included as part of the life-cycle.

Figure 2.1 therefore includes data collection as part of the overall method and thus this chapter is an essential part of the overall thesis.

This chapter makes recommendations for data recording (Figures 8.1 and 8.2).

8.2 BEST PRACTICE AND RECOMMENDATIONS

The following list summarises the best practice (see also Blanks H S, 1998 and Cross A, 1996) together with recommended enhancements for both manual and computer based field failure recording.

Recorded field information is frequently inadequate and it is necessary to emphasise that failure data must contain sufficient information to enable precise failures to be identified and failure distributions to be identified. They must, therefore, include:

a) Adequate information about the symptoms and causes of failure. This is important because predictions are only meaningful when a system level failure is precisely defined. Thus component failures which contribute to a defined system failure can only be identified if the failure modes are accurately recorded. There needs to be a distinction between failures (which cause loss of system function) and defects (which may only cause degradation of function).

b) Detailed and accurate equipment inventories enabling each component item to be separately identified. This is essential in providing cumulative operating times for the calculation of assumed constant failure rates and also for obtaining individual calendar times (or operating times or cycles) to each mode of failure and for each component item. These individual times to failure are necessary if failure distributions are to be analysed by the Weibull method dealt with in chapter 7.

c) Identification of common cause failures by requiring the inspection of redundant units to ascertain if failures have occurred in both (or all) units. This will provide data to enhance the model developed in chapter 6. In order to achieve this it is necessary to be able to identify that two or more failures are related to specific field items in a redundant configuration. It is therefore important that each recorded failure also identifies which specific item (ie tag number) it refers to.

d) Intervals between common cause failures. Because common cause failures do not necessarily occur at precisely the same instant it is desirable to be able to identify the time elapsed between them. This is necessary, as emphasised by Walls et al, 1989 and Cross A, 1996 if the BETAPLUS model in chapter 6 is to be developed further.

e) The effect that a "component part" level failure has on failure at the system level. This will vary according to the type of system, the level of redundancy (which may postpone system level failure) etc.

f) Costs of failure such as the penalty cost of system outage (eg loss of production) and the cost of corrective repair effort and associated spares and other maintenance costs.

g) The consequences in the case of safety-related failures (eg death, injury, environmental damage) not so easily quantified.

h) Consideration of whether a failure is intrinsic to the item in question or was caused by an external factor. External factors might include:

process operator error induced failure
maintenance error induced failure
failure caused by a diagnostic replacement attempt
modification induced failure

i) Effective data screening to identify and correct errors and to ensure consistency. There is a cost issue here in that effective data screening requires significant manhours to study the field failure returns. In the author's experience an average of as much as one hour per field return can be needed to enquire into the nature of a given failure and to discuss and establish the underlying cause. Both codification and narrative are helpful to the analyst and, whilst each has its own merits, a combination is required in practice. Modern computerised maintenance management systems offer possibilities for classification and codification of failure modes and causes. However, this relies on motivated and trained field technicians to input accurate and complete data. The option to add narrative should always be available.

j) Adequate information about the environment (eg weather in the case of unprotected equipment) and operating conditions (eg unusual production throughput loadings).

Thus, the following recommended list of items (Figure 8.1) should be called for in an incident/maintenance report form.

Since the use of Figure 8.1 might be regarded as onerous, Figure 8.2 offers a suggests MINIMUM (and thus more cost effective) data recording format. Although the reduced amount of information precludes the analysis of failure distribution and common cause failure, basic failure rate and failure mode information (restricted to the assumption of constant failure) is possible.

Figure 8.1 FAILURE DATA RECORDING FORM (Number .....)

DATE (and time) OF INCIDENT/EVENT/FAILURE

DATE ITEM INSTALLED (or replaced or refurbished)

MAINTENANCE TECHNICIAN (Provides traceability)

DISCIPLINE (eg Electrical, Mechanical, Instrumentation)

FAILED COMPONENT ITEM DESCRIPTION (eg Motor)

SUBSYSTEM (eg Support system)

DESCRIPTION OF FAULT/CAUSE (Failure mode, eg Windings open circuit)

"TAG", "SERIAL NUMBER" (HENCE DATE OF INSTALLATION & REFURB)
eg System xyz, Unit abc, Motor type zzz, serial no def,

DOWN TIME [if known]/ REPAIR TIME
eg 4 hrs repair, 24 hrs outage

TIME TO FAILURE (COMPUTED FROM DATE AND TAG NUMBER)
eg This date minus date of installation
eg This date minus date of last refurbishment

PARTS USED (in the repair)
eg New motor type zzz, serial number efg

ACTION TAKEN (eg Replace motor)

HOW CAUSED
Intrinsic (eg RANDOM HARDWARE FAILURE) v extrinsic (GIVE CAUSE IF EVIDENT)

HOW FOUND/ DIAGNOSED
eg Customer report, technician discovered open circuit windings

RESULT OF FAILURE ON SYSTEM
eg Support system un-useable, process trip, no effect

COMMON CAUSE FAILURE eg redundancy defeated
time between CCFs .....
attributable to SEPARATION/DIVERSITY/COMPLEXITY/HUMAN FACTOR/ENVIRONMENT

ENVIRONMENT/OPERATING CONDITION
eg temp, humidity, 50% throughput, equipment unattended

NARRATIVE.....

Figure 8.2 MINIMAL FAILURE DATA RECORDING FORM

(Number.....)

DATE (and time) OF INCIDENT/EVENT/FAILURE

MAINTENANCE TECHNICIAN
Provides traceability

FAILED COMPONENT ITEM DESCRIPTION
eg Motor

SUBSYSTEM
eg Support system

DESCRIPTION OF FAULT/CAUSE (Failure mode)
eg Windings open circuit

PARTS USED (in the repair)
eg New motor type zzz, serial number efg

ACTION TAKEN
eg Replace motor

HOW FOUND/ DIAGNOSED
eg Customer report, technician discovered open circuit windings

RESULT OF FAILURE ON SYSTEM
eg Support system un-useable, process trip, no effect

NARRATIVE .....

The use of codes to provide multiple choice entries for some fields has a number of advantages. It serves as an "aid memoir" to the technician by providing a list of possible entries. On the other hand a checklist can never foresee the need for an additional code thus making it essential that the technician is motivated to make use of the narrative section of the report form. An example of multiple choice codes, chapter 12 of Smith D J, 1997 is:

DESCRIPTION OF FAULT:
01 Short circuit
02 Open circuit
03 Leak
04 Drift

.....

12 Other (see narrative)

Note the instruction for code 12 to enter a description in the narrative. There should not be too many codes (maximum 12) otherwise the accuracy of recording is likely to reduce.

8.3 DATA ANALYSIS

As well as collecting field data it is necessary to analyse the distributions of times to failure of specific failure modes in order to determine if constant failure rates may be inferred or if preventive overhaul or replacement is called for as a result of increasing failure rate.

In general confidence limits (and or measures of significance) should be applied, as emphasised by Blanks H S, 1998, in order to warn of potential inaccuracies due to small quantities of data.

The author's COMPARE (User manual, 1997 - in Appendix 4) provides a means of establishing a statistically significant distribution of times to failure as described in chapter 7.

Data analysis has a number of purposes:

- Demonstrating field RAMS performance
- Establishing the warranty situation
- Reliability growth, by elimination of repetitive failures
- Optimising maintenance policies
- Identifying primary failure causes
- Comparison of vendors and equipment types

Frequently, software tools are used to fit an assumed model to data values. This can lead to assumptions, concerning the underlying failure distribution, which are not statistically significant. For example, a group of times to failure may suggest a Weibull shape parameter indicating wearout whereas the significance of the inference may not justify an assumption other than random failures. The COMPARE package (Appendix 4) ensures that the user:

a) views the Weibull loglog/log data plot for a preliminary subjective view of the goodness of fit

b) addresses the results of a Gnedenko significance test

Figure 8.3 shows a typical Weibull plot from COMPARE, User manual, 1997.

8.4 CONCLUSIONS AND RECOMMENDATIONS

Development of in-company reliability data banks is encouraged since it enhances the accuracy (see chapter 3) of RAMS predictions.

Inter-company pooled data schemes (exchanges) further enhance the quantity of industry specific data available to users. Such schemes require the "quality control" features of data audit in order to ensure that "like for like" descriptions of the data fields (outlined above) are maintained. For example "intermittent operation" as described by one operator might be recorded as "degraded performance" by another. Again, a "medium size" ESD valve might be classified as "8cm - 12cm" by one organisation but "1cm - 5cm" by another.

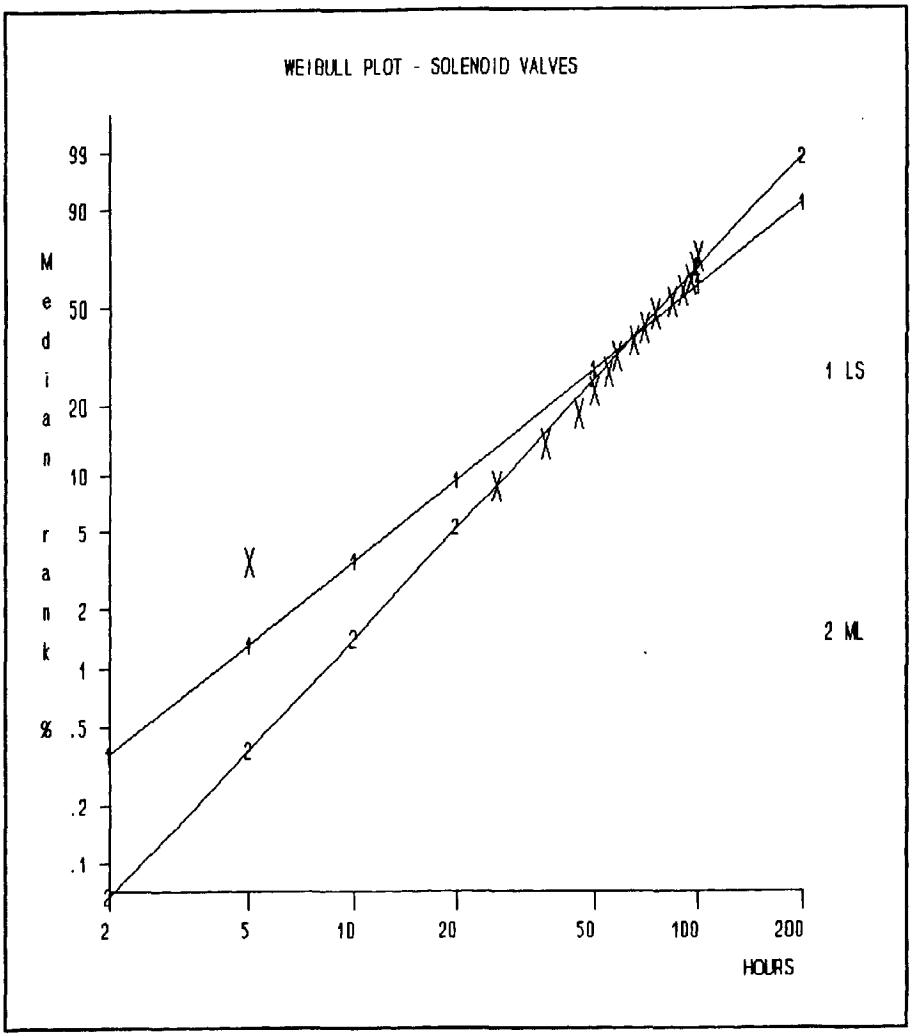
Data collection should be followed by data analysis in order that the raw data can be processed into a form (eg failure rates and Weibull parameters) suitable for use in RAMS predictions (including QRCM).

Computerised maintenance management systems should be developed to provide specific benefits as, for example:

- easier identification of root causes of failure.
- identification of major cost drivers and performance killers as related to items within the failure data.
- easier and hence more motivated and cost effective collection of data.
- fast and thus cost effective analysis of data leading to revised RCM calculations which, in turn, lead to more optimum maintenance policies.

There are dangers, as well as benefits, from data collection as mentioned by Cross et al, 1987. If the plant has accurate records and operators accurately record data (without significant omissions) then data analysis can lead to meaningful RCM decisions being made, as outlined in chapter 7. If, on the other hand, incident recording is haphazard, or data inventories are incorrect, then inaccurate predictions may lead to errors in RAMS prediction which may be costly in terms of safety or plant availability.

Figure 8.3 - A "COMPARE" Weibull plot



Least Squares Beta	=1.4
Least Squares Scale	=106 hours
Maximum Likelihood Beta	=1.9
Maximum Likelihood Scale	=93 hours
Gnedenko: Reject BETA=1 hypothesis at	8%

PART 4 - CONCLUSIONS

CHAPTER 9

CONCLUSIONS AND RECOMMENDATIONS

9.1 SUMMARY

The inherent imprecision in reliability data, due to the wide range of parameters affecting failure rate, calls for a confidence related approach to expressing predicted reliability based on such data. This thesis offers such an approach in chapter 3.

Comparison of predicted reliability with target values must therefore take account of the correlation between data and predictions. A method is outlined in chapter 4.

RAMS prediction methods need to take account of the inaccuracy of failure data. Quantification of redundancy modelling need not involve undue accuracy in the estimation of random coincident failures. The modelling of common cause failures, which frequently dominate random coincident failures, warrants more detailed attention. This thesis addresses these issues in chapters 5 and 6.

QRCM involves quantifying parameters which are relevant to RAMS prediction. RCM must therefore be addressed at the design stage and chapter 7 offers improved techniques in this area.

The collection and analysis of failure data is essential to this topic and chapter 8 encourages a thorough approach to the task.

9.2 USE OF IMPRECISE FAILURE RATE DATA

Analysis of an extensive collection of failure rate and failure mode data (chapter 3) has made more realistic RAMS system predictions, expressed as confidence ranges, possible. Current practice has been to use a single predicted value of reliability for comparison with each target.

The study was based on forty four pairs of failure rate data and their associated earlier RAMS predictions (Appendix 3). Efforts should be made to extend this comparison in order to improve the significance of the findings in chapter 3. Users of the method can adapt it to make use of any desired confidence level.

In order to make best use of generic data (when site and industry specific sources are not available) the FARADIP data ranges are offered (chapter 3 and Appendix 2). The extent of the ranges was shown to agree closely with the correlation study in Appendix 3. It is intended that the data ranges approach be extended and updated by the regular comparison of FARADIP with new data.

9.3 RELIABILITY MODELLING

Simple, but sufficiently accurate, reliability models are provided to address redundancy and repair regimes (chapter 5). They enable availability and failure rate of random coincident failures to be calculated using simple equations shown in chapter 5. These should be used rather than more complex equations involving unjustified precision.

A new Partial BETA factor common cause failure model (chapter 6) is provided and offers:

- greater visibility of scoring/assessment criteria than other models
- recognition of the effect of diagnostics
- calibration of the model against gas industry data
- the facility to review the relative effect, on CCF, of proposed changes to the design
- flexibility for re-calibration by the user
- capability for development of the model by addition of further checklist features perceived, by any user, as relevant

More CCF data is desirable for comparison with the BETAPLUS model in order improve the calibration.

9.4 DATA COLLECTION AND ANALYSIS

Data collection is essential (chapter 8). Without continually refreshed data bases RAMS techniques will dwindle due to increasing imprecision of predictions based on out of date data.

A software package is described (Appendix 4) which provides a realistic tool for the analysis of times to failure, including the statistical significance of analyses.

9.5 RELIABILITY CENTRED MAINTENANCE

Quantification of RCM decisions is encouraged in order to optimise the benefits from assessing discard intervals, spares levels and proof-test intervals.

A software package is described in chapter 7 for optimising these maintenance parameters.

9.6 HUMAN FACTORS AND SOFTWARE QUALITY

Although not the direct concern of this thesis, these sources of failure are of increasing importance due to the complexity of modern systems.

Human error is of increasing concern, particularly in the area of disastrous failures. It is important that data continues to be collected for the development of the existing models (UKAEA, 1995, SRDA R-11).

Software quality involves addressing qualitative features of design and of quality control, Smith D J, 1995 (Achieving Software Quality). In addition to the quantification of random hardware failures (the subject of this thesis) qualitative requirements are specified, for each of four safety integrity levels (IEC 61508).

9.7 FUTURE WORK

In a subject requiring continuous improvement it is intended to continue collecting and analysing data, beyond this thesis, in order to develop and calibrate the models shown.

The data ranges, described and developed in chapter 3, could well be dependent on factors other than the data source. For example, the accuracy of RAMS predictions could be different for simplex than for redundant architectures as a result of the accuracies applying to CCF models. Only further data collection and analysis will reveal these types of relationship.

Companies and organisations are urged to collect and analyse their own failure data in order to enhance the accuracy of their RAMS predictions. Only careful data collection will yield adequate information for significant wearout distributions to be identified. It is important to identify and then eliminate failure causes and this can only be achieved through data collection and analysis.

As with most developments of models, the enhanced CCF model in chapter 6, is based on a limited amount of data. Further data collection aimed specifically at identifying the time intervals between CCF failures and at identifying the underlying causes is highly desirable for the future development of the BETAPLUS model.

APPENDIX 1 - REFERENCES

Balbir S, Dhillon B S and Rayapati S N, 1988, Common cause failures in repairable systems, IEEE Proceedings Annual R and M Symposium.

Bazovsky I, 1961, Reliability theory and practice, Prentice Hall, London.

Blanks H S, 1998, The challenge of quantitative reliability, Q & R Eng Int Vol 14 No. 3.

British Standard, BS 5760, 1981, Reliability of systems equipments components, Part 2.

Busse D, 1998, Cognitive modelling of human error to support accident analysis, PhD 1st year report, Glasgow University.

Comer P J and Kirwan B J, 1986, A reliability study of a platform blowdown system, automation for safety in shipping and offshore petroleum operations, Elsevier.

Cross A and Stevens B, 1987, Reliability data banks, friend, foe or a waste of time? UK Reliability Symposium Paper 5C/5.

Cross A, 1996, Effective strategies for data collection and management, AEA report SRDA - R14.

Denson W K et al, c1996, A new system - reliability assessment methodology, IIT Institute, Rome, New York, USA.

Edholm K, 1996, New model for reliability prediction of telecommunication hardware, Q & R Eng Int Vol 12 No. 4.

Edwards G and Watson I A, SRD of UKAEA, 1979, Study of common-mode failures, SRD R 146.

Farnum N and Booth P, 1997, Uniqueness of maximum likelihood estimators of the 2 parameter Weibull distribution, IEEE transactions on Reliability Vol 46 No 4.

Hale A and Baram, 1998, chapters 4 & 13, Safety management, the challenge of change, Pergammon.

APPENDIX 1 - REFERENCES

Hale A.R, Costa M.A.F, Goossens L.H.J & Smit K, 1999, Relative importance of maintenance management influences on equipment failure and availability in relation to hazards. ESREL 1999.

Hanks B J, 1998, An appreciation of common cause failures in reliability, Proceedings Institution of Mechanical Engineers Vol 212 Part E.

Holmes D S and Erhan Mergen A, 1995, An alternative method to test for randomness of a process, Q & R Eng Int Vol 11 No 3.

HSE, 1992, Tolerability of risk for nuclear power stations, UK Health and Safety Executive, ISBN 0118863681.

HSE, 1991, Major hazard aspects of the transport of dangerous substances.

HSE, 1999, The COMAH regulations, Control of major accident hazards regulations.

HSE, 1999, Reducing risks protecting people. A discussion document.

Humphreys R, 1987, Assigning a numerical value to the Beta factor, common cause evaluation, Reliability 87 paper 2c/5/1.

IEC 61508, 1999, Functional safety: safety related systems - 7 Parts.

IEE, 1999, Competency guidelines for safety related systems practitioners, ISBN 085296787X.

IEE, 1992, Safety related systems postgraduate qualifications syllabus proposals, Institution of Electrical Engineers, PAB Report 13 ISBN 0852966326.

IEE, 1992, Education and training requirements for safety critical systems, Institution of Electrical Engineers, PAB Report 12 ISBN 0852965338.

IEEE standard 500, 1994, Reliability data for pumps, drivers, valve actuators and valves, Library of Congress 83-082816.

APPENDIX 1 - REFERENCES

I Gas E, 1999, Programmable equipment in safety related applications, Edition 3, 1998 and Amendments 2000. ISSN 0 367 7850, Institution of Gas Engineers publication IGE/SR/15.

Jiang R and Murthy D.N.P, 1997, Two sectional models involving 3 Weibull distributions, Q & R Eng Int Vol 13 No. 2.

Lawson C et al, 1997, Comparison of robust and least squares regression in computer-generated probability plots, IEEE transactions on Reliability Vol 46 No 1.

Ling-Yau Chan et al, 1997, Reliability analysis and maintenance policy of radiators for a large fleet of buses, Q & R Eng Int Vol 13 No 3.

Majeske K D and Herrin G D, 1998, Determining warranty benefits for automobile design changes, Proceedings of Annual R and M Symposium.

Motor Industries Research Association, MISRA, 1994, Development guidelines for vehicle based software, Motor Industries Software Reliability Association, ISBN 0952415607.

Moubray J, 1991, Reliability centred maintenance, Butterworth Heinemann UK, ISBN 07506 0230 9.

Mudholkar G S and Srivastava D K, 1993, Exponential Weibull family for analyzing bathtub failure rate data, IEEE transactions on Reliability Vol 42 No 2.

Neswadba H and Nitsch R, 1988, Quality of telecommunication systems after sales: evaluation of data, IEEE Journal on selected areas in communications Vol 6 No 8.

Nowlan F S and Heap H, 1978, Reliability centred maintenance, Springfield, Virginia, NTIS, US Dept of Commerce.

O'Connor P D T, 1991, Practical reliability engineering, Wiley UK, ISBN 0471 92902 6.

O'Connor P D T, 1994, The practice of engineering management, Wiley UK, ISBN 0471 93974 9.

APPENDIX 1 - REFERENCES

Pirovano G and Turconi G, 1988, Telecommunications reliability data bank from components to systems, IEEE Journal on selected areas in communications Vol 6 No 8.

Quantum Inc, 1996, HDD operational vs theoretical MTBF, Corporate reliability engineering paper.

Rutledge and Mosleh, 1995, Dependent-failures in spacecraft: Root causes, coupling factors, defences and design implications, Proceedings Annual RAM symposium, IEEE.

Safety and Reliability Society, 1992, Directory of software programs used in safety and reliability assessment.

SARS93 Symposium, 1993, Various papers 13,15,17, Guidance on education syllabi, Manchester UK.

Smith D J, 1986, A comparison of microelectronic failure rates - 9th Advances in Reliability Technology, Bradford University (paper C3/R) and reproduced in Quality & Reliability Management Volume 2 No 3 1985.

Smith D J, 1994, The cost and safety benefits of reliability centred maintenance - Gas Processors Association Conference Proceedings, Copenhagen.

Smith D J, 1996, The benefits of quantified reliability centred maintenance, Safety and Reliability Society Journal, Vol 15 No 3.

Smith D J, 1997, Common mode failure: a proposed model for use in IEC 61508, Technis T076.

Smith D J, 1997, Reliability, maintainability and risk, 5th Edition, (Butterworth Heinemann UK) ISBN 0 7506 3752 8.; 1st Edition 1981. 2nd Edition 1985. 3rd Edition 1988. 4th Edition 1992.

Smith D J, 1995, Achieving quality software, 3rd Edition, (Chapman Hall UK) ISBN 0 412 6227 0 X; 1st Edition 1989. 2nd Edition 1992 (Elsevier UK).

APPENDIX 1 - REFERENCES

Smith D J, FARADIP.THREE, Version 4.1, 1999, User's manual, Reliability software package ISBN 0 9516562 3 6.

Smith D J, COMPARE Version 1.1, 1997, User's manual, Reliability centred maintenance software package ISBN 0 9516562 2 8.

Smith D J, BETAPLUS Version 1.0, 1997, User's manual, Common cause failure software package ISBN 09516562 5 2.

Snaith E R, 1981, The correlation between the predicted and the observed reliabilities of components, equipment and systems, UK AEA NCSR paper NCSR R18.

Talmor M and Arueti S, 1997, Reliability prediction: the turn over point, IEEE Proceedings of Annual R and M Symposium.

UKAEA, UPM 3.1, April 1996, A pragmatic approach to dependent failures assessment for standard systems, UKAEA, ISBN 085 356 4337.

UKAEA, 1995, Human reliability assessors guide (SRDA-R11), June 1995, Thomson House, Risley, Cheshire WA3 6AT ISBN 085 3564 205. ISBN 0853564205.

US Military Handbook 472, 1966, Maintainability prediction.

US MIL STANDARD 499B, 1992, Engineering management.

Walls L A and Bendell, 1989, Exploring field reliability data for potential dependent failures, UK Reliability Symposium, Reliability 89. Paper 4Ab/3.

Wood A P and Elerath J G, 1994, A comparison of predicted MTBFs to field and test data, Proceedings of Annual R and M Symposium.

Wray A M, 1996, Common cause failures in relation to programmable electronic systems used for protection, HSE UK paper CI/96/15.

Young-Ju, 1997, Dynamic system of terminal pair reliability with dependent components, Master's thesis, Dept Ind Eng, Pusan University, Korea.

FAILURE RATE DATA IN PERSPECTIVE

USER MANUAL

ISBN 09516562 3 6

A FAILURE RATE AND FAILURE MODE DATA BANK
AND FAILURE MODE AND EFFECT ANALYSIS PACKAGE
Version 4.1 (1999) applicable to Program Versions 4.0/4.1

Microelectronics - Logic, Linear and Memory
Discrete semiconductors, tubes and lamps
Passive electrical components
Instruments and analysers
Connectors, switches, PCBs and cables
Electromechanical and rotating machinery
Power supplies, sources and transformers
Mechanical (including pumps and valves)
Pneumatic and hydraulic equipment
Computers, data processing and communications
Alarms, fire protection, arresters & fuses

CONTENTS

APPENDIX 2 - FARADIP User's Manual

FARADIP.THREE is a failure rate and failure mode data bank and failure mode analysis program giving ranges of failure rates from over 30 sources. Version 4.0 contains 30% more data than Version 1.0. In a single run, failure rates may be ascribed to two failure modes. A parts count total is also generated. Failure mode percentages are included and the program prints out component lists, failure rates and their totals and displays Mean Time Between Failures. There are facilities for editing data lines and for duplicating files. The data includes:

Microelectronics - Logic, Linear and Memory
Discrete semiconductors, tubes and lamps
Passive electrical components
Instruments and analysers
Connectors, switches, PCBs and cables
Electromechanical and rotating machinery
Power supplies, sources and transformers
Mechanical (including pumps and valves)
Pneumatic and hydraulic equipment
Computers, data processing and communications
Alarms, fire protection, arresters & fuses

Note: This manual has been carefully written to help you get the maximum benefit from FARADIP.THREE. Please Read It !

1. GENERAL FAILURE RATES

In compiling the ranges and modes, over 7,500 items from 30 diverse sources have been consulted. These include:

US MIL HDBK 217
UK BT HRD
OREDA DATA BOOK
US NPRD
UK DEFENCE INDUSTRY RSRE250
UK MOD DEF STAN 00-41
UK RAIL
DNV
UKAEA
EPRI
Reliability Technology (Green and Bourne)
Safety in the Process Industries (Lees)

SINTEF publications
AGA (American Gas Association) publications
Dexter and Perkins
CONCAWE reports
UK Gas industry studies (offshore and onshore)
Safety and Reliability Conference proceedings
Technis data collection experience
Associated consultants' data banks

In some cases there is close agreement between different data sources and in others there is a wide range between values. This is due to a number of factors:

* Some failure rates are based on only critical failures which have led to total loss of function of the equipment of which they are part. On the other hand failure rates are sometimes quoted which include all degraded items. Similarly, some failure rates include items replaced during preventive maintenance whereas others do not. This can affect the rates by as much as an order of magnitude. This is thought to be the main source of variability in the FARADIP ranges. The user should therefore think carefully about what type of failure he or she is predicting and choose a figure from the range accordingly.
* Failure rates are affected by the tolerancing of the design which will cause a variation in values.
* Although the nominal environment and the quality levels are stated in most data sources the range of parameters covered by these broad descriptions is large. This is another source of variability.
* Component parts are usually described by reference to a broad type (eg transformer). Data is therefore combined for a range of similar but not identical devices thus creating a range of values.
* Quality control and the manufacturing environment play a major role in influencing field reliability. Failure data combine items from a wide range of manufacture.

Each data item in this package is therefore presented in one of four ways:

A SINGLE VALUE where the various references are in good agreement.
TWO VALUES INDICATING A RANGE which may be as great as an order. The user, as does the author, must apply engineering judgement in choosing a value having regard to the physical size and source of component as well as the application in question.

THREE VALUES INDICATING A RANGE implying that there are several data sources spanning a wide range. Where the data tends to predominate around a particular value then this is indicated in the centre column.
TWO VALUES OF WHICH ONE IS IN THE CENTRE COLUMN indicating a range of values but where the data predominates at one end of the range, shown as the centre value.

The program allows for the variation of different environments and quality levels which are displayed in menu form on the screen.

A general interpretation of the ranges is as follows:

> The lower figure in the range, used in a prediction, is likely to yield an assessment of the credible design objective reliability. That is the reliability which might reasonably be targeted after some field experience and a realistic reliability growth programme. The initial (field trial or prototype) reliability might well be an order of magnitude less than this figure.
>
> The centre column figure indicates a failure rate which is more frequently indicated by the various sources. It is therefore a matter of judgement, depending on the type of prediction being carried out, as to whether it should be used in place of the lower figure.
>
> The higher figure will probably include a high proportion of maintenance revealed defects and failures. The fact that data collection schemes vary in the degree of screening of maintenance revealed defects explains the wide ranges of quoted values.

In general it can be assumed that the failure rates are based on, and refer to, calendar time. In other words the per million hours rate can be converted to years by multiplying by 8760. It should be borne in mind that some items (eg a fire water pump, a particular compressor) operate for a very small percentage of the time. The failure rate expressed in units of operating time would therefore be very much greater than the calendar time failure rate. Allowance should be made for this factor when carrying out reliability analysis.

2. MICROELECTRONICS

Because of the large number of variables involved in describing a microelectronic device, the failure rate is often expressed in the form of a regression model. These regression equations attempt to model such parameters as:
- Complexity (number of gates, bits or transistors)
- Number of pins
- Junction temperature
- Package (ceramic or plastic)
- Length of time in manufacture
- Technology (CMOS, TTL etc)
- Type (memory, linear etc)
- Number of EEPROM refresh cycles (< 100 has been assumed)
- Quality
- Environment

These models, however, offer a wide range of values covering a far wider tolerance than the precision implied by the model. This data base, therefore, presents a summary of the ranges. Where a wide range exists, and there is no particular reason to choose one or other of the extremes, then the geometric mean of the extremes offers one option which gives appropriate weighting to the two values. As a result, the microelectronic failure rate tables, in FARADIP.THREE, occupy three columns. The centre column is the geometric mean of the range extremes. Junction temperature and environmental factors, already mentioned, are allowed for.

Whereas earlier versions of FARADIP applied a multiplying factor for non-ceramic encapsulation, this has now been discontinued. It was once the case that plastic encapsulated devices had weaknesses in several areas including moisture absorption, glass transition temperature and thermal expansion. Due to improvements in materials and process control it is now considered reasonable to attribute the same failure rate to plastic and ceramic devices.

The main sources of credible microelectronics data are the BT HRD5 and MIL217F documents. Neither has been updated for over 5 years and some small allowance has been made, in constructing the FARADIP ranges, for the general trend of continually improving failure rates.

The range of component types and choice of complexities, offered in the FARADIP screens, is considered sufficient to choose a credible failure rate. Using the nearest value of complexity is likely to be adequate having regard to the wide tolerances involved.

3. FAILURE MODES

Just as failure rates vary according to a large number of parameters then so do the relative percentages of the failure modes. The proportions of a number of failure modes (open and short circuit, leak, fail to operate etc) are included with the displayed failure rates so that failure mode analysis can be carried out. The program allows two specific failure modes and rates, in addition to the part failure rate, to be input for each component. In the next section an example of the diode failure modes can be seen.

Some "common sense" interpretation needs to be made of the failure mode proportions shown. For example, a solenoid valve may be sprung to the closed position and magnetically actuated to open. In that case the "fail closed" mode might credibly be 90% and the "fail open" mode 10%. The opposite could also be the case according to the design of the particular valve. A ball valve may be positively actuated in both directions in which case the 35/25 ratio shown on the screen is realistic. If the same valve where to be sprung closed and pneumatically actuated to open then the same argument applies as to the solenoid valve above.

The failure mode percentages do not necessarily sum to 100% because data frequently are not sufficiently comprehensive to provide a complete picture.

4. FAILURE MODE ANALYSIS

FARADIP.THREE allows failure mode analysis to be performed. Two equipment failure modes will be requested and you will be given the option of entering mode proportions, where applicable, for each component. The program will calculate a total failure rate and MTBF (Mean Time Between Failures) for each mode as well as providing a parts count failure rate and MTBF.

5. USING THIS DATA BANK

Although some replies are shown, in this manual, as being in upper case the program will also accept lower case responses.

5.1 LOADING FARADIP.THREE

The program may be run from the floppy disk or from a hard disk. To run on a hard disk create a directory e.g.

MD C:\FARADIP3

then copy the files from the floppy supplied e.g.

COPY A:*.* C:\FARADIP3

Switch to the drive or directory containing FARADIP.THREE and type FARA3-4. The program will automatically load and a title screen will be displayed, followed by a MAIN MENU which is shown at the top of Figure 1 **(not included in this thesis)**.

Figure 1 also provides a graphical summary of the interrelationship of the various screens which will be seen whilst using FARADIP.THREE.

FARADIP.THREE Version 4.0 will handle any Version 3.0 or any FARADIP.TWO files you may have created.

5.2 STARTING/ACCESSING A FILE

By selecting Option F (-file handling menu) from the main menu the file menu (left in Figure 1) will be displayed. If files have already been entered then they will be listed followed by a statement of the number of bytes free.

- OPTION P (-change path)
Use this option if you wish to store your data files on a different disk or directory to that holding the FARADIP.THREE program. You will be asked to:

"Enter the new path, WITHOUT the final \".
To store data on a floppy disk, enter A: or B: as appropriate. To use a directory on a hard disk, enter the complete directory name e.g. C:\FMEADATA. To return to the program directory, enter a blank name (i.e. press RETURN immediately). Note that changing the path will cause a currently opened file to be closed.

- OPTION O (-open file)
You will be asked to "Enter your equipment data filename". You should enter a filename (without the DOS extension i.e. without the 'full stop' and subsequent three characters). If this file already exists in the working directory, FARADIP.THREE will summarise the "Global" information (title, environment and quality factors and failure modes) and will ask you if you wish to alter any of them. If you answer 'yes' you will be prompted with each value in turn and given the opportunity to alter it. When this has been completed, or in the event of your answering 'no' to the original request, FARADIP.THREE will return to the file menu.

The specified existing file may be output to the printer, viewed on the screen or edited by escaping to the main menu and exercising option D (-FMEA datafile menu) as described in 5.4. If a new filename has been entered then FARADIP.THREE will respond with "New file. Do you wish to continue?". You should respond 'Y' or 'N' (yes or no), indicating whether or not you wish to proceed with the new file.

If you do not wish to proceed FARADIP.THREE leaves you in the file menu. Otherwise, if you wish to proceed, it requests a title line to be associated with the data file. It then requests you to input the global information (i.e. environment and quality factors). The options offered on the screen are specific values but the program will accept values in the range 0.1 to 10.

You then define the two failure modes for which the assessment will be carried out. The user-defined file is then created. FARADIP.THREE actually creates two separate files, one with a file extension ".FDP" to contain component information and one with the file extension ".GBL" containing the global information. The program then returns you to the file menu.

- OPTION E (-edit globals)
This enables the globals (title environment, quality factor and failure modes) to be edited, as described above, for the file already opened. It achieves this by effectively re-opening the file in question and utilising the same procedure which is used when

opening a file in OPTION O, above.

- OPTION C (-copy)
This enables files to be copied using a new name. In this way FMEAs of assemblies or circuits, similar to ones already analysed, can be performed quickly by adding and deleting components to a copy of the existing file (see 5.4).

- OPTION D (-delete)
This enables files to be deleted. Both the component file and the global file will be deleted.

5.3 THE FAILURE RATE MENU OPTIONS

Assume that the MAIN MENU is displayed either because you have just entered FARADIP.THREE or because you have escaped from the other menus (see Figure 1).

Note that the current datafile is displayed at the top of the screen. If no file has been opened then the screen will read "FMEA file: Not defined". Note, also, that the title for the run (entered in OPTION O of 5.2 above) is not necessarily the same as the filename and may contain up to 60 characters. Notice, in the sample printout (section 6), that the filename is CCT22 whereas the run is called DETECTOR CIRCUIT.

The top left of the MAIN MENU (see Figure 1) will display the 12 primary component groups of the nested hierarchy of failure rate and failure mode data.

The component group can be selected by use of the vertical cursor keys. As each group is selected the lower level menus are displayed on the right hand side of the MAIN MENU. Entering RETURN will display the selected failure rates (see middle right hand side of Figure 1).

For some selections (e.g. alarms) the list of failure rates is displayed on selecting the primary (left hand) group whereas for others (e.g. discrete semiconductors, tubes and lamps) sub menus will be offered.

Microelectronics involves four options for each of the two primary groups (logic/linear and memory). These four options allow the user to take account of junction temperature. It is not considered justified to specify temperature any more

precisely in view of the wide tolerance inherent in the failure rate parameter. In the case of the microelectronics options earlier versions of FARADIP asked you to specify either CERAMIC or PLASTIC packaging. This no longer considered necessary, as discussed in Section 2 of this Manual.

The total failure rate, after all multiplying factors, is the figure shown in the FMEA print out.

If Passive Components are selected then the sub-menus displayed on the right hand side of the menu will be:

Capacitors
Resistors
Inductive components
Microwave components

If CAPACITORS are selected then the following will be displayed;

```
                    DATA SCREEN                FMEA file : Not defined
-------------------------------------------------------------------------------
Capacitor aluminium          0.0020     0.02      0.40
Capacitor ceramic            0.0004     0.05       .
Capacitor glass              0.0003      .        0.03
Capacitor mica               0.0005      .        0.06
Capacitor paper              0.0002     0.06      0.10
Capacitor plastic            0.0005     0.001     0.08
Capacitor tant nonsolid      0.0020     0.10      0.60
Capacitor tant solid         0.0007     0.10      0.30
Capacitor variable (air)     0.0050      .        4.00
Capacitor hv distribution    0.25        .         .

Failure Modes :
    Aluminium          S/C 0.30  O/C 0.40  Drift 0.05  Leak 0.15
    Ceramic            S/C 0.50  O/C 0.10  Drift 0.40
    Glass or mica      S/C 0.70  O/C 0.15  Drift 0.10
    Met. paper/film    S/C 0.30  O/C 0.65
    Paper              S/C 0.90  O/C 0.05
    Plastic            S/C 0.60  O/C 0.40
    Tantalum           S/C 0.55  O/C 0.30  Drift 0.05  Leak 0.10
-------------------------------------------------------------------------------
A-add record to FMEA file          ESC-previous menu
```

Notice - A SINGLE VALUE for the 3 phase power capacitor
- TWO VALUES indicating a range for the glass capacitor
- THREE VALUES for the mica capacitor indicating a most likely value of 0.002
- TWO VALUES for the ceramic capacitor indicating a range but with the higher value in the centre column. The centre column suggests the more likely value.

The failure modes are displayed below the failure rates.

- BROWSING (ESC-previous menu)
The menus can be studied, without adding to or creating a file, by using the ESCAPE option. ESCAPE will always lead to the next higher level in the hierarchy and, eventually, to the MAIN MENU.

- ADDING (-add record to FMEA file)
This option allows components to be added to your file. If the option is selected with no file open then the program routes you to the FILE MENU (see section 5.2).

If you wish to add a component to the file you will be asked to enter:

COMPONENT REF (6 chars)	Usually a component number from a drawing (e.g. IC21).
COMP NAME (8 chars)	Enter a name (e.g. SiDiode).
FAILURE RATE	Select a value from the range.
FAILURE MODE 1 (6 chars)	Enter N if not applicable (in other words, that component cannot contribute to the mode in question. Enter A if all failures of that component cause the mode. Enter suitable characters (e.g. O/C for open circuit).
PROPORTION (0 to 1)	Enter the failure mode proportion (e.g. 0.5 for O/C zener). If N or A have been selected 0 or 1 will automatically be entered.
FAILURE MODE 2 (6 chars)	as above
PROPORTION (0 to 1)	as above

If you wish to escape press carriage return before entering a component reference. When asked to confirm, the options allow;

Y for accept,
N for re-input

- COMPONENT QUANTITY
In some cases (e.g. solder connections and relay contacts) it may be necessary to enter a multiplier so that a number of identical components can be accommodated in a single line. Remember that they must be identical for all the FARADIP.THREE parameters including the effects of their failure modes. These entries are made by typing, in place of the component reference:

*(followed by the number of components as shown in lines 7 and 9 of the sample printout in section 6). Thus *25 signifies 25 of that component.

When all the data has been entered for each component, you will be given the opportunity to state whether the entered values are correct or whether you wish to alter any of them. A response that the data is correct causes the line to be saved in RAM. However, it is wise to save one's data, from time to time, on disk. This can be achieved by reopening the file in question. All data is, of course, saved on exiting the program.

After each line FARADIP.THREE remains with the same component group leaving you the option of returning to the MAIN MENU by using ESC.

The failure rate shown in the "The total failure rate" column of the print out is the rate after multiplication by the quality, environment and package parameters.

5.4 EDITING AND PRINTING

By selecting option D (-FMEA datafile menu) from the MAIN MENU, the FMEA file is displayed enabling one to scroll through the entries (bottom of Figure 1).

- OPTION S (-summary)
This provides the failure rates and MTBFs for the 2 failure modes and for the parts count total.

- OPTION E (-edit line)
The line to edited is selected by cursor. This option allows individual component entries to be altered or deleted. Any part of the entry (mode, rate, component ref: etc) may be changed. Pressing carriage return after each parameter has been offered causes it to be retained. The failure rates and MTBFs are automatically adjusted.

- OPTION D (-delete line)
The line to be deleted is selected by cursor. This option allows a line to be removed from the file. The failure rates and MTBFs are automatically adjusted.

- OPTION P (-print file)
This allows the current file to be printed. To print a different file the desired file must be opened as described in 5.2. An example of FARADIP.THREE output is given in section 6. Line numbers are included for your convenience but have no significance within the file. The remaining line numbers are readjusted after deletion of a line. The current file may be printed to a file for purposes of importing/retrieving into a word processor document (eg Word Perfect). When using the print option specify the file name and destination (eg A:\WP\FILENAME) instead of defaulting to the line printer. Note that, after importing the file into a document, it may be necessary to amend the margins in order to accommodate the print out.

5.5 EXITING FARADIP.THREE

- OPTION X (-exit program)
This causes all files to be closed and saved. You should always use this option to exit from the program in order not to risk losing data.

5.6 GENERAL

For both failure modes, and for parts count, failure rates are expressed per million hours and MTBFs are given in years. The data is a considerably updated version of the ranges published in Reliability Maintainability and Risk, 5th edition, Butterworth Heinemann ISBN 07506 37528, David J Smith. The book is also a comprehensive overview of practical reliability techniques and theory.

One way of utilising FARADIP.THREE is to input the failure rates using the minimum of each range and then to carry out an edit run on a copy of the file, changing the rates to the maxima. In this way a prediction range can be established.

In order to carry out this procedure it would be necessary to mark up a printed copy of the file since the edit routine does not route you via the data screens.

6. SAMPLE PRINTOUT

The following is a sample of FARADIP.THREE printout.

FARADIP-THREE PRINTOUT - 18/12/96 - DETECTOR CIRCUIT
Environment factor is : 1 Quality factor is : 1

	Comp Ref	Comp name	Total failure rate	Failure Mode 1	Mode 1 factor	Failure rate mode 1	Failure mode 2	Mode 2 factor	Failure rate mode 2
1	IC1	8086	.1500	LOW	0.80	.1200	HIGH	0.01	.0015
2	IC12	CMOS	.0800	HIGH	0.25	.0200	LOW	0.25	.0200
3	D21	SiLP	.0010	O/C	0.25	.0003	O/C	0.15	.0002
4	TR30	NPNLP	.0500	S/C	0.30	.0150	O/C	0.30	.0150
5	Z3	QCRYST	.1000	All	1.00	.1000	None	0.00	.0000
6	C9	TANT	.0050	S/C	1.00	.0050	None	0.00	.0000
7	*25	RFILM	.0500	O/C	0.50	.0250	None	0.00	.0000
8	UV3	UVDET	5.000	SPUR	0.50	2.500	FAIL	0.50	2.500
9	*150	CONNS	.0600	50%	0.50	.0300	50%	0.50	.0300
10	SW2	MSWTCH	.500	O/C	0.30	.1500	S/C	0.10	.0500
11	PCB	PTPCB	.0100	20%	0.20	.0020	20%	0.20	.0020
12	R5C'1	COIL	.2000	O/C	0.10	.0200	None	0.00	.0000
13	R5CON	CONT	.200	O/C	0.80	.1600	S/C	0.10	.0200
14	X1	TRANS	.0300	All	1.00	.0300	None	0.00	.0000
15	F1	FUSE	.1000	All	1.00	.1000	None	0.00	.0000

Parts count
Total Failure rate = 6.536 per Million hours
Total MTBF = 17.47 Years

SPURIOUS OUTPUT
Failure mode 1 rate = 3.277 per Million hours
Failure mode 1 MTBF = 34.83 Years

FAILURE OF OUTPUT
Failure mode 2 rate = 2.639 per Million hours
Failure mode 2 MTBF = 43.26 Years

APPENDIX 3 - CORRELATION BETWEEN PREDICTED RELIABILITY AND SUBSEQUENT FIELD DATA

REFERENCE NUMBERS IN THIS APPENDIX REFER TO DOCUMENTS WITHIN THE AUTHOR'S DATA BANK (THEY ARE NOT LISTED IN APPENDIX 1)

SUMMARY

OBJECTIVES

To assemble a number of reliability predictions for which subsequent field failure data are available. To group these predictions according to the relevance of the failure rate data used therein. To ascertain the accuracy of these predictions by expressing them as ratios of predicted to observed MTBF or failure rate. To draw conclusions about the use of different types of reliability data (ie site specific, industry specific, generic). To propose a method, based on the above findings, of expressing the confidence of a reliability prediction according to the source of failure rate data used.

METHOD

Forty four examples were collected whereby field data were available for an item which had been subject to a reliability prediction.

Ratios were calculated of predicted to field failure rate and the distribution of these ratios studied to establish whether there is a pattern.

RESULTS

The data shows a clear distinction between predictions using the following types of data:

- SITE SPECIFIC
- INDUSTRY SPECIFIC
- GENERIC

APPENDIX 3 - CORRELATION BETWEEN PREDICTED RELIABILITY AND SUBSEQUENT FIELD DATA

Section 4 provides tables showing the likely inference from predictions. They contain statements that one is 90% confident that an eventual field failure rate will be BETTER than:

2½ TIMES THE PREDICTED WHEN SITE SPECIFIC DATA IS USED
4 TIMES THE PREDICTED WHEN INDUSTRY SPECIFIC DATA IS USED
6 TIMES THE PREDICTED WHEN GENERIC DATA IS USED

and 95% confident that it will be BETTER than:

3½ TIMES THE PREDICTED WHEN SITE SPECIFIC DATA IS USED
5 TIMES THE PREDICTED WHEN INDUSTRY SPECIFIC DATA IS USED
8 TIMES THE PREDICTED WHEN GENERIC DATA IS USED

1. OBJECTIVES & ASSUMPTIONS

1.1 To assemble a number of reliability predictions for which subsequent field failure data are available.

1.2 To group these predictions according to the relevance of the failure rate data used therein.

1.3 To ascertain the accuracy of these predictions by expressing them as ratios of predicted to observed MTBF or failure rate.

1.4 To draw conclusions about the use of different types of reliability data (ie site specific, industry specific, generic).

1.5 To propose a method, based on the above findings, of expressing the confidence of a reliability prediction according to the source of failure rate data used.

1.6 Assume that failure rates, in this context, are constant and that therefore an MTBF (meantime between failures) is the reciprocal of the corresponding failure rate.

APPENDIX 3 - CORRELATION BETWEEN PREDICTED RELIABILITY AND SUBSEQUENT FIELD DATA

2. PREDICTIONS AND ASSOCIATED FIELD DATA

The following is a list of predictions carried out by (or under the supervision of) the author, together with corresponding field failure data. It is grouped according to the specific nature of the original failure data used in the prediction. There are 3 classifications:

- SITE SPECIFIC (< 3 years old)
- INDUSTRY SPECIFIC
- GENERIC

Site specific data is that failure rate data collected within 3 years of the prediction and for a site having the same type of equipment under more or less identical operating and maintenance regimes. Industry specific data implies very similar operating and maintenance conditions and equipment of the same general type and technology. Generic data involves published data bases which embrace multiple industries and equipment types.

Some of the original predictions and data reports were expressed as MTBFs. All figures have been converted to failure rates (per million hours) for consistency in this study.

2.1 Site Specific (< 3 years)

Example 2.1.1 - An electronically corrected flow meter

Predictions were carried out on 4 such meter types in 1985 (reference Technis RR102/1&2 and notebook p172).

Field failure rate data were collected over the period 1984 to 1988 for the instruments in question and over a range of identical environments/sites.

APPENDIX 3 - CORRELATION BETWEEN PREDICTED RELIABILITY AND SUBSEQUENT FIELD DATA

The results were, for 1984 data (collected after the prediction):

ITEM	λ pmh FIELD DATA	λ pmh PREDICTION	RATIO OPTIMISTIC	RATIO PESSIMISTIC
Manufacturer 1	16	12.6	1.3	-

The results were, for 1986 data (collected after the prediction):

ITEM	λ pmh FIELD DATA	λ pmh PREDICTION	RATIO OPTIMISTIC	RATIO PESSIMISTIC
Manufacturer 1	12.6	11	1.1	-
Manufacturer 3	9.5	11	-	1.2
Manufacturer 4	19	8.8	2.2	-

The results were, for 1987-88 data (collected after the prediction):

ITEM	λ pmh FIELD DATA	λ pmh PREDICTION	RATIO OPTIMISTIC	RATIO PESSIMISTIC
Manufacturer 1	4.8	12.6	-	2.6
Manufacturer 2	2.8	9.5	-	3.4
Manufacturer 3	4.4	11	-	2.5
Manufacturer 4	7.6	8.8	-	1.2

2.2 Industry Specific

Example 2.2.1 - A token operated flow meter

The example in 2.3.5 was also predicted, in 1987, using industry specific data for a similar construction of corrected flow meter (reference Technis RR186). Field failure rate data were also available from the user for 1989 (reference RR234).

ITEM	λ pmh FIELD DATA	λ pmh PREDICTION	RATIO OPTIMISTIC	RATIO PESSIMISTIC
Meter	16	7.1	2.3	-

Example 2.2.2 - An electronically corrected flow meter

Predictions were carried out on the 4 meter types referred to in section 2.1.1 above in 1985 (reference Technis RR102/1&2 and notebook p172).

Field failure rate data were collected over the period 1989-90 for the instruments in question and over a range of identical environments/sites. The results were:

ITEM	λ pmh FIELD DATA	λ pmh PREDICTION	RATIO OPTIMISTIC	RATIO PESSIMISTIC
Manufacturer 1	5.1	12.6	-	2.5
Manufacturer 2	2.4	9.5	-	4
Manufacturer 3	2	11	-	5.5
Manufacturer 4	3.4	8.8	-	2.6

APPENDIX 3 - CORRELATION BETWEEN PREDICTED RELIABILITY AND SUBSEQUENT FIELD DATA

Example 2.2.3 - A gas pressure reduction process

Predictions were carried out for the loss of supply mode in a pressure reduction facility (reference Technis RR236) in 1988. The data used were industry specific from similar sites.

Field failure rate data were collected over a period from 1975-92 and analysed subsequent to the prediction (reference RR423) in 1993. The results were:

ITEM	λ pmh FIELD DATA	λ pmh PREDICTION	RATIO OPTIMISTIC	RATIO PESSIMISTIC
Station Loss	0.088	0.029	3	-

Example 2.2.4 - A volumetric gas offtake process

Predictions were carried out for the loss of supply mode in a facility (reference Technis RR179p13) in 1987. The data used were industry specific from similar sites.

Field failure rate data were collected over a period from 1975-92 and analysed subsequent to the prediction (reference RR423) in 1993.

The results were:

ITEM	λ pmh FIELD DATA	λ pmh PREDICTION	RATIO OPTIMISTIC	RATIO PESSIMISTIC
Station Loss	0.64	0.55	1.2	-

APPENDIX 3 - CORRELATION BETWEEN PREDICTED RELIABILITY AND SUBSEQUENT FIELD DATA

Example 2.2.5 - A natural gas storage facility (ie gas holder)

Predictions were carried out for the overfilling, overextraction and seal loss failure modes (reference Technis RR299,266,299 respectively) in 1989/90. The data used were industry specific from similar sites. Field failure rate data were collected over a period from 1973-92 and analysed subsequent to the prediction (reference RR326) in 1993.

The results were:

ITEM	λ pmh FIELD DATA	λ pmh PREDICTION	RATIO OPTIMISTIC	RATIO PESSIMISTIC
Overfill	0.32	0.11	2.9	-
Overfill	0.32	0.16	2	-
Overextract	0.035	0.011	3.2	-
Seal	1.3	1.1	1.2	-

NB: The duplicate entry above is due to there being more than 1 attempt at the prediction in reference RR299.

2.3 Generic

Example 2.3.1 - An oncology linear accelerator

4 printed board assemblies were subject to a parts count reliability prediction, in 1996, using the author's FARADIP data base. [Source reference Technis notebook p 155 and 173]. Field failure rate data were also obtained for the same assemblies for the year 1994, but after the predictions had been carried out. The results were:

APPENDIX 3 - CORRELATION BETWEEN PREDICTED RELIABILITY AND SUBSEQUENT FIELD DATA

ITEM	λ pmh FIELD DATA	λ pmh PREDICTION	RATIO OPTIMISTIC	RATIO PESSIMISTIC
Move enable	1.1	0.69	1.6	-
Move enable	1.1	3.7	-	3.4
Digital i/p	1	0.72	1.4	-
Thyristor control	3.4	2.2	1.5	-

Note: The duplicate entry above is due to the use of the FARADIP ranges whereby two predicted results were calculated.

Example 2.3.2 - A programmable logic controller

4 printed board assemblies were subject to a parts count reliability prediction (reference Technis T024), in 1988, using the author's FARADIP data base.

Field failure rate data were also obtained for the same assemblies for the year 1991 and 1995, after the predictions had been carried out (reference T024). The results were:

ITEM	λ pmh FIELD DATA	λ pmh PREDICTION	RATIO OPTIMISTIC	RATIO PESSIMISTIC
24/28dc isolation	4.9	6	-	1.2
115/125v isolation	8.2	4.9	1.7	-
Analog	4	5.8	-	1.5
115 8 point	8.8	3.5	2.5	-

APPENDIX 3 - CORRELATION BETWEEN PREDICTED RELIABILITY AND SUBSEQUENT FIELD DATA

Example 2.3.3 - A programmable logic controller

5 printed board assemblies were subject to 2 parts count reliability predictions (reference Technis DJS08), in c1983, by the manufacturer and by a system manufacturer using (it is believed) US MIL217.

Field failure rate data were also obtained from the operator/user for the same assemblies for the period 1983 to 1988, after the predictions had been carried out (reference DJS08). The results were:

ITEM	λ pmh FIELD DATA	λ pmh PREDICTION	RATIO OPTIMISTIC	RATIO PESSIMISTIC
MD8	0.79	4.5	-	5.7
MD8	0.79	1.5	-	1.9
MD3	4	8.1	-	2
MD3	4	3	1.3	-
SA7	0.66	10	-	16
SA7	0.66	2.4	-	3.7
SC3	1.2	10	-	8.6
SC3	1.2	1.25	-	1
CPU	25	28	-	1.1
CPU	25	30	-	1.2

Note: The duplicate entries above are for the 2 predictions.

APPENDIX 3 - CORRELATION BETWEEN PREDICTED RELIABILITY AND SUBSEQUENT FIELD DATA

Example 2.3.4 - A programmable logic controller

A PLC was subject to FMEA and parts count reliability prediction. (reference Technis RR194), in 1987, using FARADIP.TWO (an earlier version of FARADIP.THREE).

Field failure rate data were also available from the user for the mid 1980's (reference RR194). The results were:

ITEM	λ pmh FIELD DATA	λ pmh PREDICTION	RATIO OPTIMISTIC	RATIO PESSIMISTIC
PLC	9	27.4	-	3

The same exercise was conducted on a later model of the same PLC. The prediction (reference RR236) was in 1988.

Field data were obtained for the early 1990s (reference DJS07). The results were:

ITEM	λ pmh FIELD DATA	λ pmh PREDICTION	RATIO OPTIMISTIC	RATIO PESSIMISTIC
PLC	1	1.6	-	1.6

Example 2.3.5 - A token operated flow meter

A swipe card token meter was subject to FMEA and parts count reliability prediction (reference Technis RR186), in 1987, using FARADIP.TWO and also MIL217E.

Field failure rate data were also available from the user for 1989 (reference RR234).

The results were:

APPENDIX 3 - CORRELATION BETWEEN PREDICTED RELIABILITY AND SUBSEQUENT FIELD DATA

ITEM	λ pmh FIELD DATA	λ pmh PREDICTION	RATIO OPTIMISTIC	RATIO PESSIMISTIC
Meter	16	38	-	2.4
Meter	16	5	3.2	-
Meter	16	11	1.5	-

The duplicated results refer to the FARADIP range and the single result to MIL217E.

Example 2.3.6 - A rail track-circuit

Reference DJS01 contains a parts count prediction, using FARADIP.THREE, for a rail dc track circuit.

DJS01 also contains field data, from two separate geographical regions, for that item.

The results were:

ITEM	λ pmh FIELD DATA	λ pmh PREDICTION	RATIO OPTIMISTIC	RATIO PESSIMISTIC
Region 1	36	5.6	6.4	-
Region 2	50	5.6	8.9	-

APPENDIX 3 - CORRELATION BETWEEN PREDICTED RELIABILITY AND SUBSEQUENT FIELD DATA

3. CORRELATION OF PREDICTIONS AND DATA

3.1 Worksheet

Section 5 is a worksheet in which the statistical computations, based on the foregoing data (in section 2), are carried out.

The data are grouped into the 3 categories described (Site/Industry/Generic).

Section 5.1 shows the 3 data groups without distinction between optimistic (negative) and pessimistic (positive) ratios. This enables optimistic and pessimistic ratios (eg 2 and 0.5) to be treated symmetrically. The ratios are ranked and the means of the ratios are calculated.

Section 5.2 shows the same data but distinguishing between optimistic and pessimistic ratios. This enables the standard deviations of the spreads of ratios to be calculated.

Section 5.3, in view of the small quantity of data, groups it together to test for a Gaussian distribution. The actual numbers of ratios between specific limits are compared with those inferred from the Normal distribution. A 75% goodness of fit is obtained.

3.2 Predictions v Data

Figures 1-3 show plots of the ratios of predicted to field data against the median rank of the items in the sample. The ratio is expressed with the smaller failure rate as the divisor but as:

- Negative for an optimistic prediction (ie field failure rate < predicted)
- Positive for a pessimistic prediction (ie field failure rate > predicted)

3.3 Balance between optimistic and pessimistic results

There is no evidence to reject the assumption that predictions are equally likely to be optimistic or pessimistic. 21 of 44 were optimistic and 23 of 44 were pessimistic. The χ^2 test indicates that, without bias, this result is at least 75% likely to occur by chance. Furthermore, section 5.3 shows (at the bottom) the average ratio to be < 1 (ie 0.5) which indicates a distribution more or less balanced between optimistic and pessimistic predictions.

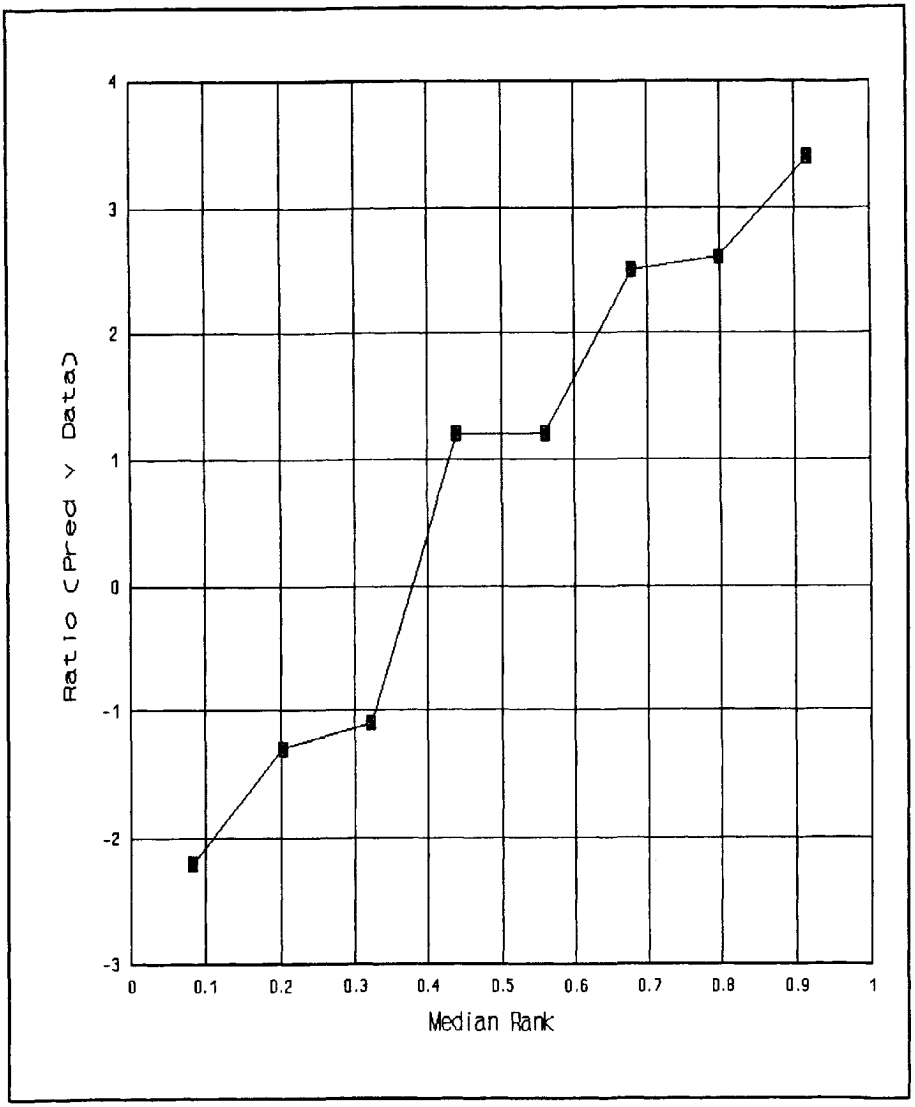
3.4 FARADIP.THREE data base

The author's FARADIP.THREE data ranges are based on numerous sources and are therefore GENERIC. They indicate that the range ratio of failure rates, from maximum to minimum, based on a wide range of quoted data sources is 7:1.

This is consistent with the findings (8:1) in section 4.3 below.

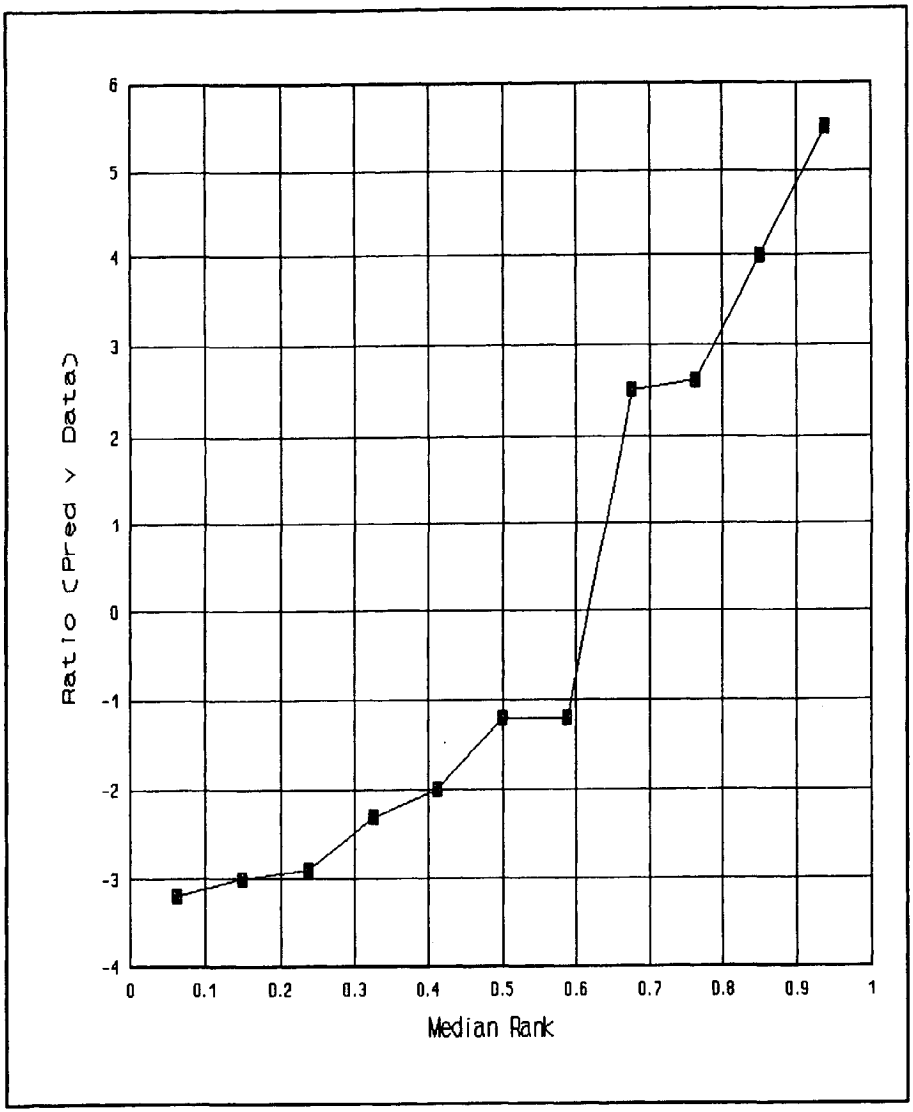
APPENDIX 3 - CORRELATION BETWEEN PREDICTED RELIABILITY AND SUBSEQUENT FIELD DATA

Figure 1 - Distribution of ratios (site specific)



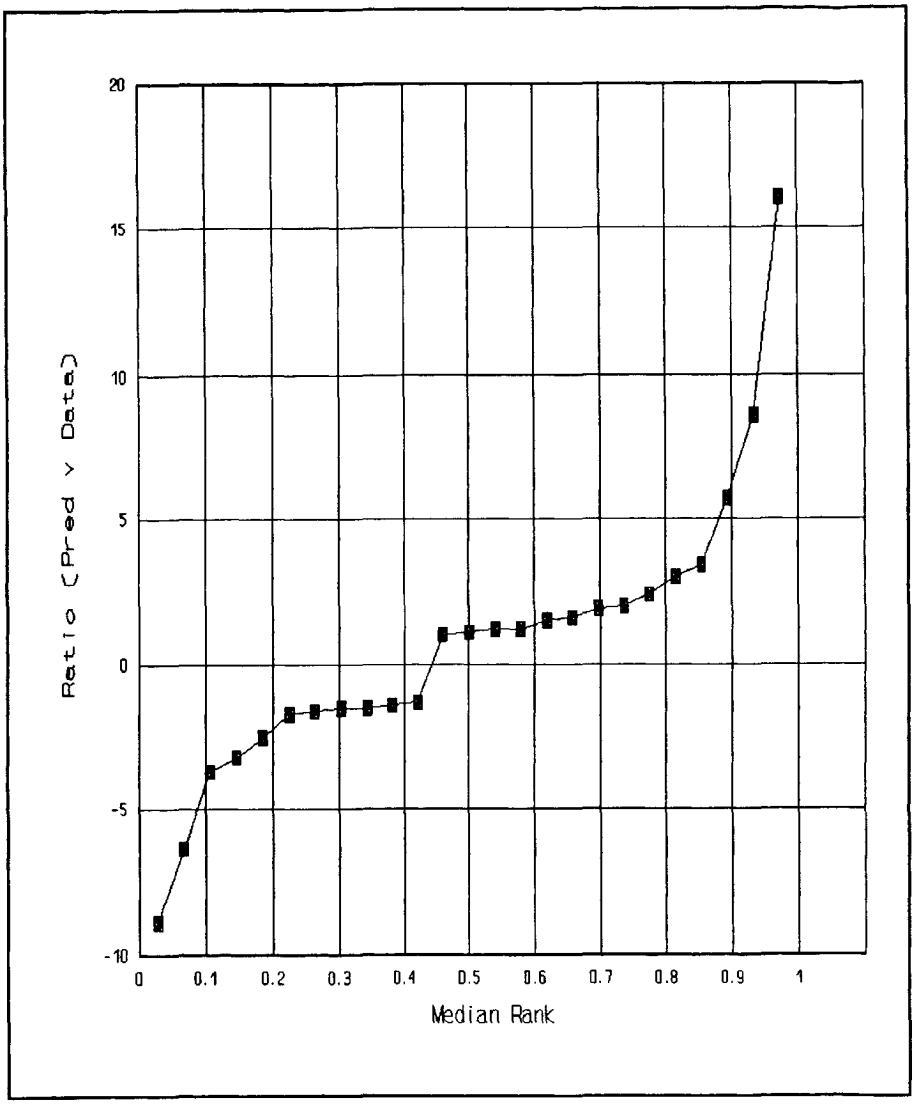
APPENDIX 3 - CORRELATION BETWEEN PREDICTED RELIABILITY AND SUBSEQUENT FIELD DATA

Figure 2 - Distribution of ratios (industry specific)



APPENDIX 3 - CORRELATION BETWEEN PREDICTED RELIABILITY AND SUBSEQUENT FIELD DATA

Figure 3 - Distribution of ratios (generic)



APPENDIX 3 - CORRELATION BETWEEN PREDICTED RELIABILITY AND SUBSEQUENT FIELD DATA

4. PROPOSED METHOD OF EXPRESSING PREDICTIONS

The following tables show the inferences which can be made from the Gaussian distribution.

4.1 For a prediction using site specific data (less than 3 years old)

One can be this confident:	That the eventual field failure rate will be BETTER than:
95%	3½ times the predicted
90%	2½ times the predicted
60%	1½ times the predicted
One can be this confident:	That the eventual field failure rate will be in the range:
90%	3½:1 to 2/7:1

4.2 For a prediction using industry specific data

One can be this confident:	That the eventual field failure rate will be BETTER than:
95%	5 times the predicted
90%	4 times the predicted
60%	2½ times the predicted
One can be this confident:	That the eventual field failure rate will be in the range:
90%	5:1 to 1/5:1

APPENDIX 3 - CORRELATION BETWEEN PREDICTED RELIABILITY AND SUBSEQUENT FIELD DATA

4.3 For a prediction using generic data

One can be this confident:	That the eventual field failure rate will be BETTER than:
95%	8 times the predicted
90%	6 times the predicted
60%	3 times the predicted
One can be this confident:	That the eventual field failure rate will be in the range:
90%	8:1 to 1/8:1

Comparing these inferences with Figures 1-3 shows broad agreement. The Gaussian inferences are slightly pessimistic (never optimistic) due to the distributions not being precisely Normal and to all three categories bring weighted slightly towards the pessimistic ratios.

APPENDIX 3 - CORRELATION BETWEEN PREDICTED RELIABILITY AND SUBSEQUENT FIELD DATA

5.1 WORKSHEET: RATIOS (means)

	GENERIC		INDUSTRY SPECIFIC		SITE SPECIFIC	
	Ratio	**MedRnk**	**Ratio**	**MedRnk**	**Ratio**	**MedRnk**
1	8.9	0.027559	3.2	0.061404	2.2	0.083333
2	6.4	0.066929	3	0.149123	1.3	0.202381
3	3.7	0.106299	2.9	0.236842	1.1	0.321429
4	3.2	0.145669	2.3	0.324561	1.2	0.440476
5	2.5	0.185039	2	0.412281	1.2	0.559524
6	1.7	0.224409	1.2	0.5	2.5	0.678571
7	1.6	0.26378	1.2	0.587719	2.6	0.797619
8	1.5	0.30315	2.5	0.675439	3.4	0.916667
9	1.5	0.34252	2.6	0.763158		
10	1.4	0.38189	4	0.850877		
11	1.3	0.42126	5.5	0.938596		
12	1.0	0.46063				
13	1.1	0.5				
14	1.2	0.53937				
15	1.2	0.57874				
16	1.5	0.61811				
17	1.6	0.65748				
18	1.9	0.69685				
19	2	0.73622				
20	2.4	0.775591				
21	3	0.814961				
22	3.4	0.854331				
23	5.7	0.893701				
24	8.6	0.933071				
25	16	0.972441				
Mean ratio	3.3724		2.763636		1.9375	

APPENDIX 3 - CORRELATION BETWEEN PREDICTED RELIABILITY AND SUBSEQUENT FIELD DATA

5.2 WORKSHEET: RATIOS (standard deviations)

	GENERIC		INDUSTRY SPECIFIC		SITE SPECIFIC	
	Ratio	**MedRnk**	**Ratio**	**MedRnk**	**Ratio**	**MedRnk**
1	-8.9	0.027559	-3.2	0.061404	-2.2	0.083333
2	-6.4	0.066929	-3	0.149123	-1.3	0.202381
3	-3.7	0.106299	-2.9	0.236842	-1.1	0.321429
4	-3.2	0.145669	-2.3	0.324561	1.2	0.440476
5	-2.5	0.185039	-2	0.412281	1.2	0.559524
6	-1.7	0.224409	-1.2	0.5	2.5	0.678571
7	-1.6	0.26378	-1.2	0.587719	2.6	0.797619
8	-1.5	0.30315	2.5	0.675439	3.4	0.916667
9	-1.5	0.34252	2.6	0.763158		
10	-1.4	0.38189	4	0.850877		
11	-1.3	0.42126	5.5	0.938596		
12	1.0	0.46063				
13	1.1	0.5				
14	1.2	0.53937				
15	1.2	0.57874				
16	1.5	0.61811				
17	1.6	0.65748				
18	1.9	0.69685				
19	2	0.73622				
20	2.4	0.775591				
21	3	0.814961				
22	3.4	0.854331				
23	5.7	0.893701				
24	8.6	0.933071				
25	16	0.972441				
Mean	0.67644		-0.10909		0.7875	
Overall Mean	**-0.5002**					
STD	4.83		3.15		2.08	

APPENDIX 3 - CORRELATION BETWEEN PREDICTED RELIABILITY AND SUBSEQUENT FIELD DATA

5.3 WORKSHEET: RATIOS (Gaussian fit)

The forty four ratios yield a standard deviation of 4.02. From the Gaussian distribution:

Between +/- standard deviations	Expected number of Ratios	Actual number of Ratios
2	42	41
1.5	38	40
1.3	36	38
1	30	37
0.7	23	29
0.5	17	19
0.3	10	9

A comparison, using χ^2, suggests 75% confidence of goodness of fit.

APPENDIX 4 - COMPARE User's Manual

COMPARE

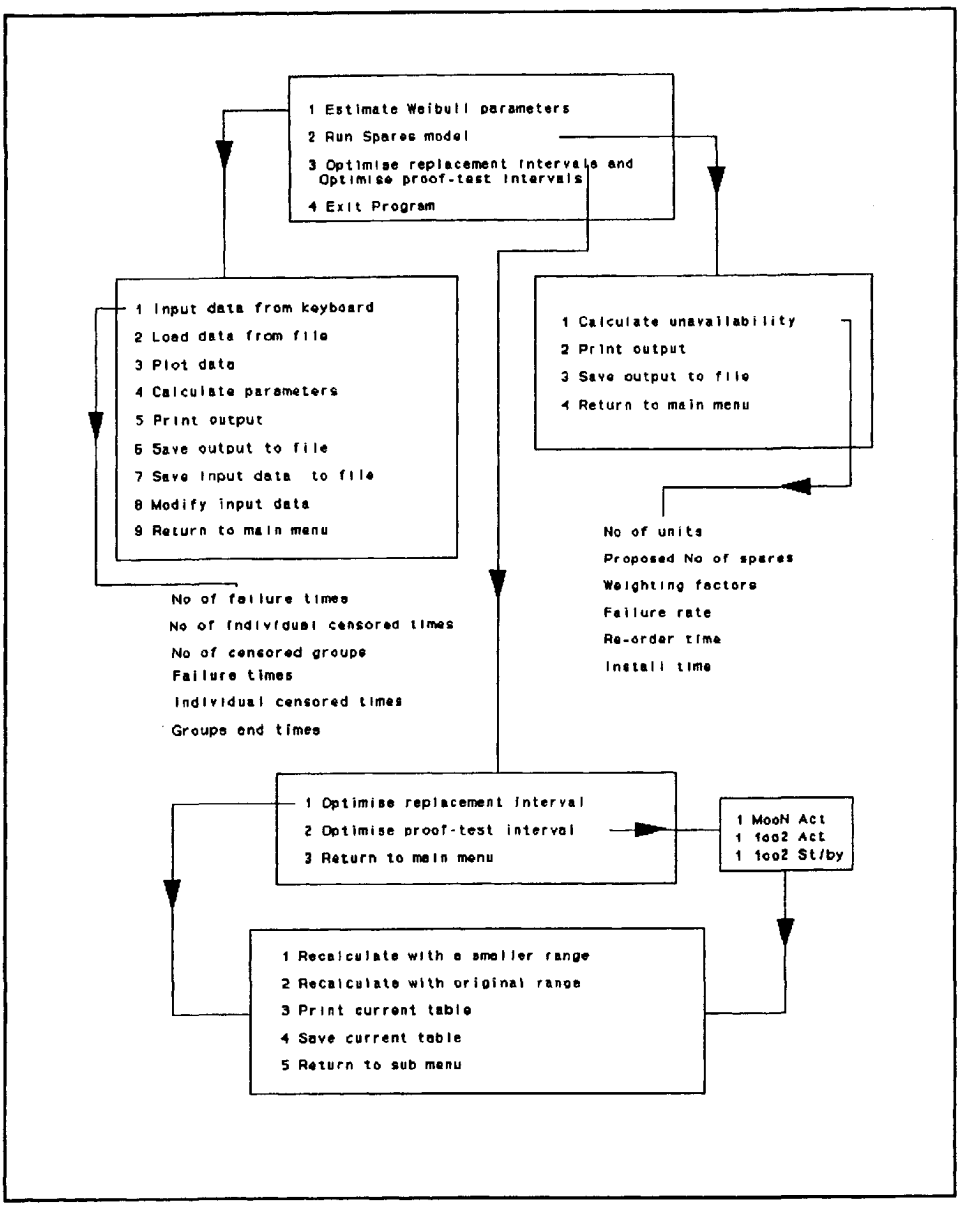
CALCULATING OPTIMUM MAINTENANCE PARAMETERS

USER MANUAL
ISBN 09516562 2 8
Version 1.1 (1998)

CONTENTS

APPENDIX 4 - COMPARE User's Manual

Figure 1 - Summary of screens



APPENDIX 4 - COMPARE User's Manual

PART 1 - BASIC RELIABILITY THEORY

Part 1 of the COMPARE manual is not included in this thesis.

PART 2 - RELIABILITY CENTRED MAINTENANCE

Reliability Centred Maintenance (RCM) is the process of using failure data to optimise the frequency of maintenance activities and of spares holdings. The following three sections (2.1 - 2.3) cover the main types of calculation.

2.1 Variable Failure Rates

In section 1.2, the meaning of Weibull analysis, and its associated shape parameter, BETA, and characteristic life parameter, ETA, was explained.

COMPARE provides a method of probability plotting whereby Weibull parameters are found which best fit the data being analysed.

It MUST be remembered that a computerised algorithm will allocate parameters to any data for a given distribution. It is, therefore, important to be aware of the limitations of probability plotting.

As times to failure are normally plotted on the horizontal axis, Least Squares estimation calculates the horizontal distance from each data point to an assumed line. It squares and then sums each of these values. A line is calculated which offers the minimum of this sum. It is that line which is used to provide the Weibull parameters.

Maximum Likelihood estimation plots a potential line. It calculates the probability of each data point being viable for the Weibull parameters associated with that line. A line is found which maximises the total probability of the data points fitting that line.

Because the Least Squares method minimises the sum of the distances from the data points to the assumed line on a linear basis, then it favours the lower values of time. Maximum Likelihood, however, gives equal value to each data point by virtue of calculating its probability of causing the estimated parameter.

The Maximum Likelihood estimation takes account of censored data beyond the last observed failure whereas Least Squares estimation only takes account of intermediate

censorings. Censored data are the operating times of items which did not fail or were removed from the test.

Maximum Likelihood estimation is usually taken as the realistic estimate. A comparison of the answers from the two methods provides another judgement (where there are no censored data) as to the goodness of fit to the Weibull assumption.

A large number of data collection schemes do not readily provide the times to failure of the items in question. For example, if an assembly (such as a valve) is replaced from time to time then its identity and its time to failure and replacement might be obtainable from the data. However, it might well be the diaphragm which is eventually the item of interest. Diaphragms may have been replaced during routine maintenance and the identity of each diaphragm not recorded. Subsequent Weibull analysis of the valve diaphragm would not then be possible. Careful thought has to be given when implementing a data collection scheme as to what subsequent DATA ANALYSIS will take place.

As in the above example of a valve and its diaphragm each of SEVERAL FAILURE MODES will have its own failure distribution for which Weibull analysis may be appropriate. It is very likely, when attempting this type of modelling, that data not fitting the 2 parameter distribution actually contains more than one failure mode. Separating out the individual failure modes may permit successful Weibull modelling.

If $\beta =< 1$ then there is no justification for replacement or even routine maintenance. If, on the other hand, $\beta > 1$ then there may be some justification for considering a preventive replacement before the item has actually failed. This will only be justified if the costs associated with an unplanned replacement (due to failure) are greater then those of a planned discard/replacement.

If this is the case then it is necessary to calculate:

a) the likelihood of a failure (ie $1\text{-}\exp\text{-}(t/\eta)^{\beta}$) in a particular interval times the cost of the unplanned failure.
b) the cost of planned replacements during that interval.

The optimum replacement interval which minimises the sum of the above two costs can then be found. Two maintenance philosophies are possible:

- AGE REPLACEMENT
- BLOCK REPLACEMENT

For the Age Replacement case, an interval starts at time t=0 and ends either with a failure or with a replacement at time t=T, whichever occurs first. The probability of surviving until time t=T is R(T) thus the probability of failing is 1-R(T). The average duration of all intervals is given by:

$$\int_0^T R(t)dt$$

Thus the cost per unit time is:

$$\frac{[£_u \times (1-R(T))] + [£_p \times R(T)]}{\int_0^T R(t)dt}$$

where $£_u$ is the cost of unplanned outage (ie failure) and $£_p$ is the cost of a planned replacement.

For the Block Replacement case, replacement always occurs at time t=T despite the possibility of failures occurring before time t=T. For this case the cost per unit time is:

$$(£_u \times T)/MTBF \times T + £_p/T$$
$$= £_u/MTBF + £_p/T$$

Note that, since the failure rate is not constant ($\beta > 1$), the MTBF used in the formula varies as a function of T.

COMPARE provides a package for each of these calculations (see section 3.4.1).

2.2 Spares Levels

In order to propose an optimum spares level it is necessary to calculate the unavailability which will occur taking account of the following variables:

- Number of spares
- Failure rate of the item
- Number of identical items
- Degree of redundancy within those items
- Lead time of procurement
- Replacement (Unit Down Time) time when an item fails

This relationship can be modelled by means of Markov state diagram analysis as described in detail in Smith D J, 1997, chapter 8.

Appendix A shows a typical state diagram for a situation involving 4 units and 2 spares. The lower left hand state represents 4 good items, with none failed and 2 spares. This is the "start" state. A failure (having the rate 4λ) brings the system to the state, immediately to the right, where there are 3 operating with one failure but still 2 spares. The transition diagonally upwards to the left represents a repair (ie replacement by a spare). The subsequent transition downwards represents a procurement of a new spare and brings the system back to the "start" state. The other states and transitions model the various possibilities of failure and spares states for the system.

If no redundancy exists then the availability (1-unavailability) is obtained by evaluating the probability of being in any of the 3 states shown in the left hand column of the state diagram. "3 out of 4" redundancy would imply that the availability is obtained from considering the probability of being in any of the states in the first 2 left hand columns, and so on.

Numerical evaluation of these states is obtained from COMPARE (see section 3.3) for each case of Number of Items, Procurement Time and Repair Time. Values of unavailability can be obtained for a number of failure rates and curves are then drawn for each case to be assessed. These are shown in Appendix B.

The appropriate failure rate for each item can then be used to assess the unavailability associated with each of various spares levels.

It should be noted that, as the number of spares increases, there is a diminishing return in terms of improved unavailability until the so called "infinite spares" case is reached. This is where the unavailability is dominated by the repair time and thus increased spares holding becomes ineffectual. At this point, only an improvement in repair time or in failure rate can increase the availability.

2.3 Redundancy with Proof-Testing

In the case of redundant systems where failed redundant units are not revealed then the option of periodic proof-test arises. Although the failure rate of each item is constant, the system failure rate actually increases.

The unavailability of a system can be calculated using the methods described in "Reliability, Maintainability and Risk", David J Smith, Butterworth Heinemann, and in section 2.2 above. It is clearly dependent partly on the proof-test interval which determines the down time of a failed (dormant) redundant item.

The technique involves calculating an optimum proof test interval for revealing dormant failures. It seeks to trade off the cost of the proof test (ie preventive maintenance) against the reduction in unavailability.

It applies where coincident dormant failures cause unavailability. An example would be the failure to respond of both a "high" alarm and a "high high" signal.

The unavailability is a function of the instrument failure rates and the time for which dormant failures persist. The more frequent the proof test, which seeks to identify the dormant failures, then the shorter is the down time of the failed items.

Assume that the "high" alarm and "high high" signal represent a duplicated redundant arrangement. Thus, one instrument may fail without causing plant failure (shutdown).

It can be shown that the reliability of the system is given by:

$$R(t) = 2\, e^{-\lambda t} - e^{-2\lambda t}$$

Thus the probability of failure is 1 - R(t)

$$= 1 - 2\,e^{-\lambda t} + e^{-2\lambda t}$$

If the cost of an outage (i.e. lost production) is $£_u$ then the expected cost, due to outage, is:

$$= (1 - 2\,e^{-\lambda t} + e^{-2\lambda t}) \times £_u$$

Now consider the proof test, which costs $£_p$ per visit. If the proof test interval is T then the expected cost, due to preventive maintenance, is:

$$= (2\,e^{-\lambda t} - e^{-2\lambda t}) \times £_p$$

The total cost per time interval is thus:

$$= [(1 - 2\,e^{-\lambda t} + e^{-2\lambda t}) \times £_u] + [(2\,e^{-\lambda t} - e^{-2\lambda t}) \times £_p]$$

The average length of each interval is $\int_0^T R(t)dt$

$$= 3/2\lambda - 2/\lambda\, e^{-\lambda T} + 1/2\lambda\, e^{-2\lambda T}$$

The total cost per unit time can therefore be obtained by dividing the above expression into the preceding one.

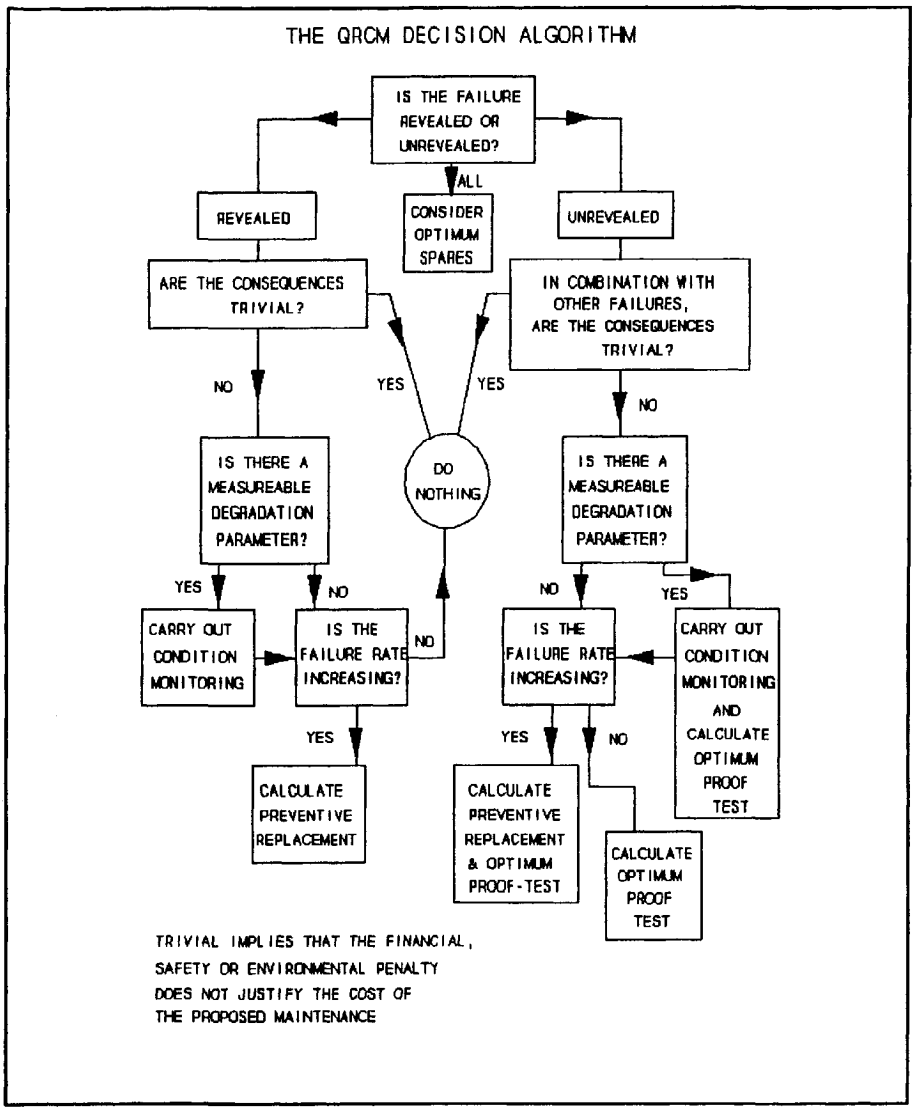
The minimum cost can be found by tabulating the cost against the proof-test interval (T). In the general case the total cost per unit time is:

$$\frac{[£_u \times (1-R(T))] + [£_p \times R(T)]}{\int_0^T R(t)dt}$$

2.4 The QRCM decision algorithm

Quantified RCM (QRCM) involves the techniques described above. The use of each of the techniques depends upon the failure distribution, the degree of redundancy and whether the cost of the maintenance action is justified by the saving in either operating costs, safety or environmental impact. Figure 2 is the QRCM decision algorithm which can be used during FMEA (failure mode and effect analysis). As each component failure is considered the QRCM algorithm provides the logic which leads to the use of each of the techniques.

Figure 2 - QRCM Algorithm



APPENDIX 4 - COMPARE User's Manual

PART 3. USING COMPARE

3.1 Loading COMPARE

COMPARE requires a maths co-processor. A non co-processor version can be compiled on request but will, as a result, run slower. The program may be run from the floppy disk or from a hard disk. To run on a hard disk create a directory e.g.

MD C:\COMPARE.

Then copy the file from the floppy supplied e.g.

COPY A:*.* C:\COMPARE

Switch to the drive or directory containing COMPARE and type compare. The program will automatically load and a title screen will be displayed, followed by a MAIN MENU which is shown at the top of Figure 1.

Options are: Estimate Weibull Parameters (see 3.2), Run Spares Model (see 3.3), Optimisation Routines (see 3.4).

> Note: In the following sections a number of the options involve COMPARE saving input and/or output data to disk. If no destination is specified it will save to the drive from which COMPARE is being run. If a different drive is required then it must be specified (e.g. A:\TEST).

3.2 Estimate Weibull Parameters

Options are:

(1) Input data from keyboard

There are three types of input may total up to 1000 entries made up of: a) Individual failure times. b) Individual censored times, in other words times for single items either removed at some point or allowed to survive beyond the last failure. c) Up to 10 groups of censored items where groups of items have either been removed at some point or allowed to survive beyond the last failure.

The program requests each of these inputs in turn and will accept up to a total of 1000 times (failures and censored items). A nil return for either of the censored categories causes that input request option to be skipped. See option (8) for editing the input data.

(2) Input data from file

If a previous set of data, saved using option (7), is to be analysed then enter the file name without an extension. A likely use of this facility is for a previous data set with some amendments. The .WBI Files can be edited with a standard text editor (eg EDIT in DOS). Alternatively the data can be loaded from this option and amended using option (8).

(3) Plot data

This is an important option since it allows the data to be viewed, after input, for a preliminary visual "goodness of fit" judgement. As emphasised in section 2.1, a computerised algorithm will find parameters for any data against a given distribution. It is dangerous to obtain Weibull parameters for data which is not a good fit to the Weibull assumption. COMPARE uses three techniques to assist the user in this respect and the graphical plot is the first of them.

There is an option to view the plot on the screen or to send it directly to the printer or to save it for subsequent importing into a Word Processor for use in a report. In the second two cases it is better to access this option AFTER the Calculate Parameters (4) option has been run. The parameters will then (and ONLY then) be superimposed onto the plot, below the 'x' axis.

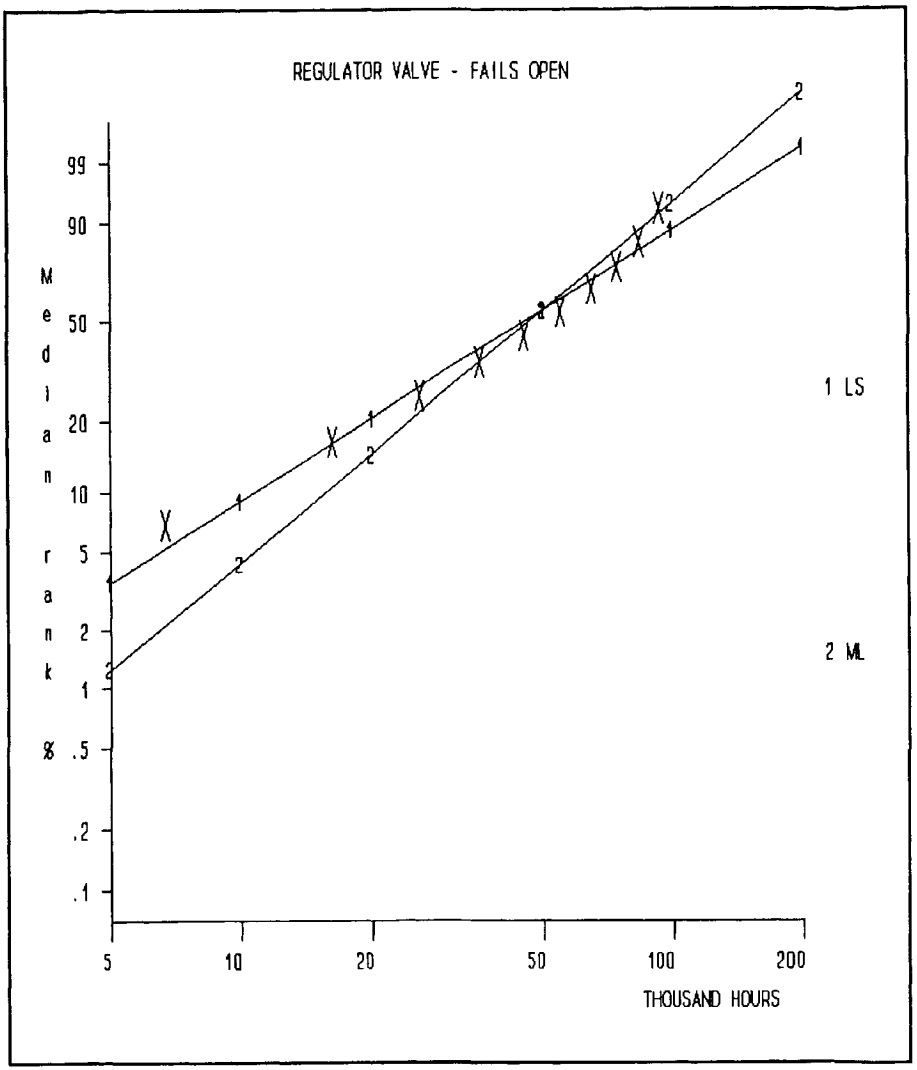
There are also options to add to the graph:

- A title
- The units of the 'x' axis (eg HOURS, CYCLES)
- One or both of the Least Squares and Maximum Likelihood lines

Note that the plotting options are offered ONLY after option (4) (calculate parameters) has been used.

Figure 3 shows a typical plot with the η (ETA) and β (BETA) parameters added.

Figure 3 - Weibull Plot



LEAST SQUARES η (ETA) = 58,000 HRS and β (BETA) = 1.4
MAX LIKELIHOOD η (ETA) = 56,000 HRS and β (BETA) = 1.8
Reject the hypothesis that β (BETA) = 1 at a significance of 17%

(4) Calculate parameters

In this option the values of the shape parameter, scale parameter and mean life are calculated. A further two means of protecting against making invalid inferences about the Weibull distribution are provided.

The first involves the use of the two estimation techniques (Least Squares and Maximum Likelihood) as described in section 2.1. The Mean Life is estimated only in the Maximum Likelihood calculation because the Least Squares method does not fully take account of censored items.

If (in addition to the confidence obtained from the above plot) the two values of Shape Parameter, obtained from the two methods, are in good agreement there is further evidence that the Weibull assumption applies.

A further test is provided by way of the Gnedenko test which tests for constant failure rate. This is an 'F' test which tests the hypothesis that the failure times are at random, ie $\beta = 1$. The screen will state whether or not it is valid to reject the assumption that $\beta = 1$. The lower the value of the significance % then the more likely it is that the failure rate is significantly different from constant.

Essentially the test compares the MTTF of the failure times as grouped either side of the middle failure time and tests for a significant difference.

If the total number of failure times is n, and the time of the $n/2_{th}$ failure is T, the two estimates are:

$$\frac{\sum_{i=1}^{n/2} t_i + n/2 \times T}{n/2} \text{ and } \frac{\sum_{i=n/2+1}^{n} (t_i - T)}{n/2}$$

That is to say we are comparing the MTTF of the "first half" of the failures and the MTTF of the "second half". The ratio should be one if the failure rate is constant. If it is not then the magnitude of the ratio gives an indication of significance. The ratio follows an 'F' distribution and the significance level can therefore be calculated. The 2 values of MTTF are shown on the screen.

It should be remembered that a small number of failure times, despite a high value of β, may not show a significant departure from the "random" assumption. In

practice 10 or more failure times is a minimum desirable data set for Weibull analysis. Nevertheless, engineering judgment should always be used to temper statistical analysis. The latter looks only at numbers and does not take account of known component behaviours.

> Note: If a poor fit is obtained from the 2 parameter model, and the plot is a simple curve rather than 'S' shaped or disjointed, then it is possible to attempt a 3 parameter model by estimating the value of γ described in section 1.2.2. The usual approach is to assume that γ takes the value of the first failure time and to proceed, as above, with the 2 parameter model to find η and β. Successive values of γ can be attempted, by iteration, until the 2 parameter model provides a better fit. It must be remembered however that if the reason for a poor fit with the 2 parameter model is that only a few failure times are available then the use of the 3 parameter model is unlikely to improve the situation.

(5) Print output

This prints the output displayed in option (4) above. See section 3.6.1 for an example.

(6) Save output to file

This enables the output to be saved as a file for future importing into a report on a word-processor. A file extension of .WBO is used.

(7) Save input data to file

This enables the input data to be saved for future editing and re-analysis. A file extension of .WBI is used.

(8) Modify input data

This option offers 5 possibilities:

> (1) Modify the failure times:
> Modify, delete, add, cursor and escape functions are described at the bottom of the screen. The current input is modified and

applies after returning to the "calculate" and "plot" options.

(2) Modify censored times:
Similar format to (1) above.

(3) Modify censored groups:
Similar format to (1) above. Return or Tab moves between the number of groups and the value of each group.

(4) Save data and return to Weibull menu:
Offers the opportunity to save or over-write an existing file.

(5) Return to Weibull menu without saving.

(9) Return to main menu

3.3 Run Spares Model

Options are:

(1) Calculate unavailability

The program requests the following data:
- The number of units for which the spare is to be held.
- The proposed number of spares.
- Weighting factors which are used to define unavailability and are explained in the next paragraph.
- The failure rate of the item in question.
- The reordering (procurement) time.
- The effective down time given that a spare is available.

The weighting factors allow the program to be used to calculate unavailability taking account of the throughput available from redundant items having less than 100% capacity.

For example, a 2 out of 3 redundant system whereby each stream provides 50% throughput has 4 states. These are a) None failed, b) One failed, c) Two failed, d) Three failed. States a) and b) result in 100% throughput and state c) in 50% throughput. The weighting factors to be entered would therefore be 0,0,0.5,1. This would result in the availability being calculated so as to allow some contribution from state c) rather than treating it as a failed state.

On the other hand, if the 2 out of 3 redundant system is regarded as failed unless 2 units are running then the weighting factors would be 0,0,1,1. In other words state c) is now treated as a failed state.

Note: 0 = no unavailability and 1 = 100% unavailability.

After inputting the data the program provides a reminder of the inputs together with:

- The weighted unavailability.
- The infinite spares unavailability.

The infinite spares unavailability is the unavailability which would be obtained with no possibility of running out of spares. It provides a useful indication of how close to the maximum credible spares level are the spares proposed. Eventually the unavailability is limited by the repair time and any increase in spares has no effect.

There is an option to re-run for a different number of spares or with different values of failure rate, re-order time and down time. Each of the runs will be stored, pending exit from this section of the program, and they will all be printed if the following option (2) is used.

(2) Print output

COMPARE offers a "short" and a "full" output. It will print the outputs for all runs made in the most recent use of option (1) above.

The "short" output provides the original screen of option (1) plus a summary of the possible numbers of units available with their probabilities, durations and weightings. See section 3.6.2 for a sample SHORT print out.

The "long" output also provides a full list of the possible states in the Markov analysis described in section 2.2.

(3) Save output to file

The program outputs are saved as SPARES1.SPO and SPARES2.SPO for the "short" and "long" versions. These remain on the drive and directory from which the program is being run until they are over-written by a subsequent use of the program.

They can be imported into a report on a word-processor. Option (3) allows one of these files to be saved permanently with a .SPO extension.

(4) Return to main menu

Graphs may be constructed, from the outputs of this package, as described in section 2.2.

3.4 Optimisation Routines

There are two options:

(1) Optimise Replacement Interval
(2) Optimise Proof-test Intervals

(1) Optimise Replacement Interval

Note that units are not specified for time. This allows hours, '000 hours, cycles, operations or any other suitable base to be used.

There are two maintenance strategies involving preventive replacement (discard):

a) If a failure occurs replace it and then wait the full interval before replacing again. This known as AGE replacement.
b) If a failure occurs replace it and nevertheless replace it again at the expiration of the existing interval. This is known as BLOCK replacement.

AGE replacement would clearly be more suitable for expensive items whereas BLOCK replacement might be appropriate for inexpensive items of which there are many to replace. Furthermore, BLOCK replacement is easier to administer since routine replacements then occur at regular intervals.

COMPARE calculates the replacement interval for both cases and such that the sum of the following two costs is minimised:

- The cost of Unplanned replacement taking account of the likelihood that it will occur.
PLUS

- The cost of the Scheduled replacement.

The program requests the Unplanned and Planned maintenance costs as well as the SHAPE and SCALE parameters.

Clearly the calculation is not relevant unless:

- SHAPE parameter, $\beta > 1$
AND
- Unplanned Cost > Planned Cost

COMPARE provides a table of total costs (for the two strategies) against potential replacement times (see section 3.6.3).

Option (1) allows a different range to be declared after viewing the initial table. A more precise optimum time can thus be obtained.
Option (2) allows a return to the original table.
Option (3) enables the table to be printed. See section 3.6.3 for a sample.
Option (4) allows the table to be saved for future viewing or for importing into a report on a word-processor. A file extension of .ORO is used.

Option (5) returns to the previous menu.

3.4.2 (2) Optimise Proof-Test Intervals

This enables the optimum proof-test interval (described in section 2.3) to be calculated. It finds the minimum of the total of the following two costs:

- Unavailability due to failures defeating the redundancy.
- Cost of the regular proof-tests.

Initially the sub-menu is:

(1) MooN (Active redundancy - identical)
(2) 1oo2 (Active redundancy - different)
(3) 1oo2 (Standby redundancy - different)
(4) Return to proof-test menu

The program requests the total number of units, the number of units required to operate, the MTBF of a unit and the Unplanned and Planned maintenance costs. For the Standby case both of the active and standby failure rates are requested.

COMPARE provides a table of total costs against potential replacement times in the same format as for optimum replacement above (see section 3.6.3).

Option (1) allows a different range to be declared after viewing the initial table. A more precise optimum time can thus be obtained.
Option (2) allows a return to the original table.
Option (3) enables the table to be printed. See section 3.6.3 for a sample.
Option (4) allows the table to be saved for future viewing or for importing into a report on a word-processor. A file extension of .OPO is used.
Option (5) returns to the previous menu.

(3) Return to Main menu

3.5 Exiting COMPARE

Use the "RETURN" commands until the screen with the "EXIT PROGRAM" option is reached. Use the "EXIT" option.

3.6 Sample print-outs

The following examples are the print-outs referred to in the preceding text.

3.6.1 Sample Weibull Results

Maximum Likelihood Estimation for a Two-Parameter Weibull distribution

Data Number	Data Value	Failure /Censured	Order number	Median Rank
1	1.00	F	1.00	0.07
2	3.00	F	2.00	0.16
3	8.00	F	3.00	0.26
4	12.00	F	4.00	0.36
5	19.00	F	5.00	0.45
6	22.00	F	6.00	0.55
7	33.00	F	7.00	0.64
8	66.00	F	8.00	0.74
9	99.00	F	9.00	0.84
10	120.00x1	C		

Total hours = 383.00 hours
Sample MTTF = 42.56 hours
Least Squares Median Rank estimation :
Shape estimate = 0.711
Scale estimate = 37.987 hours
Maximum Likelihood estimation :
Final estimate :
Shape = 0.759
Scale = 38.360 hours
Mean Life = 45.224 hours
MTTF(1) = 24.00 hrs MTTF(2) = 57.40 hrs
Gnedenko's test for constant failure rate :
There is no evidence to reject the hypothesis that Beta = 1
(Significance level = 23 %)

3.6.2 Spares Analysis (Sample SHORT printout)

COMPARE version x.x
Calculation of unavailability of a system of units with spares

With no redundancy (ie 2 out of 2)

Input data

Number of units = 2

Number of spares = 1

Failure rate = 10.0 per 1E6 hours

Re-order time = 300.0 hours

Install time = 2.0 hours

Cumulative state results

No of units available	Steady state probability		Frequency per 10^6 hrs	Average duration hours	Weighted probabil'y
2	0.99994	0.99994e+0	0.19999e+2	0.50000e+5	0.00000e+0
1	0.00006	0.57829e-4	0.19999e+2	0.28915e+1	0.57829e-4
0	0.00000	0.18978e-7	0.57826e-3	0.32819e+2	0.18978e-7

Weighted unavailability = 0.57848E-04

Infinite spares unavailability = 0.39999E-04

3.6.3 Sample Optimum Replacement Table

COMPARE version x.x

Calculation of optimum replacement interval
Shape parameter (Beta) = 2.000
Scale parameter (Eta) = 1,000 hours
Cost of unscheduled replacement = £20,000.000
Cost of planned replacement = £100.000

Replacement Interval	Cost/unit time Age Replacement	Cost/unit time Block Replacement
110	3.1	3.1
220	4.7	4.8
330	6.5	6.7
440	8.3	8.5
550	9.9	10.2
660	11.3	11.7
770	12.6	12.9
880	13.9	14.0
990	15.0	14.9
1100	16.1	15.6

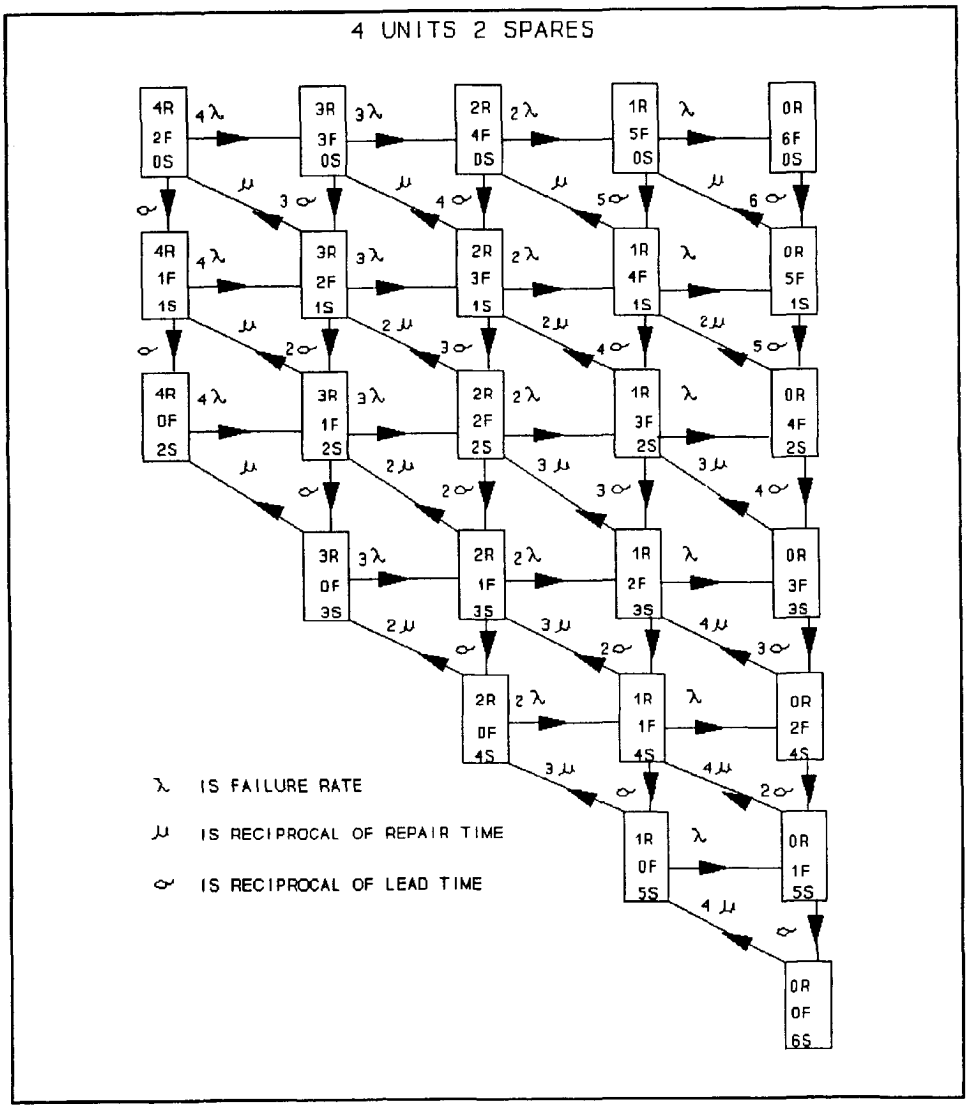
NOTE: In the above example, the optimum replacement interval is clearly < 110 hours. Thus option 1 (the smaller range request) would be used to examine 0-200 hours. See below.

WITH A SMALLER RANGE

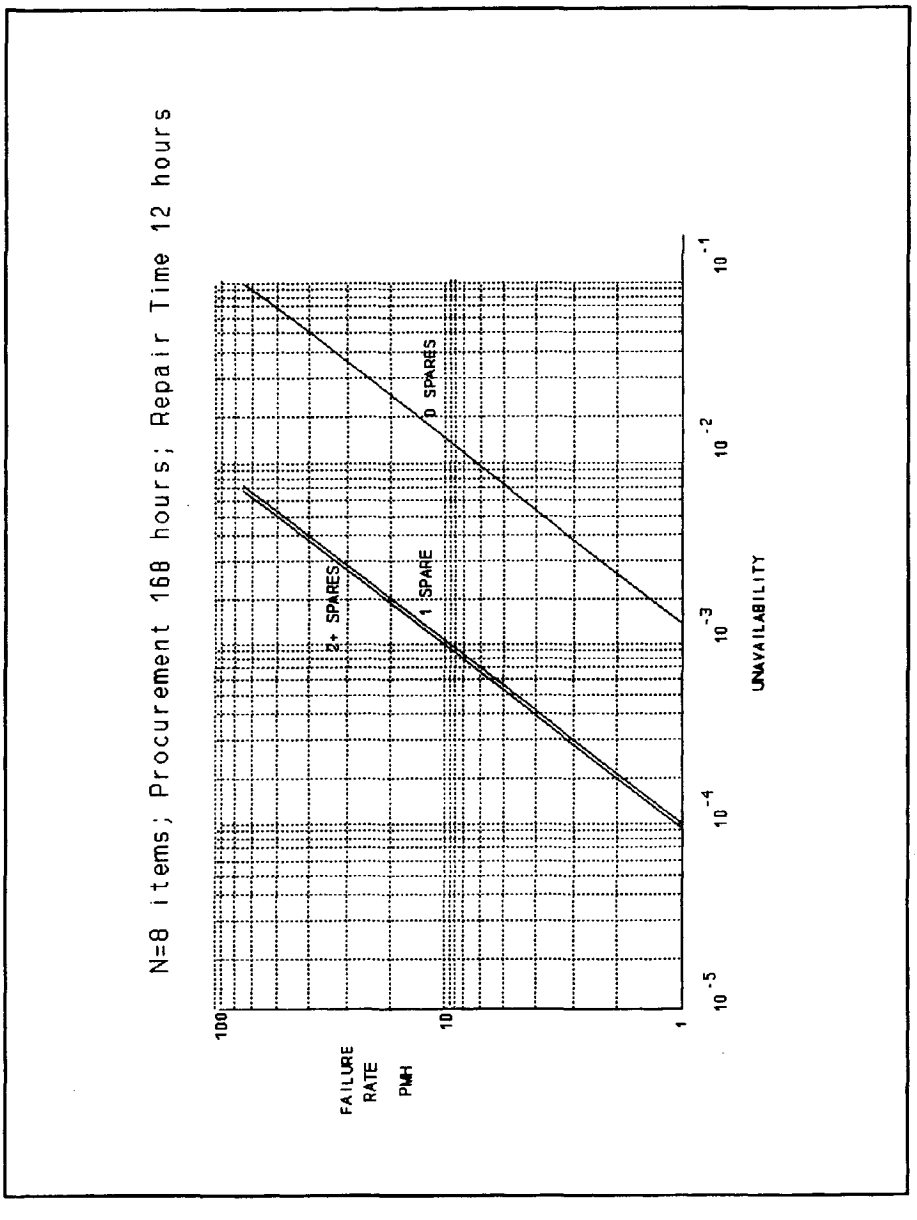
Replacement Interval	Cost/unit time Age Replacement	Cost/unit time Block Replacement
20	5.4	5.4
40	3.3	3.3
60	2.9	2.9
80	2.8	2.8
100	3.0	3.0
120	3.2	3.2
140	3.5	3.5
160	3.8	3.8
180	4.1	4.1
200	4.4	4.4

Thus, the optimum replacement interval, for both age replacement and block replacement, is 80 hours.

APPENDIX A - MARKOV STATE DIAGRAM



APPENDIX B - UNAVAILABILITY/SPARES CURVES



APPENDIX 5 - FAILURE RATE DATA SOURCES USED IN THE AUTHOR'S DATA BANK

The following data sources comprise the author's data bank. The FARADIP.THREE data ranges (chapter 3 and Appendix 2) are based on this composite data bank.

A.5.1 Published failure rate data documents

Generic Data

Extracts from the UKAEA SRD Data bank
IEE, Reliability of power supplies, 1977
UK MOD DX/99/013-100, Guided weapons systems, 1980
UK MOD RSRE method 250, 1977
RADC, non electronic Parts Data Bank, NPRD5, 1995 (also 2 & 3)
US MIL HANDBOOK 217F, 1993
Smith's aviation data bank, 1973 (retained for comparison)
Safety in the Process industries Prof Frank Lees
Dexter and Perkins data summaries, 1982
French P&T CNET, 1983
UK DEF STAN 00-41 (PART 3)/1, 1985.
RMC Consultants Ltd Data Handbook. 2nd Edition February, 1991
Manchester University, Valve & Pipeline Reliability symposium February 1994

Industry Specific Data

OREDA data books, 1982 and 1992
UK British Telecom HRD HRD5 1993
RB211, start and run assessment, 1978 (retained for comparison)
DNV, Pipeline reliability, 1980
Bonner & Moore Offshore data, 1977 (retained for comparison)
GE Co USA EPRI Report 5823, 1988, Gas & Steam Turbine Instrumentation
SINTEF STF38 F96409, 1996, Fire & Gas Detection Data

APPENDIX 5 - FAILURE RATE DATA SOURCES USED IN THE AUTHOR'S DATA BANK

A.5.2 The author's failure rate data studies

Industry and some Site Specific Data (author's report numbers)

Report T042 PHILIPS BACTON - AMINE AND H_2S, 1994
Report T049 ROUGH MORECAMBE FAILURE RATES & RCM, 1995
Report T050 TRANSCO/NTS FAILURE RATES, 1995
Report T059 GAS NTS FAILURE RATES, 1996
Report T061 REINEX Gas DATA REVIEW, 1996
Report T065A SLAMSHUTS TIMES TO FAILURE, 1996
Report T071 REGULATORS TIMES TO FAILURE, 1997
Report T079 FAILURE ANALYSIS CF41 PCs

A.5.3 UK gas industry failure rates

Industry and some Site Specific Data

101 references to the series RR1 to RR405 of UK gas industry failure data analyses reports over the periods 1984-1993.

A.5.4 Miscellaneous

Industry and some Site Specific Data

Over 100 memo type references each containing 1 or more failure rates, in the series D1/1 -1/104 in the author's data bank (1982-1996).

APPENDIX 6 - EXTRACT FROM THE AUTHOR'S DATA BANK

DETECTOR - SMOKE

ITEM	MODE	RATE	ENV	DATE	*	PFD	Reference	SOURCE
GENERAL	FAIL	8.4	GRF	96	*		T059	WARRINGTON
GENERAL	DRIFT	4.8	GRF	96	*		T059	WARRINGTON
GENERAL	TOTAL	12	GRF	96	*		T059	WARRINGTON
SMOKE		1.7	OFF	89	*		RR252	ROUGH
SMOKE		3	OFF	87	*		RR 170	MORECAMBE
SMOKE								
SMOKE	SPURIOUS	3.7	GRF	85	*		RR 112	ST FERGUS
SMOKE	FAIL	4	GRF	85	*		RR 112	ST FERGUS
SMOKE	FAIL	0.5	OFF	96		0.007	D44	SINTEF
SMOKE	SPURIOUS	2	OFF	96			D44	SINTEF
SMOKE	AUTODETECT	1.5	OFF	96			D44	SINTEF
SMOKE	TOTAL	4	OFF	96			D44	SINTEF
IONIZE	MAX	0.54	OFF	93			D29A	OREDA
IONIZE	ZERO O/P	0.22	OFF	93			D29A	OREDA
IONIZE	TOTAL	4.6	OFF	93			D29A	OREDA

* indicates original rather than data from a published source
PFD indicates probability of failure on demand (dimensionless)
Rate is per million hours

APPENDIX 7 - MARKOV AND RELATED EXPRESSIONS

From chapter 8.1.2 of Smith D J, 1997 .....

.....In order to cope with systems whose redundant units are subject to a repair strategy the Markov analysis technique is used. The technique assumes both constant failure rate and constant repair rate. For other distributions (e.g. Weibull failure rate process or logNormal repair times) Monte Carlo simulation methods are more appropriate.

The Markov method for calculating the MTTF of a system with repair is to consider the 'states' in which the system can exist. Consider a system with two identical units each having failure rate λ and repair rate (reciprocal of mean down time) μ. The system can be in each of three possible states.

State (0) Both units operating
State (1) One unit operating, the other having failed
State (2) Both units failed

It is important to remember one rule with Markov analysis, namely, that the probabilities of changing state are dependent only on the state itself. In other words, the probability of failure or of repair is not dependent on the past history of the system.

Let $P_i(t)$ be the probability that the system is in state (i) at time t and assume that the initial state is (0).

Therefore

$$P_0(0) = 1 \text{ and } P_1(0) = P_2(0) = 0$$

Therefore

$$P_0(t) + P_1(t) + P_2(t) = 1$$

We shall now calculate the probability of the system being in each of the three states at time $t + \Delta t$. The system will be in state (0) at time $t + \Delta t$ if:

1. The system was in state (0) at time t and no failure occurred in either unit during the interval Δt or,

2. The system was in state (1) at time t, no further failure occurred during Δt, and the failed unit was repaired during Δt.

The probability of only one failure occurring in one unit during that interval is simply $\lambda\Delta t$ (valid if Δt is small, which it is). Consequently $(1 - \lambda\Delta t)$ is the probability that no failure will occur in one unit during the interval. The probability that both units will be failure free during the interval is, therefore,

$(1 - \lambda\Delta t)(1 - \lambda\Delta t) = 1 - 2\lambda\Delta t$ (ignoring the $\lambda^2\Delta t^2$ term)

The probability that one failed unit will be repaired within Δt is $\mu\Delta t$, provided that Δt is very small. This leads to the equation:

$$P_0(t+\Delta t) = [P_0(t) \times (1 - 2\lambda\Delta t)] + [P_1(t) \times (1 - \lambda\Delta t) \times \mu\Delta t]$$

Similarly, for states 1 and 2:

$$P_1(t+\Delta t) = [P_0(t) \times 2\lambda\Delta t] + [P_1(t) \times (1 - \lambda\Delta t) \times (1-\mu\Delta t)]$$
$$P_2(t+\Delta t) = [P_1(t) \times \lambda\Delta t] + P_2(t)$$

Now the limit as $\Delta t \rightarrow 0$ of $[P_i(t+\Delta t)-P_i(t)]/\Delta t$ is $P_i(t)$ and so the above yield:

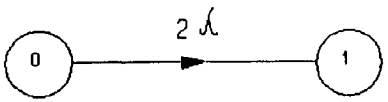
$$P'_0(t) = -2\lambda P_0(t) + \mu P_1(t)$$
$$P'_1(t) = 2\lambda P_0(t) - (\lambda+\mu)P_1(t)$$
$$P'_2(t) = \lambda P_1(t)$$

In matrix notation this becomes:

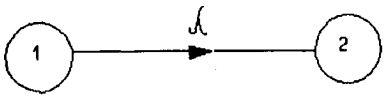
$$\begin{matrix} P'_0 \\ P'_1 \\ P'_2 \end{matrix} = \begin{matrix} -2\lambda & \mu & 0 \\ 2\lambda & -(\lambda+\mu) & 0 \\ 0 & \lambda & 0 \end{matrix} \begin{matrix} P_0 \\ P_1 \\ P_2 \end{matrix}$$

The elements of this matrix can also be obtained by means of a Transition Diagram. Since only one event can take place during a small interval, Δt, the transitions between states involving only one repair or one failure are considered. Consequently, the transitions (with transition rates) are:

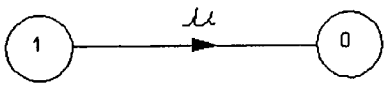
by failure of either unit



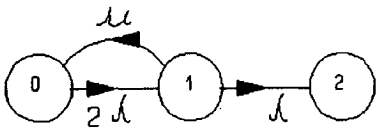
by failure of the remaining active unit



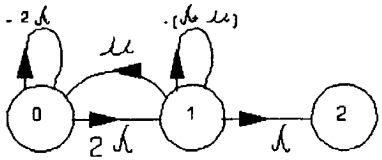
by repair of the failed unit of state 1



the transition diagram is



Finally closed loops are drawn at states 0 and 1 to account for the probability of not changing state. The rates are calculated as minus the algebraic sum of the rates associated with the lines leaving that state.



APPENDIX 7 - MARKOV AND RELATED EXPRESSIONS

A (3 x 3) matrix, $(a_{i,j})$, can now be constructed, where $i=1,2,3$; $j=1,2,3$; $a_{i,j}$ is the character on the flow line pointing from state j to state i. If no flow line exists the corresponding matrix element is zero. We therefore find the same matrix as before.

The MTTF is defined as:

$$\begin{aligned}\theta_s &= \int_0^\infty R(t)\,dt \\ &= \int_0^\infty [P_0(t) + P_1(t)]dt \\ &= \int_0^\infty P_0(t)dt + \int_0^\infty P_1(t)dt \\ &= T_0 + T_1\end{aligned}$$

The values of T_0 and T_1 can be found by solving the following:

$$\int_0^\infty \begin{bmatrix} P'_0(t) \\ P'_1(t) \\ P'_2(t) \end{bmatrix} dt = \int_0^\infty \begin{bmatrix} -2\lambda & \mu & 0 \\ 2\lambda & -(\lambda+\mu) & 0 \\ 0 & \lambda & 0 \end{bmatrix} \begin{bmatrix} P_0 \\ P_1 \\ P_2 \end{bmatrix} dt$$

which reduces to:

$$\begin{bmatrix} P_0(\infty)-P_0(0) \\ P_1(\infty)-P_1(0) \\ P_2(\infty)-P_2(0) \end{bmatrix} = \begin{bmatrix} -2\lambda & \mu & 0 \\ 2\lambda & -(\lambda+\mu) & 0 \\ 0 & \lambda & 0 \end{bmatrix} \begin{bmatrix} T_0 \\ T_1 \\ T_2 \end{bmatrix}$$

However:

$$P_0(0) = 1 \qquad P_1(0) = P_2(0) = 0$$
$$P_0(\infty) = P_1(\infty) = 0 \qquad P_2(\infty) = 1$$

Therefore:

$$\begin{bmatrix} -1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} -2\lambda & \mu & 0 \\ 2\lambda & -(\lambda+\mu) & 0 \\ 0 & \lambda & 0 \end{bmatrix} \begin{bmatrix} T_0 \\ T_1 \\ T_2 \end{bmatrix}$$

thus

$-1 = -2\lambda T_0 + \mu T_1$
$0 = 2\lambda T_0 - (\lambda+\mu)T_1$
$1 = \lambda T_1$

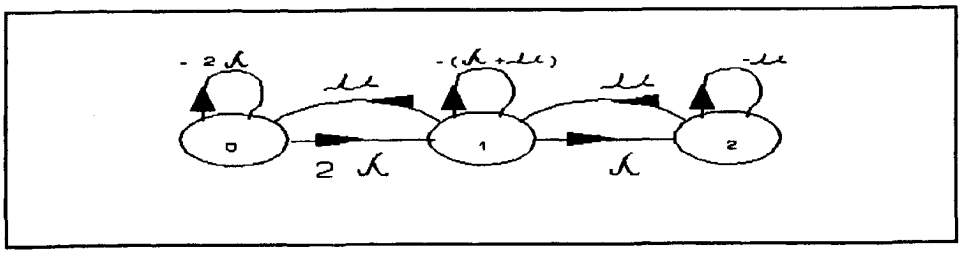
which gives:

$T_0 = (\lambda+\mu)/2\lambda^2$ and $T_1 = 1/\lambda$

$\theta_s = T_0 + T_1 = (\lambda+\mu)/2\lambda^2 + 1/\lambda$

$= (3\lambda+\mu)/2\lambda^2$

The Markov analysis technique can equally well be applied to calculating the steady state unavailability. To do this, one must consider recovery from the system failed state. The transition diagram is therefore modified to allow for this and takes the form:



The path from state (2) to state (1) has a rate of μ. This reflects the fact that only one repair can be considered at one time. If more resources were available then two simultaneous repairs could be conducted and the rate would become 2μ. Constructing a matrix as shown earlier:

P'_0	-2λ	μ	0	P_0
P'_1	2λ	$-(\lambda+\mu)$	μ	P_1
P'_2	0	λ	$-\mu$	P_2

APPENDIX 7 - MARKOV AND RELATED EXPRESSIONS

Since the steady state is being modelled the rate of change of probability of being in a particular state is zero, hence:

$$\begin{matrix} -2\lambda & \mu & 0 \\ 2\lambda & -(\lambda+\mu) & \mu \\ 0 & \lambda & -\mu \end{matrix} \begin{matrix} P_0 \\ P_1 \\ P_2 \end{matrix} = \begin{matrix} 0 \\ 0 \\ 0 \end{matrix}$$

Therefore

$$\begin{aligned} -2\lambda P_0 + \mu P_1 &= 0 \\ 2\lambda P_0 - (\lambda+\mu)P_1 + \mu P_2 &= 0 \\ \lambda P_1 - \mu P_2 &= 0 \end{aligned}$$

However, the probability of being in one of the states is unity, therefore:

$$P_0 + P_1 + P_2 = 1$$

The system unavailability is required and this is represented by P_2, namely, the probability of being in the failed state. Thus:

$$\text{Unavailability} = P_2 = 2\lambda^2/(2\lambda^2 + \mu^2 + 2\lambda\mu)$$

In a similar manner:

SYSTEM MTTF FOR PARTIAL ACTIVE REDUNDANCY WITH n REPAIR CREWS

1 UNIT	$1/\lambda$		
2 UNITS TOTAL	$(3\lambda+\mu)/2\lambda^2$	$1/2\lambda$	
3 UNITS TOTAL	$\frac{(11\lambda^2+7\lambda\mu+2\mu^2)}{6\lambda^3}$	$(5\lambda+\mu)/6\lambda^2$	$1/3\lambda$
	1 UNIT REQUIRED	2 UNITS REQUIRED	3 UNITS REQUIRED

APPENDIX 7 - MARKOV AND RELATED EXPRESSIONS

SYSTEM MTTF FOR PARTIAL ACTIVE REDUNDANCY WITH 1 REPAIR CREW

1 UNIT	$1/\lambda$		
2 UNITS TOTAL	$(3\lambda+\mu)/2\lambda^2$	$1/2\lambda$	
3 UNITS TOTAL	$\frac{(11\lambda^2+4\lambda\mu+\mu^2)}{6\lambda^3}$	$(5\lambda+\mu)/6\lambda^2$	$1/3\lambda$
	1 UNIT REQUIRED	2 UNITS REQUIRED	3 UNITS REQUIRED

APPENDIX 8 - SYLLABUS OF RAMS TOPICS FOR NON-SPECIALISTS

The purpose of this syllabus is to support the statement (in section 1.6e) that non-RAMS specialists require a level of training necessary to apply the method described in this thesis.

The Institution of Electrical Engineers (UK) Safety Critical Systems Committee have published recommendations for postgraduate qualifications syllabi and general educational requirements, 1992. It has also provided a benchmark for the assessment of competencies.

Having regard to these documents, the author proposes that the following syllabus is applicable to engineers who are not RAMS specialists. A study based on this syllabus would enable a competent engineer to apply the RAMS prediction methods described in this thesis.

TERMS

Vital importance of failure definition and of LCC **(1 hr)**
Understanding rate versus probability **(1 hr)**
Understanding availability versus reliability **(1 hr)**
The importance of using the appropriate RAMS term **(2 hrs)**
Definitions applicable to risk **(1 hr)**

FAILURE DATA

Meaning of a sample estimate versus actual failure rate **(1 hr)**
Understanding that exp $(-\lambda t)$ is the 1 parameter version of the more general Weibull case **(2 hrs)**
Realising that Weibull allows ANY fit and that significance is important **(2 hrs)**
RAMS ranges and confidence **(3 hrs)**

APPENDIX 8 - SYLLABUS OF RAMS TOPICS FOR NON-SPECIALISTS

RELIABILITY PREDICTION AND MODELLING

Practical implications of redundancy (ie improves one failure mode often at the expense of others) **(2 hrs)**
Coincident random failures versus dependent (CCF) effects **(2 hrs)**
FMECA, block diagrams and fault trees **(2 hrs)**
Human error **(1 hr)**
MDT = MTTR + function of proof-test + logistics **(1 hr)**
Reliability centred maintenance (optimum discard, optimum spares, optimum proof-test) **(3 hrs)**

RELIABILITY GROWTH

Duane model **(1 hr)**
Cusum plotting **(1 hr)**

RELIABILITY TESTING AND DEMONSTRATION

Discrimination in testing **(1 hr)**
Constructing test plans **(2 hrs)**

SAFETY INTEGRITY

Quantitative and qualitative features **(1 hr)**
Safety-integrity levels **(1 hr)**
Requirements for each SIL **(3 hrs)**

TOTAL = 35 HRS (c 1 WEEK)

APPENDIX 9 - COMPARISON OF FAILURE RATE DATA 1980s/1990s

The author's data bank was searched for entries which appeared in both the 1980s and the 1990s, which either:

- had the same description and source
- had the same description and more than 3 different sources in both the 1980s and 1990s

Some difficulty was experienced in that even with the same source an item appearing in the 1980s might have a slightly altered description in the 1990s. An example would be "Total" as opposed to "Critical" failures in the case of the OREDA source. Nevertheless it was possible to find 57 component types, covering 221 entries, for comparison. It was not possible to discriminate more closely than simply comparing the 1980s and 1990s. Further discrimination would reduce the number of available data sets. In general, the failure rates decreased but a few increased. Overall the trend was to a 40% improvement. The improvement was measured by taking the ratio of 1990s to 1980s failure rates and forming a weighted average to take account of the number of failure rate entries for each component type. The following Table shows the data.

COMPONENT	1980'S	1990'S	RATIO (r)	SOURCE	No of entries (n)	(n)x(r)
Cap: Ag Mica	0.002	0.0005	0.25	HRD4/5	2	0.5
Cap: Al foil	0.02	0.002	0.1	HRD4/5	2	0.2
Cap: Al solid	0.002	0.001	0.5	HRD4/5	2	1
Cap: Tantalum wet	0.075	0.0015	0.02	HRD4/5	2	0.04
Cap: Glass	0.0003	0.0003	1	HRD4/5	2	2
Cap: Metal Polyester	0.0009	0.0009	1	HRD4/5	2	2
Cct Breaker: 220V	1.6	0.84	0.525	OREDA 84 and 92	2	1.05
Cct Breaker: 440V-6kV	21	10	0.47619	OREDA 84 and 92	2	0.9523
Computer : PLC	133	74	0.55639	Average 24 entries Gas Ind	24	13.353

APPENDIX 9 - COMPARISON OF FAILURE RATE DATA 1980s/1990s

COMPONENT	1980'S	1990'S	RATIO (r)	SOURCE	No of entries (n)	(n)x(r)
Connection: wrap	0.001	0.0002	0.2	NPRD1/5	2	0.4
Connector: coax	0.01	0.01	1	HRD4/5	2	2
Gas detector: Pellistor	26	25	0.96153	OREDA 84 and 92	2	1.9230
Gas detector: Pellistor	32	14	0.4375	Average 9 entries, Misc	9	3.9375
Smoke detector: ionize	3.9	5.4	1.38461	Average 9 entries, Misc	9	12.461
Diode: signal	0.08	0.0046	0.0575	Gas Ind RR102	2	0.115
Transistor: signal	0.044	0.04	0.90909	Average 6 entries, Misc	6	5.4545
Flow sensor: fluid	75	14	0.18666	Average 5 entries, Misc	5	0.9333
Flow sensor: gas	38	11	0.28947	Average 5 entries, Misc	5	1.4473
Flow switch: elec gas	4.2	4.2		OREDA 84 and 92	2	2
Flow switch: elec liquid	7.5	3	0.4	OREDA 84 and 92	2	0.8
Flow switch: pneum gas	5.3	4	0.75471	OREDA 84 and 92	2	1.5094
Meter: electrical	0.9	0.5	0.55555	HRD4/5	2	1.1111
Voltmeter: dc	1.2	1.2	1	MIL217E and F	2	2

APPENDIX 9 - COMPARISON OF FAILURE RATE DATA 1980s/1990s

COMPONENT	1980'S	1990'S	RATIO (r)	SOURCE	No of entries (n)	(n)x(r)
Voltmeter: ac mil	35	19	0.54285	NPRD1/5	2	1.0857
Voltmeter: dc mil	39	29	0.74359	NPRD1/5	2	1.4871
Level switch: electric	13	9.7	0.74615	BG offshore RR191	2	1.4923
Level switch: electric	8.7	1.5	0.17241	OREDA 84 and 92	2	0.3448
Level switch: pneumatic	2.7	0.62	0.22963	OREDA 84 and 92	2	0.4592
Micr've load: 100W-1KW	0.072	0.06	0.83333	MIL217E and F	2	1.6666
Microwave load: > 1KW	0.24	0.2	0.83333	MIL217E and F	2	1.6666
Microwave load: < 100W	0.024	0.02	0.83333	MIL217E and F	2	1.6666
Micr've Fe isolator <100W	0.24	0.2	0.83333	MIL217E and F	2	1.6666
Micr've Fe isolator >100W	0.42	0.4	0.95238	MIL217E and F	2	1.9047
Micr've phase shifter	0.24	0.2	0.83333	MIL217E and F	2	1.6666
Microwave terminations	0.072	0.06	0.83333	MIL217E and F	2	1.6666
Ge Micr've detector	0.39	0.4	1.02564	HRD4/5	2	2.0512
Ge Micr've mixer	0.7	0.7	1	HRD4/5	2	2
Microwave load	0.015	0.015	1	HRD4/5	2	2

APPENDIX 9 - COMPARISON OF FAILURE RATE DATA 1980s/1990s

COMPONENT	1980'S	1990'S	RATIO (r)	SOURCE	No of entries (n)	(n)x(r)
Si microwave detector	0.18	0.2	1.11111	HRD4/5	2	2.2222
Si microwave mixer	0.25	0.25	1	HRD4/5	2	2
Laser 1300 mm	0.5	0.3	0.6	HRD4/55	2	1.2
Laser 850 mm	0.3	0.3	1	HRD4/5	2	2
Pressure sensor	1.3	0.66	0.50769	Gas industry RR102	2	1.0153
Pressure switch: electric	6.8	6.8	1	OREDA 84 and 92	2	2
Pressure switch: offshore	13.2	13	0.98484	Gas Ind 13 entries	13	12.803
CRT	3.5	4	1.14285	NPRD 1 and 5	2	2.2857
Relief Valve	11	5	0.45454	Misc 28 entries	28	12.727
Pressure Transmitter	7.4	6.8	0.91891	Misc 17 entries	17	15.621
Variable resistor	0.024	0.027	1.125	Gas Ind RR102	2	2.25
Temp switch: offshore	13.7	6.4	0.46715	Misc 6 entries	6	2.8029
Thermocouple	9	9.5	1.05555	Gas Ind 7 entries	7	7.3888
Transformer: power	0.025	0.025	1	HRD4/5	2	2
Transformer: 240V	2.9	2.9	1	OREDA 84 and 92	2	2
npn transistor	0.05	0.03	0.6	Gas Ind RR102	2	1.2

APPENDIX 9 - COMPARISON OF FAILURE RATE DATA 1980s/1990s

COMPONENT	1980'S	1990'S	RATIO (r)	SOURCE	No of entries (n)	(n)x(r)
FET: power	0.075	0.05	0.66666	HRD4/5	2	1.3333
FET: signal	0.05	0.004	0.08	HRD4	2	0.16
Fisher 310 control valve	15	14.5	0.96666	Gas Ind "PIMS"	2	1.9333
TOTAL OF 57 COMPONENT TYPES					**221**	**0.701**

CURRICULUM VITAE

The author was born on June 22, 1943, in Purley, England. In 1966 he graduated in Electrical Engineering from the then Lanchester College of Advanced Technology (now Coventry University). The topic of the final year project was Comparison of Frequency Modulator Circuits.

Between 1972 and 1998 he has written books on Reliability and Maintainability Engineering, Statistics, Software Quality and Quality Assurance. He has been Chairman of the Safety and Reliability Society and is a Chartered Engineer being a Fellow of the Institution of Electrical Engineers and an Honourary Fellow of the Safety and Reliability Society.

From 1982 to 1993 he was involved with British Gas in Reliability and Risk Engineering and chairs the Institution of Gas Engineers committee responsible for their guidance on safety-related systems. From 1985 to 1998 he devised and created software tools, being the FARADIP reliability data base, the COMPARE RCM package, the BETAPLUS common cause failure model and the TTREE fault tree package.

In 1996 he commenced the preparation of this doctoral thesis at Delft, supervised by Prof ir K Smit.