CHAPTER 8

PRACTICAL DEMONSTRATION OF R&M

CONTENTS

1 INTRODUCTION

1.1 The practical demonstration of R&M performance is important in the acceptance of systems into service both initially and following major modification or change in use. Theoretical estimations of the performance parameters are very subjective and suffer from a large degree of uncertainty since they are significantly affected by potential systematic problems in the design. Practical Demonstrations however address the actual design under reasonably representative conditions.

1.2 This chapter addresses:

a) what practical Demonstrations are;

b) why they are carried out;

c) the benefits to be gained;

d) the drawbacks;

e) the available techniques; and

f) their specification.

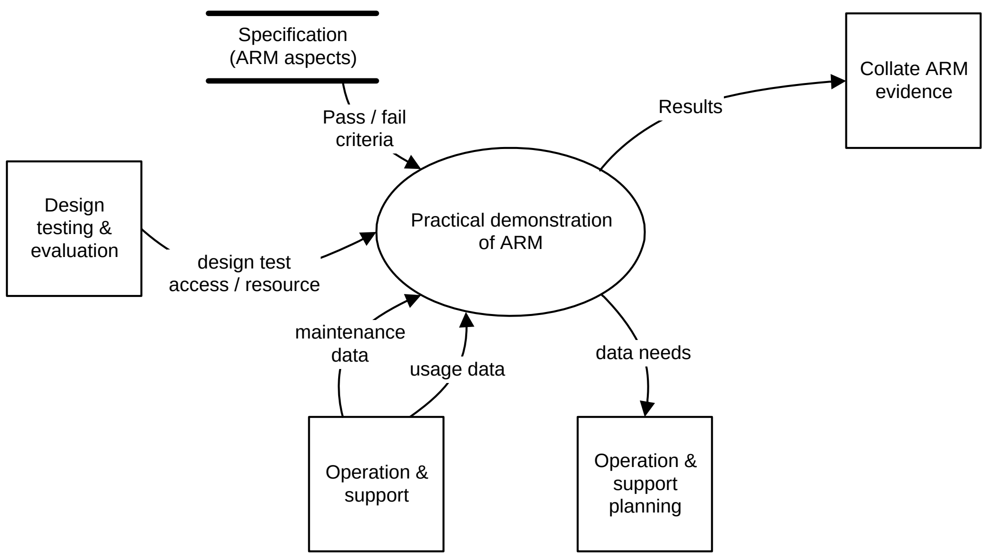

Figure 1: Data and material flow in and out of the demonstration

2 DEFINITION

2.1 In R&M terminology, a demonstration is a practical exercise carried out to test a hypothesis that addresses a statistical R&M parameter of a system. The techniques can, with care, be applied to statistical operational performance parameters but this extension is not discussed in this Manual.

2.2 Many R&M parameters are statistical in nature. The performance of an item is related to a statistical distribution and the specifications are written in terms of the means and maxima of those distributions*. Examples of such parameters include:

a) the MTBF shall be at least 60 hours; and

b) the maximum (95%) MTTR shall be no more than 3 hours.

A demonstration of these statistical requirements will need to exercise the equipment through sufficient time or number of activities in order to determine whether the distribution as displayed during the test is consistent with the requirement.

2.3 R&M Demonstrations do not apply to non-statistical parameters. Many clauses in a specification (colour, defence in depth {two or more equipment failures required before the function fails}, size, basic functionality, etc) can be adequately checked by inspection or a non-repeated test. Such items do not require the repeated testing and accumulation of pass/fail data of a statistical demonstration.

3 PURPOSES AND BENEFITS

3.1 R&M Demonstrations provide a good assessment of the achievement against the R&M requirements. They may be used:

a) to assess compliance with contractual requirements;

b) to assess whether the equipment is fit for entry into service; and

c) to emphasise the R&M requirements.

3.2 A demonstration tests a hypothesis. For example: the probability is at least 50 hours. This hypothesis can be accepted or rejected by the demonstration. In theory, no other information is produced. In practice, however, multiple hypotheses can be demonstrated at the same time, failure trends noted and other tests that do not involve design changes conducted.

3.3 The use of Demonstrations to emphasise the R&M requirements addresses an increasingly commercial world. All too often R&M is not addressed by the design process in a manner that affects the resulting performance. Coupled with meaningful contractual penalties, the requirement for a formal demonstration of R&M achievement provides a management focus which can lead to the design process taking proper pro-active account of the R&M requirements.(see PtBCh3).

* A more detailed study of the mechanisms of failure at the micro level is generally not cost effective and hence the subject is addressed at the macro level, necessitating the use of statistics.

4 PROBLEMS

4.1 Demonstrations can be expensive. They can require significant resource and time. A justification should therefore be made when they are introduced into the specification or programme. It is not intended to suggest that justification is difficult but that the cost implications should be considered. Often the life cycle cost benefits of reducing the risk of accepting equipment with a poor R&M performance will readily override the costs of the demonstration.

4.2 The duration of a demonstration rises with the level of confidence required. Over specifying the level of confidence (too low a consumer's risk) can be non-productive in the wider context. The justification introduced in the previous paragraph should address the level of confidence.

4.3 The probability of failing the demonstration with good equipment and attracting a contractual penalty is difficult for producers to accept. This is however inherent in a statistical test and statistical tests are unavoidable if statistical parameters are to be tested. No fully researched solution exists at the time of writing. Further work could usefully be done in this area. One suggestion (to be applied with care) is to specify a range of concurrent Demonstrations, varying the value of either the parameter itself or the level of confidence, and apply a range of penalties (or incentives) based on where in the range acceptance began. An acceptable balance between the consumer's and producer's risks, together with the parameter values to which they apply, must be found.

4.4 Strictly speaking, no improvement can be made to the system during a demonstration[†]. Normal repairs must take place but only to the same build standard, otherwise the test will be invalid. A demonstration is not part of a growth programme. It may follow the conclusion of a growth programme or trigger a growth programme following a reject decision. Figure 2 shows the resulting effect of a lower achieved MTBF from reducing the time of the growth programme in order to increase the demonstration confidence level under an overall time constraint.

4.5 Often a requirements specification states that there shall be a demonstration but there is no meaningful contractual clause identifying the action following a rejection result. This requires understanding of the nature of such statistical test requirements and implementation of appropriate by the contracts engineer (see Section 6).

4.6 Also parameters are often given for the test which require design to different values to requirements stated elsewhere in the specification or result in the demonstration being conducted based on a value that is significantly less onerous than that the customer originally required. It has become common practice for the customer's risk of accepting a system borderline system to be based on a borderline equal to half the specified value (see Section 6).

[†] In practice, pragmatic considerations often require some modification to be incorporated during the demonstration. However great care is needed if the demonstration is not to be affected, or even invalidated.

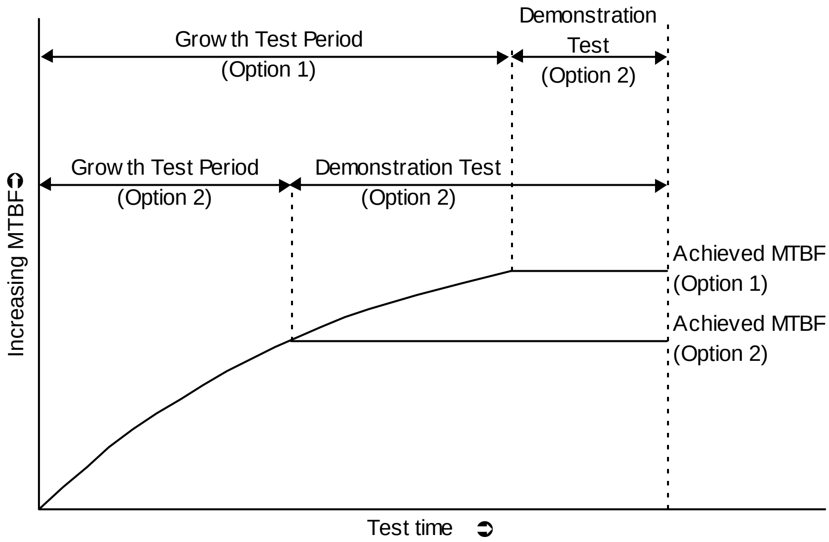

Figure 2: Growth testing and MTBF demonstration in a time constrained programme

5 AVAILABLE TECHNIQUES

5.1 The general process for a demonstration is that the appropriate operation is carried out, either in a simulated environment or the real situation. The events that contribute to the parameter are then measured and compared with the test criteria.

5.2 Statistical tests are based on two values of the parameter under test, the upper test point (θ_0) and the lower test point (θ_1), a producer's risk (α) and a consumer's risk (β). The producer's risk is the probability of equipment with an actual performance equal to the upper test point being rejected. The consumer's risk is the probability of equipment with an actual performance equal to the lower test point being accepted. This is explained further in PtDCh5-7.

5.3 A demonstration may take place at any appropriate site provided the conditions are representative. Maintainability Demonstrations often take place in the development environment. Reliability and Availability Demonstrations, however, are normally carried out following installation on site but examples of their performance on test rigs do exist. The site chosen depends on the project programme, the need for timely information from tests and the Availability of representative samples.

5.4 Figure 1 shows the data flow into and out of the activity allowing for performance at factory or in service. In all cases the specified criteria are needed from the specification in order to determine the appropriate hypotheses. The accept/reject result will also be sent to the R&M evidence collation. For factory testing, the R&M process will need access to equipment under test and the test resource in order to control the testing and ensure the necessary level of rigour. For in-service testing, the R&M process will need to pass its future data needs to the operation and support planning process so that appropriate data collection and transmission is planned.

5.5 There are two basic forms of test. One addresses a number of discrete trials. Each trial may pass or fail. This might be Reliability trials of a single shot device (eg a shell fuze) or Maintainability trials where a maintenance (preventive or corrective) task is carried out and the time taken compared with the specified maximum time. The other form addresses tests where the value of the parameter is collated over a number of trials or a continuous test. For example the Reliability of a repairable system or Maintainability where the time taken is collated. Both forms relate to Reliability, Maintainability and Availability and are discussed in more detail in PtCCh39-41 and PtDCh5-7 inclusive.

6 SPECIFYING

6.1 Section 0.6 listed problems that arise out of poor specification of the Demonstrations. These need to be addressed in the writing of the specification.

6.2 Requirement specification clauses relating to demonstration parameters should be closely linked with those defining the parameter to be demonstrated. For example, if the MTBF is specified to be at least 100 hours in one part of the specification and somewhere else a demonstration is required based on 100 hours and 200 hours, then is the producer being required to design to 100 hours or 200 hours. The customer would read this as the latter but custom and practice requires the former. Where a demonstration is required, the specification writer should avoid defining the parameter directly and use a form such as:

> 'The design MTBF shall be deemed acceptable on being demonstrated with a minimum lower test MTBF of 100 hours and a maximum customer's risk of 10%.'

6.3 The above clause might allow the producer to repeat the demonstration with the same equipment to get an accept decision the second time. The specification writer may reduce this possibility by specifying that the results of previous tests should be included in any collation of results unless the failures experienced have been analysed and subject to corrective action.

6.4 The specification should make very clear what the scope of the parameter relates to. Common terms are often used in slightly different ways. With MTBF and Availability, clarity is needed as to whether a specific functional failure is being referred to or the general need for corrective maintenance. With MTTR it should be made clear whether the requirement addresses the time for which the equipment is unavailable for operation or just the active corrective maintenance time. Definitions differ from one source to another to an extent that requires definitions to be provided with the specification.

LEAFLET 8/1

ISR&MD SUPPORT BY ARM MODELLING

CONTENTS

1 INTRODUCTION TO ISR&MP

1.1 Prior to acceptance into service, a system should be evaluated to establish whether the Reliability exhibited under service conditions exceeds the minimum acceptable requirement. The system may be a new design, a modification of an existing system or an Off-The-Shelf product entering service. Similar evaluation may be required if an existing system is required to operate in a new way or in a new environment.

1.2 Theoretical estimations of the performance parameters, either by analytical analysis or modelling, suffer from varying degrees of uncertainty, since they are significantly affected by the quality of the data used for estimation. In-service performance often deviates significantly from theoretical estimates due to factors such as design standards, manufacturing quality and operational environment.

1.3 In some cases previous field history will provide sufficient confidence for acceptance. In others, one or more Reliability Demonstrations will have to be conducted. Practical demonstrations have the advantage of measuring the actual design under reasonably representative conditions.

1.4 An In Service Reliability & Maintainability Programme (ISRMP) (synonymous with “In Service Reliability Demonstration”) is one such Reliability Demonstration. A dedicated ISRMP will provide a detailed evaluation of an equipment’s reliability when used under realistic in-Service conditions and will provide clear evidence whether the specified levels of reliability have been achieved by production standard equipment. A well constituted ISRMP is an effective method of measuring this achievement

1.5 Def Stan 00-42, Part 5 and Def Stan 00-42, Part 6 describes the purpose, rationale and procedures for In Service Reliability Demonstrations (ISRDs) and Maintainability Demonstrations (MDs) respectively.

1.6 The ISRD is seen as a final test to establish that the contractual requirements have been met and a means of motivating the contractor to achieve these requirements through a comprehensive and vigorous reliability programme. An ISRD defers final acceptance of the equipment until achievement of the contractual reliability requirements has been verified under Service conditions.

1.6.1 It should be noted that an ISRMP will not be appropriate for the acquisition of every system, platform or equipment.

2 POTENTIAL PROBLEMS WITH AN ISR&MP

2.1 Statistical Confidence

2.1.1 In any reliability demonstration, there are statistical risks to both contractor and purchaser of "good" equipment failing the demonstration and "bad" equipment passing. The risks of these undesirable conditions are termed the contractor’s and purchaser’s risks respectively. These risks are a consequence of the statistical nature of the demonstration process. The estimation of reliability parameters on which the success of the demonstration is assessed uses methods based on statistical sampling techniques. This ‘uncertainty’ factor is well understood but must be managed to optimise the effectiveness of the demonstration. These risks can be managed in the trial planning process where optimal values are calculated and set for the duration and acceptance criteria of the demonstration. The values to be used in an ISRMP need to be agreed before award of contract. Management of the ‘uncertainty’ factor is also only possible by applying an effective scheme for the collection, classification and sentencing of incident data, i.e. a DRACAS.

2.2 Incident Classification

2.2.1 The success of a demonstration is assessed using a pre-defined measure of system achievement, be it reliability, availability or maintainability. The assessment of achievement is central to the whole demonstration activity. All criteria that have any bearing on this assessment must be defined in unambiguous terms and agreed before the commencement of the demonstration.

2.2.2 Sentencing of all incidents should be conducted by an Assessment Team or Incident Sentencing Committee, which should include representation from both the producer and consumer, and which is responsible for interpreting the failure definition(s) and classifying incidents.

2.2.3 Definition of attributable and non-attributable faults is probably the single most important area of contention. Reported incidents must be defined as “faults”, “failures” and “defects”. The use of the terminology of “faults”, “failures” and “defects” needs to be clearly defined. Failures must be further defined as attributable and non-attributable, or in other terms, R&M-relevant and non-R&M-relevant. Only R&M-relevant data is used to calculate the R&M parameters of the system and its components.

2.2.4 It is also important when calculating R&M parameters at the system level to define and agree which sub-system failures result in a system failure. This is not always a simple procedure particularly when the system includes elements in redundancy configurations. System failures may occur only when specific combinations of elements experience concurrent failures. Again, this can be a contentious area as it often has direct consequences on the final acceptance of the system.

2.3 A Solution

2.3.1 This Leaflet describes a method developed for the ISRMP of an IT system, which ameliorated to a large extent the problems described above. This was a method whereby the observed equipment R & M characteristics collected by a DRACAS were analysed to a set of agreed criteria and the system R&M evaluated by use of an agreed system model and analysis tool.

3 APPLICATION OF ISR&MP TO A CURRENT IT SYSTEM

3.1 The subject of the ISRMP was an IT System which gathered and collated operational information and supported the issuing of orders, preparation of briefs and dissemination of information to other systems.

3.2 The system consisted of a central site and six remote sites connected in a Wide Area Network (WAN) topology. The central site supported 34 user positions, 2 Computer Manager stations and 1 Security Manager station. There were a further 18 user positions located at remote sites

3.3 The IT System had the following characteristics:

- It used large volumes of identical items, e.g. workstations, printers, network hardware and application software. Hence, similar incident reports were expected on standard equipment types;
- The system incorporated significant functional redundancy hence definitions of system failure were not straightforward to achieve;
- The system installation connected widely distributed sites both in the UK and in Europe;
- The system was operational 24 hours a day and 365 days a year, hence there was no clearly defined 'mission time' for R&M calculations.

4 THE DEVELOPED ISRMP PROCESS

4.1 Description

4.1.1 The ISRMP was conducted for the IT System over a 2 year period beginning from delivery of the Full Operational Capability (FOC) standard of the system.

4.1.2 The Programme defined 'reliability' in terms of Availability of the Operational System and the Mean Time Between Failures of the Operational System (MTBFOS), and the term 'maintainability' as Mean Active Repair Time (MART) of repair times for the Operational System. These requirements originated from the System Requirements Specification (SRS) for the IT System, and were the measures of achievement by which the success of the ISRMP was to be measured.

4.1.3 The ISRMP plan specified the following activities:

a) Data Collection;

b) Incident classification;

c) Data Monitoring;

d) Calculation of the achieved Availability, Reliability and Maintainability.

4.1.4 These activities were accomplished by the application of a Data Reporting, Analysis and Corrective Action System (DRACAS).

4.1.5 The monitoring of the R&M performance of the IT System during the demonstration for compliance with the requirements was achieved by the use of R&M modelling. The IT System was modelled using the RAM4 Reliability Analysis Program. The model was produced prior to the ISRMP by the Supplier and agreed by the Customer to be a reasonable and supportable representation of the system under test.

4.1.6 The definition of the 'system' was encapsulated in the model in 'dependency' terms. This meant that the consequences for system operation, and hence availability, of the failure of any element of the system was pre-defined by the model, and not the subject of constant interpretation by the Failure Review Board.

4.1.7 At the start of the ISRMP the model was populated with data from two sources; reliability predictions and equipment suppliers or manufacturers. Thereafter for the duration of the demonstration, Incident Reports for which sentencing had been completed and were classified as R&M-relevant were used to calculate the reliability parameters, MTBF and MTTR, for the constituent parts of the system. At regular intervals this data was used to update the data input to the RAM4 models and the models run to produce new estimates of system reliability parameters.

4.1.8 In this way the system was monitored for performance and its potential to meet the operational requirements.

4.2 The Modelling Tool Options

4.2.1 When considering a modelling tool to be used to implement the IT System model, the two candidates considered were RAM4 (Reliability, Availability and Maintainability Analysis program) and SAM (Systems Availability Model). Both programs provided similar facilities in a number of modelling areas. Both used Monte Carlo sampling methods to simulate life failures. One major difference between them was in the simulation of mission profiles. A mission profile defines a number of successive time periods when the function, hence the configuration, of the system changes. For instance, a radar system may be switched off or in a 'standby' state for part of a mission and then switched to full readiness for a short part of the mission. Such phases of operation comprise a mission profile.

4.2.2 SAM had facilities to model mission profiles, whereas RAM4 was a tool more suited to the simulation of continuously running equipment. However, mission profiles were not essential in the modelling of the IT System, which in normal operation, was running continuously 24hrs a day. Since RAM4 also had a simpler User Interface and was faster in execution, RAM4 was therefore chosen as the preferred modelling tool.

4.2.3 Another important feature of RAM4 that supported the modelling approach to ISRMP was the ability to import and export 'element type' data. Elements of the same type have identical hardware or software specifications and are assumed to have identical reliability parameters. For example, Monitor A and Monitor B are unique items within the system, however, as they are the same manufacturer's model, they are of the common element type, Computer Monitor.

4.2.4 The RAM4 system model created for the IT System was built entirely using element types. Element reliability data was calculated from incident data for each element type and then imported into RAM4 via the element type interface. The use of element types thus enabled an efficient exchange of information between the IR Database and the RAM4 model.

4.3 DRACAS

4.3.1 A well-defined DRACAS was essential to support the ISRMP. The DRACAS used was introduced at the start of system development and used throughout the acquisition cycle. Hence, as a result of its use during the various acquisition phases it was already a mature system when called upon to support the ISRMP.

4.3.2 A DRACAS of the type used for the IT System is described in Leaflet C18/1.

4.3.3 All data captured during normal operational use was recorded on an Incident Report Database, which was then used to support the DRACAS. The database was under the central control of the Supplier but copies of the database were used by various agencies supporting the project.

4.4 Incident Report Forms

4.4.1 The data collection and reporting function was achieved with the use a set of three Incident Report (IR) Forms, tailored specifically for the IT System. Based on a Microsoft Access template, they were issued in three parts, Part 1, Part 2 and Part 3.

a) **The IR Part 1 form**, recorded the incident data;

b) **The IR Part 2 form**, provided for all subsequent investigation reports and recommended corrective action and the efficacy of the action in preventing reoccurrence. The IR Part 2 was amended with updates of any investigation for reporting purposes and traceability;

c) **The IR Part 3 form**, allowed for the recording of the closure proposal for the IR and was signed by the MoD Chairman of the IR Panel to indicate the closure of the IR and to record the agreed incident sentencing.

4.5 Failure Review Board

4.5.1 A Failure Review Board was established to monitor the ISRMP. The FRB met when required, to monitor the data gathering and analysis activities and to reach agreement over the classification of incidents.

4.5.2 The FRB was made up from representatives of the Supplier, the System IT Support Authority, representing the User and the MoD Project IPT. Other appropriate authorities were called upon to provide technical inputs as required.

4.6 The ISRMP Incident Progress Plan

4.6.1 The incident reports arising from the Users were processed according to the procedure shown in Figure 1 below.

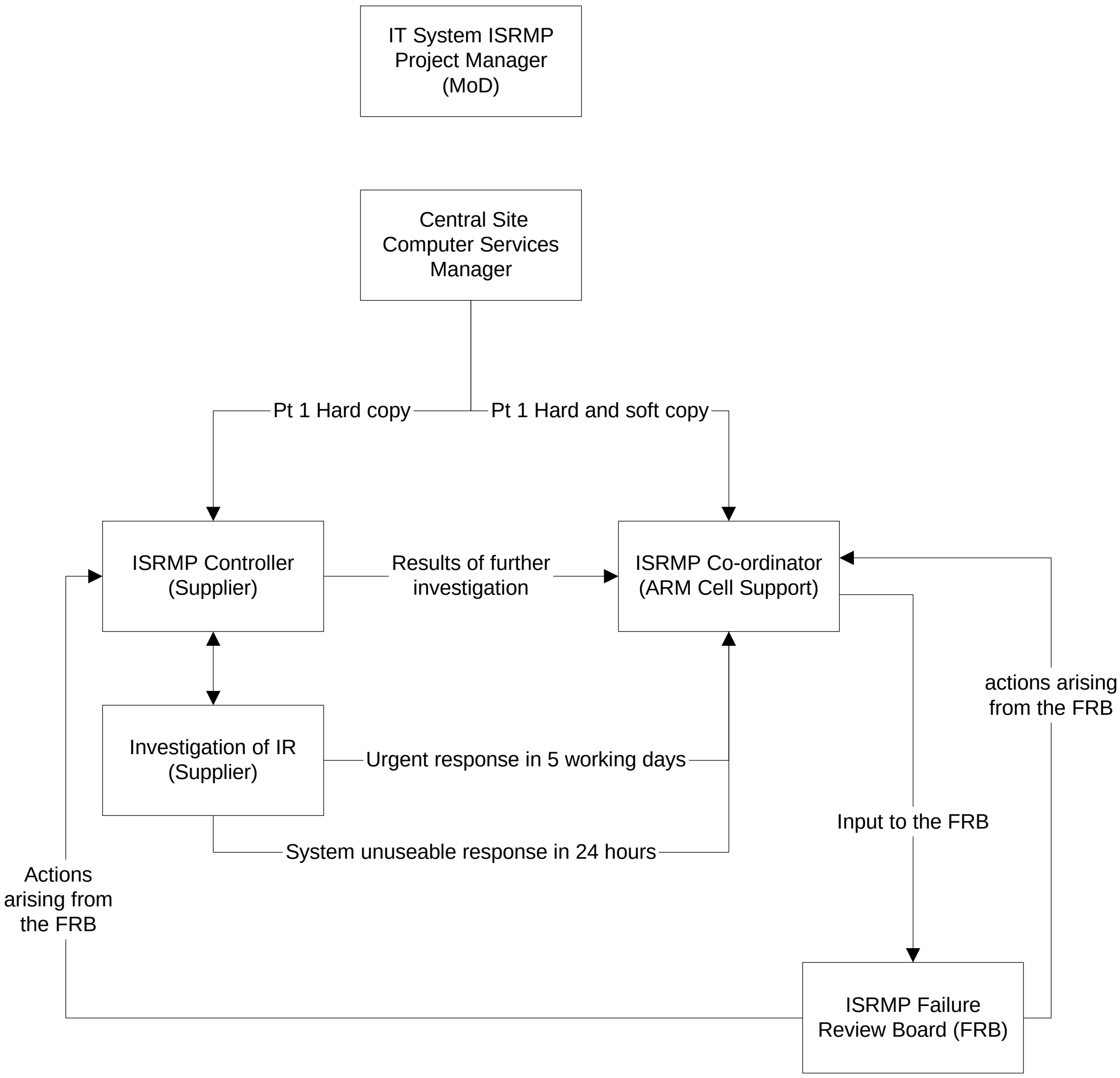

Figure 1 Incident Report Progress Procedure

5 THE PROCESS DATA INTERFACES AND ANALYSIS METHODOLOGY

5.1 Element Data Analysis

The extraction of RAM4 'element type' failure (Mean Time Between Failure) and repair (Active Repair Time 50 and 95 percentile) characteristics from contributory incidents was performed in the following steps:

a) A query was defined in the IR Database to extract the IR data from the relevant records;

b) The query was run and extracted data used to create a new table. The output from this phase was in a format suitable for transferring to an Excel spreadsheet;

c) The data obtained was transferred into an Excel spreadsheet. This spreadsheet then calculated the required RAM4 parameters against equipment type;

d) The results from the calculated results worksheet were transferred to a further worksheet to be used as the input source for RAM4.

5.2 Derivation of Element MTBF

5.2.1 For the case where number of relevant records >2 then

MTBF = running hours/number of failures, for each equipment

5.2.2 For items with <=2 failures the MTBF was calculated in accordance with GR-77 Leaflet 8. The single-sided confidence limit was set at 80%.

5.2.3 For equipment with 1 or 2 failures, the MTBF should be calculated, for each case, as:

$$MTBF = \frac{2T}{\chi^2_{(1-\alpha);2r+2}}$$

where:

χ^2 is tabulated in Table 8 of Leaflet 8/8, for 80% C.I, and 1 or 2 failures

i.e. for the 1 failure case = 5.989

for the 2 failures case = 8.558

$2T$ = twice accumulated running time

$2r + 2 =$ twice number of failures + 2

i.e. for the 1 failure case = 4

for the 2 failures case = 6

α = 0.2

5.2.4 For equipment with 0 failures recorded, the MTBF should be calculated as:

$$\text{MTBF} = \frac{T}{-\log_e \alpha}$$

where:

T = accumulated running time

$-\log_e \alpha = -\log_e 0.2 = 1.6094$

5.3 Derivation of Element MART

RAM4 Repair Time distribution parameters were calculated as the 50th and 95th percentiles of the measured Active Repair Times:

a) 50% percentile = (product of repair_times)$^{1/n}$

where:

n = total_no_equipment_records

b) 95% percentile = $e^{\theta + 1.645\,\sigma}$

where:

θ = arithmetic mean of the $\log_e$ of repair times

σ = standard deviation of the $\log_e$ of repair times

5.4 Derivation of System Availability

The availability of the IT System was calculated at specified intervals using the agreed RAM4 model populated by in-service data, for the two year duration of the ISRMP. This was compared with the requirement.

5.5 Further Operational System R&M Requirements

5.5.1 It was specified in the ISRMP Plan that the following R&M parameters be derived. These were derived from IR data held in the IR Database.

5.5.2 The reliability requirement for the IT System was specified as a minimum value of the “Mean Time Between Failures of the Operational System” (MTBFOS). This corresponded to a maximum number of failures of the Operational System in the two-year period. Hence the number of system failures was monitored.

5.5.3 The achieved Mean Active Repair Time (MART) was calculated as an average of the ARTs recorded during unscheduled maintenance of failures of the Operational System.

5.5.4 The percentage of all ARTs of less than 4 hours was calculated and compared with the requirement.

5.5.5 The percentage of all ARTs of less than 3 hours recorded as a result of rectification of a failure in the Operational System was calculated and compared with the requirement.

6 LESSONS LEARNT

6.1 An In Service Reliability and Maintainability Programme (ISR&MP) has been described which illustrates a pragmatic and reasonable approach to managing the problems presented in carrying out a reliability demonstration on a typical IT/communications system. Procedures have been outlined for efficient incident processing and sentencing and the benefits of an approach to the assessment of system achievement using system modelling have been demonstrated. Further benefits of the implemented scheme are described below.

6.2 'Pre-Agreeing' The Assessment System Representation (Model)

6.2.1 The benefits of using a system model approach for the IRS&MP were seen as follows:

6.2.2 Consistency - The use of a model approach for the IT System meant that a consistent approach was possible to the assessment of the system reliability parameters. All judgements on system failures were made by the agreed model and not the FRB.

6.2.3 Contention - The FRB was relieved of the task of deliberating on each incident to sentence according to whether or not they caused a system failure. Any possible contention on this area was thus avoided.

6.2.4 Efficiency – Performing the system model definition up-front of the ISRMP, led to a reduction in the workload of the FRB and hence a more efficient working group.

6.3 Grouping Common Data And Defects

6.3.1 Effort was applied in identifying incidents that were of a systematic nature, i.e. those that tended to repeat themselves over a period of time and which were known to be due to identical causes. Investigation work to determine the underlying causes of the problem was generally undertaken for the first report of such incidents. But thereafter, incidents that could be identified as further occurrences of an earlier known and investigated incident were tagged and classified/sentenced in accordance with the earlier classification. This scheme proved to be valuable in saving time and effort on nugatory investigations.

6.3.2 Also, because large volumes of identical items, e.g. workstations, printers, were used in the IT System, faults reported on common types of equipment could be batched together for the purposes of identifying the cause of fault, and for the calculation of equipment reliability values for element types.

6.4 Data Processing Options – The Use Of CL Or Best Estimates

6.4.1 Best estimates are formed from raw reliability data. For instance, if an equipment clocks up 100 running hours and experiences 2 failures, then a best estimate of its true MTBF is 100/2=50 hrs. Best estimates give no measure of the confidence (statistical) that the estimated value represents the true value. They also assume that the underlying failure distribution of failure times for the component is exponential in nature, which is not always the case.

6.4.2 Applying more rigorous statistical tests to the results, we can calculate a confidence limit based on the number of failures and on whether the test period was time or failure

a) For a time terminated test we can be 90% confident that the MTBF is greater than 18.7hrs or 50% confident it is greater than 37.4hrs

b) For a failure terminated test, we can be 90% confident that the MTBF is greater than 21.0 hrs or 50% confident it is greater than 59.5hrs

6.4.3 The modelling tool used in the ISR&MP was capable of taking multiple samples of a system 'life' and then automatically calculating confidence limits about the point estimates of results. The simulation could also be configured to give the required confidence limits about the estimates. This was a further justification for the approach to ISR&MP using R&M modelling.