CHAPTER 18

DATA REPORTING, ANALYSIS AND CORRECTIVE ACTION SYSTEM

CONTENT

1. INTRODUCTION

Defence Standard 00-40, Part 1 describes the management responsibilities and requirements for R&M programmes and plans and provides guidance to implement these. Section 2 to that standard in compliance with JSP 886, Chapter 7, Part 8.04 describes the responsibility of defence contractors to establish and maintain an appropriate closed loop reliability related data management system (i.e. DRACAS) throughout the design, development, production and subsequent assessment and evaluation phases of a procurement contract. In particular, a properly designed and implemented DRACAS is needed for an In-Service Reliability Demonstration performed to facilitate formal acceptance of the procured system.

2. THE DRACAS PROCESS

2.1 An important feature of any DRACAS is that it should be a closed-loop system. Such a system begins with incident reporting, and then continues with collecting, recording, analysing, categorising, investigating and where appropriate resolving. The loop is closed by identifying and taking timely, effective corrective action to ensure the reported incident does not reoccur.

2.2 Defence Standard 00-40 Part 1 further stats that: “The Supplier shall establish and maintain a Data Reporting, Analysis and Corrective Action System (DRACAS) throughout the design, development and production phases of the contract. The system shall be a documented closed-loop system for reporting, collecting, recording, analysing, categorising, and investigating data and taking timely, effective corrective action. A DRACAS shall be applied to all non-conformances and failures relating to design, manufacturing and test processes that occur during any project activity whether conducted at the premises of the contractor or elsewhere. Operational and usage data, together with operating conditions, shall also be recorded. The DRACAS shall cover all materiel being supplied under the contract and shall provide for the reporting of suspected failures and non-conformances as well as observed failures, failure indications and non-conformances”.

3. THE APPLICATION OF THE DRACAS PROCESS

3.1 Leaflet A describes the application of a Data Reporting, Analysis and Corrective Action System (DRACAS) to a project for the supply of a Naval IT System. This example has been purposely kept generic to illustrate that the application can be applied to any system, equipment, assembly or component. Unfortunately one example does not fit all and there will be very few projects where the DRACAS will not need a degree of tailoring to enable its application to be optimised specifically to that project.

3.2 Tailoring a DRACAS to a specific project may seem daunting however as long as you remember it needs to be a closed loop reliability related issues management system and; that what could go wrong with any specific project eventually probably will, you will not go far wrong. Other than the obvious information requirements such as what, when, where, how and by whom; brainstorming the equipment requirements with other members of the Project Team will usually capture the majority of the data entry lines required to populate the DRACAS.

3.3 It is also imperative to cultivate a no-blame culture for the reporting of incidents. Much time and expenditure can be wasted investigating and incident caused by human error or operating equipment outside their design parameters. It is however equally important that human errors are reported because if one person can make such an error so can others which may result in a health and safety issue or be prevented by simple and cost effective design or procedure change.

4. DEFINITIONS

4.1 Definitions and assumptions for a critical part of the specification process for any project prevent ambiguity and disagreement and contribute to the successful delivery of the project on time and within budget. They also provide clarification during the DRACAS data classification process by ensuring that a common understanding is maintained and that individual incident will be managed appropriately with each other.

4.2 Where definitions and assumptions have not been agreed as part of equipment specification process and ideally included within contractual negotiations it is important they are agreed prior to the commencement of the data classification process.

4.3 Def Stan 00-49 in conjunction with IEC 60050-191 Ed 2 provide detailed guidance on generic definitions and the tailoring process to enable them to be optimised for specific projects. Examples of definitions may include but not be limited to:

a) Failure - A failure is an event that prevents the equipment from performing within previously specified limits.

b) Observation - Technical observations from hands-on personnel are used for keeping a record of problems which are not defects or failures in their own right. For example, an item may be superficially degraded but still fully capable of operating satisfactorily. These records are useful in anticipating failures from progressive, worsening conditions. The observation of a degradation condition may initiate a design review, even though failure has not arisen.

c) Test or Trial - The terms test or trial are used to denote any exercise used to provide data for the estimation of equipment R&M. Examples include, but are not limited to, development trials, reliability qualification tests (RQT), performance tests and in-service reliability demonstrations (ISRDs).

5. DATA CLASSIFICATION

5.1 Data classification is a general term used to describe the process by which incidents are examined and classified for the purpose of assessment to determine their significance, and priority in relation to each other on the same equipment and in association with other equipments within the same system. Usually it is the responsibility of the contractor to prepare and structure a data classification system to ensure that all events are accurately and completely categorised as to cause, criticality/significance, environment, frequency and chargeability. The contractor shall agree the criteria for the classification of data with the purchaser at the outset of the design.

5.2 Data classification should allow trends to be identified, by categorising incidents by both the part affected and the mode of the incident. Further guidance can be found in Def Stan 00-44 and in Part C, Chapter 46.

6. DATA VILIDATION

6.1 It is important that any DRACAS represent a true picture of the system behaviour in a typical or specific operational environment. Therefore the DRACAS needs to be easy to use; so that no unnecessary overhead is introduced into the operational environment and that the user is willing to record any abnormality of the system, to ensure the completeness of the data.

6.2 A culture should be established to encourage people to report any types of incident as accurately as possible. This would include a no-blame culture, to ensure that people who are involved in the incidents or event describe the scenario honestly. The use of pick lists and tick boxes will assist the user inputting data which is easily categorised while mentoring and feedback will enable the user to develop confidence and appreciate that their contribution is aiding the projects development.

7. INVESTIGATION AND REMEDIAL ACTION

7.1 In general, investigations are carried out under contract as part of a development or as part of any PDS/support contract. For in-service equipment this will often follow initial investigation by the relevant equipment branch.

7.2 After completion of their investigation, the contractor (or with the assistance of the MOD for in-service equipment) will propose remedial measures to prevent recurrence of the condition or measures to alleviate the effects. This solution may involve a change in operating or maintenance procedure or, more often, a modification to improve or replace items related to the defect/failure/fault. The procedures for the promulgation of modifications and their implementation to in-service equipment will vary between the Services.

8. DRACAS via FRACAS

8.1 The terms DRACAS (Data Reporting, Analysis and Corrective Action System) and FRACAS (Failure Reporting, Analysis and Corrective Action System) are frequently confused, miss used and interchanged unfortunately too often to the determent of equipment development. Whereas FRACAS specifically addresses failure, DRACAS embraces failure and other incidents and observations which with failures if appropriately addresses may lead to an overall improvement to the equipment capability.

8.2 It is MOD policy (JSP 886, Volume 7, Part 8.04 Reliability and Maintainability refers) that a Supplier shall provide an R&M Case Report supported by a DRACAS as specified within the R&M Case Evidence Framework as part of the evidence in support of their assurance process.

LEAFLET 1

AN APPLICATION OF THE DRACAS PROCESS

CONTENT

1. INTRODUCTION

1.1 To illustrate the development and application of a DRACAS in the following example a fictitious IT System has been created comprising a number of discrete equipments with their associated connectivity. The same approach however would be taken for that of a more complicated system or an individual equipment. In each instance the approach and methodology would be extremely similar whereas the process may be quite different.

1.2 The initial data capture in this example is via the paper based, multi-part Incident Report Form however a discrete IT based system may in some circumstances facilitate a better data capture option. Under other circumstances perhaps the equipment itself would provide the functionality to enable data capture. But remember, the easier it is to capture and retain the required incident data the more likelihood there is of obtaining credible data that is accurate, complete and most of all useful.

2. IT SYSTEM DESCRIPTION

2.1 Overview

2.1.1 The IT System for which the DRACAS was developed was a system which gathered and collated operational information and supported the issuing of orders, preparation of briefs and dissemination of information to other systems.

2.1.2 The system consisted of a central site and six remote sites connected in a Wide Area Network (WAN) topology. The central site included a number of role cells and supported 34 user positions, 2 Computer Manager Stations and 1 Security Manager Station. There were a further 18 user positions located at remote sites.

2.1.3 At the central site the system also provided direct interfaces with a number of other MoD information systems, including command support, weather and oceanographic and office technology systems.

2.1.4 The system architecture and design reflected the requirement for Succession of Command (SUCOC) to alternative headquarters following the loss of facilities at the central site.

2.1.5 All workstations were identically configured for hardware and software installation, except that some workstations had two monitors.

2.2 System Characteristics

2.2.1 The IT System was a ‘non-classical’ system in comparison with the more traditional type of MoD procurement, in that it was neither a weapon system nor a communications system nor any other form of hitherto standard marine system.

2.2.2 The IT System had the following characteristics:

a) It made extensive use of Commercial off the Shelf (COTS) hardware and software items. The use of COTS equipment can mean that elements of the traditional phases of a MoD procurement cycle, i.e. specification, design and production of system components, are, to a large extent, outside the control of the customer. However, in the case of the IT System, the integration of those components into a system that met the System Functional/Requirement Specification became a critical activity in the acquisition process. Proper specification of the hardware and software interfaces between the components to achieve integration was essential for the successful operation of the system.

b) 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.

c) The system incorporated significant functional redundancy hence definitions of system failure were not straightforward to achieve.

d) The system installation connected widely distributed sites both in the UK and in Europe.

e) 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.

2.2.3 The acquisition of this type of system was becoming more commonplace at the time and required a different approach in the assessment of R&M performance.

2.3 Incremental Acquisition

2.3.1 Incremental development and deployment were features of the acquisition of the IT System. The processes applied to achieve the acquisition were part of the Incremental Acquisition component of the MoD Acquisition Management System (AMS). This provides for equipment capability to be supplied with an initial delivery of a specified baseline capability Initial Operational Capability (IOC), then upgraded in a planned way to eventual achievement of a full capability Full Operational Capability (FOC). This is illustrated in Figure 1 below.

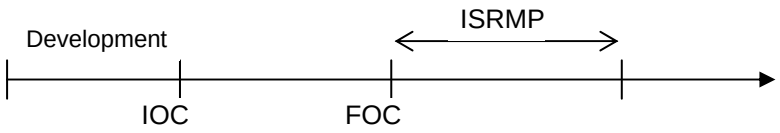

Figure 1 – Incremental Acquisition

2.3.2 Incremental Acquisition is particularly beneficial in the acquisition of systems with a significant element of IT hardware and software, including elements of Commercial Off-The-Shelf equipment (COTS), or with systems in areas where technology is evolving rapidly. It enables a system to be introduced to service earlier and allows system performance to be progressively evaluated while achieving FOC. Note that incremental acquisition is often a mixture of development and PDS activity, since at any stage the 'system' can comprise

components that have been tested and accepted into service and components that are still under development and test.

2.3.3 In the case of the IT System, the IOC comprised the central site but none of the six remote sites. A number of the direct interfaces with other MoD information systems were also not included in the initial capability. This was then developed and deployed to the FOC as described above.

3. DATA RECORDING, ANALYSIS & CORRECTIVE ACTION SYSTEM (DRACAS)

3.1 The DRACAS operated for this particular IT System evolved over a period of 3 years in response to a requirement for the capture and swift resolution of equipment failures associated with such IT systems.

3.2 The DRACAS was introduced at the start of system development and used throughout the acquisition cycle. Hence, the procedures described here covered the raising and progressing of Incident Reports (IRs) for the IT System during the activities of installation, testing and commissioning the various acquisition phases. It was also used to support a Reliability Growth Programme, a Reliability Demonstration and an In Service Reliability and Maintainability Programme (ISRMP). Thus the DRACAS procedures described here were applicable from the start of development until the end of the ISRMP, 2 years beyond FOC.

3.3 The procedure covers the monitoring of:

a) The complete IT System under normal operating conditions.

b) Corrective action taken to rectify incidents and correct the causes of failure where possible.

c) The approach taken for identification of Operational System Failures during the Reliability Demonstration.

4. DOCUMENTATION FOR INCIDENT REPORTING

4.1 Incident Report Forms

4.1.1 IR Forms, tailored specifically for the IT System, were based on a Microsoft Access template, and were issued in three parts, Part 1, Part 2 and Part 3.

a) The IR Part 1 form, shown at Figure 2, recorded the incident data.

b) The IR Part 2 form, shown at Figure 3, 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.

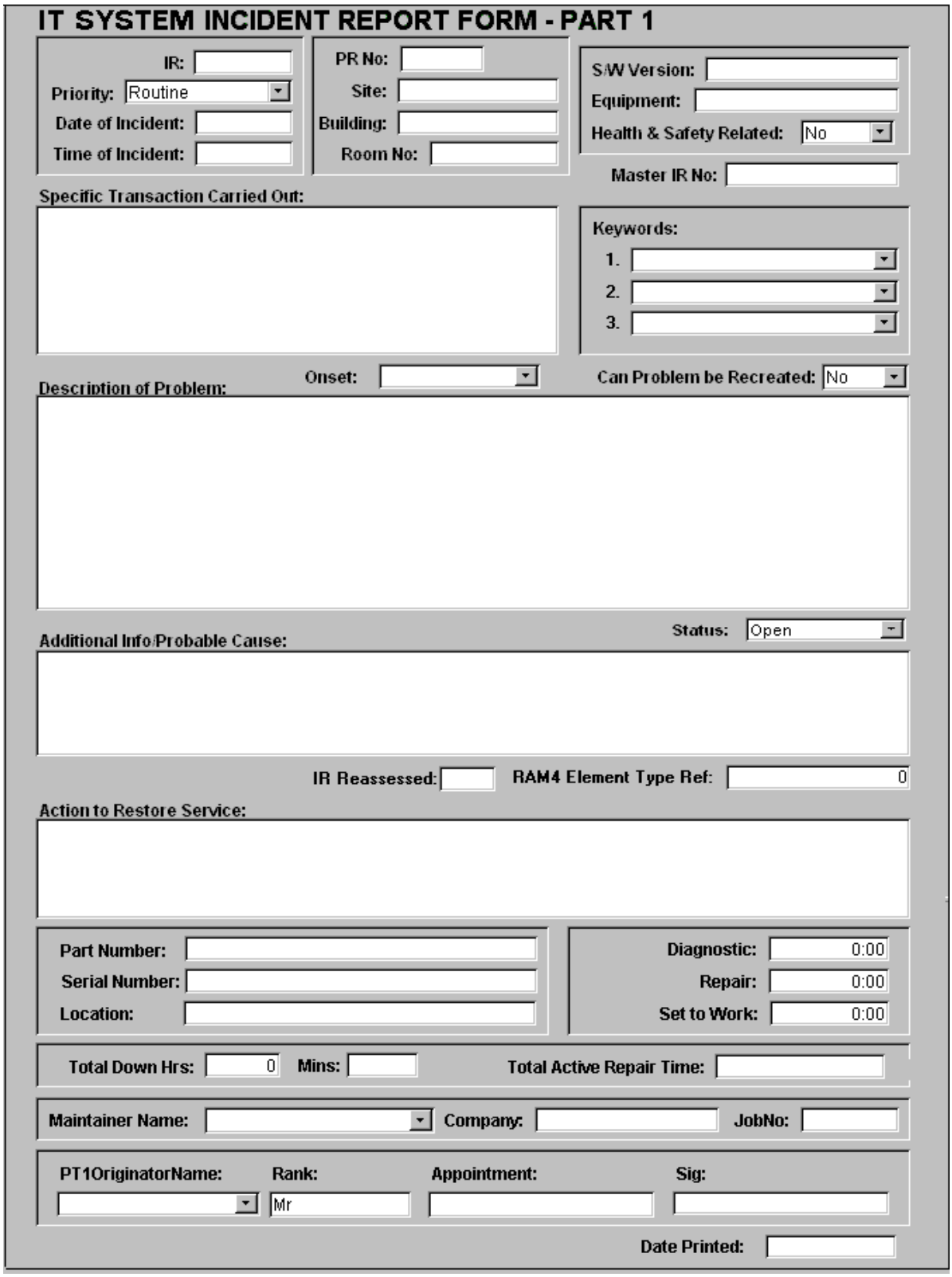

Figure 2 – Incident Report Form – Part 1

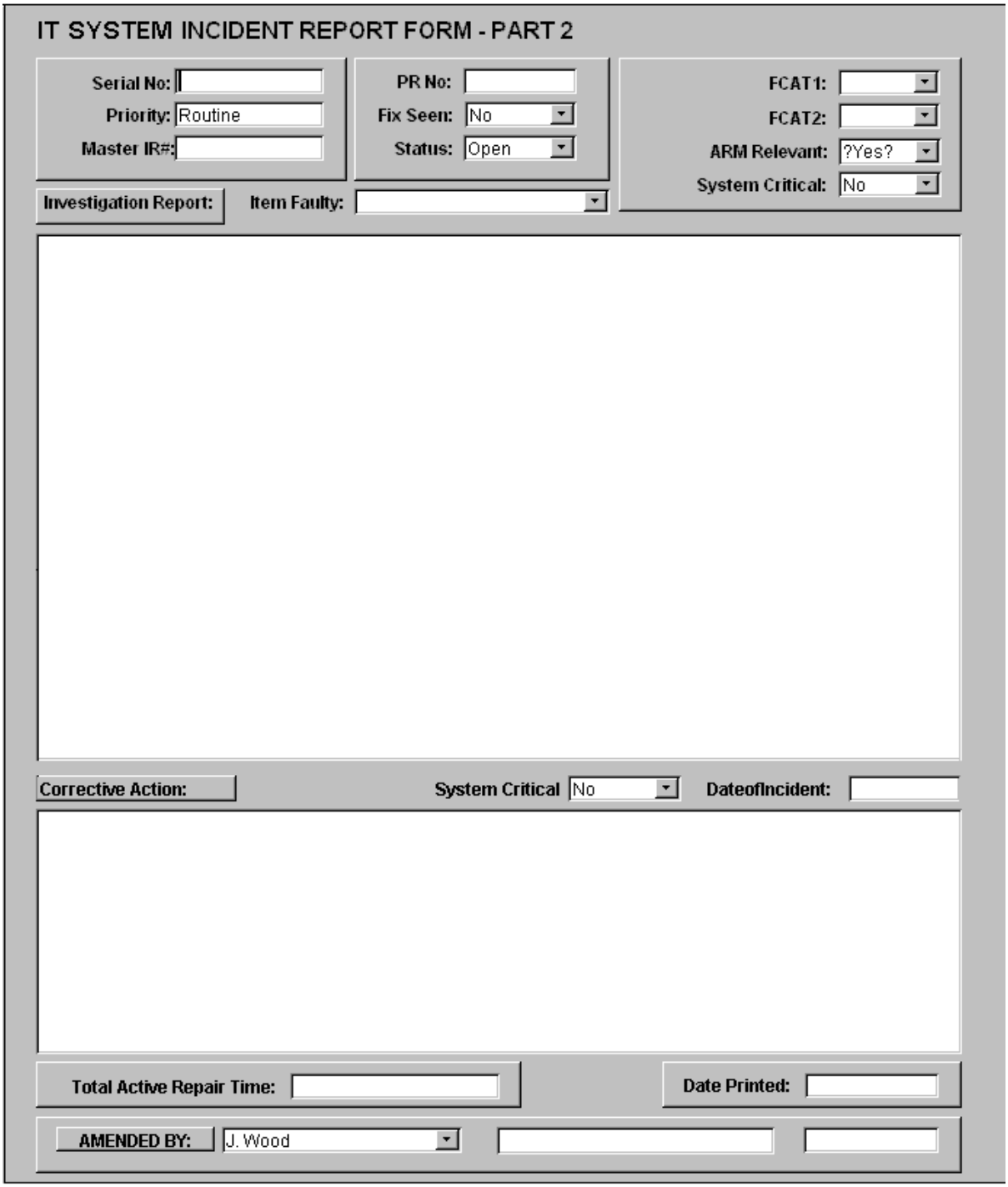

Figure 3 – Incident Report Form – Part 2

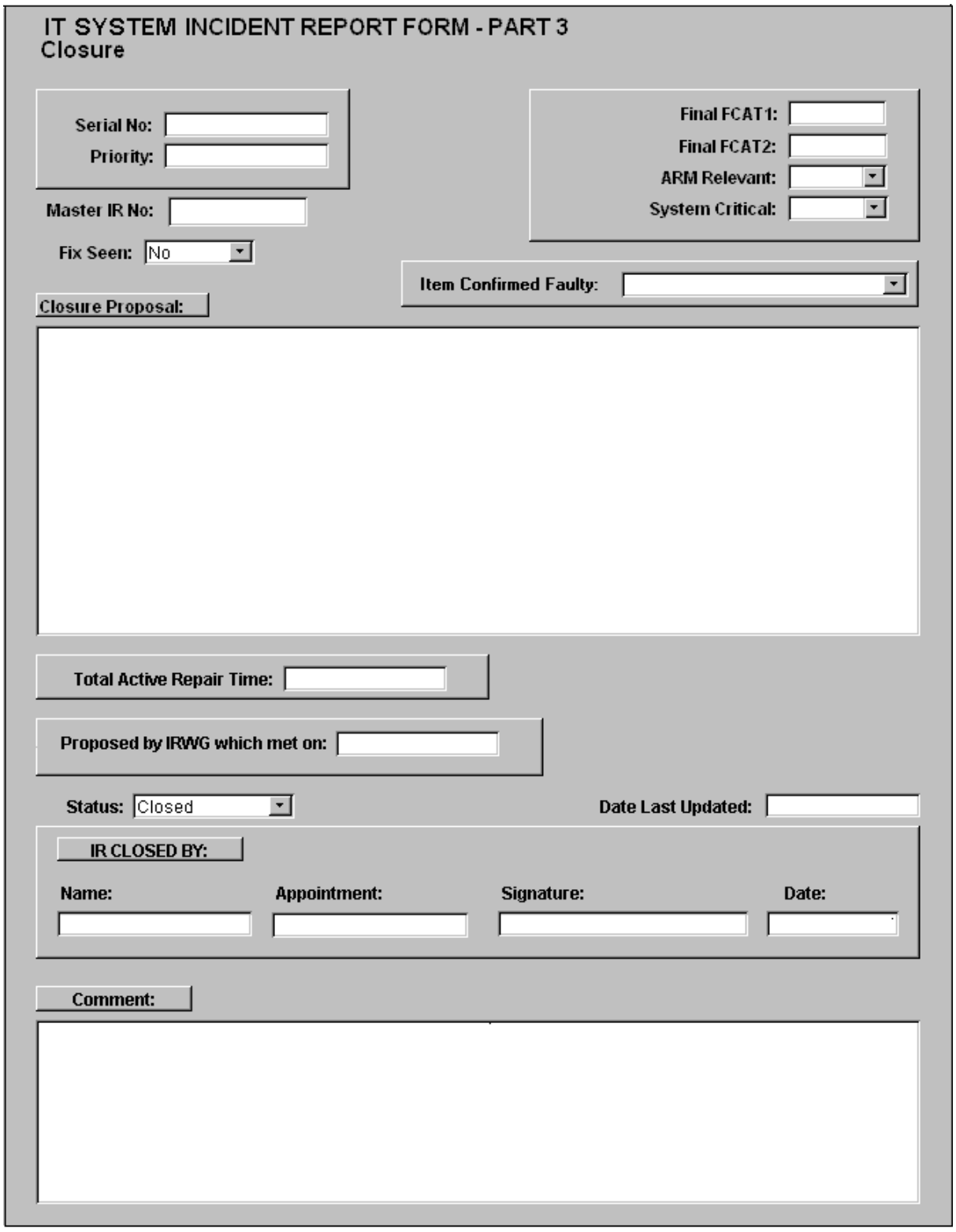

Figure 4 - Incident Report Form – Part 3

c) The IR Part 3 form, shown at Figure 4, 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.

4.1.2 The forms were designed to capture information sufficient to allow the calculation of the relevant R&M parameters, such as MTBF, MART, and Intrinsic Availability of the Operational System, etc. Although there was no specific requirement to measure operational availability, logistic delay times were recorded as part of the total downtime for each incident.

4.1.3 IR Part 2s and Part 3s were required for every IR Part 1. The Part 2 detailed the investigation process to resolve the incident, and the Part 3 described how the IR had been closed. All IR Parts were stored with the IR Part 1.

4.2 Scope of Reporting

4.2.1 The incident reporting procedure implemented in the DRACAS was used for reporting faults in hardware, software, procedures and documentation, and Health and Safety and System Critical issues.

4.2.2 All Incidents reported at MOD sites were normally reported using a User Report Form. Any User noticing a fault, experiencing operational difficulties, or simply wishing to highlight an observation could raise a User Report Form.

4.2.3 The originator of a User Report Form had reasonable freedom to raise anything that caused a problem. It was therefore the duty of System Operators to determine whether an IR Part 1 should be raised in response to a User Report Form. Part 1 forms raised were numbered sequentially and grouped for ID purposes, numbers from 10,000 being used for normal IRs and numbers from 15,000 used for incidents reported during testing.

4.3 Incident Review Groups

The DRACAS was operated using two Incident Report review groups; an Incident Review Panel (IRP) and an Incident Review Working Group (IRWG). The two groups worked closely together in co-ordinating incident reporting, investigation and corrective action. The functions of these two groups are described below.

4.4 Incident Review Panel (IRP)

4.4.1 The IRP was the formal DPA/User/Supplier committee that agreed and accepted IR closure and sentencing. The functions of the IRP were to:

a) Review IRs on the Project

b) Classify the Incidents as Failures or Incidents

c) Classify the Incidents as relevant or not relevant to R&M calculations

d) Sentence the Incidents

e) Ensure a closed loop procedure

f) Direct the activities of the IR Working Group (IRWG).

4.4.2 The IRP comprised representation in the following areas:

a) Supplier ILS Manager

b) Supplier R&M Engineer

c) MOD Project Office - (Chairman)

d) MoD R&M Cell

e) System IT Support Authority

f) User Support Group

4.5 Incident Review Working Group (IRWG)

4.5.1 The purpose of the IRWG was to provide a forum in which the engineering level issues raised by the IRs could be addressed. The IRWG provided recommendations to the IRP on the sentencing, classification, categorisation and closing down of incidents, but was subservient to the IRP.

4.5.2 The IRWG comprised, as a minimum, one representative of the Supplier, one nominated representative of the System IT Support Authority, representing the User and one representative of the Project IPT, although it also called upon technical inputs from appropriate authorities as required. The lower number of attendees at the IRWG improved the efficiency of the group.

4.5.3 Meetings of the IRWG resulted in an agreed set of recommendations being produced, which were presented to the next meeting of the IRP for ratification and acceptance.

4.6 The Incident Report Database

4.6.1 All data captured during normal operational use was recorded on a Microsoft ACCESS 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.

4.6.2 Reports could be generated on any combination of database fields by agreement with The Supplier, and distributed to all members of the IRP.

4.6.3 "One off" reports to assist in the investigation of specific problems were available to the next IR Panel Meeting on request. Such reports could be:

a) Status report of open IRs by priority grouping

b) Number of IRs raised by time

c) Number of IRs raised by MOD or The Supplier

d) Number of IRs closed

e) Number of IRs by supplier/product

f) A listing of Master IRs together with associated linked IRs

4.6.4 Copies of the active IR forms on the database were also distributed to designated parties in the DRACAS loop covering incident reporting, sentencing and corrective action.

5. INCIDENT REPORT PROCESSING

5.1 General

This section describes the procedure adopted from the raising of an IR through to the eventual resolution of the action initiated by the report.

5.2 Procedure

Figure 5 outlines the IR routing scheme and shows the eventual destination of each copy of the report.

5.3 Classification Of Incident Reports

5.3.1 It was the responsibility of the System IT Support to determine which of the following priority classifications to assign to each IR Part 1 raised. The assigned IR priority defined how quickly the Supplier was contracted to respond to the problem:

a) System Unusable - A System Unusable IR was always classified as an Operational System Failure, that is the denial of an application to all user workstations, or a failure causing disruption to more than 10% of user workstations.

   The IR Part 1 was distributed by fax within one working day. A Part 2 IR was raised and distributed by fax within one working day of the requisite information becoming available.

b) Urgent - The problem can be worked around but requires resolution. This classification was applied when there was significant degradation in service, usually when an Operational System Failure had occurred but a work around had been instigated perhaps for a known bug. This category also catered for the failure of critical workstations when the overall failure impacted on less than 10% of User workstations.

   The Supplier endeavoured to respond to Urgent IRs within 5 working days.

c) Routine - This covered equipment failures of redundant items such that the Operational System capability was not restricted. Similarly, software bugs fell into this category if a bug caused disruption to less than 10% of users but had a greater operating impact than aesthetics.

   These would be resolved as the opportunity presented itself but the Supplier would usually provide an interim response within 20 working days.

d) Observation - This covered unanticipated occurrences that were outside the system requirements and did not impact on use of the system.

Their impact was assessed, but significant changes were not predicted for resolution of Observation IRs unless specifically requested by the MOD.

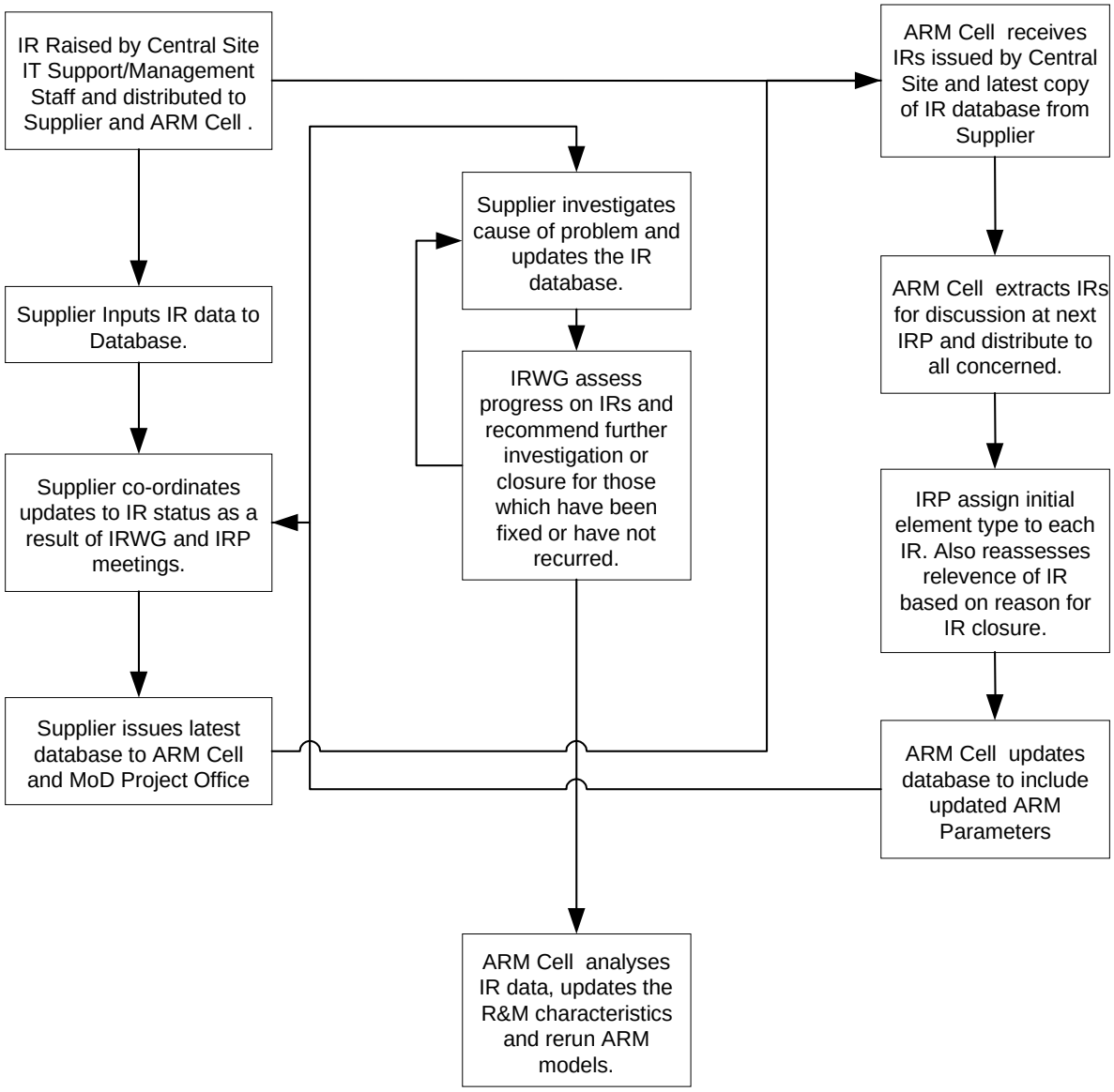

Figure 5 - Incident Report Assessment Loop

5.3.2 A secondary prioritisation system was introduced from FOC. These categories were used to indicate the precedence of items in each category. This was normally related to the repetition of the IR and was used to identify the MOD's concern over specific occurrences. These were:

a) High Priority - This was used when a problem that affected many users or multiple occurrences that caused concern was observed. This would not normally be used for IRs in the Observation category.

b) Medium High Priority - IRs that required rectification but did not occur frequently, (if Operational System Failure) or demonstrated a regular inconvenience if attributed to a minor effect. This would not normally be used for IRs in the Observation category.

c) Medium Low Priority - This was applied to non-repeatable Operational System Failures after a reasonable time period had elapsed, minor effect items to be rectified as the opportunity arises, and observations causing irritation.

d) Low Priority - Was applied whenever none of the above were applicable.

5.3.3 This secondary prioritisation system was initially identified by the Supplier on the IR part 2 and was altered as deemed appropriate by the IR Working Group (IRWG). Alterations followed recommendations from the MOD with agreement of the Supplier.

5.3.4 IR Part 1 Forms were initially issued to the Supplier, with copies going to the following agencies:

a) MoD Procurement Project Office.

b) IT Services/Management System.

c) User's Support Group.

d) R&M Cell Supporting DPA Project Office.

5.4 Supplier Action

5.4.1 On receipt of the Part 1 IRs at the Supplier, the Supplier ILS Manager would:

a) Enter the IRs on the IR Database.

b) Initiate investigation of Part 1 IRs on IT System equipment as necessary.

c) For "Major Effect" and "System Unusable" IRs liaise with the relevant design authority and provide a response within the timescales at paragraph 5.3.1.

d) Raise Part 2 IRs in response to Part 1 IRs and distribute as shown in Table.

e) Address all IRs as agenda items for the IR Working Group (IRWG) and propose the category, classification and the appropriate action to be taken in each case, within the IRWG's Terms Of Reference. (see Section 4.5).

5.4.2 Investigations into incidents were reported on IR Part 2 Forms, with updates as the investigation continued being presented to the MOD by the Supplier. All correspondence associated with each IR, including Part 2 Forms, were given at least the same Distribution as the IR Part 1 Form.

5.5 IR Working Group

5.5.1 IR Part 1 and Part 2 forms were presented for consideration at a meeting of the IR Working Group. It was the responsibility of initially the IRWG and subsequently the IR Panel to establish whether the problem was:

a) An incident.

b) An Operational System Failure.

c) R&M Relevant.

d) Non-IT System failure.

e) Any other kind of failure.

f) An observation,

g) Outside the current requirement.

5.5.2 The analysis of incident reports is described in the following section.

6. INCIDENT ANALYSIS

6.1 General

6.1.1 The analysis of incidents comprised 3 individual activities:

a) Provision of data to the IRP to enable the IRP to monitor progress of Incidents through the DRACAS Procedure and to ensure "Closed Loop"

b) Analysis of incidents by System Design Teams to identify the cause of Incidents and provide corrective action where necessary

c) Analysis of accountable Failures and running hours to provide achieved MTBF, MART and Availability.

6.2 Analysis

6.2.1 In order to enable the IRP to monitor progress of Incidents through the DRACAS procedure and to ensure a "Closed Loop", the IRP and IRWG meetings required the following information to be available. This list is not exhaustive:

a) Total quantity of Incidents, including total quantity per period.

b) Status of System Unusable / Urgent / Routine / Observation IRs.

c) Status of IRs by priority number.

d) Total quantity of R&M relevant Failures.

e) Quantity of "Open" Incidents.

f) List of Open Incidents by date, with actionee.

g) List of Incidents by LRU.

h) List of any equipment, LRU or Software requiring close attention.

6.2.2 This information was normally made available by the presence of an ILS Support Engineer accessing the IR Database during the meeting; however database reports were also printed in advance of the meetings as required.

6.2.3 The classification of incidents is described in the following section.

6.3 Investigation

The Analysis of Incidents to identify causes and any necessary corrective action were reported on IR Part 2's and monitored by the IRP.

7. CLASSIFICATION OF INCIDENTS

7.1 Identification of Failures

7.1.1 Failure - A Failure was defined as the termination of the ability of a previously functional element (hardware or software) to perform its intended task. Failures were further classified into:

a) R&M Relevant Failures.

b) Non-R&M Relevant Failures.

c) Operational System Failure.

7.1.2 R&M Relevant Failures - All Failures were relevant unless determined by the IRP to be caused by a condition external to the equipment. Relevant Failures included, but were not necessarily limited to:

a) Failures due to design deficiencies or poor workmanship of either the equipment or component parts.

b) Failures due to component part failure. (Where multiple component Failures occurred, each component Failure was relevant unless the IRP agreed that the Failure of one component caused the Failure of one or more of the others).

c) Where parts had a known limited life and Failed, or caused Failure, within that known limited life. (Failures were not considered R&M relevant if they occurred after the known limited life of an item had been exceeded).

d) Where simultaneous multiple Failures occurred each Failed item was counted as an R&M relevant Failure, unless the IRP agreed that they were dependent on a single event. In such a case only the cause of the multiple Failures was considered R&M relevant, this assumed that the cause is part of the IT System.

e) Where the IRP agrees that a Failure is intermittent, only the first occurrence of the intermittent Failure is relevant.

f) Failure of BITE to identify fault condition.

g) Where adjustments were necessary, each adjustment was classified as relevant unless:

(1) The adjustment was an operator control, accessible to the operator during normal use and the indication that adjustment was needed was an indicator which was an integral part of the equipment.

(2) The period since the last adjustment has exceeded any stated period of "operational stability" for the equipment.

(3) The adjustment is made to reflect the preference of an operator.

7.1.3 Non-R&M Relevant Failures - Although non-R&M Relevant Failures were not used for MTBF or MTBFOS calculations, nevertheless they were reported and recorded. The following Failures were considered non-R&M Relevant (this list is not intended to be exhaustive):

a) Failures caused by neglect, misuse or accidental damage will not be classed as R&M Relevant

b) Failures resulting from operator error (where the correct procedure is documented)

c) Dependent Failures other than the cause of the dependent Failure

d) Failures caused by external influences (e.g. GFE)

e) The second and subsequent occurrences of the same intermittent Failure on the same unit

f) Failures clearly attributable to an over stress condition which is outside the requirements of equipment operation

g) Failures of the test environment

h) Use of non-representative system

7.1.4 Operational System Failure - Operational System Failures was used specifically during the Reliability Demonstration, and the In-Service Reliability and Maintainability Programme which in this case ran for 2 years from FOC. They were identified in the "System Critical" Field on the Part 2 and Part 3 of the post FOC Incident Reports and agreed by the IRP. Operational System failures included:

a) Failure of any of the Critical Workstations, for instance, those of the System Operators and Security Managers.

b) Failure of any of the Critical Functions, for instance, the main servers and the Backup functions, such that more that 10% of the Users workstations were affected.

c) Failure of any other item such that more than 10% of the Users workstations were affected.

7.2 Sentencing

7.2.1 It was the task of the IRP/IRWG to examine and sentence incidents as being "attributable" or "non-attributable" faults for the purposes of R&M assessment. All incidents were classified with a scheme that used two Fault Category codes, known as FCAT1 and FCAT2. These two codes were used to sentence incidents for "Cause" at two levels. Incident data could then be called up on the IR Database and reported on using a combination of Fault Category codes to select incidents of interest.

7.2.2 FCAT1 codes were alphabetic and the FCAT2 codes were numeric. Codings from previous projects were adapted for use on the IT System project, but because of the software nature of the system many standard codings were found to be irrelevant. Many of the incidents were finally sentenced as either:

FCAT1=B – Software Related Problem,

or

FCAT1=C – Design Related,

and

FCAT2=008 – Software Design,

or

FCAT2=009 – Software Code Error.

7.3 System Performance

Achieved MTBF, MART and Availability of the IT System equipment were calculated in accordance with the R&M Plan. The calculations and a summary of all incidents having been identified for R&M relevance and categorised by the IRP during the R&M reporting period were included in the ILS Report.

7.4 Trend Analysis

Any trends (high failure rates of specific items and design or control problems) which became apparent during the IR monitoring process were reported to the IRP and dealt with as appropriate.

7.5 Master/Slave Incident Association

A technique used by the incident review groups was particularly effective in minimising the workload of processing the IRs. Special 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 as "Slave" incidents to the earlier "Master" incident. Slave incidents were not subjected to further investigation but were immediately

classified and sentenced in accordance with the Master classification. The identification of a Master/slave association also allowed work on failures still undergoing investigation to be curtailed. This scheme proved to be valuable in saving time and effort on nugatory investigations.

8. CLOSING THE 'IR LOOP'

8.1 There were various ways in which agreement was reached on how to 'close' the loop on an incident. The three main methods were as follows:

a) Some Incidents were found to have an identifiable cause, which if removed would make the incident preventable. Therefore where appropriate the IRP would refer an IR to the MOD for consideration as a requirement change or enhancement.

b) Other incidents were considered to be of a transitory nature where investigation had not identified any direct cause. In this case, if no reoccurrence had been reported within a particular timescale, the incident would be declared closed.

c) In other cases the situation in which the original incident had been reported had changed. This would occur due to design changes, hardware changes or changes in procedures. In this case the incident was closed because it was no longer relevant to the current system build standard.

8.2 The process of closing an IR began with the IRWG recommending IRs for closure upon receipt of a completed IR Part 2. Lists of IRs to be proposed for closure were produced 1 week prior to every IRWG and IRP Meeting. These identified the IR number and date, Part 1 and Part 2 detail, suggested FCAT codes, R&M Relevant, System Critical and ART plus the suggested reason for closure and confirmation as to whether the IR fix had been seen.

8.3 The decision on whether to close an IR was made by the IRP, with the closure of an IR and its final sentencing recorded on an IR Part 3. An Incident Report was only considered closed when the MOD Project Office-nominated Chairman had signed the Part 3.

9. LESSONS LEARNED

9.1 General

An example of a DRACAS has been described, which has been applied to the acquisition of a modern IT system. The example illustrates various means of streamlining the reporting/sentencing/action processes. They include an appropriate system of forms for incident reporting and tracking, the use of a central database for the secure capture and dissemination of incident data, and the operation of the incident review groups with an efficient system for identifying master/slave associations and sentencing incidents.

9.2 Application To Future Systems

9.2.1 The IT System for which the DRACAS was developed was a 'non-classical' system in comparison with the more traditional type of MoD procurement.

9.2.2 It made extensive use of Commercial off the Shelf (COTS) hardware and software items, used large volumes of identical items in significant functional redundancy. The system installation connected widely distributed international sites and the system was operational 24 hours a day.

9.2.3 The acquisition of this type of system was becoming more commonplace at the time. The DRACAS described here could successfully be applied to other communications systems having significant proportions of software to hardware.