CHAPTER 23

R&M CHECKLISTS

CONTENTS

INTRODUCTION

General

R&M Design Checklists are a powerful tool which may be used from the design stage to facilitate the identification and elimination of potential sources of unreliability and poor maintainability. The process involves extensive and detailed checking of design features that may influence the reliability and/or maintainability of the item, referring to design drawings, specifications etc. as necessary. Design checklists provide a means to ensure that checks are carried out in a detailed and ordered manner so as to identify and register any design oversights from an R&M viewpoint and to provide a record of intended corrective actions. Design checklists provide a documented input to Design Reviews and will form a key element of the R&M Case during the Assessment Phase of a Project.

This Chapter describes how checklists should be prepared and what their content should be. The aim is not to derive detailed and exhaustive lists for general application since this would be impractical. However, examples are provided of questions that are representative of those which would be included and form a guide to the type of questioning that should be developed. Examples are also given of suitable worksheets.

The R&M achievements of a system depend on all its aspects, including hardware, software, people and man/machine interfaces. R&M engineering efforts have traditionally concentrated on the hardware components. Conversely, software reliability was largely overlooked (because it was assumed that it will ‘work’). More often than not, however, its reliability has been observed to fall well short of the required level. The impact can be of such an extent that failures arising from the software associated with these devices has come to dominate their Reliability and Availability performance. Similarly, in many areas the effect of the interface between the operator or maintainer and the system on its reliability and maintainability has been overlooked. R&M engineering is a system engineering discipline, so R&M programmes should adequately address all these elements. The increasing use of computers, embedded microprocessors and Application Specific Integrated Circuits (ASICs), all of which utilise or embody software to a greater or lesser extent, requires that design checks also cover this aspect of system design.

Example checklists are presented at the end of this chapter but should be considered to be examples only. The Checklists here are based upon those compiled for the original GR77 issued in 1978 using sources such as the US DoD Reliability Design Handbook and industry examples. These checklists have been updated on two occasions since. Initially when they were migrated from GR77 into Issue 1 of Defence Standard 00-41 at which time checklists for software R&M were added. The latest examples provided here are based upon those in the current Defence Standard 00-41 and have been further updated and refined to include guidance on how Human Factors may be addressed.

FORMAT AND CONTENT OF CHECKLISTS

General

Checklists should be raised for each item on which a design check is to be carried out. They should be identified in a way that enables them to be easily collated to present a comprehensive evaluation of the complete design to which they relate.

The basic format of the checklist should provide for:

a) Reference data appropriate to a particular check.

b) Details of the checks to be carried out; as far as possible, these should be phrased in the form of questions.

c) The answers to the questions - preferably a simple Yes or No.

d) Reference to any documentation (for example, design specifications, test reports etc.) that provides supporting evidence of compliance.

e) A unique reference number which clearly identifies the particular checklist worksheet.

f) A brief description of the item to which the checklist applies and the item's parent system/equipment, as appropriate.

g) The status of the item checked (i.e. build standard, drawing number and issue etc.).

h) The date on which the check was carried out.

i) A summary of any follow-up action required as a result of the check.

j) Signatures of the evaluator and approving authority.

Examples of suitable forms are given in Figures 1 and 2. Figure 1 provides for the reference data appropriate to the particular item being checked, such as design parameters, any special features of the design and the various requirements that are applicable. Figure 2 provides for a detailed list of questions that stem from the reference data and also a record of results, supporting references and any follow-up action required.

The content of checklists should cover all design, manufacturing and procedural aspects, which are essential to the reliability and maintainability of the item to be checked, and should be clearly sub-divided under appropriate headings and sub-headings.

Checklists should be treated as active documents because design changes and associated implications arising from them may well raise new areas for investigation. Therefore they should be continuously updated to reflect the latest state of the design. Some checklists may have a general application and these should always be reviewed before they are used. A management procedure should be established to ensure that action is taken on comments arising during a Review and this might be effected through early implementation of a DRACAS (Part C Chapter 18).

The depth and scope of a checklist will vary depending upon the particular item concerned. At the lower levels of assembly, the checklist will generally comprise many detailed questions whilst at the higher levels (i.e. sub-system and system) it will be more concerned with interfaces, compatibility and whether the overall requirements have been satisfied.

PREPARATION OF CHECKLISTS

General

The preparation of design checklists should be started early in the design stage so that they are available for use as soon as detailed drawings become available. Their early preparation should also benefit the designer by providing him or her with a list of those features that are important from an R&M viewpoint.

There are two distinct stages in the preparation of a design checklist:

a) Identify and assemble data on the various requirements that the design must satisfy. These reference data provide the background for the next stage and also serve as a ready-reference during the checking process.

b) Using the reference data as necessary, determine those features and requirements that specifically influence reliability and maintainability. Develop the appropriate checklist questions.

These two stages are considered in more detail in paragraphs 3.2 and 3.3 below.

Stage 1 - Reference Data

Checklist 1 provides an example of checklist worksheet for recording Reference Data and is shown in Figure 1.

Design Parameters - By reference to the User Requirements Document (URD), System Requirements Document (SRD), outputs from the Potential Scenario Analysis (Part B Chapter 1), Operational Needs Analysis (Part C Chapter 1), Performance and Environmental Analyses, Design Specification and any other relevant documents, determine the following design parameters, as applicable for the particular item concerned:

a) Functionality and Performance

b) Environment

c) Size and Weight

d) Handling and Deployment

e) Reliability - This may be the value that has been apportioned to this item as a result of trade-off studies, a known, measured value, or the output of a modelling exercise. It may be a combined figure taking account of both hardware and software characteristics of the item.

f) Maintainability - The derivation of a maintainability figure may also follow similar routes as that for a reliability figure.

3.2.1 The appropriate references should be entered on the worksheet (Figure 1) and also the salient facts for ease of reference.

Special Design Features - By reference to the designer, schematics, design drawings etc. identify all new concepts or special features in the proposed design and note them on the worksheet. Any major assumptions made and their justification should also be noted.

Applicable Standards and Specifications - Identify all standards, specifications, requirements documents and other instructions applicable to the particular item and list their reference numbers (for example Def Stan 00-41) on the worksheet. Those that are mandatory should be listed separately.

Stage 2 – Checks and Results

Checklist 2 provides an example of checklist worksheet for recording Checks and Results as shown in Figure 2.

General - Detailed checklist questions stem from two main sources:

a) Reliability and maintainability design philosophy

b) General engineering standards and practices

When appropriate the source document for any particular check should be quoted on the worksheet and its status shown, for example - Mandatory (M), Advisory (A) etc. (see Figure 1).

Reliability and Maintainability Design Philosophy - Part B Chapter 3 discusses those aspects of design that have particular significance in achieving the required levels of reliability and maintainability in systems. These fall under the following headings:

a) Simplicity of design

b) Ruggedness (or strength)

c) Component, parts and material suitability

d) The use of redundant elements to cover mission critical functions

e) High integrity, structured design and development of software

f) Environment

g) Producibility

h) Testability

i) Human Factors

General Engineering Requirements - Each engineering discipline has its own design, manufacturing and procedural requirements that will apply to any item which is predominantly of that discipline. Although of a general nature they will nevertheless influence reliability because shortcomings will result in reliability degradation through 'systematic failures'. Also care needs to be taken to ensure that a requirement intended to improve reliability or maintainability does not degrade the other attribute. Such requirements should, therefore, be included in design checklists and examples of representative questions are given in Appendix 2.

It should be noted that design evaluation by means of a checklist is an unsatisfactory technique because of its serious conceptual and technical deficiencies. Checklists should not be taken as a substitute for human domain experience.

CHECKLIST WORKSHEET (1) - REFERENCE DATA

System ______________________________

Equipment ___________________________

Assembly ___________________________

Drawing No/

Build Standard _______________________

Worksheet

Ref. No. _____________________________

Date ________________________________

1. DESIGN PARAMETERS	*For example, data and references should be included on:* *(a) Functionality and performance* *(b) Reliability* *(c) Maintainability* *(d) Environment* *(e) Size and weight* (f) *Handling and deployment*
2. PROPOSED DESIGN - SPECIAL FEATURES	*For example, brief details and relevant references should be included on:* *(a) New design concepts* *(b) Major assumptions made* (c) *Any other points of special interest or significance*
3. APPLICABLE REQUIREMENTS AND STANDARDS DOCUMENTS	(a) Mandatory: *For example, all relevant documents and standards quoted in Contracts, internal Company Engineering Instructions and Directives etc. should be included.* (b) Advisory: *For example, general Design Requirements and other relevant documents such as British Standards etc. not specifically called up in contracts.*

FIGURE 1 Example of Design Checklist Worksheet for Recording Reference Data

CHECKLIST WORKSHEET (2) - CHECKS AND RESULTS

System ______________________________ Equipment ___________________________ Assembly ___________________________ Drawing No/ Build Standard ________________________	Worksheet Ref. No. _____________________________ Date _________________________________

No	Source	M* or A*	Checklist Question	Result Yes/No	Supporting References (if any) or Remarks
RELIABILITY DESIGN REQUIREMENTS					
1.	*R&M*	*M*	*Have non-preferred electronic components been used?*	*Yes*	-
2.	*R&M*	*M*	*Are non-preferred electronic components essential to the design?*	*Yes*	-
3.	*R&M*	*M*	*Have the correct qualification procedures been used for non-preferred electronic components?*	*No*	*Application for approval still to be raised for 3 items.*
:	:	:	:	:	:
MECHANICAL DESIGN REQUIREMENTS					
52.	*Def Stan 16-3*	*M*	*Has a stress analysis been carried out?*	*Yes*	*DO/1672/03*
53.	*Def Stan 16-3*	*M*	*Is the design strength satisfactory throughout the whole design envelope?*		*Above reference still to be checked in detail.*

M* - Mandatory A* - Advisory

Follow-up action required - *For example:*

(a) *Corrective action required*

(b) *Supporting references to be checked*

(c) *Summary of shortcomings from an R&M viewpoint*

Signature: ________________________ Evaluator	___________________________________ Approving Authority

FIGURE 2 **Example of Design Checklist Worksheet for Recording Checks and Results**

RELATED DOCUMENTS LIST

1. Def Stan 00-41 Reliability And Maintainability Mod Guide To Practices And Procedures, Issue 3 dated 25 June 1993.

2. GR77/075. Applied Reliability Manual for Guided Weapons Systems. Issued November 1978. Rex Thompson and Partners.

3. Def Stan 00-25 Part 12 – *Human Factors for Designers of Equipment*. Part 11: Design for Maintainability, Issue 1 dated 31 August 1988

4. Def Stan 00-25 Part 12– *Human Factors for Designers of Equipment*. Part 12: Systems, Issue 1 dated 15 July 1989

APPENDIX 1

RELIABILITY AND MAINTAINABILITY DESIGN REQUIREMENTS

This appendix provides examples of representative questions that stem mainly from the content of this manual. They are by no means exhaustive and are intended to act only as a guide to the type of questioning which should be developed. The examples given do not draw any distinction between the assembly levels at which the checks may be applied.

EXAMPLES - GENERAL RELIABILITY AND MAINTAINABILITY

1. DESIGN PARAMETERS

(a) Are all the necessary design parameters clearly specified and available to the designer?

(b) Have any major assumptions been made?

(c) Have they been justified?

(d) Do they affect other areas of the design?

(e) Do they affect reliability and/or maintainability?

2. DESIGN CONCEPT

(a) Are departures from existing design solutions justified?

(b) Will alternative design concepts improve or degrade reliability and/or maintainability?

(c) Will alternative concepts influence other areas of the design?

3. DESIGN REQUIREMENTS

(a) Have all applicable specifications, requirements, etc, been identified by the designer?

(b) Are the interface requirements with other design areas clearly specified?

(c) Are all sub-system or sub-contract requirements clearly specified?

(d) Are all test requirements clearly specified?

4. ENVIRONMENT

(a) Are all anticipated environments and conditions clearly specified (both natural and induced)?

(b) Will these requirements require updating as a result of preliminary environmental testing? e.g. self-induced environments.

(c) Are the arrangements for this satisfactory?

(d) Have all the environments been considered for their applicability to the design?

(e) Have the particular effects of operational use, storage, handling and transportation been evaluated

EXAMPLES - GENERAL RELIABILITY AND MAINTAINABILITY

in depth?

(g) Is the item subject to frequent handling in-Service? Has allowance been made for mishandling?

(h) Can the anticipated environments and conditions be accurately represented in development tests? Have tests been carried out? Has the design demonstrated its capability of meeting the specified requirements?

5. COMPONENTS, PARTS AND MATERIAL SUITABILITY

(a) Have non-preferred components, parts and materials been used?

(b) Are these non-preferred items essential to the design concept?

(c) Have the correct qualification procedures been followed for the 'non-preferred' items?

(d) Are the 'state of art' items used in the design significantly better than any alternative from a performance viewpoint or from a reliability viewpoint? Are adequate failure rate data available for these items?

(e) Have component aging and drifting been allowed for?

(f) Have the junction temperatures of integrated circuits and semi-conductor devices been limited, ideally to below 100°C, and heat sinking used?

6. SIMPLICITY

(a) Is the design as simple as possible?

(b) Can the number of components and parts be reduced?

(d) Does the design include redundant elements? If so, are they justified?

7. DURABILITY

(a) Is the design as durable as possible within the weight and space constraints?

(b) Are electrical components adequately de-rated?

(c) Are components and parts that are susceptible to incorrect operation or installation adequately protected?

(d) Are components and parts that are removed in Service, e.g. for testing, capable of withstanding the degree of handling required?

8. PRODUCIBILITY AND SUPPORTABILITY

(a) Have design checks been carried out (production and QA evaluation) to ensure suitability for production?

(b) Does the item need to be dismantled for inspection and test? Has the extent of dismantling been minimized? Can it be avoided completely? Are sufficient test points provided? Are test procedures designed to minimize the risk of damage and reliability degradation during test?

(c) Are test procedures as simple and concise as possible?

(d) Has the factory and field test equipment been designed in parallel with the item design?

Is the test equipment design as effective as possible?

What proportion of the item is untested?

(e) Is the accessibility for maintenance, repair and replacement of failed items satisfactory?

(f) Are suitable connectors provided where frequent disconnection is necessary?

Can they be connected incorrectly?

Is there sufficient space for their engagement and disengagement?

(g) Are 'lifed' items situated for easy removal?

(h) Can consumables be replenished easily?

Are content indicators easily visible?

EXAMPLES - GENERAL RELIABILITY AND MAINTAINABILITY
Are all inlets suitably protected from ingress of foreign matter? (i) Has provision been made for adequate handling facilities, e.g. hand-holds, jacking points, lifting eyes?

APPENDIX 2

GENERAL DESIGN REQUIREMENTS

This Appendix provides examples of representative questions of a general nature that are relevant to a particular engineering discipline. The will stem mainly from specifications, guides and requirements documents and from accepted engineering practices.

The examples given are not exhaustive. They are only a guide to the type of questions that should be developed.

Examples are provided under the following main headings:

(a) Electronic and electrical.

(b) Mechanical, including hydraulic, pressurisation, fuel systems and general propulsion.

(c) Explosives and weapons propulsion.

(d) Human factors.

EXAMPLES - ELECTRONIC AND ELECTRICAL DESIGN

1. POWER SUPPLY

   (a) Do the power supplies provide sufficient capability to cater for contingencies; e.g. incorrect switching sequence, inadequate voltage and frequency regulation, etc?

   (b) Has the effect of load variation, within specified limits, on voltage and frequency stability been considered?

   (c) Has the effect of transients due to load switching been considered?

   (d) Has the effect of harmonics due to reactive loads been considered?

   (e) Is there fail safe operation in the event of power failure?

2. ELECTRONIC COMPONENTS

   (a) Have all components been selected in accordance with approved procedures?

   (b) Have critical tolerance components been identified and minimized?

   (c) Has the use of variable components been eliminated as far as possible?

   (d) Are all components adequately de-rated?

   (e) Is the earth’s magnetic field likely to have any effect on components during storage?

   (f) Have precautions been taken to ensure that electrostatic discharge does not damage components during assembly, testing and handling?

3. WIRING

   (a) Are the connectors suitable for the environment and location in which they are to be used?

   (b) Is each cable and wiring loom sufficiently current rated at maximum operating temperature?

EXAMPLES - ELECTRONIC AND ELECTRICAL DESIGN

(c) Are cables protected at each feed through point against potential damage during manufacture, assembly, test and field use?

(d) Where individual wire links have been used, are they suitably supported and protected?

(e) Where disconnection is necessary for test or repair, is sufficient free wire available for reconnection?

(f) Can the routing of cables cause interference with adjacent circuits?

(g) Have signal lines been screened from interference and transient pick-up from adjacent power lines?

(h) Has all circuit wiring been identified in accordance with specified procedures?

(i) Is there an approved process specification for internal connections, i.e. soldered , wrapped, crimped or welded?

4. SAFETY

(a) Have all necessary protective devices been included?

(b) Can ozone produced by contact arcing cause chemical reaction or insulation breakdown?

(c) Can contact arcing occur which might constitute a fire or explosive hazard?

(d) Are materials used which could be toxic or produce toxic smoke?

5. FEEDBACK AND EARTH LOOPS

(a) Has sufficient feedback been included in the design to make circuits insensitive to component parameter variation arising from temperature variation and aging effects?

(b) Has all stray capacitance and lead inductance been taken into account?

(c) Have all earthing connections been designed to avoid unnecessary earth loops and to reduce undesired interference effects due to ground currents?

EXAMPLES - MECHANICAL DESIGN RELIABILITY AND MAINTAINABILITY

1. DESIGN STRENGTH

(a) Has a stress analysis been carried out to ensure that all parts have adequate strength?

(b) Is the design strength greater than the applied stress throughout the whole design envelope?

2. FATIGUE

(a) Has the fatigue life of each part been established?

(b) Have all internal corners been suitably contoured to minimize fatigue stress?

(c) Are materials used ‘corrosion resistant’ either by inherent characteristics or by subsequent protective treatment?

(d) Is isolation provided between dissimilar metals to prevent corrosion due to galvanic action?

3. SAFETY

(a) Are the potential fire zones isolated using barriers or firewalls?

(b) Is protection from static electricity provided where fuels or propellants are used?

(c) Are there any explosive hazards?

(d) Are fumes given off by materials toxic/flammable?

4. ORIENTATION

(a) Is it possible to assemble incorrectly any component or part?

(b) Are adjacent connectors of all types keyed, sized or marked to prevent cross connection?

(c) Has flow direction been identified on all pipelines, e.g. gases, air, hydraulics?

5. FASTENERS

(a) Are all nuts, bolts and screws suitably locked to prevent loosening under vibration?

(b) Are all bolt lengths adequately specified, i.e. not too long and not too short?

6. FOULING

(a) Have all moving parts been given sufficient clearance to avoid fouling adjacent structure and wiring looms?

(b) Are mechanisms enclosed or guarded to prevent jamming by loose items during maintenance, testing and operation?

7. STORAGE

(a) Will lubricants deteriorate during prolonged storage?

8. PACKAGING

(a) Has the design of a 'protective packaging for shipment' been completed?

EXAMPLES - MECHANICAL DESIGN RELIABILITY AND MAINTAINABILITY

9. FLUID SYSTEMS

(a) Can gases or liquids that may come into contact during normal operation affect hydraulic/pressurization/fuel system?

(b) Does the hydraulic/pressurization/fuel system include a pressure relief valve or other automatic pressure control device and what is the specified relief pressure?

(c) Can settings of relief valves be adjusted in Service and can these adjustments be effected by accidental change?

(d) Can pressure be relieved during servicing or under emergency conditions?

(e) Are all pipelines adequately marked, all couplings positively locked and all metal pipes bonded to the main earth system?

(f) Is the hydraulic/pressurization/fuel system readily accessible for periodic inspection and servicing?

10. REPLENISHMENT

(a) Are replenishment points suitably marked to identify the replenishment fluid to be used?

(b) Can the ‘full’ state of the system be easily identified?

(c) Can spilled fluid at replenishment points be drained away clear of the system?

11. HYDRAULIC SYSTEMS

(a) Can failure of a pressure gauge or transducer cause failure of the hydraulic system?

(b) Can filters be serviced without draining the hydraulic system?

(c) Has provision been made for a warning or alternative operation in the event of a filter blockage?

12. PRESSURIZATION SYSTEMS

(a) Can injury to personnel arise in the event of a ´burst´?

(b) Are duplicate lines placed as far apart as possible?

(c) Are all sealing gaskets compressed by predetermined amounts, and limited by metal-to-metal contact?

13. FUEL SYSTEMS

(a) Are refueling points readily accessible?

(b) Are fuel drains vented outside of equipments?

EXAMPLES - EXPLOSIVES AND WEAPONS PROPULSION

1. DESIGN REQUIREMENTS

(a) Does the design of explosive or propulsive items comply with the appropriate requirements and will there be correct function when intentionally demanded?

2. SAFETY

(a) Has provision been made to ensure that Electro-Explosive Devices (EED) cannot be initiated unintentionally by:

(i) Electrolytic effects?

(ii) Electrostatic effects?

(iii) Thermo-electric effects?

(iv) Induction from electrical transients?

(v) Induction from AC power sources?

(vi) Induction from RF sources?

(vii) Fault conditions?

(viii) Lightning strikes?

(ix) Shock effects?

(x) Nuclear effects?

(xi) Human error?

(b) Has provision been made to ensure EEDs can only be initiated in the 'armed' condition?

(c) Does the 'safe arming distance' of missiles allow for violent manoeuvres immediately after launch?

(d) Has protection been provided against exposure and proximity to:

(i) Heat sources including fire?

(ii) Flammable fluids?

(iii) High electric or magnetic fields?

(e) Are all firing circuit controls clearly labeled as to function?

(f) Are starting positions of all rotary controls clearly marked?

(g) Is chemical stability of the explosive commensurate with the environmental requirements for the explosive component?

(h) Is there any incompatibility between the explosive filling and any other material used in the manufacture of the explosive component which could result in chemical changes which will cause premature degradation of the safety of the explosive component during its planned life?

EXAMPLES – HUMAN FACTORS

1. SYSTEM DESIGN

a) Do manuals ensure that the text describes adequately how to operate or maintain the system or subsystem in question?

(b) Do they ensure that the information contained in the text conforms to established principles of typography, e.g. legibility?

2. EQUIPMENT DESIGN

a) Has the design of the equipment addressed the agreed anthropometric percentile range of the user population?

b) Have meters/gauges and controls been grouped by related components? Are they distinguishable from each other by using labelling, lines of demarcation, spacing etc.?

c) Is there a logical sequence of operation? For example, do control panels lend themselves to a sequential arrangement of control/display components? Are the sequences left-to-right and top-to-bottom to ensure correct actions made in proper order? Application of this principle minimises operator movements required in performing time-critical or safety-related operations.

d) Are the most important controls and displays within the primary field of view around an operator’s line of sight and reach envelope?

e) Does the availability of the controls and displays match their frequency of use and level of importance?

f) Is there consideration to human strength and lifting capabilities?

g) How will the system be maintained? Are there adequate provisions for ease of access, connecting/disconnecting components, labelling and user manuals?

3. SOFTWARE DESIGN

a) Is the data logically organised? For example, is the information coding (e.g. colour, shape), density, labelling, format and screen layout acceptable?

b) Is the dialogue acceptable? Is the language and structure of dialogue correct?

c) Is there adequate feedback and control? For example, are system messages, hard-copy output, user control, error correction and recovery, and help facilities available?

4. MAINTENANCE

a) Is the system accessible and/or removable for some level of maintenance?

5. ENVIRONMENTAL FACTORS

a) Has the design considered that the user may be wearing protective clothing (i.e. cold weather clothing) and requires a generous allowance of space? Are the controls suitable for use with such clothing? Is there surface texturing to reduce the effect of perspiration?

b) Is a supplementary lighting supply required to provide adequate lighting?

c) Does access for maintenance expose personnel to potentially hazardous situations, such as extreme temperatures or electrically live components?

6. ACCESS

a) Unit Access – has provision been provided for:

i. Pull-out/roll-out approach capability?

ii. Suitable designated areas for working test equipment and/or handbooks?

iii. Identified and easy access for short life items that require frequent replacement?

iv. The tooling and test equipment required for maintenance including visual control/monitoring?

v. The space required to fit and see/use tooling and test equipment?

vi. The use of standard tooling?

b) Standardisation in the use of fasteners should be considered for the whole equipment by using common types and standard sizes. Has the number of fasteners been kept to a minimum and within safety limits? Are the fasteners hand-operated?

General Notes:

The following queries should be applied to reviewing for the purposes of assessing how in a specification the design and implementation have been carried out in the light of the reliability and maintainability requirements. Note that starred items would be used in cases where higher than usual reliability is sought.

The list however cannot be comprehensive and represents only some of the techniques which may be used on a specific project. Their use will depend on the integrity and system reliability requirements and will not necessarily be appropriate in all circumstances. Advice shall be sought from the responsible authority when selecting the techniques to be employed.

EXAMPLES – SOFTWARE RELIABILITY/INTEGRITY

1. SPECIFICATION

Has a specification review been completed which asserts that the specification has characteristics commensurate with reliability requirements such that:

(a) The specification is “complete” e.g. uses a ‘problem description language’ to check?

(b) It contains no ambiguities?

(c) It has been subjected to validation by modeling?

(d) It specifies all external interfaces adequately?

(e) It defines the operational environment for transaction rates/event timings/data volume?

(f) Areas of likely change have been identified?

(g) It does not pre-define a hardware configuration?

(h) It is sufficient to completely define the system acceptance tests?

2. DESIGN

Has a design review(s) been completed which asserts that the design technique (to be) used is commensurate with the reliability requirements such that:

(a) * Mathematical proving of algorithm and program against formal requirements has been completed?

(b) * The design has been duplicated (diverse design) by independent teams?

(c) * Programs are modular with data accessibility and validity checks applied, e.g. Every access by code of a data item is checked for legality of access?

(d) The design is resilient to errors in data and programs e.g. Errors do not propagate?

(e) The design is soundly structured using a method such as MASCOT?

(f) The code uses control flow and data structuring techniques such as those used in PASCAL or ADA?

(g) * The design allows auto-reconfiguration of software/equipment in detection of errors?

(h) * There are independent checks on elapsed time of computation, e.g. Watchdog timers?

(i) Peer group design reviews have been completed?

EXAMPLES – SOFTWARE RELIABILITY/INTEGRITY

3. SYSTEM

Has a configuration review been completed which:

(a) Assures that the hardware configuration is capable of supporting the software to meet the reliability requirements such that adequate computing facilities are provided to support the software techniques required (i.e. to avoid reducing reliability as a result of performance optimization and there is adequate protection of one program from another to prevent failure propagation?

(b) Assures that the hardware and software configuration allow the operator to quickly and accurately reboot and recover the system following a crash, including restoration of any operational configuration, overview or picture in hand immediately prior to the crash?

4. DOCUMENTATION

Has a documentation review been completed which asserts that the documentation is adequate to support the reliability requirements such that it:

(a) Corresponds to the version of software in use?

(b) Is sufficiently error free?

(c) Provides complete and simple instructions for setting up?

(d) Assures that tests are repeatable for subsequent modification?

(e) Is not unnecessarily problematic to new programmers?

5. TESTING

Has provision been made for:

(a) Independent test teams?

(b) Boundary testing?

(c) * All-path testing, e.g. each path through each module has been traversed at least once but not necessarily all combinations?

(d) * Validation of support items, e.g. compilers, operating systems, simulations?

6. UNDESIRABLE TECHNIQUES

Has provision been made to avoid:

(a) Patching?

(b) Unconditional jumps?

(c) Backward jumps?

(d) Multiple entries to procedures?

(e) Self-modifying code?

(f) Use of recursion in procedural languages?

(g) Making programs serially independent?