BS 5760-18:2010

BSI Standards Publication

Reliability of systems, equipment and components

Part 18: Guide to the demonstration of dependability requirements – The dependability case

Publishing and copyright information
The BSI copyright notice displayed in this document indicates when the document was last issued.

ISBN 978 0 580 58624 8

ICS 03.120.01; 21.020; 29.020

The following BSI references relate to the work on this standard:
Committee reference DS/1
Draft for comment 09/30202368 DC

Publication history
First published May 2010

Amendments issued since publication

Date	Text affected

Contents

Summary of pages
This document comprises a front cover, an inside front cover, pages i to ii, pages 1 to 42, an inside back cover and a back cover.

Foreword

Publishing information

This part of BS 5760 is published by BSI and came into effect on 31 May 2010. It was prepared by Technical Committee DS/1, *Dependability and terotechnology*. A list of organizations represented on this committee can be obtained on request to its secretary.

Relationship with other publications

This part of BS 5760 is based upon Defence Standard 00-42 Part 3 [1], adapted for general usage.

Information about this document

Whilst mainly addressing system and equipment level reliability, many of the techniques described in the different parts of BS 5760 can also be applied at the component level. Further guidance on component reliability is given in BS CECC 00804:1996.

Use of this document

As a guide, this part of BS 5760 takes the form of guidance and recommendations. It should not be quoted as if it were a specification or a code of practice and claims of compliance cannot be made to it.

Presentational conventions

The word "should" is used to express recommendations of this standard. The word "may" is used in the text to express permissibility, e.g. as an alternative to the primary recommendation of the Clause. The word "can" is used to express possibility, e.g. a consequence of an action or an event.

Notes and commentaries are provided throughout the text of this standard. Notes give references and additional information that are important but do not form part of the recommendations. Commentaries give background information.

Contractual and legal considerations

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Compliance with a British Standard cannot confer immunity from legal obligations.

Introduction

Dependability is a vital performance characteristic. The provision of systems with acceptable levels of dependability is therefore essential to the achievement of performance effectiveness and optimized whole life costs.

A dependability case provides a convenient and convincing means of recording and presenting an argument supported by evidence that the necessary dependability performance has been or will be achieved.

The dependability performance of a system depends on all aspects of that system, including components, processes, hardware, software, people and all interfaces, including human. Dependability programmes need to adequately address all these aspects.

BS IEC 60300-1 recognizes that different systems and technologies require different engineering activities that might be unique to a particular system. In order to satisfy the dependability requirements for a system, the requirements need to be fully understood and a suitable strategy with defined project management tasks developed to meet those requirements. This includes the identification of dependability risk areas and a description of how these risks are to be managed.

The strategy needs to be flexible in its approach to providing progressive dependability assurance, in that the results of dependability activities need to be reviewed against the dependability requirements and the dependability programme modified as necessary. In particular:

a) the dependability requirements of the purchaser need to be determined and demonstrated to be understood by the purchaser and supplier;

b) a programme of activities needs to be planned and implemented to satisfy the requirements, and investigate the risks;

c) the purchaser needs to be provided with progressive assurance that the dependability requirements are being, or will be, satisfied and that confidence in the dependability is increasing over the course of the programme.

The supplier needs to determine and agree with the purchaser which activities are required to fulfil the second objective. The third objective is to be satisfied by the provision of progressive assurance. It is intended that this assurance is provided by means of a dependability case.

The dependability case is fully described in Clause **4**. It remains with the system throughout its life and record all dependability evidence and data from design activities, trials, etc., through to in-service including field data.

Progress is monitored via dependability case reports which are periodic evaluations of the dependability case and fully defined in Clause **5**.

This part of BS 5760 provides the purchaser and suppliers with guidance on how to manage the dependability case and also provides guidance on assessing and judging the adequacy of the outputs from dependability methods used in the programme. The dependability case is produced by a process that progresses and records achievement in an evidence framework set against the supplier's target dependability measures.

Throughout this part of BS 5760, the term dependability includes reliability, availability, maintainability and maintenance support. The dependability case might also cover testability and durability. Safety is not directly considered in this guide. However, much of the guidance in this part of BS 5760 could also be applied to the production of safety cases.

1 Scope

This part of BS 5760 provides a description of the principles of the dependability case and provides guidance on its content and application in systems engineering. The dependability case can be used throughout the life cycle, from concept and definition, through design and development; manufacture and installation, to operations and maintenance; mid-life enhancement, and eventual disposal.

Whilst this part of BS 5760 is primarily intended for application by the system developers, it will be of value to bodies who might be contracted to manage the dependability case for a project, where deemed necessary.

This part of BS 5760 has five main clauses which describe:

a) principles of the dependability case (Clause **5**);

b) development of the dependability case (Clause **6**);

c) providing the evidence (Clause **7**);

d) presenting the evidence (Clause **8**);

e) assessing the adequacy of the evidence (Clause **9**).

The activities required for the achievement of dependability depend on the nature and development state of the system and are likely to vary significantly from one project to another. The guidelines are not to be considered as being prescriptive in nature: they are generic and do not attempt to be exhaustive.

Annex A describes the general requirements for the dependability case and dependability case report

Annex B provides examples of dependability management risks at different stages of a system's life cycle.

Annex C provides a checklist of points for assessing the adequacy of evidence. The checklist is not to be considered to be prescriptive or exhaustive; it is generic and provides guidance to supplement the generic guidance provided in Clause **8**.

Annex D describes the dependability risk reduction process shown in Figure 7 using illustrative examples where appropriate.

Annex E describes the dependability evidence framework, expanding on the information given in **5.1**.

Whilst this part of BS 5760 does not specifically address safety cases, the same principles can be applied.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

BS 4778-3.2, *Quality vocabulary – Part 3: Availability, reliability and maintainability terms – Section 3.2: Glossary of international terms* (IEC 60050-191)

BS EN 60300-2, *Dependability management – Part 2: Guidelines for dependability management*

3 Terms and definitions

For the purposes of this part of BS 5760, the terms and definitions given in BS 4778-3.2 (BS EN 60050-191) and the following apply.

3.1 dependability risk
potential for non-fulfilment of a specified dependability characteristic requirement

3.2 purchaser
party which orders the item, including the dependability requirements

NOTE This could be an organization, sponsor, department, company or an individual and can change through the life cycle.

3.3 sub-system
part of a system, which is a system in its own right

3.4 system
set of interrelated or interacting elements

[BS EN ISO 9000:2005, **3.2.1**]

NOTE A system can include hardware, software and human elements.

3.5 validation
confirmation by examination and provision of objective evidence that the particular requirements for a specific intended use are fulfilled

*NOTE 1 Adapted from BS EN 61508-3:2002, **3.8.2**, by excluding some of the notes.*

NOTE 2 Validation is the activity of demonstrating that the system under consideration, before or after installation, meets in all respects the requirements specification for that system. Therefore, for example, software validation means confirming by examination and provision of objective evidence that the software satisfies the software requirements specification.

3.6 verification
confirmation by examination and provision of objective evidence that the requirements have been fulfilled

[BS EN ISO 6000:2005, **3.8.4**. Adapted from BS EN 61508-3:2002]

NOTE 1 In the context of this part of BS 5760, verification is the activity of demonstrating for each phase of the relevant life cycle, by analysis and/or tests, that, for the specific inputs, the deliverables meet in all respects the objectives and requirements set for the specific phase.

NOTE 2 Example verification activities include:

a) reviews on outputs (documents from all phases of the life cycle) to ensure compliance with the objectives and requirements of the phase, taking into account the specific inputs to that phase;

b) design reviews;

c) tests performed on the designed systems to ensure that they perform according to their specification;

d) integration tests performed where different parts of a system are put together in a step-by-step manner and by the performance of environmental tests to ensure that all the parts work together.

4 Purpose and description of the dependability case

The purpose of the dependability case is to provide: "A reasoned, auditable argument created to support the contention that a defined system will satisfy the dependability requirements". As the management of dependability is fundamental to the achievement of the dependability requirements and dependability requirements are not absolute measures, the management, control and mitigation of the risks of not meeting the requirements makes up the majority of the evidence in the dependability case.

Starting with the initial statement of requirement, the dependability case includes identified perceived and actual risks, strategies for the management, control and mitigation of these risks and the associated evidence. This evidence refers to associated and supporting information, including dependability evidence and data from design and development, testing, etc., through to operational and maintenance data as appropriate and also record any changes. The dependability case, thus, manifests itself as a top-level control document, summarized periodically through the issue of dependability case reports linked to the evidence. It records progress and remains with the equipment/system throughout its life until disposal and is, therefore, a progressively expanding body of evidence.

The dependability evidence framework is a matrix of dependability risks, requirements for evidence to mitigate the risks, activities necessary to obtain the required evidence, the evidence acceptance criteria, references to the evidence actually provided and confirmation of its acceptance (or rejection). It provides traceability of the dependability case process through the life of the system. It is equally applicable to the purchaser's and supplier's risks and is typically presented in the form of a matrix.

Dependability case reports are periodic updates to the dependability case (usually at predetermined points in the programme as agreed in the evidence framework). They report on the evidence, arguments and conclusions drawn from work since the last report (referring out to papers and data sources where necessary), provide an assessment of overall dependability achievement/progress and a review and evaluation of the dependability plan. When required by a contract, they can be used to provide sufficient detail to allow a decision whether to proceed from one phase of a project life cycle to the next.

BS EN 60300-2 defines a typical system life cycle including the following phases.

a) Concept and definition.

b) Design and development.

c) Manufacture and installation.

d) Operations and maintenance.

e) Mid-life up-dating/enhancement.

f) Decommissioning and disposal.

Different types of purchase or project can involve different combinations of these life cycle phases. For example, if a purchaser is buying an off-the-shelf (OTS) system, the design and development might have been completed some time earlier and the dependability case only includes the manufacture, operations and maintenance phases.

This part of BS 5760 describes the dependability case throughout a full system life cycle. Project managers should tailor the dependability case programme to apply the guidance in this part of BS 5760 to match the project concerned.

5 Principles of the dependability case

5.1 Introduction

As a reasoned, auditable argument created to support the contention that a defined system satisfies the dependability requirements, the dependability case provides an audit trail of the engineering considerations from requirements through to evidence of compliance. It provides the traceability of why certain verification and validation activities have been undertaken and how they can be judged as successful. It is initiated at the concept stage, revised progressively during a system life cycle and is typically summarized in dependability case reports at predefined milestones. Figure 1 illustrates the concept of building and arguing claims in the dependability case using the evidence source.

In practice, the collation of all documentation might be unmanageable, particularly where there are many and diverse sources of evidence. An acceptable solution is to present the dependability case as the body of accumulated dependability case reports, which in turn refer out to source evidence (this is illustrated in Figure 2).

A number of specialist methods and techniques exist that can be used to generate evidence of software reliability; these are broadly divided into confidence-building claims based on analysis of the software development process, and techniques that generate direct evidence of the software's reliability.

All the analyses, strategies, plans, evidence, assumptions, arguments and claims that make up the dependability case are illustrated in Figure 2.

The evidence framework captures the current set of compliance and mitigation activities (and their success criteria) to address the dependability risks. It is typically presented in the form of a matrix.

The number, content, objectives and timescales of the dependability case reports are determined and prescribed by the evidence framework. This starts with the initial work on the dependability strategy and plan and is updated throughout the project. Each dependability case report reflects the latest state of the evidence framework (this is illustrated in Figure 3). This element of the dependability case contains details of the initial requirement and justification of the proposed system.

Figure 4 shows the relationship between the dependability activities and the overall process. It also shows that the evidence produced from the dependability activities can provide input to the safety case.

Figure 1 **The development of claims**

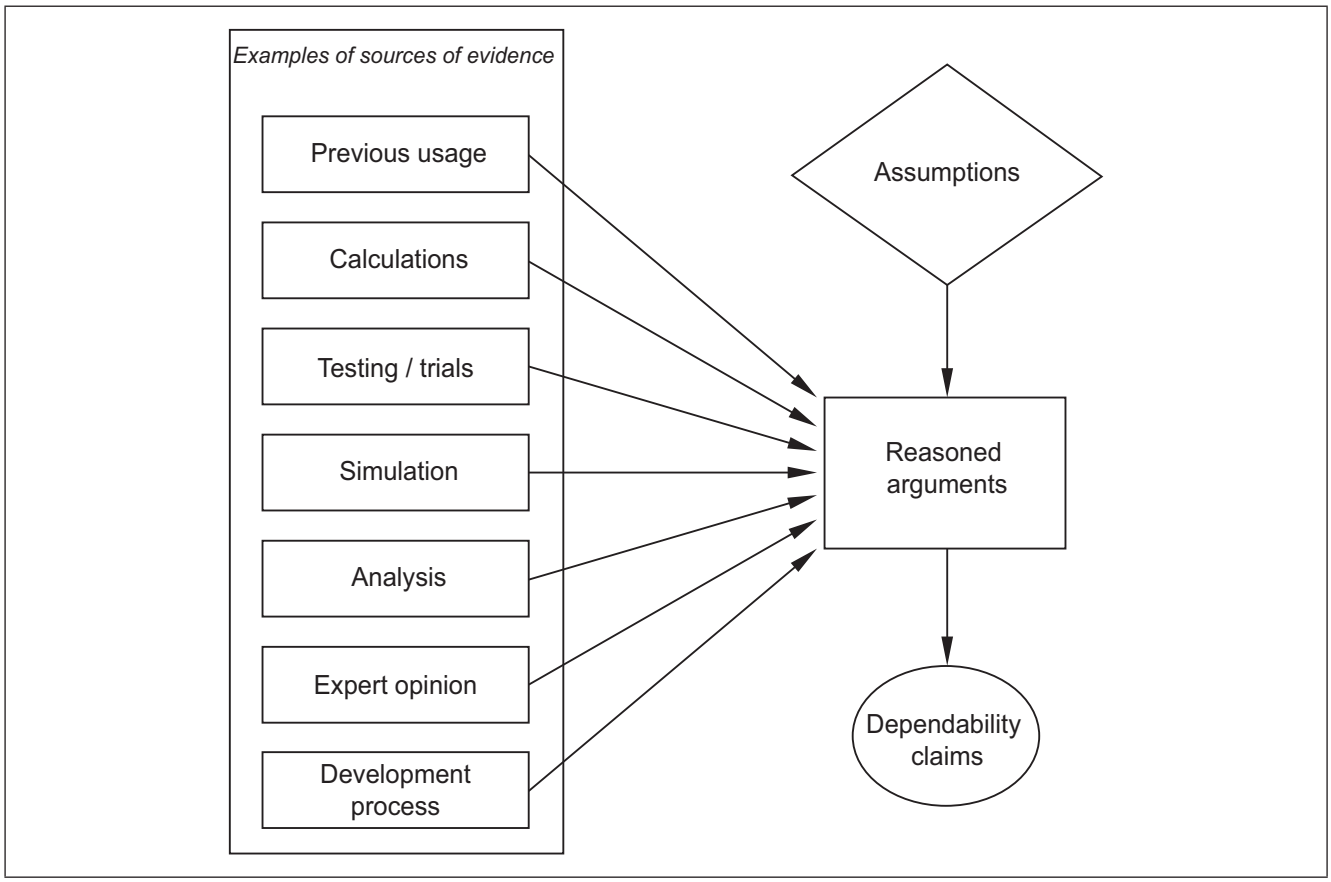


Figure 2 **The concept of the dependability case**

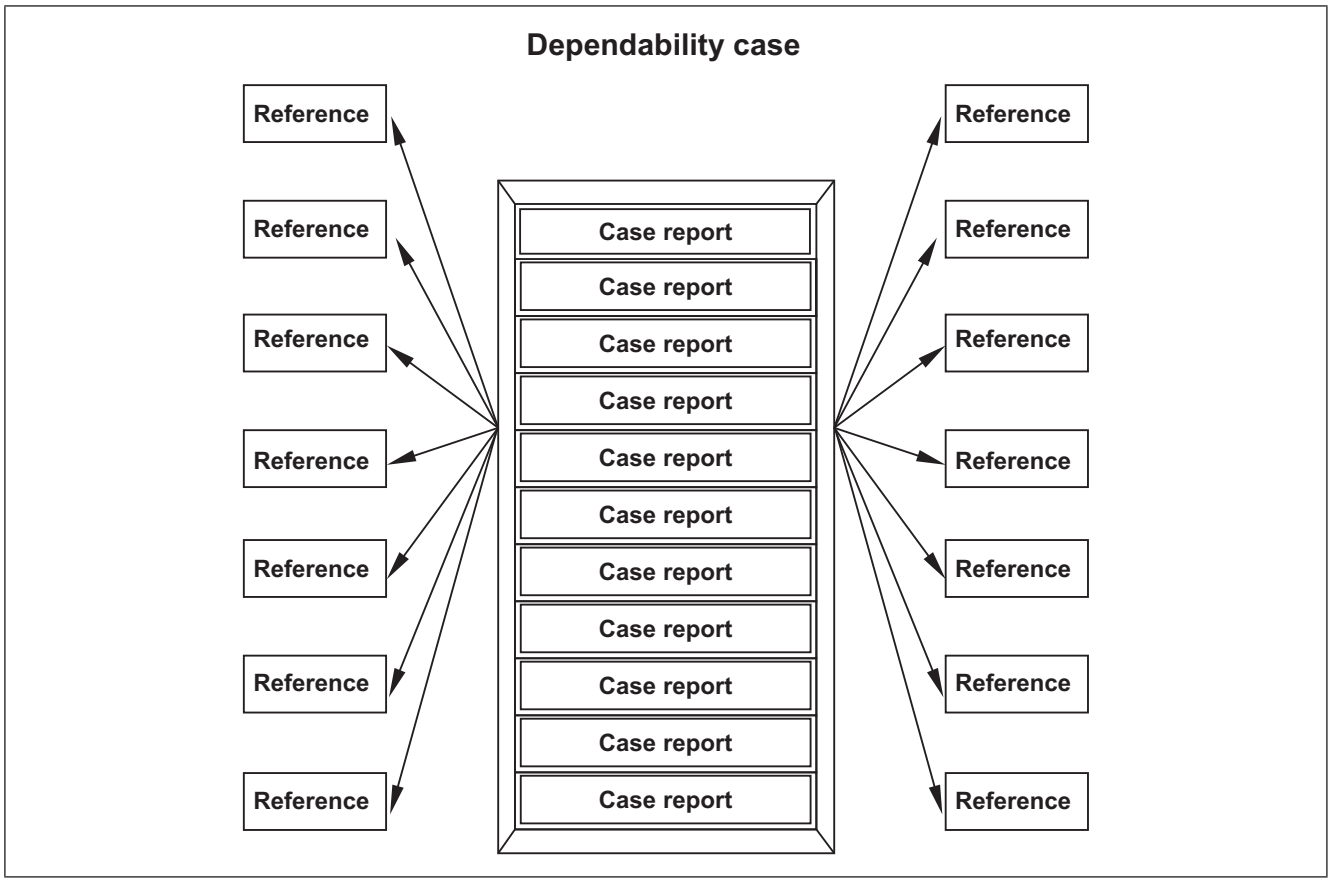


Figure 3 **Establishing and developing the evidence framework**

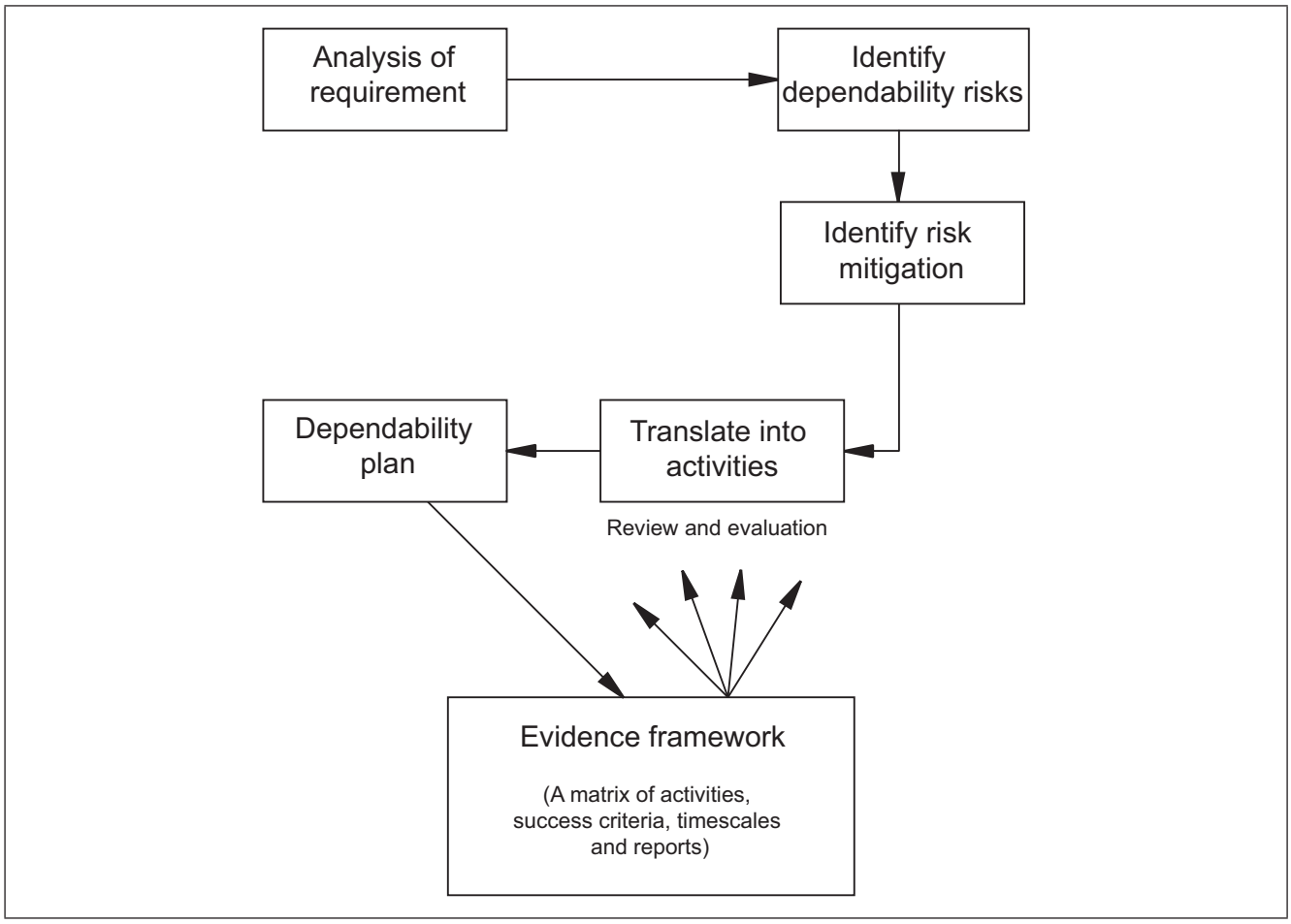
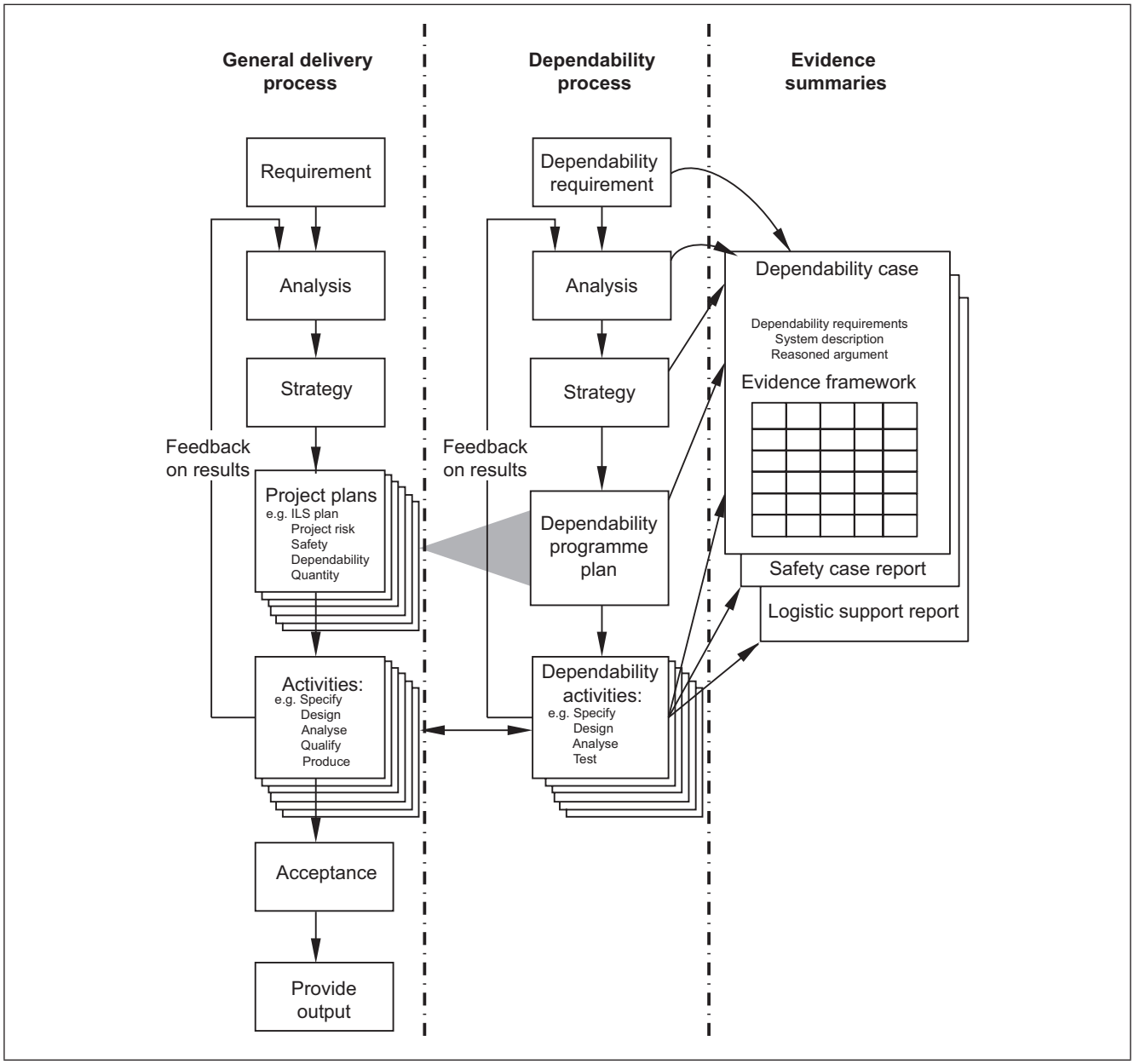


Figure 4 **The relationship between the dependability process, the overall delivery process and the evidence produced**



5.2 Dependability strategy overview

All "projects" should have and maintain an over-arching dependability strategy in the dependability plan. This is to ensure that the capability being procured demonstrates the required dependability characteristics through out its life. The strategy should also detail how the dependability characteristics should continue to be monitored during operation and maintenance.

The purchaser should determine the dependability requirements and their measurement base. The dependability requirements should include the anticipated system usage and its environment. In the absence of specific direction from the purchaser, the onus should be on the supplier to take the initiative and propose appropriate dependability design targets and a measurement base.

Through analysis of the dependability requirements, the supplier should decide upon a robust design philosophy for the eventual solution. The consideration of the risks to achievement of the dependability requirements result in a strategy for managing the risks and delivering the necessary assurance. The programme of activities should include verification and "feedback" to review the dependability plan in the light of achievements.

The details of how this strategy can be implemented are discussed in Annex D.

5.3 The dependability plan

The dependability plan and the dependability case report are two important documents that support the achievement of dependability. The dependability plan should contain a clear description of the management and organizational structure for dependability and a systematic programme of activities for satisfying the requirements and providing progressive dependability assurance.

At the concept stage the dependability plan might incorporate the supplier's dependability case report as a section or annex. During the project, the supplier's dependability case report might be submitted at predefined project milestones with a progress report, and finally submitted at the end of the contract as evidence that the dependability requirements have been satisfied. This might require modifications to the dependability plan.

The dependability plan should be considered as a live document. If results from engineering and other risk mitigation activities indicate that one or more dependability measures are not at the expected level and in order to satisfy the dependability requirements, additional or modified activities should be undertaken. The dependability plan should be maintained to reflect these changes necessary to satisfy the dependability requirements.

The dependability plan might include some activities traditionally considered to be part of a dependability programme that do not provide dependability assurance, but that are included in order to generate information for other disciplines, such as safety and supportability. Although these activities might appear in the dependability plan, they might not necessarily be used to produce the dependability assurance that appears in the dependability case.

5.4 Progressive assurance of dependability

In every project there is potential for shortfalls in dependability characteristic achievement. The recognition of dependability risks should prompt the selection of a programme of specific dependability activities as well as the core design proving activities, which mitigate the risks. The objective is to build up a body of evidence, which provides assurance that the dependability requirements are being achieved.

The risks of not achieving the dependability requirements should be evaluated and managed by the application of risk management practice, which conventionally involves "scoring" of each risk in accordance with a set of criteria defined at the start of the project. The risk management process commences at the bid stage and

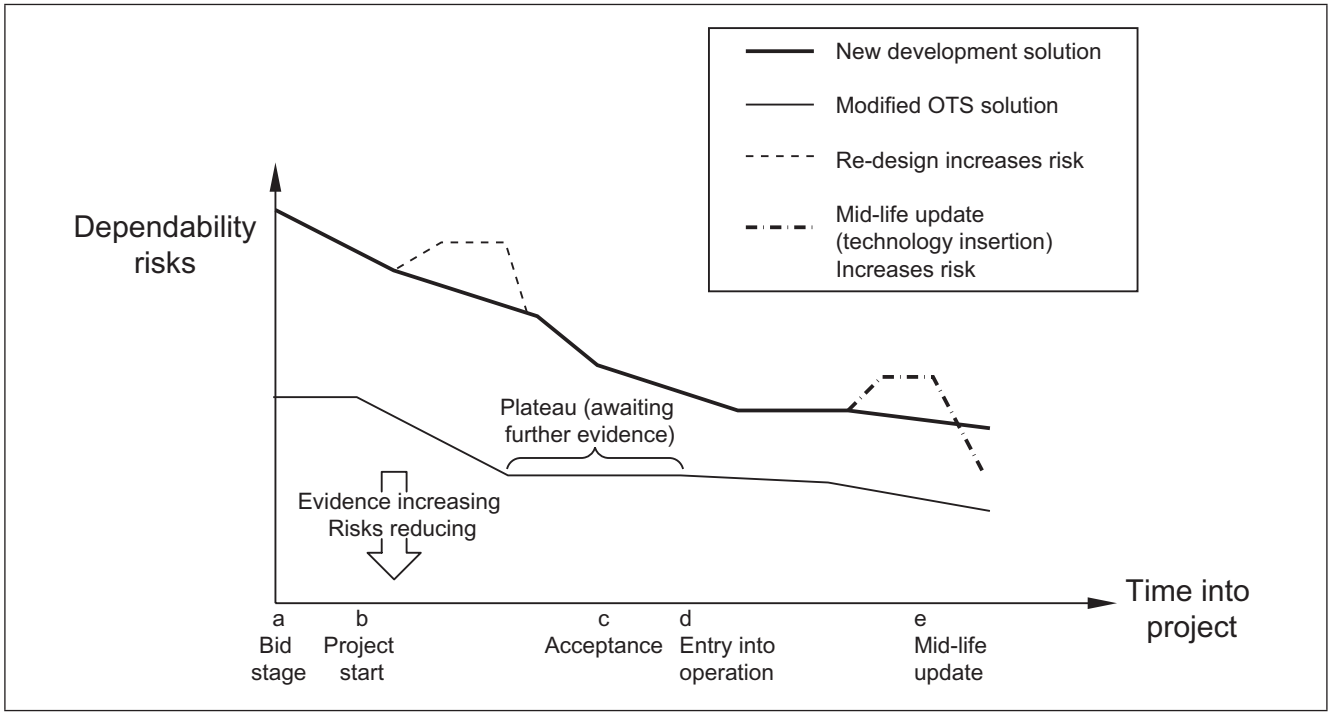
continues through the development, manufacture and operational stages. This is an active process, which reacts to changing levels of risk, and the emergence of new risks as the project progresses.

Figure 5 is presented as an illustration of the manner in which the level of dependability risks change during the course of a project. The vertical axis represents the level of dependability risks identified at any point in the project. As the body of dependability evidence increases, the dependability risks reduce and progressive assurance is obtained. The horizontal axis represents the time into the project, from the bid stage "a", through project start "b", to formal acceptance "c", initial operation, and "d", possible revision/update and beyond.

The figure illustrates two types of product development: new development and modified OTS. At time "a" (bid stage) the level of dependability risk is relatively high, but as the project progresses this level decreases until at "c" (acceptance) the body of evidence is sufficient to assure the dependability at entry into service. The body of evidence (assurance) should continue to build in operation as successful trials and usage are recorded and the residual dependability risks can be seen to reduce still further.

It should be recognized that the dependability risks might not always decrease. There might be occasions when the selection of a different design option, technology insertion or model revision/update renders a proportion of the evidence obsolete, and fresh evidence needs to be generated accordingly. Also there might be periods when no evidence is being provided, for example during testing, prior to the release of the test results.

Figure 5 **Illustration of progressive assurance process**



5.5 Dependability case review

The dependability case might need to be reviewed and, if necessary, updated in the event of significant changes to the following.

a) Design.

b) Conditions of use or environment.

c) Interfacing systems.

d) Client requirements or expectations.

e) Actual performance and design intent.

6 Development of the dependability case

6.1 Introduction

The balance of effort on the development of the dependability case during the life cycle of a typical system is illustrated at Figure 6. This figure refers to the solution which the supplier develops or proposes to meet the purchaser's requirements. During the concept and definition stage the supplier(s) might develop multiple solutions, one of which is selected by the purchaser and taken forward to be manufactured and operated.

6.2 Initial dependability case

The purchaser should determine the dependability requirements and their measurement base. The dependability requirements should include the availability, reliability, maintainability and maintenance support requirements, but also other aspects such as:

a) system usage, including the less obvious aspects of use such as storage and transportation;

b) definition of failure;

c) environment (including atmospheric, regional/terrain and maintenance and support arrangements); and

d) human–machine interfaces.

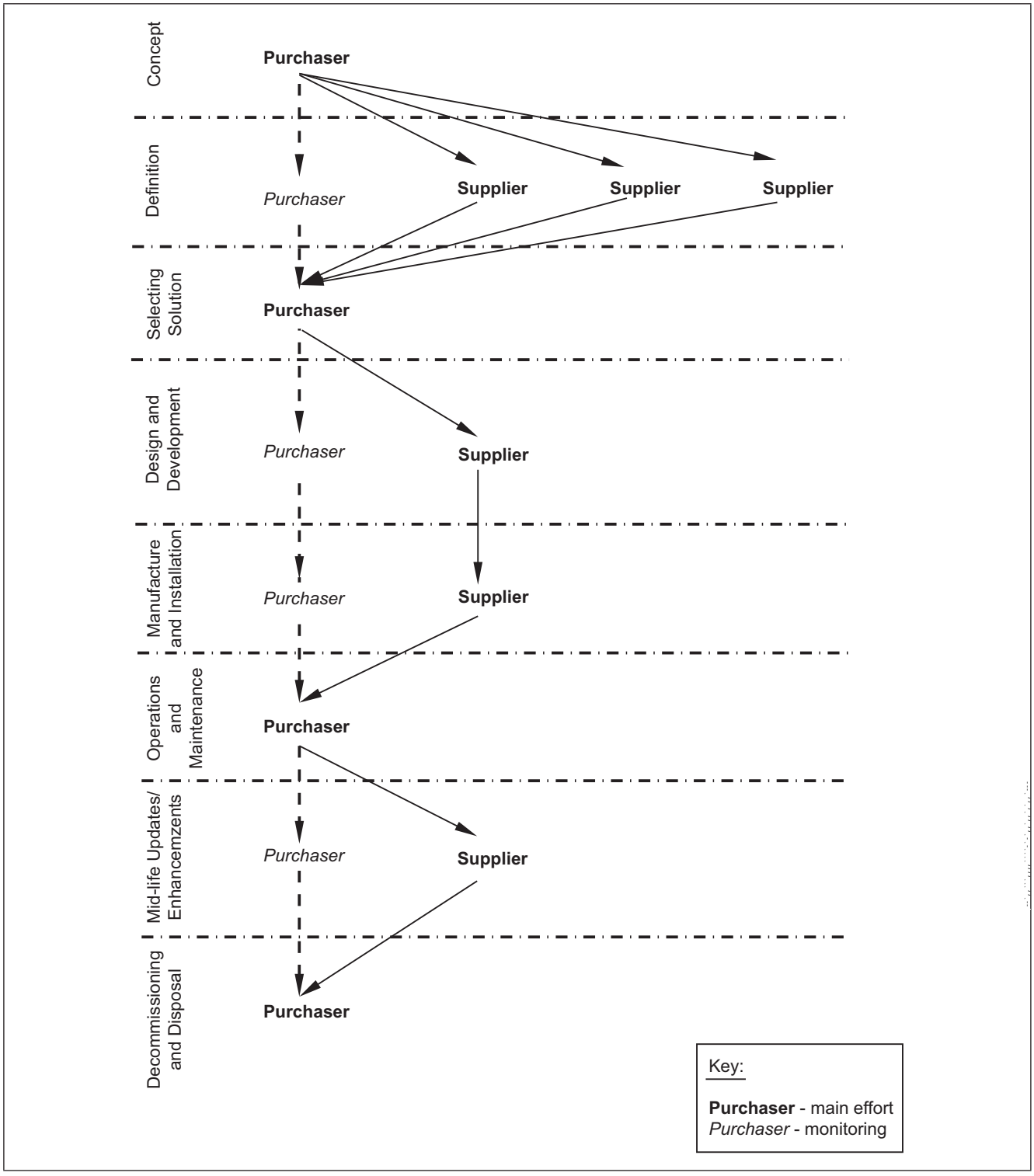
All of these items can have an impact on system dependability.

In the absence of specific direction from the purchaser, the onus is on the supplier to take the initiative and propose dependability design targets and measurement base. Where necessary, references to other documents or evidence (such as the documents that detail the proposed risk, safety, maintenance support and environmental management arrangements) are also included.

It is essential that all the dependability stakeholders are consulted at this stage to ensure that the requirements are fully captured. Specialist advice and the use of dependability modelling techniques are probably necessary to verify that requirements are suitable and sufficient. The purchaser should also identify dependability risks to be included in the overall project risk register. Risks might be identified at this stage that are common to any potential solution and that require specific and timely mitigation activities. These risks might lead to an

initial evidence framework of required minimum assurance activities and these activities might, in turn, form part of the contractual requirements or scope of supply. Where there is a lengthy programme including a significant competitive design or development phase then this aspect is critical and might be necessary in some detail in order to ensure that dependability is included within a common assessment methodology between bidders.

Figure 6 **Example of change of balance of effort over system life cycle**



6.3 Tender stage dependability case and case reports

On receipt of a purchasing request containing an initial dependability case report, the supplier should analyse the dependability requirements and develop a strategy to satisfy these requirements. In the absence of specific direction from the purchaser, the onus is on the supplier to develop suitable dependability requirements together with a strategy to meet them. Strategy development should consider the following.

a) Understanding the requirements.

b) Analysis of requirements to define system dependability targets.

c) Consideration of existing evidence.

d) Identification of risk areas (within the overall project risk register).

The development of the strategy leads to a plan of dependability activities and an outline dependability case report. The content of the dependability plan (to be included in the response to the purchaser) is based on the work to achieve the dependability requirements and mitigate the dependability risks. At this stage the dependability case report should discuss the development of the strategy for providing dependability assurance and document the justification for the proposed activities within the dependability programme. The objective of developing the strategy is to provide confidence to the supplier and the purchaser that the risk of failing to meet the dependability requirements is minimized, before committing resources.

It is essential that the supplier fully understands the requirements. These requirements should be considered in the widest sense, in that they should not only include dependability requirements, but also other aspects such as system operation, its environment, the human–machine interfaces, and supportability, all of which have an impact on system dependability. To gain this understanding, the supplier should be involved in dialogue with the purchaser. This dialogue results in a definitive statement of the purchaser's requirement and all the operational and environmental conditions thereof. This statement gives confidence that the first objective of the dependability programme (see BS EN 60300-1) has been fulfilled.

The dependability requirements need to be understood and analysed to determine the supplier's target dependability measures. The supplier's target value is thus a design aim, to give a margin over the dependability requirement. All the requirements that affect the system dependability should be analysed to determine their impact at system and sub-system level and the results of these analyses form part of the dependability case. For example, the purchaser's requirements for the environment might be relevant to the system as a whole, but due to their location, some items might experience very different environmental conditions.

The supplier should outline the design philosophy and principal design features and then identify the dependability risk areas for the proposed design. The key aspects that should be considered are system maturity, (e.g. a new concept versus systems which already exists), the likely dependability characteristics, time-scales and cost. The risks can be determined using a checklist, but engineering judgement should have a significant input. These dependability risks should be aggregated with other contract risks into the overall project risk management plan. The dependability risks and the strategy for their management form part of the dependability case.

At the bid stage the dependability case report should also include a partially completed evidence/acceptance framework consisting of the proposed dependability activities, their "success criteria", and the project milestone at which this evidence should be produced. The evidence framework should be updated as the contract progresses, with references to the outputs from the activities. The "success criteria" are the criteria by which the dependability case reports are be judged as providing the necessary evidence. The criteria might be quantitative and/or qualitative evidence, i.e. numeric and/or non-numeric. For example, the success criterion for an improvement in reliability activity might be to grow the system reliability to 0.95, whereas for a failure consequence activity, it might be to identify and eliminate all single point critical failures.

6.4 Purchaser's dependability activities during procurement

During procurement the purchaser should study the dependability case reports produced by the supplier and monitor the mitigation of the dependability risks and the progressive achievement of the dependability requirements.

6.5 Purchaser's operations and maintenance dependability case

Once the system enters operations and maintenance it is important that the dependability of the system be maintained. Actual performance of the system and changes in the way that it is used or the environment in which it is used, should be carefully monitored. Significant changes should be analysed and corrective action undertaken to restore the levels of dependability identified in the requirement(s) and incorporated where feasible and justifiable.

The foundation for the dependability case depends on who is responsible for the management of the system in operations and maintenance. If the original supplier is contracted to manage the system, they are able to continue the supplier's dependability case. If the purchaser is responsible for managing the system, then it is likely that they will base the dependability case on their interpretation of the dependability case reports together with evidence from any dependability demonstrations.

6.6 Modifications

It is possible that the system might require modifications during the operations and maintenance phase, involving contract action on a supplier. If this happens, the supplier should build a dependability case using the purchaser's dependability case as a base line. The purchaser's monitoring actions and the results should be captured in the dependability case.

7 Providing the evidence

The dependability case draws on various forms and levels of evidence, ranging from plans and programmes, standards, resources and competencies, to detailed results of numerical analysis and testing.

These forms of evidence might include:

a) performance in previous operation;

b) analysis of the required operational cycle;

c) design calculations;

d) predictions and modelling;

e) testing;

f) simulation;

g) expert opinion including previous recorded success of the supplier;

h) correct implementation of best practice

i) supplier's dependability cases.

During the design and development phase, dependability activities are undertaken in order to generate evidence. It is essential that the activity results (the evidence) are reviewed progressively against their defined "success criteria", and also assessed in terms of meeting the ultimate target dependability measures. If the results indicate that any of the system dependability characteristics are not at the expected level for the specific stage of the programme or that the evidence does not satisfy its "success criteria", then the strategy might have to be modified. The dependability plan would be amended to include additional or modified activities.

As the life cycle progresses, evidence is generated and gathered. Initially the evidence might only provide guidance that the requirements are likely to be achieved. However, as the project progresses the evidence becomes more precise to substantiate the achievement of the dependability requirements. At the end of the contract the expectation is that the evidence framework demonstrates that the dependability requirements have been met. It is difficult to describe the full range of evidence in its many forms that might be provided, however, indicative examples of what the dependability evidence might encompass are shown in Annex E.

Figure 1 shows that the reasoned arguments in the dependability case can combine different types of evidence and also build on assumptions. It is important that these assumptions should be declared openly. During the dependability programme, the key assumptions should be validated where possible effectively replacing each with substantiated evidence. The reasoned arguments enable claims to be made about the dependability expectations, together with their supporting evidence, make up the dependability case.

8 Presenting evidence

This clause provides guidance on how to present the evidence in the dependability case. The activities required for the achievement of dependability depend on the nature and development state of the system and are likely to vary significantly from one project to another.

Before undertaking a dependability activity it is essential that the objective of the task is fully understood, and success criteria defined. The success criteria should be those by which the activity can be judged, and will substantiate a claim in the dependability case report. It should be noted that not all activities lend themselves to a quantified success

criteria, and might require qualitative criteria based on the objectives of the activity. For example, the success criteria for modelling are not simply that the predictions and modelling show compliance of the proposed design with the requirements. More important are considerations such as; does the modelling include representative operation of the system or have all system elements (e.g. software) been included in the modelling.

Many of the available dependability methods do not deliver dependability assurance on their own: this is only provided when used in combination with other associated methods. For example, an analysis technique such as fault tree analysis might identify a design weakness, but improvement and assurance are only provided when the weakness is dealt with at design reviews.

The evidence of dependability assurance does not just result from the generation of the activity results, but also from the implementation of actions arising from the risk identified by the activity. Undertaking the activity at the appropriate time such that it influences the design is very important. Therefore the evidence from the analysis consists of the documentation showing that actions have been implemented in a timely manner.

Activities should be carried out in parallel with the design process, so that the analysis can influence the design and reflect the final design. If more than one design option is being considered, then each outcome should be considered separately, so that the implications on reliability and the consequences of failure can be assessed before deciding on the preferred design option.

The input to the dependability case from an activity can be considered to include the following parts.

a) Objective and success criteria (what the activity plans to achieve, and defining when the activity has been successful).

b) Outputs (the outputs from the activity).

c) Assumptions.

d) Evidence (how the outputs substantiate claims in the dependability case report).

e) Development and maintenance of the evidence framework (how will the results of the activity be maintained to reflect the latest design).

9 Assessing the adequacy of evidence

The adequacy of evidence is primarily a function of its practical impact on the reduction of dependability risks, i.e. progressive assurance. Whilst it is not necessary to assess the adequacy of specific, detailed dependability tasks in their own right, the visibility, traceability and quality of evidence produced are crucial factors. It is therefore necessary to confirm that the evidence is generated, managed, validated and used within a closed loop system of dependability practices and controls, and that it achieves the principal objectives of BS EN 60300-1. Figure 7 illustrates a representative closed loop system (dependability risk reduction process), based upon which, criteria for assessing the adequacy of evidence are derived in this clause.

Figure 7 comprises four main sections from left to right.

a) Firstly, the left hand section reiterates the principal objectives of BS EN 60300-1. These represent the highest level criteria for the adequacy of evidence and need to be borne in mind as key objectives, throughout the risk reduction process.

b) Secondly, the dependability practices, which are fundamental to assuring dependability, are high level, "objectives-oriented" processes which depend on the appropriate traditional dependability activities, (or tailored dependability activities), for specific analyses, tests and results. The dependability practices exchange evidence between themselves and output evidence to the dependability controls.

c) Thirdly, the dependability controls are processes based on "review the evidence" and lead to the dependability strategy, "dependability plan" and "manage dependability". At any stage, inadequate evidence should stimulate a review of the dependability strategy within the "dependability plan". "manage dependability" provides a control feedback path to all of the dependability practices (and selected dependability activities within them), to deliver the evidence required. In this way, the dependability processes are focused at all times on providing progressive assurance that the risks are being managed.

d) Fourthly, the right hand side of Figure 7 identifies the key outputs of the risk reduction process, including the "dependability risk register" (which is part of the project risk register), "dependability case and reports" and the "assessment of adequacy" of the evidence. Note that the latter does not address adequacy of the dependability case and reports intrinsically.

The dependability risk reduction process is applicable at any project phase, and to any contractual arrangement. In Figure 7, an identifier has been allocated to each process block for reference purposes only. The identifiers do not signify chronological sequence, as the processes are interactive and often concurrent. Depending on the stage in the procurement cycle for a new, developing or OTS system, both the relevance of different practices and the order in which they are conducted vary. However, there should always be a risk register and dependability plan as core elements of the process. Wherever possible, the two general practices, "collate existing evidence" and "DRACAS/operational feedback" (DRACAS: Data Recording and Corrective Action System) should be on-going, spanning different generations and versions of similar systems. All relevant, available information on the dependability achievements and lessons learnt a particular design should be used to provide assurance of dependability in similar systems.

For a particular system life cycle, entry into the process is achieved by developing a Dependability case, using at least the practices (a) to (e) of Figure 7, including dependability modelling/simulation as an activity. The available evidence (including dependability risks) is reviewed, a dependability strategy is determined and dependability planning and management implemented to control and monitor dependability activity. Once the process is established for a particular project, the dependability practices and controls should be implemented and maintained in the most expedient manner to generate and manage evidence which mitigates dependability risks and provides, within

the procurement cycle, the earliest possible indication that the dependability requirements have been achieved.

The principal criteria for assessing the adequacy of evidence are therefore as follows.

1) The evidence as a whole is clearly derived from a closed loop dependability risk reduction process such as Figure 7, see Annex D for guidance on the principles of specific process blocks.
2) The origin of any specific item of evidence is unambiguously linked to specific dependability practice(s) and/or control process(es).
3) The links between any specific item of evidence and the dependability risk register, and dependability plan are shown.
4) The evidence from any particular dependability activity is presented in accordance with Annex A.
5) The status of each item of evidence, in terms of its relevance, completeness, accuracy and how it has been used to influence the system and reduce risk, can be readily identified in the evidence framework.

In order to assess the adequacy of evidence, auditable methods/techniques, assumptions, and detailed results should be sought. Consequently, an open, honest dialogue between partners is of high importance. Judgement is required to assess the evidence presented, including its visibility, traceability and quality in accordance with the criteria listed in items 1) to 5). Annex C provides a checklist of generic points which are not prescriptive, but which should provide additional guidance on assessing the adequacy of evidence in appropriate circumstances.

Annex D outlines the principles of the process blocks in Figure 7 and provides guidance on the context for assessing the adequacy of evidence against the criteria listed in items 1) to 5). Normally, all of the dependability control processes, and the relevant dependability practice processes, need to be considered for a particular system/life cycle phase, the selection of any particular process being driven by the need to provide evidence against the dependability risks. Due to the broad scope of the guidance, Annex D does not recommend specific dependability activities but it identifies examples where appropriate to help illustrate a point.

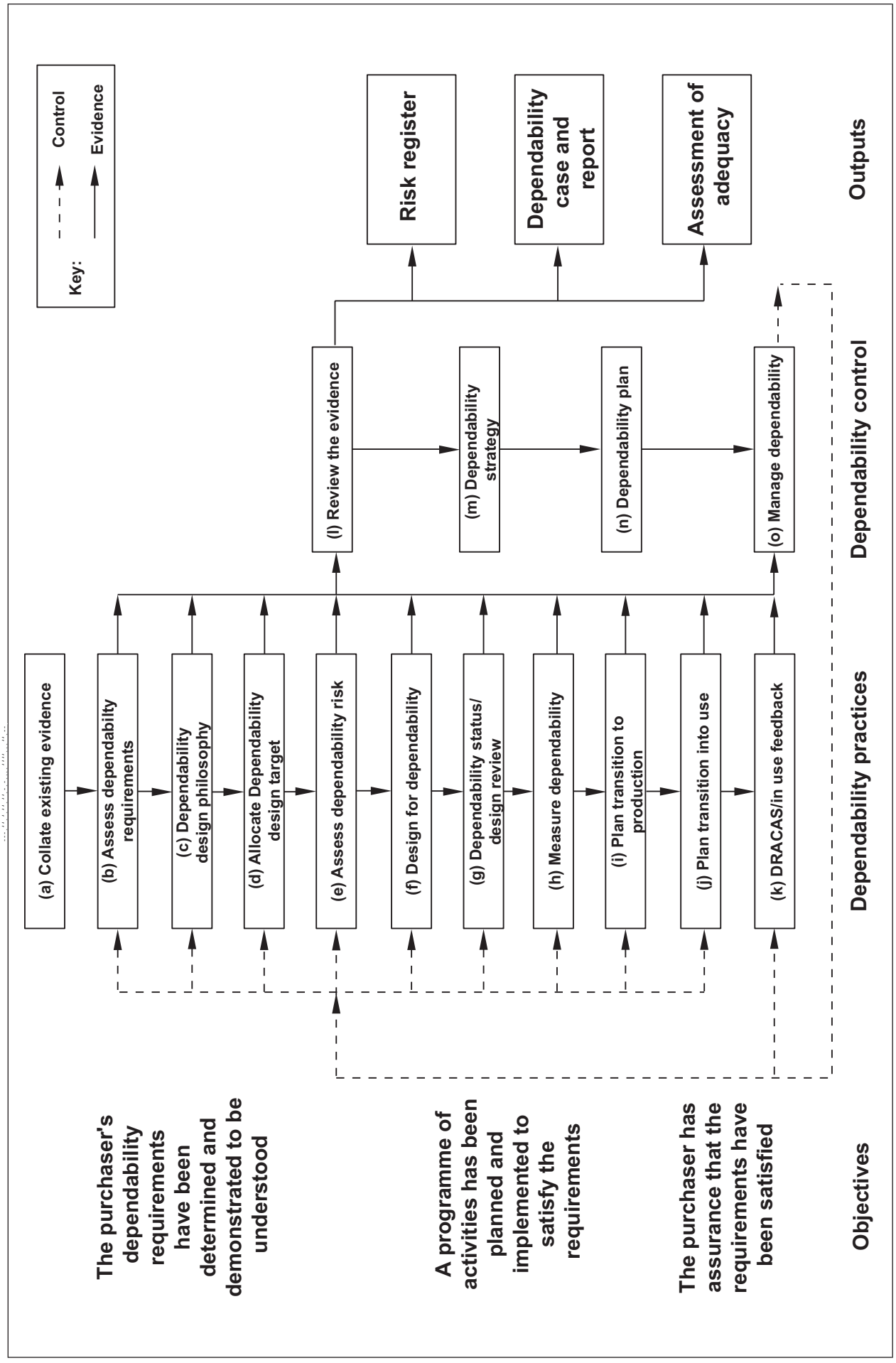


Figure 7 Dependability risk reduction process

Annex A (informative) General requirements for the dependability case and dependability case report

A.1 Dependability case

NOTE The following subclauses provide the headings and describe the content for sections within the dependability case. It is not envisaged that this structure will be suitable for every contract, but it is intended to provide guidance on the information that should be contained within the reports.

A.1.1 System description

The system description should contain the following items.

a) System description – this should briefly describe the system's physical or functional characteristics.

b) System boundary – this should describe the system's physical or functional boundary. Block diagrams can provide a good method of illustrating the boundary of the system considered in the case.

c) Operation – this should describe the system's primary role or function, and any secondary roles. It should include its typical anticipated duty cycle.

d) Environment – this should describe the system's operating environments.

e) Interfaces with other equipment/systems – this should define equipment associated with the inputs, outputs and services to the subject system. Where appropriate, it should also describe such equipment physically near to the installed system.

f) Build standard/software version – this should relate to a specific build standard of the system, including software version(s) where appropriate.

g) Configuration control – to ensure the report reflects the latest build standard/version, the description should indicate where the latest build standard/version is defined, for example, the master record index.

h) Personnel skill levels and training – the skill level and the training required to operate and maintain the system should be described.

i) Maintenance policy – this should describe the support regimes for each of the system's role or anticipated duty cycle profiles.

A.1.2 Dependability requirements

This should reflect the purchaser's requirements and the supplier's understanding of those requirements. The requirements should be considered in their widest context, in that they should include the environment and usage requirements, as well as the explicitly defined dependability requirements. The supplier should describe how the requirements have been interpreted for his proposed design solution and developed into contract target dependability measures.

A.1.3 Dependability risk areas

Through analysis of the dependability requirements, the supplier should identify the risk areas associated with the system satisfying the dependability requirements, and the how these risks will be, or have been managed during the contract.

A.1.4 Dependability strategy

Based on the risks identified, the maturity of the proposed design solution and the dependability requirements, the supplier should determine a strategy for meeting the requirements and providing the necessary assurance. This strategy justifies the activities in the supplier's dependability programme and identify the success criteria for these activities. The dependability strategy is to be outlined in the dependability plan.

A.1.5 The evidence framework

This section should provide a complete overview or plan of evidence to be provided during design and development phases. It should also show when and by whom dependability case reports are to be issued. Specific entries in the evidence framework can be selected by the purchaser and might be matched to payment milestones for control purposes.

A.1.6 Dependability claims

Typically, the claims will be that the system satisfies each of the dependability requirements. This section should provide a reasoned argument why each of the requirements will be met in operation and maintenance, based on the evidence and any assumptions. All assumptions should be listed explicitly.

A.1.7 Limitations on use

This section should define the boundaries on system use, which if exceeded means that the dependability claim might no longer be valid. These limitations include the system's operating envelope, the environment and important maintenance activities.

A.1.8 Conclusions and recommendations

This section should contain a diary of the conclusions drawn from the dependability evidence accumulated to date, including whether the system is likely to satisfy its dependability requirements. In interim issues, it should recommend whether the project should proceed to its next milestone, or what further work is required to enable the project to progress. In addition, it should recommend what activities should be conducted in the future in order to generate the necessary assurance that the dependability requirements will be satisfied.

A.2 Dependability case reports

The remainder of this annex provides guidance on the content of dependability case report. The dependability case report provides dependability evidence at a specific stage within the dependability case evidence framework. The reports present an argued claim, based on evidence and assumptions that the system will satisfy the

dependability requirements. The report is not expected to contain all the evidence produced for that stage, but to summarize and act as a "signpost", indicating where the detailed evidence can be found.

This part of BS 5760 jointly refers to dependability, which might be taken to imply that documentary evidence for dependability will be summarized in a single report. However, this does not mean that the dependability case reports should be documented in the same report. If the evidence framework requires separate reports, or the purchaser or supplier considers that having separate reports presents a clearer picture, or provide a more focused approach, separate reliability and maintainability case reports are considered perfectly acceptable.

A.3 Format for dependability case report

Where appropriate, to improve readability and the transfer of information dependability case reports associated with a given project should attempt to adopt a common format. Such a format is described as follows.

a) **Introduction**. Each dependability case report should list and cross reference the parent requirements in the evidence framework, against which the evidence is to be judged, and be traceable to the original purchaser's requirement.

b) **Body of evidence**. This should index the existing evidence. Every item of evidence should be cross-referenced to the evidence framework, and each of the risks to which it mitigates. The following list comprises examples of the type of evidence which should be included.

- Information from relevant similar systems' dependability cases or operational and maintenance experience.
- Suppliers' evidence and dependability case reports.
- Analysis of dependability requirements and operating conditions.
- Design philosophy.
- Targets.
- Risks.
- Strategy, including assumptions, arguments, claims.
- Plan of dependability activities.
- Outputs from dependability activities; these should include the relevant design dependability calculations, use of best practice, predictions and modelling, analyses, simulation, testing, DRACAS/operational and maintenance feedback and expert opinion.
- On going re-assessment of risks.

The body of evidence should also trace the history of reviews and updates of the dependability design philosophy, targets, strategy and plan, which keep these in line with the changing status of the original risks, as well as any new/emerging risks.

c) **Review of evidence to date**. This section should provide a balanced review of the body of evidence in terms of its completeness, timeliness and acceptability with regard to the criteria contained in the evidence framework.

d) **Conclusions**. The status of the dependability assumptions, evidence, arguments, claims and residual risks should be summarized and discussed. Conclusions should be drawn with regard to the status of the progressive assurance and the activities necessary to mitigate the residual risks.

e) **Recommendations**. The recommendations should be based on current shortfalls in the evidence available and propose changes, as appropriate, to the dependability design philosophy, targets, strategy, and plan in order to maximize the progress towards assuring that the system satisfies each of the dependability requirements.

Annex B (informative) Examples of dependability management risks at the different stages of a systems life cycle

Concept of the system	**Failure** of the purchaser to define the requirements adequately.
	Failure of the purchaser to define the requirements correctly.
	Failure of the purchaser to allocate sufficient resources to achieve requirements.
Identifying solutions	**Failure** of the purchaser to communicate the requirements to the supplier.
	Failure of the supplier to understand the requirements.
	Failure of the supplier to identify all the dependability risks.
	Failure of the supplier to produce an appropriate plan to mitigate the dependability risks.
	Failure of the purchaser to monitor progress.
Selection of solution	**Failure** of the purchaser to select the most appropriate solution.
	Failure of the purchaser to modify the requirements where appropriate.
	Failure of the purchaser to communicate the modified requirements to the supplier.
	Failure of the supplier to understand the modified requirements.
	Failure of the supplier to identify all the dependability risks.
	Failure of the supplier to produce an appropriate plan to mitigate the dependability risks.
	Failure of the purchaser to monitor progress.
Demonstrating the solution	**Failure** of the supplier to work to their plan to mitigate the dependability risks.
	Failure of the supplier to monitor and review progress and amend their plan where appropriate.
	Failure of the supplier to capture all available data and process it appropriately to produce evidence.
	Failure of the supplier to produce sufficient evidence to demonstrate dependability to the satisfaction of the purchaser.
	Failure of the purchaser to monitor progress.

Producing the solution	**Failure** of the supplier to identify and manage the dependability risks associated with the transition from development to production.
	Failure of the supplier to monitor and review progress and amend their plan where appropriate.
	Failure of the supplier to demonstrate the dependability of their systems to the satisfaction the purchaser.
	Failure of the purchaser to monitor progress.
Supporting the solution	**Failure** of the purchaser to ensure that the solution is used, maintained and supported as specified.
	Failure of the purchaser to monitor changes in use, environment and support.
	Failure of the purchaser to identify the dependability risks that result from a change in use, environment and support.
	Failure of the purchaser to mitigate the dependability risks that result from a change in use, environment and support.
	NOTE 1 The purchaser might choose to delegate some/all of the responsibility for managing these support risks to a supplier.
	NOTE 2 Risks associated with obsolescence have been included in "support".
Disposal of the solution	**Failure** of the purchaser to capture, record and disseminate dependability "lessons learnt" (including evidence) from the project.
	NOTE 3 Specific examples of technical risk have not been included but should be considered on a case-by-case basis.

Annex C (informative)

Checklist of points for assessing the adequacy of evidence

This annex provides a checklist, which should be considered as a prompt to initiate action where the checklist points have relevance and does not imply a "Yes" and "No" answer. Judgement is required to evaluate the evidence presented. The checklist should not be considered as being prescriptive or exhaustive: it is generic and provides guidance to supplement the general guidance provided in Clause **9** of this part of BS 5760.

Checklist:

a) Are the objectives for the activity clearly defined?

b) Has the activity been undertaken in a systematic manner and is it complete?

c) Has the activity been undertaken at a time that allows influence on the design?

d) Has the usage and environment considered for the activity been documented?

e) Has the physical and functional boundary of the activity been defined?

f) Are any assumptions defined (e.g. inputs from other systems or services), and are they realistic and reasonable?

g) Is justification given for the activity method/technique used, and is it reasonable?

h) Who was consulted during the activity, (e.g. user, maintainer, designer)? Was this level of consultation reasonable?

i) Are the activity recommendations clearly defined, and are they reasonable?

j) Does documentary evidence indicate that the recommendations have been implemented?

k) Have the activity results been progressively updated to reflect the latest design, and are these being used as an input to design reviews?

Annex D (informative) Dependability risk reduction process

This annex presents the principles of the process blocks, which are illustrated in Figure 7. It contains guidance on the context for assessing the adequacy of evidence against the criteria of Clause **9**. The process identifiers and titles from Figure 7 are listed, followed by an indication of the principles of what the evidence should comprise and how it would relate to other processes. Illustrative examples are included, where appropriate. Normally, all of the dependability control processes, and the relevant dependability practice processes, would need to be considered during each life cycle phase.

a) Collate existing evidence – information from relevant similar system dependability cases or operational dependability experience, including both successes and failures; arguments and justification for using it to mitigate risks and generate assurance; confirmation of an on-going commitment to dependability improvement.

b) Assess dependability requirements – interpretation of operating and maintenance scenarios, environmental profiles and the understanding of:

- the purchaser's dependability case;
- permissible/degraded modes of operation;
- anticipated duty cycle operational success and failure criteria;
- qualitative and quantitative dependability requirements;
- storage and transportation needs;
- design loads.

c) Dependability design philosophy – a process of continuous improvement and commitment to providing assurance of robust design, eliminating known failure mechanisms or increasing time to failure to an acceptable level; fault avoidance techniques for software development; specific dependability design criteria (e.g. redundancy/fault detection and recovery) necessary to achieve the assessed requirements [b)], using lessons learnt from previous systems [a)]; necessary dependability resources to implement the philosophy.

d) Allocate dependability targets – based on appropriate dependability analysis and modelling, quantitative/qualitative targets allocated to subsystems/components; confirmation that these are practicable, realistic and fully consistent with the dependability requirements.

e) Assess dependability risks – formalized, systematic identification and evaluation of dependability risks; details of technical and timescale risks with regard to the dependability requirements; input to and maintenance of the dependability risk register detailing the current status, whether open or closed, of all identified dependability risks; integration with the project risk register; links to the dependability strategy in the dependability plan and re-evaluation of risks in order to assess the risk reduction available from dependability practices contained in the strategy; links with the evidence Framework.

f) Design for dependability – design to meet the dependability requirements, design philosophy, targets and strategy [b), c), d) and m)]; system description/justification; design margins; confidence in dependability at internal and external interfaces.

g) Dependability status/design review – evidence of independent assessment and review of design decisions, analyses and tests that impact on dependability, documented to provide an auditable trail; dependability contributions to formal design reviews; confirmation that the status of dependability processes and activities are in accordance with the strategy and dependability plan.

h) Measure dependability – results of dependability tests on specific components/subsystems and a representation of the final system, as determined by the strategy and dependability plan; software performance testing; confirmation of use and impact of DRACAS [k)] to mitigate all recorded failures.

i) Plan transition to production – plan for the design and validation of manufacturing systems and processes in order to protect critical items, realize the design performance and quality requirements and safeguard a smooth transition to production.

j) Plan transition to operation and maintenance – plan for dependability risk control activities and dependability demonstration plans for the transition to operation and maintenance.

k) DRACAS/operational feedback – all incidents should be subject to DRACAS; relevant lessons learnt and corrective actions determined from this and previous systems; confirmation that these have been implemented on the system.

l) Review the evidence – this should be a routine review of all evidence arising and conducted, exceptionally, whenever the findings from any of the dependability practices need to be considered urgently; all items of evidence should be specifically linked to, and traceable with regard to, the dependability strategy [m)], risk register [e)], dependability plan [n)] and the evidence framework.

m) Dependability strategy – this forms the response to the assessment of available evidence [l)]; creation and maintenance of a structure of assumptions, claims, arguments and evidence needed to assure dependability; definition of appropriate dependability practices necessary to deliver the evidence; the assumptions should be justified and the claims should be practicable and realistic, based on what has been achieved in the past; the strategy should be

linked to the dependability requirements and justified by a re-assessment of the dependability risks [e)], assuming the strategy had been implemented; timescales and acceptance criteria for the required evidence, should be derived; dependability test strategy, covering the dependability functional testing provisions, should also be derived; specific requirements for the dependability plan; definition and development of the evidence framework to manage the evidence requirements.

n) Dependability plan – this responds to the dependability strategy by defining a schedule of specific dependability activities, e.g. system dependability modelling, FMEA, accelerated testing, in context with the appropriate dependability practices; evidence and justification for the task selection, clearly linked to risk control activities of the strategy; success criteria, including outputs and milestones; dependability management, monitoring and control activities and review schedules; links with the evidence framework.

o) Manage dependability – to complete the loop, evidence of dependability management, including status of the plan, should feed into l).

Annex E (informative) Dependability case evidence framework

The dependability evidence framework is a matrix comprising the dependability requirements, the dependability risks associated with achieving and satisfactorily delivering the requirements, and one or more programmes of activities to mitigate such risk and enable the requirements to be delivered. As with the risk register the dependability evidence framework is a living document which needs to be maintained throughout the acquisition cycle to enable assurance and confidence to be developed in the solution and presented through the population of the dependability case.

The dependability plan should comprise a number of discrete activities that, when integrated together, are employed to add value to the project and mitigate these risks. For each activity; the plan requires:

a) the aim of the activity;

b) the pass and fail criteria for that activity;

c) the method by which success will be measured;

d) the fall back activity in the event of failure.

Together these criteria form part of the evidence framework and in due course populate the dependability case.

In these early stages of the project such plans are generic recognizing the requirement for development and growth, and later that of prove and demonstrating compliance. Potential suppliers are required to specify exactly how they intend to mitigate the perceived risks accompanied by detailed proposals to provide just such evidence. Where resources are limited alternative strategies are required, hence the importance of addressing these at the earliest opportunity and recognizing that one dependability strategy might not fit all.

The dependability case evidence framework is defined in Clause **4**. Suitable column headings and contents are described as follows:

Column No.	Heading	Contents
1	Life cycle phase	Relevant phase in the product life cycle
2	Risk ref.	Relative to the project risk register
3	Risk description	Relative to the project risk register
4	Risk cause	A description of the underlying cause of the risk
5	Initial risk score	This is the dependability risk score which, in the examples, is assumed to be on a scale of 0 to 1, for increasing risk
6	Evidence required	Evidence needed to mitigate the risk (information, not deliverable reports)
7	Dependability practice	Process required to generate the necessary evidence (usually a combination of traditional dependability and other activities, i.e. not necessarily an individual dependability activity or technique)
Acceptance criteria		
8	Evidence	Deliverable document/contents
9	Target risk score	Acceptable risk score
10	Time Due	Time the evidence is due
Acceptance status		
11	Evidence	References to the latest evidence, including Issue no., and date delivered
12	Approval	Signature of approving authority and date of acceptance

Two example dependability case evidence frameworks are illustrated in Figure E.1 and Figure E.2. Each covers a selection of risks at various stages in the system life cycle, assuming the system involves substantial development activity. However, the examples are not intended to cover all the dependability risks with the system, and should not be used as a template. When creating an evidence framework, the system should be considered in its own right. The risk scores are arbitrary and, in practice, should be used to prioritize the dependability activities.

Figure E.1 **Evidence framework for system "X"**

Evidence framework for system "X"						Issue:	Date:		Signature:	
Project phase	**Risk ref.**	**Risk description and initial risk score**	**Risk cause**	**Evidence required**	**Dependability practice**	**Acceptance criteria**			**Acceptance status**	
						Evidence	**Target risk score**	**Time due**	**Evidence reference:** **issue no.:** **Date delivered:**	**Approval signature and date:**
Tender (for design and development)	RM 003	There is a risk that the system will fail to achieve its specified reliability: 99.9% over a 24 hour duty cycle. Initial score = 0.25	Intrinsic reliability of solution components not assessed/ understood	Part failure rates	Parts count prediction using in-service experience of similar parts, defaulting to industry standard data sources, e.g. generic failure rate data if no other data available.			2 weeks prior to preliminary design review, update prior to critical design review.		
			Failure modes and criticality of solution(s) not assessed/ understood.	Critical failure modes and failure rates for single and double faults.	FMECA: this information will be provided by the design FMECA, conducted as design practice (OP Procedure 21).					
					Development tests and DRACAS: a) to support previous assumptions on failure modes and failure rates; b) to trigger further development and testing of unsatisfactory items and, c) to initiate selection of alternative parts.					
			Reliability of solution system not assessed/ understood.	System reliability over 24 hour duty cycle.	System reliability RBD modelling and analysis for 24 hour duty cycle, based on 1 to 3.					
			Solution does not perform as predicted in use.	Operational and maintenance demonstration of ARM.	Monitoring and reporting of operational and maintenance defects through defect reporting via analysis of DRACAS database.	Draft operational and maintenance demonstration plan (OMDP) including acceptance criteria with regard to the 24 hour duty cycle requirement. OMDP report showing compliance with the requirement.		2 weeks prior to final design review 1 year after entry into use.		

Figure E.1 **Evidence framework for system "X"** *(continued)*

Evidence framework for system "X"						Issue:	Date:		Signature:	
Project phase	**Risk ref.**	**Risk description and initial risk score**	**Risk cause**	**Evidence required**	**Dependability practice**	**Acceptance criteria**			**Acceptance status**	
						Evidence	**Target risk score**	**Time due**	**Evidence reference:** **issue no.:** **Date delivered:**	**Approval signature and date:**
Tender (for design and development) (cont)	RM 022	There is a risk that the system BIT requirements will not be achieved. Initial score = 0.3	No clear approach by the purchaser to testability.	Testability design strategy.	1) Review BIT design strategy in the light of the functional hierarchy developed in the FMECA (see RM 001).	Internal document providing results of the review and showing that the testability design strategy is consistent with the functional hierarchy and the BIT requirements for: Start-up Continuous checks Diagnostics Location.	0.2	6 weeks prior to critical design review.		
			Testability requirements not verified.	Testability evaluation.	Extension of the FMECA to provide an evaluation of BIT coverage.	BIT evaluation report showing that the system testability is consistent with BIT requirements for: Start-up Continuous checks Diagnostics Location.	0.1	6 weeks prior to final design review.		
	RM 023	There is a risk that the integration of latest sat-nav and communications equipment into the design will compromise the dependability performance of the complete system. Initial score = 0.3	System integration fails to address wild heat and maintainer access.	Technology demonstration programme (TDP) to include dependability assessments.	Dependability predictions conducted to support the TDP.	TDP dependability prediction report.	0.1	6 weeks prior to critical design review.		

Figure E.1 **Evidence framework for system "X"** *(continued)*

Evidence framework for system "X"						Issue:	Date:		Signature:	
Project phase	**Risk ref.**	**Risk description and initial risk score**	**Risk cause**	**Evidence required**	**Dependability practice**	**Acceptance criteria**			**Acceptance status**	
						Evidence	**Target risk score**	**Time due**	**Evidence reference:** **issue no.:** **Date delivered:**	**Approval signature and date:**
Design and development.	RM 032	There is a risk that sub system X will require unscheduled replacement Initial score = .35	Wear out mechanisms not fully understood.	Evaluation of expected life and determination of any changes necessary to achieve the requirement.	Review of life data on similar items and environmental evaluation /stress calculations, to determine ageing factors and critical components.	Stress calculations, justification of (any) necessary design changes and accelerated life test plan.	0.2	3 months after contract award.		
					Accelerated life testing using the highly accelerated life test methodology.	Accelerated life test report providing assurance for the final design.	<0.15	6 months after receipt of test model(s).		
Manufacture	RM 044	There is a risk that the chassis will suffer from stress/fatigue during system assembly. Initial score = 0.28	Assembly activities include loading that is very different from when system is complete.	Analysis of loads on the chassis when suspended; determination of changes to the chassis design and/or the manufacturing fixture(s) to ensure that the expected life of the chassis is not compromised. Demonstration of manufacture.	Evaluation of the load case.	Report, including analysis and calculation records, showing stress margins. The report will highlight (any) areas of potential overstress and justify changes, if needed, to ensure adequate margins.	0.2	3 months prior to completion of demonstration phase.		
					Production reliability acceptance test.	PRAT test plan. PRAT test results assuring the integrity of the chassis for manufacture.	<0.1	PRAT plan required before start of production. PRAT test results following completion of PRAT.		
					Final quality inspection of deliverables.	Quality inspection records.	<0.1	During production.		

Figure E.2 **Evidence framework for system "Y"**

Evidence framework for system "Y"						Issue:	Date:		Signature:	
Project phase	**Risk ref.**	**Risk description and initial risk score**	**Risk cause**	**Evidence required**	**Dependability practice**	**Acceptance criteria**			**Acceptance status**	
						Evidence	**Target risk score**	**Time due**	**Evidence reference:** **Issue no.:** **Date delivered:**	**Approval signature and date:**
Concept and definition	RM 001	Inadequate/ incorrect definition of dependability requirements by purchaser. Initial risk score = 0.4	Dependability aspects not addressed within systems engineering, therefore impact of dependability on capability not fully understood. Dependability requirements are not SMART.	Critical dependability system attributes. Operational availability targets. Adequate system numbers. Initial dependability targets linked to operational availability. Assessment of the impact of dependability on operational effectiveness.	Capability gap analysis. Operational analysis. Needs and numbers studies (with dependability input). Availability modelling.	Operation availability targets within the sustainability section of the requirements document. First cut dependability targets for insertion into the requirement document.	0.1	Early in the concept phase, prior to initial business case submission.		
	RM 002	Failure of the purchaser to allocate sufficient resources to achieve requirements. Initial risk score = 0.7	Purchaser fails to realize the link between dependability and cost of ownership.	Assessment of the impact of dependability on funding.	Dependability input into BOI and WLC modelling.	Realistic estimates of funding and equipment numbers by ensuring availability and reliability are included in these early studies as cost drivers.	0.2	Early in the concept phase, prior to initial business case submission.		
			The purchaser fails to consider the impact of the requirements on the need for complex or novel technology.	Assessment of the technology risks.	Feasibility studies examining the maturity of the technology likely to be used in the solution options.	Reports showing pull through from research. Formulation of technology demonstrator programmes. Input from industry through partnering.	0.2			

Figure E.2 **Evidence framework for system "Y"** *(continued)*

Evidence framework for system "Y"						Issue:	Date:		Signature:	
Project phase	**Risk ref.**	**Risk description and initial risk score**	**Risk cause**	**Evidence required**	**Dependability practice**	**Acceptance criteria**			**Acceptance status**	
						Evidence	**Target risk score**	**Time due**	**Evidence reference:** **Issue no.:** **Date delivered:**	**Approval signature and date:**
Concept and definition (cont)			Purchaser fails to understand the key timescale risks.	Assessment of the time-scale risks.	Comparison with similar, related or historical projects.	Analyses to show the time-scales have been planned in accordance with the technology and technical risks.	0.2			
			Purchaser fails to outline the strategy for dependability assurance.	Suitable dependability strategy.	An agreed dependability strategy.	A draft dependability strategy paper outlining the elements work and the strategy to mitigate the key risks. Statements of work for dependability assessment phase studies in initial business case. Draft ITEAP to outline acceptance criteria.	0.2			
Tender (for design and development)	RM 003	Failure of the purchaser to communicate the dependability requirements to the supplier. Initial score = 0.4	Dependability supporting evidence is developed in an ad-hoc manner.	Reliability predictions based on similar equipment failure rates, and any factors applied due to differences in duty cycle, usage, complexity, etc. Details of operational and maintenance analysis and operational availability studies.	Initial dependability case report issued to supplier providing an audit trail of how the dependability requirement was derived. Discussions between customer and supplier.	Clear dependability requirements with the requisite audit trail set out at the start of the dependability case. Initial dependability risk register.	0.1	Early in the assessment phase, prior to final business case submission.		

Figure E.2 **Evidence framework for system "Y"** *(continued)*

Evidence framework for system "Y"						Issue:	Date:		Signature:	
Project phase	**Risk ref.**	**Risk description and initial risk score**	**Risk cause**	**Evidence required**	**Dependability practice**	**Acceptance criteria**			**Acceptance status**	
						Evidence	**Target risk score**	**Time due**	**Evidence reference:** **Issue no.:** **Date delivered:**	**Approval signature and date:**
Tender (for design and development) (cont)	RM 004	Failure of the purchaser to select the optimum solution. Initial score = 0.5	Selection mechanism fails to rigorously address dependability.	Reliability estimates of concept options.	Assessment studies allowing dependability estimates to be input along with other attributes into a structured concept down selection system.	Concept down selection reports showing evidence that the dependability has been factored into the selection process.	0.1	In the assessment phase, prior to final business case submission.		
				An adequate tender/bid dependability assessment method with sufficient weighting on dependability.	Draft dependability assessment questions for ITT marking scheme, ensuring dependability is given equal weighting to performance, time and cost.	Final scores from the bid assessment, plus key dependability risks and dependability achievement milestones necessary to contract for the production of dependability evidence within the dependability case.	0.1	In the assessment phase, prior to final business case submission.		
				Assessment of the technological risks associated with each option.	Assessment of likely software complexity through measurements of the size and complexity of the software.	Concept down selection reports include assessment of software dependability through life.				
					Project dependability design guidelines and define how these guidelines are to be contracted against.	Obtain stakeholder acceptance for the project dependability design guidelines.				
Design and development	RM 005	Failure of the supplier to understand the requirements. Initial score = 0.6	Supplier fails to formally assess the impact of the environmental constraints on dependability.	Analysis of duty cycle, loads, temperature levels, vibration levels. Analysis of damage accumulation effects, dust, dirt ingress, moisture, etc.	Analysis of the operational environment, and mission and peacetime operation.	Supplier's dependability case report showing the environmental factors and duty cycle loads have been understood and will influence the design.	0.1	Provided with the tender or early in the demonstration phase.		

Figure E.2 **Evidence framework for system "Y"** *(continued)*

Evidence framework for system "Y"						Issue:	Date:		Signature:	
Project phase	**Risk ref.**	**Risk description and initial risk score**	**Risk cause**	**Evidence required**	**Dependability practice**	**Acceptance criteria**			**Acceptance status**	
						Evidence	**Target risk score**	**Time due**	**Evidence reference:** **Issue no.:** **Date delivered:**	**Approval signature and date:**
Design and development (cont)	RM 006	Failure of the supplier to recognize all of the dependability risks. Initial score = 0.5	Supplier fails to involve dependability staff within formal risk identification.	Identification of all dependability risks.	Analysis of the strength of design of critical components against duty cycle loads. Predictions and modelling to identify critical systems. Analysis of interface and integration issues.	Comprehensive risk matrix supported by dependability case reports showing: Modelling using the measured inputs (loads), to ensure that the strength of design of mission critical sub-systems and components is adequate to meet the needs of the mission, and have the durability to continue to function for the design life of the equipment. A structured analysis of potential failure modes to ensure that all interface and integration issues are addressed and are not overlooked as causes of unreliability. Reliability modelling, predictions and allocations to determine criticality.	<0.15	Early in the design process to influence the design of prototype equipments.		
	RM 007	OTS components fail to perform as expected. Initial score = 0.5	Unsuitable OTS components used within the design.	Dependability predictions supported by in-service data for OTS sub systems.	Assessment studies where dependability estimates for OTS sub systems consider existing data and the impact of differences between the new application and that of applicable to the source data.	Concept down selection reports include realistic predictions for OTS sub systems dependability performance.	0.15	Provided with the tender or early in the demonstration phase.		

Figure E.2 **Evidence framework for system "Y"** *(continued)*

Evidence framework for system "Y"						Issue:	Date:		Signature:	
Project phase	**Risk ref.**	**Risk description and initial risk score**	**Risk cause**	**Evidence required**	**Dependability practice**	**Acceptance criteria**			**Acceptance status**	
						Evidence	**Target risk score**	**Time due**	**Evidence reference:** **Issue no.:** **Date delivered:**	**Approval signature and date:**
Design and development (cont)	RM 008	Platform condition and usage unknown. Initial score = 0.4	Design fails to make use of automated usage and fault reporting.	HUMS to be implemented effectively and efficiently as part of the design process	HUMS to be an integral part of the design process.	Maintainability analysis report identifying functions covered by HUMS.	0.1	Provided with the tender or early in the demonstration phase.		
	RM 009	Failure of the supplier to produce an adequate plan to mitigate the dependability risks. Initial score = 0.7	Supplier expects that dependability issues will be addressed by the purchaser in service.	Production of a suitable dependability plan.	Identification of the dependability risks and the planned dependability activities to mitigate those risks, along with the technical capability, resources and controls/success criteria to ensure it will happen.	Clear dependability management and organizational structure. Systematic programme of activities for satisfying the dependability requirements set against the identified dependability risks. Dependability activities with clear objectives and success criteria. Planned dependability activities in time to influence design. Dependability target allocations to subcontractors. Subcontractors' dependability plans and case. A clear test and evaluation programme. Planned dependability milestones for dependability achievement with periodic reviews.	0.1	During proposals for ITT and during early development/ demonstration phases.		

Figure E.2 **Evidence framework for system "Y"** *(continued)*

Evidence framework for system "Y"						Issue:	Date:		Signature:	
Project phase	**Risk ref.**	**Risk description and initial risk score**	**Risk cause**	**Evidence required**	**Dependability practice**	**Acceptance criteria**			**Acceptance status**	
						Evidence	**Target risk score**	**Time due**	**Evidence reference:** **Issue no.:** **Date delivered:**	**Approval signature and date:**
Design and development (cont)	RM 010	Failure of the supplier to produce sufficient evidence to demonstrate dependability requirements have been met to the satisfaction of the purchaser. Initial score = 0.6	Test and evaluation criteria not formally agreed between the supplier and the purchaser.	Sufficient design and test and evaluation data to provide and engineering and statistical confidence that the pre-production prototype design has met the dependability requirements.	Execute, monitor and review dependability plan activities, amending where appropriate.	Suppliers dependability case reports showing: Design changes resulting from the outputs of design studies (stress analysis, FMECAs, etc.). Detailed and effective DRACAS. Component test results. Sub-system test results. Test rig results. Reliability growth test results. Reliability demonstration trials. Operational and maintenance trial results. Performance trial results. Information on design review action. Field data from other users.	0.1	During demonstration prior to system acceptance and manufacture.		
	RM 011	Reliability of OTS software packages is poor when integrated into the system. Initial score = 0.7	Supplier fails to develop OTS interfaces that are compatible with the system software architecture.	Integration testing within the software integration laboratory (SIL) includes test analyse fix process reported by formal DRACAS.	DRACAS report from the SIL testing and development activities.	DRACAS report shows evidence of: Design modifications leading to satisfactory reliability growth Input to dependability prediction reports to cover likely software failure rates and PM cycles.	0.15	During demonstration prior to system acceptance and manufacture.		

Figure E.2 **Evidence framework for system "Y"** *(continued)*

Evidence framework for system "Y"						Issue:	Date:		Signature:	
Project phase	**Risk ref.**	**Risk description and initial risk score**	**Risk cause**	**Evidence required**	**Dependability practice**	**Acceptance criteria**			**Acceptance status**	
						Evidence	**Target risk score**	**Time due**	**Evidence reference:** **Issue no.:** **Date delivered:**	**Approval signature and date:**
Manufacture	RM 012	Failure of the supplier to identify and manage the dependability risks associated with the transition from development to production. Initial Score = 0.5	Supplier under-estimates the scale of change between prototype and production system.	Evidence that lessons learned from pre-production prototype builds have influenced the production process. Sufficient test and evaluation data to provide and engineering and statistical confidence that the production build standard will meet the dependability requirements and show the reliability has not been degraded by the production process.	Mature production and quality processes along side pre-production prototype design. Procedures for the investigation and rectification of faults, failures and defects.	Suppliers dependability case reports showing- Production confirmatory/ qualification trials results. Production reliability acceptance testing (PRAT) first batch results Evidence of changes in production and quality procedures to capture defects.	0.1	Preceding and during first off production phase.		
	RM 013	Failures of the supplier to monitor the production run. Initial score = 0.4	Immature production facility and processes.	Demonstration of consistent quality of manufacture. (PRAT test plan). Evidence of the implementation of effective quality procedures.	Production reliability acceptance test. Final quality inspection of deliverables.	PRAT batch test results. Quality inspection records.	<0.1	At agreed points during manufacturing period.		

Figure E.2 **Evidence framework for system "Y"** *(continued)*

Evidence framework for system "Y"						Issue:	Date:		Signature:	
Project phase	**Risk ref.**	**Risk description and initial risk score**	**Risk cause**	**Evidence required**	**Dependability practice**	**Acceptance criteria**			**Acceptance status**	
						Evidence	**Target risk score**	**Time due**	**Evidence reference:** Issue no.: Date delivered:	**Approval signature and date:**
Manufacture (cont)	RM 014	OTS components fail to perform as expected. Initial score = 0.5	Assembly information for OTS equipment is unsuitable for application.	Demonstration of consistent quality of assembly/ integration of OTS components through PRAT test plan. Evidence of the implementation of effective quality procedures for assembly and integration.	Production reliability acceptance test. Final quality inspection of deliverables	PRAT batch test results. Quality inspection records.	0.1	At agreed points during manufacturing period.		
Operation and maintenance	RM 015	Failure of the purchaser to monitor and mitigate dependability risks that result from change in use, environment and support. Initial score = 0.5	Contract does not fully address system support.	Equipment usage and failure data along with the appropriate analysis to provide reliability estimates and failure trends. Data on repair costs and resources.	Identification of systematic failure modes and the introduction of modifications through PDS.	Operational and maintenance demonstration (OMD) trial results. OMD dependability study results. OMD data collection and analysis.		At the start and through out in-service period.		

Figure E.2 **Evidence framework for system "Y"** *(continued)*

Evidence framework for system "Y"						**Issue:**	**Date:**		**Signature:**	
Project phase	**Risk ref.**	**Risk description and initial risk score**	**Risk cause**	**Evidence required**	**Dependability practice**	**Acceptance criteria**			**Acceptance status**	
						Evidence	**Target risk score**	**Time due**	**Evidence reference:** **Issue no.:** **Date delivered:**	**Approval signature and date:**
Operation and maintenance/ disposal	RM 016	Failure of the purchaser to capture record and disseminate the dependability lessons learnt. Initial score = 0.9	System ownership and reporting responsibilities are not defined by the purchaser.	Full dossier of all elements of dependability work from concept through to in-service or disposal.	Collation of all requirements documents, dependability data and reports into a corporate data repository. Production of a final LFE report providing insight into effectiveness of the programme and the final dependability estimates achieved.	Early studies results. Mature dependability requirements. Extracts from TLMP. Outputs from dependability meetings (dependability plan, etc.). ITEAP and acceptance reports. Fully populated dependability case with all dependability evidence reports (including operational and maintenance usage). Analysis of lessons learned.	0.2	Ongoing through to in-service and disposal.		

Bibliography

Standards publications

For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

BS EN 60300-1, *Dependability management – Dependability management systems*

BS EN 61508-3:2002, *Functional safety of electrical/electronic/ programmable electronic safety-related systems – Part 2: Software requirements*

BS EN ISO 9000:2005, *Quality management systems – Fundamentals and vocabulary*

BS CECC 00804:1996, *Harmonized system of quality assessment for electronic components – Interpretation of 'EN ISO 9000:1994' – Reliability aspects for electronic components*

Other publications

[1] Defence Standard 00-42 Part 3, *Reliability and Maintainability (R&M) Assurance Guide. Part 3: R&M Case.*

This page deliberately left blank

British Standards Institution (BSI)

BSI is the independent national body responsible for preparing British Standards and other standards-related publications, information and services.
It presents the UK view on standards in Europe and at the international level.

It is incorporated by Royal Charter.

Revisions

British Standards are updated by amendment or revision. Users of British Standards should make sure that they possess the latest amendments or editions.

It is the constant aim of BSI to improve the quality of our products and services. We would be grateful if anyone finding an inaccuracy or ambiguity while using this British Standard would inform the Secretary of the technical committee responsible, the identity of which can be found on the inside front cover.

Tel: +44 (0)20 8996 9001 Fax: +44 (0)20 8996 7001

BSI offers Members an individual updating service called PLUS which ensures that subscribers automatically receive the latest editions of standards.

Tel: +44 (0)20 8996 7669 Fax: +44 (0)20 8996 7001
Email: plus@bsigroup.com

Buying standards

You may buy PDF and hard copy versions of standards directly using a credit card from the BSI Shop on the website **www.bsigroup.com/shop.** In addition all orders for BSI, international and foreign standards publications can be addressed to BSI Customer Services.

Tel: +44 (0)20 8996 9001 Fax: +44 (0)20 8996 7001
Email: orders@bsigroup.com

In response to orders for international standards, it is BSI policy to supply the BSI implementation of those that have been published as British Standards, unless otherwise requested.

Information on standards

BSI provides a wide range of information on national, European and international standards through its Knowledge Centre.

Tel: +44 (0)20 8996 7004 Fax: +44 (0)20 8996 7005
Email: knowledgecentre@bsigroup.com

Various BSI electronic information services are also available which give details on all its products and services.

Tel: +44 (0)20 8996 7111 Fax: +44 (0)20 8996 7048
Email: info@bsigroup.com

BSI Subscribing Members are kept up to date with standards developments and receive substantial discounts on the purchase price of standards. For details of these and other benefits contact Membership Administration.

Tel: +44 (0)20 8996 7002 Fax: +44 (0)20 8996 7001
Email: membership@bsigroup.com

Information regarding online access to British Standards via British Standards Online can be found at **www.bsigroup.com/BSOL**

Further information about BSI is available on the BSI website at **www.bsigroup.com/standards**

Copyright

Tel: +44 (0)20 8996 7070
Email: copyright@bsigroup.com

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Tel +44 (0)20 8996 9001
Fax +44 (0)20 8996 7001
www.bsigroup.com/standards

raising standards worldwide™