

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

bsi.

...making excellence a habit.
AVA Documents™
Document Sharing Hub

Publishing and copyright information

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

© BSI 2010

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

Foreword *ii*

Introduction 1

- 1 Scope 2
- 2 Normative references 3
- 3 Terms and definitions 3
- 4 Purpose and description of the dependability case 4
- 5 Principles of the dependability case 5
- 6 Development of the dependability case 12
- 7 Providing the evidence 15
- 8 Presenting evidence 16
- 9 Assessing the adequacy of evidence 17

Annexes

- Annex A (informative) General requirements for the dependability case and dependability case report 21
 - Annex B (informative) Examples of dependability management risks at the different stages of a systems life cycle 24
 - Annex C (informative) Checklist of points for assessing the adequacy of evidence 25
 - Annex D (informative) Dependability risk reduction process 26
 - Annex E (informative) Dependability case evidence framework 28
- Bibliography 42

List of figures

- Figure 1 – The development of claims 6
- Figure 2 – The concept of the dependability case 7
- Figure 3 – Establishing and developing the evidence framework 8
- Figure 4 – The relationship between the dependability process, the overall delivery process and the evidence produced 9
- Figure 5 – Illustration of progressive assurance process 11
- Figure 6 – Example of change of balance of effort over system life cycle 13
- Figure 7 – Dependability risk reduction process 20
- Figure E.1 – Evidence framework for system “X” 30
- Figure E.2 – Evidence framework for system “Y” 33

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

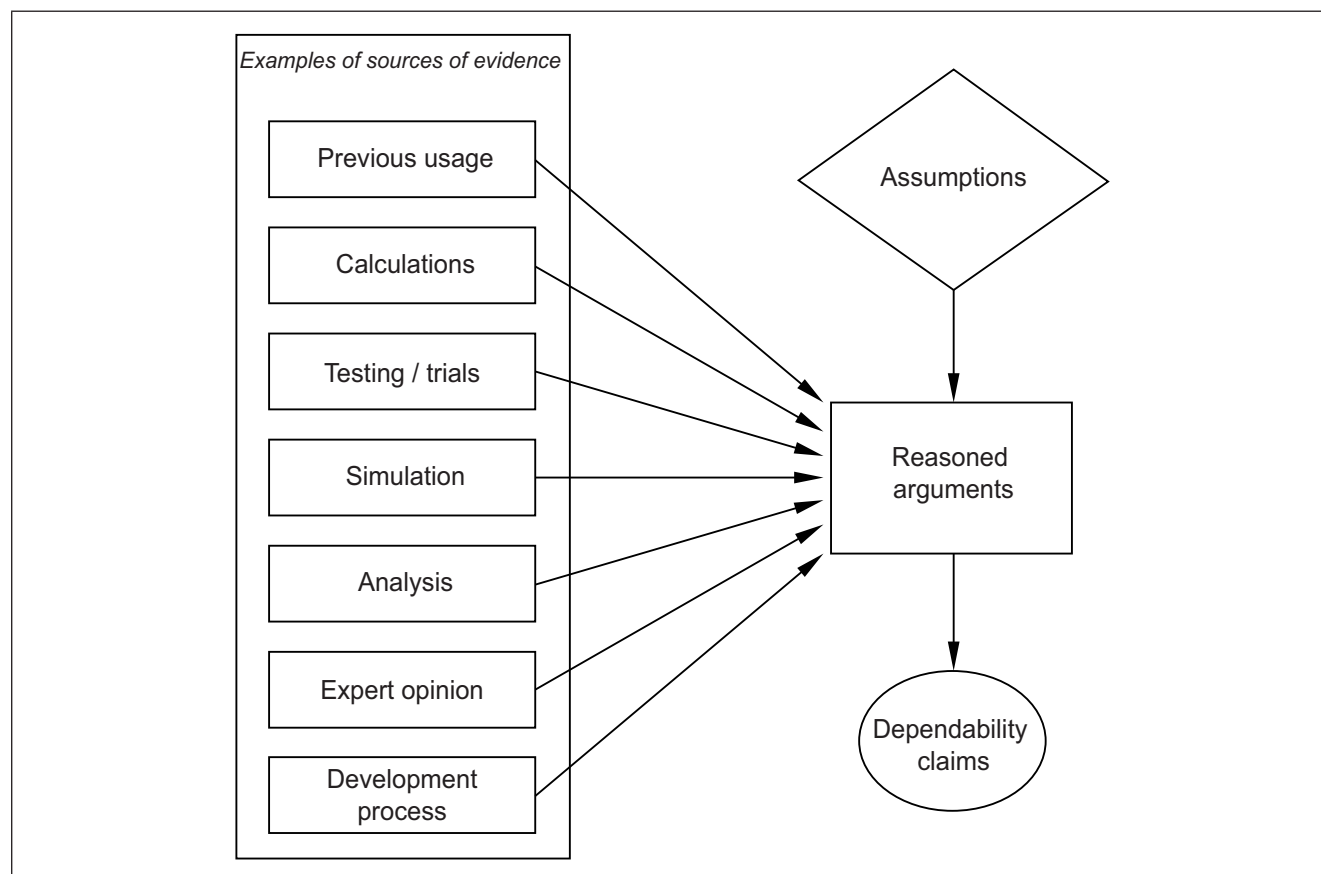


Figure 2 The concept of the dependability case

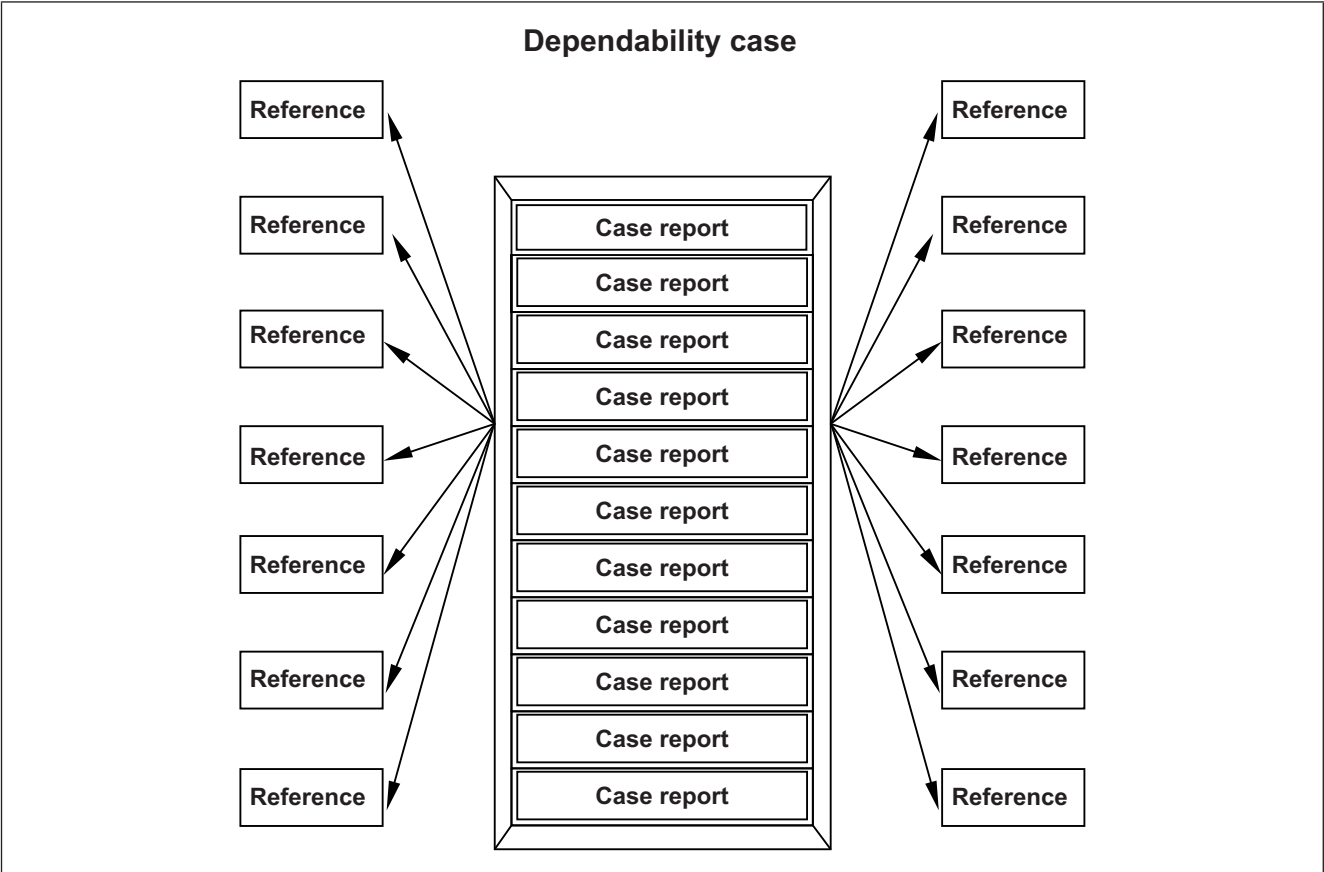


Figure 3 Establishing and developing the evidence framework

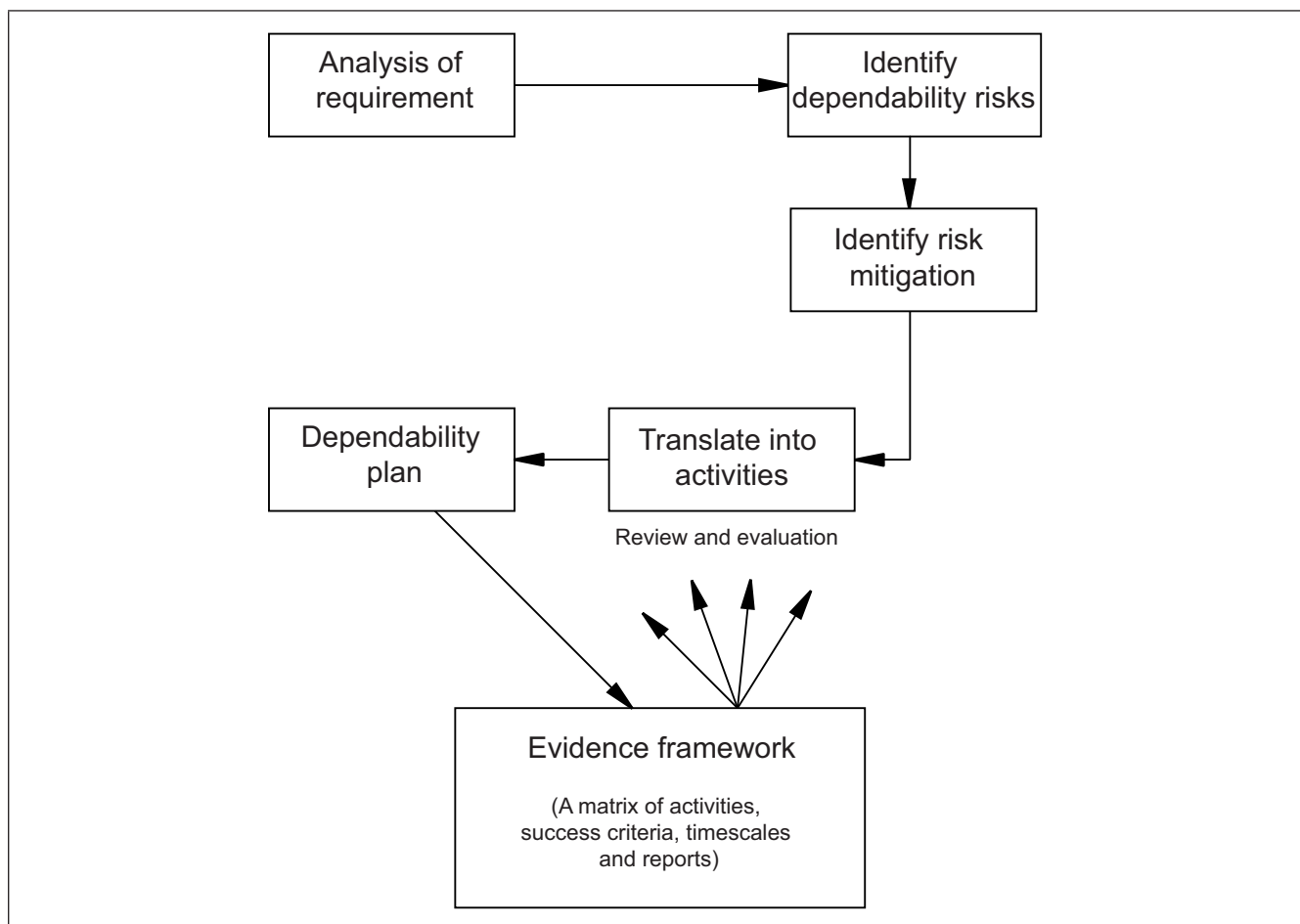
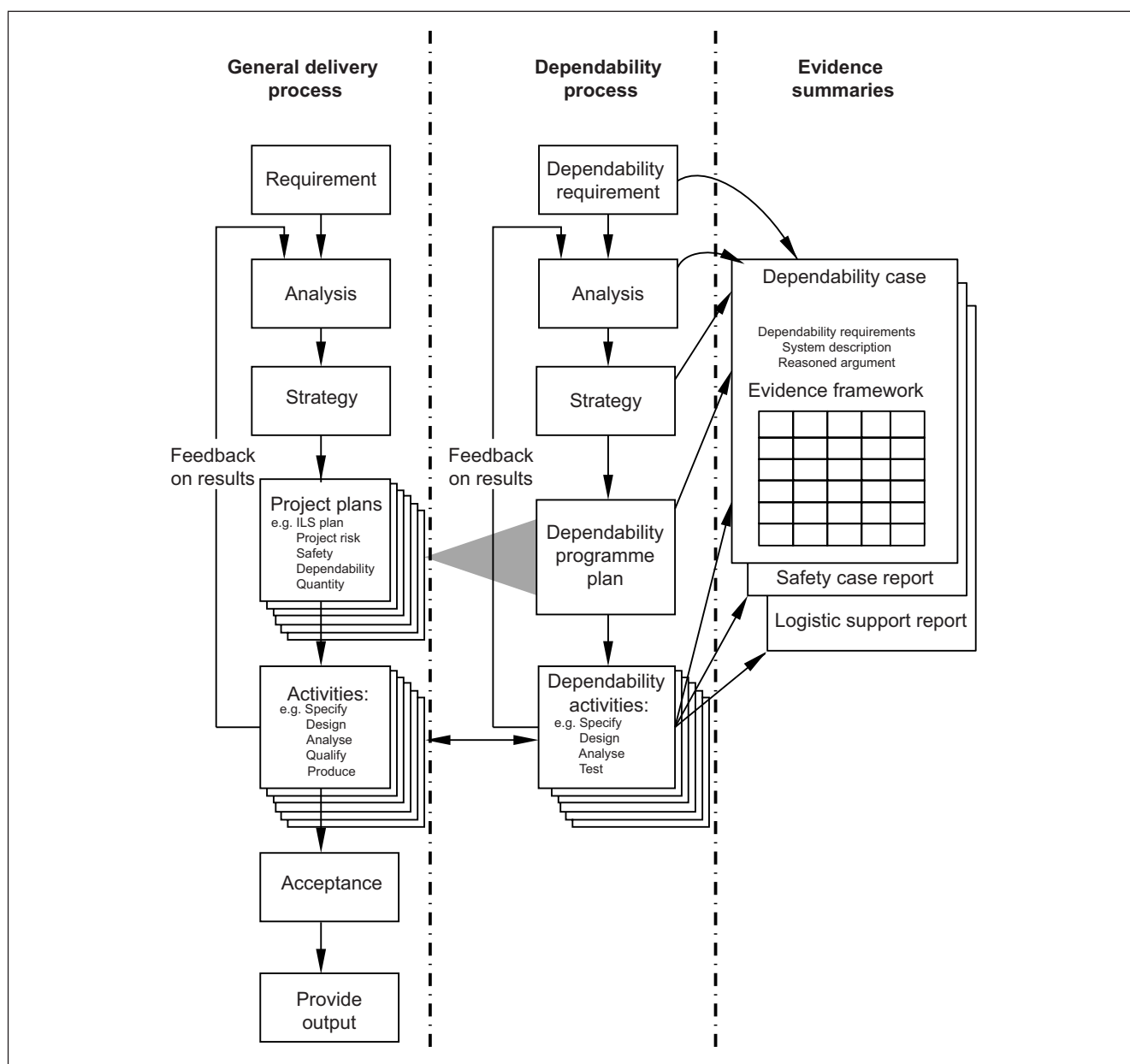


Figure 4 The relationship between the dependability process, the overall delivery process and the evidence produced



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

