BS EN 62741:2015

BSI Standards Publication

Demonstration of dependability requirements — The dependability case

bsi.

...making excellence a habit.™

National foreword

This British Standard is the UK implementation of EN 62741:2015. It is identical to IEC 62741:2015. It supersedes BS 5760-18:2010, which will be withdrawn on 24 March 2018.

The UK participation in its preparation was entrusted to Technical Committee DS/1, Dependability.

A list of organizations represented on this committee can be obtained on request to its secretary.

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

Published by BSI Standards Limited 2015

ISBN 978 0 580 80390 1
ICS 03.120.01; 21.020; 29.020

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

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 May 2015.

Amendments/corrigenda issued since publication

Date	Text affected

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 62741

March 2015

ICS 21.020; 03.120.01

English Version

Demonstration of dependability requirements - The dependability case (IEC 62741:2015)

Démonstration des exigences de sûreté de fonctionnement - Argumentaire dans le cadre de la sûreté de fonctionnement (IEC 62741:2015)

Leitfaden zur Darlegung von Zuverlässigkeitsanforderungen - Der Zuverlässigkeitsnachweis (IEC 62741:2015)

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Foreword

The text of document 56/1591/FDIS, future edition 1 of IEC 62741, prepared by IEC/TC 56 "Dependability" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN 62741:2015.

The following dates are fixed:

• latest date by which the document has to be implemented at national level by publication of an identical national standard or by endorsement	(dop)	2015-12-24
• latest date by which the national standards conflicting with the document have to be withdrawn	(dow)	2018-03-24

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC [and/or CEN] shall not be held responsible for identifying any or all such patent rights.

Endorsement notice

The text of the International Standard IEC 62741:2015 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following notes have to be added for the standards indicated:

IEC 60300-3-1	NOTE	Harmonized as EN 60300-3-1.
IEC 60300-3-4	NOTE	Harmonized as EN 60300-3-4.
IEC 61078	NOTE	Harmonized as EN 61078.
IEC 62347	NOTE	Harmonized as EN 62347.
IEC/ISO 31010	NOTE	Harmonized as EN 31010.
IEC 62198	NOTE	Harmonized as EN 62198.

Annex ZA
(normative)

Normative references to international publications with their corresponding European publications

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

NOTE 1 When an International Publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

NOTE 2 Up-to-date information on the latest versions of the European Standards listed in this annex is available here: www.cenelec.eu.

Publication	Year	Title	EN/HD	Year
IEC 60050-192	-	International electrotechnical vocabulary - Part 192: Dependability	-	-
IEC 60300-1	-	Dependability management -- Part 1: Guidance for management and application	EN 60300-1	-
ISO 31000	-	Risk management - Principles and guidelines	-	-

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

DEMONSTRATION OF DEPENDABILITY REQUIREMENTS – THE DEPENDABILITY CASE

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 62741 has been prepared by IEC technical committee 56: Dependability.

The text of this standard is based on the following documents:

FDIS	Report on voting
56/1591/FDIS	56/1609/RVD

Full information on the voting for the approval of this standard can be found in the report on voting indicated in the above table.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC website under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

INTRODUCTION

Dependability is the ability to perform as and when required. Acceptable levels of dependability are therefore essential for continued performance and optimized life cycle costs.

In order to achieve dependability of a system, dependability requirements should be established, the risks of not meeting them identified and a suitable set of activities developed to meet and demonstrate the requirements and manage the risks. A dependability case provides a convenient and convincing means of recording the output of these activities in a single location and presenting an argument, supported by evidence, that risks have been treated and that the necessary dependability has been or will be achieved and will continue to be achieved over time. It serves as the main means of communication on dependability among customers, suppliers and other stakeholders and promotes cooperation among them. This is essential for dependability achievement and providing assurance as part of the customer/supplier relationship.

Preparing a dependability case can also improve dependability through the actions taken to prepare and develop the argument within the dependability case. It can improve the cost effectiveness of a dependability programme because if an activity does not provide evidence to support the case, this may indicate that the activity is not necessary.

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.

Throughout this International Standard, the term "dependability" includes all aspects of reliability, availability, maintainability and supportability, as well as other attributes such as usability, testability and durability. In addition, dependability of a system includes all aspects of that system, including components, processes, hardware, software and the interfaces between them.

This standard is intended as guidance: the guidelines are not prescriptive in nature, they are generic, they should be tailored to the specific objectives and are not exhaustive.

This standard does not address safety or the environment.

DEMONSTRATION OF DEPENDABILITY REQUIREMENTS – THE DEPENDABILITY CASE

1 Scope

This International Standard gives guidance on the content and application of a dependability case and establishes general principles for the preparation of a dependability case.

This standard is written in a basic project context where a customer orders a system that meets dependability requirements from a supplier and then manages the system until its retirement. The methods provided in this standard may be modified and adapted to other situations as needed.

The dependability case is normally produced by the customer and supplier but can also be used and updated by other organizations. For example, certification bodies and regulators may examine the submitted case to support their decisions and users of the system may update/expand the case, particularly where they use the system for a different purpose.

2 Normative references

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

IEC 60050-192, *International Electrotechnical Vocabulary – Part 192: Dependability* [1]

IEC 60300-1, *Dependability management – Part 1: Guidance for management and application*

ISO 31000, *Risk management – Principles and guidelines*

3 Terms, definitions and abbreviations

For the purposes of this document, the terms and definitions given in IEC 60050-192, as well as the following, apply.

3.1 Terms and definitions

3.1.1
dependability case
evidence-based, reasoned, traceable argument created to support the contention that a defined system does and/or will satisfy the dependability requirements

3.1.2
evidence framework
structure identifying what evidence will be/has been produced and when

[1] To be published.

3.1.3
off-the-shelf
OTS
non-developmental item of supply that is both commercial and sold in substantial quantities in the commercial marketplace

Note 1 to entry: Sometimes referred to as COTS (commercial off-the-shelf) or MOTS (modified off-the-shelf).

3.1.4
customer
party which orders or specifies the item, including the dependability requirements

Note 1 to entry: This could be an organization, sponsor, department, company or an individual and can change through the life cycle.

3.1.5
subsystem
part of a system, which is itself a system

3.1.6
supplier
party which supplies the item, which meets its dependability requirement

Note 1 to entry: This could be an organization, department, company or an individual and can change through the life cycle.

3.1.7
system <in dependability>
defined set of items that collectively fulfil a requirement

Note 1 to entry: A system is considered to have a defined real or abstract boundary.

Note 2 to entry: External resources (from outside the system boundary) may be required for the system to operate.

Note 3 to entry: A system structure may be hierarchical, e.g. system, subsystem, component, etc.

Note 4 to entry: Conditions of use and maintenance should be expressed or implied within the requirement.

3.2 Abbreviations

COTS	Commercial off-the-shelf
FEM	Finite element modelling
FMECA	Failure mode, effects and criticality analysis
FTA	Fault tree analysis
MOTS	Modified off-the-shelf
OTS	Off-the-shelf

4 Background to the dependability case

4.1 Principles and purpose

A dependability case provides a reasoned and traceable argument based on evidence that a system satisfies the requirements and will continue to do so over time. It demonstrates why certain activities have been undertaken and how they can be judged to be successful. For maximum effectiveness it should be initiated at the concept stage, revised progressively during a system life cycle and is typically summarized in dependability case reports at predefined milestones. It records progress in obtaining evidence that dependability requirements are met and remains with the system throughout its life cycle until retirement.

The dependability case is of the greatest benefit for high value, low quantity systems where direct evidence of dependability may be difficult or expensive to obtain. Since these systems are often highly complex, involve novel technologies and have wide-ranging stakeholders, an explicit argument is necessary in order to demonstrate their detailed dependability claims with suitable evidence.

4.2 Relationship between the dependability case and dependability plans

Effective management of dependability requires organizational arrangements to implement policy, activities implemented in dependability programmes and plans and processes for performance evaluation, assurance and review.

A dependability programme involves

a) dependability plans, that define the activities, techniques and resources required to achieve dependability,

b) methods for measurement and assessment,

c) assurance and review.

The objectives of a dependability plan include ensuring that

1) the dependability requirements of the customer are determined and demonstrated to be understood by both the customer and supplier,

2) activities are planned, agreed and implemented to satisfy and demonstrate the requirements and treat the risks of failure,

3) the customer is provided with assurance that the dependability requirements are being, or will be, satisfied and that uncertainty in the dependability decreases over the course of the plan.

The dependability case provides progressive assurance that dependability requirements are being or will be satisfied and that uncertainty in the dependability is decreasing. In addition, the case demonstrates that the activities in the plan achieve the requirements and treat the risks. This forms part of the argument and evidence for why the system is, or will be, dependable. The plan is usually based on standards and the organization’s experience in managing dependability and is tailored, taking into account factors such as the relevant life cycle stages, the organization’s context, resources available and the risks that need to be managed.

The dependability plan and dependability case are often developed concurrently as both include consideration of the risks of not meeting the requirements. However, the system might meet the dependability requirements but it might not be possible to demonstrate that these requirements have been met. This might be because there is no appropriate activity which can demonstrate that the requirements have been met, or the cost or time required to do so might be excessive. Therefore the dependability plan may also include activities specifically intended to treat the risks of not being able to demonstrate that the requirements have been met and these activities also provide evidence in the dependability case.

A register of risks produced as part of a dependability case should be coordinated with the risks identified as part of planning the dependability programme and with the project risk register. Activities proposed to treat the risks are included in the dependability plan and examined as sources of evidence that risks have been treated. As the dependability plan is implemented, the dependability case is populated with evidence of the successful implementation of the plan. This provides progressive assurance that requirements are being met. If sufficient evidence is not able to be obtained, then the dependability plan should be modified accordingly.

In a well managed project, the dependability plan and dependability case are fully integrated with overall project management. In such a project, the use of the dependability case does not incur an increase in overall workload, since the cost of constructing the case is recouped by

the saving from avoided miscommunication, avoided reworking caused by late discovery of faults, avoided activities without demonstrable benefits and so forth.

In addition, preparing a dependability case assists the development of a cost-effective dependability plan because evidence sought in support of the argument in the dependability case can suggest activities which will improve the dependability plan. In addition, if an activity in the plan is not part of an argument in the dependability case, it should be reviewed to check that it performs a useful function in the plan. (Note that some activities in the dependability plan are included to support other disciplines such as safety which do not normally form part of the dependability case.)

The dependability plan and dependability case should be reviewed and updated in the event of significant changes to the following:

– customer requirements or expectations;
– environment or interfacing systems;
– conditions of use or design intent;
– design;
– actual performance.

4.3 Progressive assurance of dependability

The dependability case provides an expanding body of evidence which aims to progressively decrease the uncertainty around the achievement of the dependability requirements. However, it is the norm rather than the exception that requirements, environments, etc. change during the system life cycle. Therefore uncertainty might not always decrease. There might be occasions, for example, when a different design option renders a proportion of the evidence obsolete, leading to increased uncertainty. There might also be periods when no evidence is provided, for example during testing prior to the release of test results, when uncertainty remains unchanged. In addition, if new evidence conflicts with the existing evidence, this might increase uncertainty.

Figure 1 illustrates two types of product development: new development and MOTS. The vertical axis represents the level of uncertainty identified at any point in the project. As the quantity of dependability evidence increases, the uncertainty generally reduces and progressive assurance is obtained.

The horizontal axis represents the time into the project, from the start of the concept stage "a", through start of development "b", to the end of the realization stage "c", end of utilization “d”, and "e", possible enhancement, and beyond.

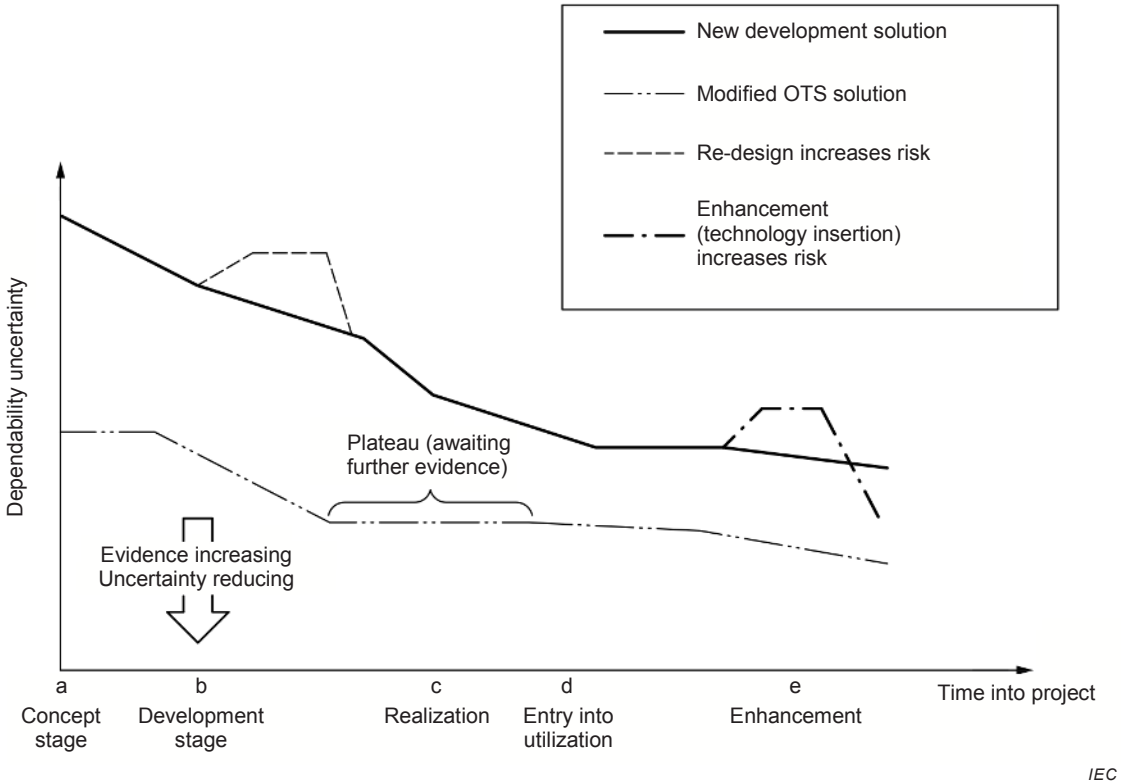

Figure 1 – Illustration of progressive assurance process

At time "a" (start of concept stage) the level of uncertainty is relatively high, but this uncertainty decreases as the project progresses. At time "c", namely at the transition from the realization stage to the utilization stage, the body of evidence is sufficient to assure the dependability to the degree that warrants this transition. The body of evidence (assurance) should continue to build in utilization as successful trials and usage are recorded and the remaining risks can be seen to reduce still further.

Having gone through its own new development period, a MOTS solution is often considered less uncertain than new development as in Figure 1, provided all other things are equal. This is not the case for an OTS solution in new applications or in a new environment and a careful re-assessment is required.

Finally, many changes to uncertainty will be step-changes rather than progressive changes.

5 Principles of the dependability case

5.1 Description of the dependability case

The dependability case starts with an initial statement of dependability requirements. These requirements might include customer's and supplier's internal goals, market strategies, regulatory requirements, etc. as well as requirements explicitly stated by the customer.

The dependability case then makes a top level claim explicitly stating the contention that the system meets the requirements (see 5.2). The dependability case then provides a multi-level structure of claims, sub-claims and connecting sub-arguments that are ultimately based on evidence (see 5.3) and assumptions.

The evidence is presented in the evidence framework (see 5.4) and summarized and referenced in the argument in the dependability case report (see 5.5).

5.2 Making claims in the dependability case

The dependability case uses evidence in order to create an argument for the claims that the dependability requirements have been or will be met.

Figure 2 illustrates the process of building and arguing the claims in the dependability case using the evidence sources.

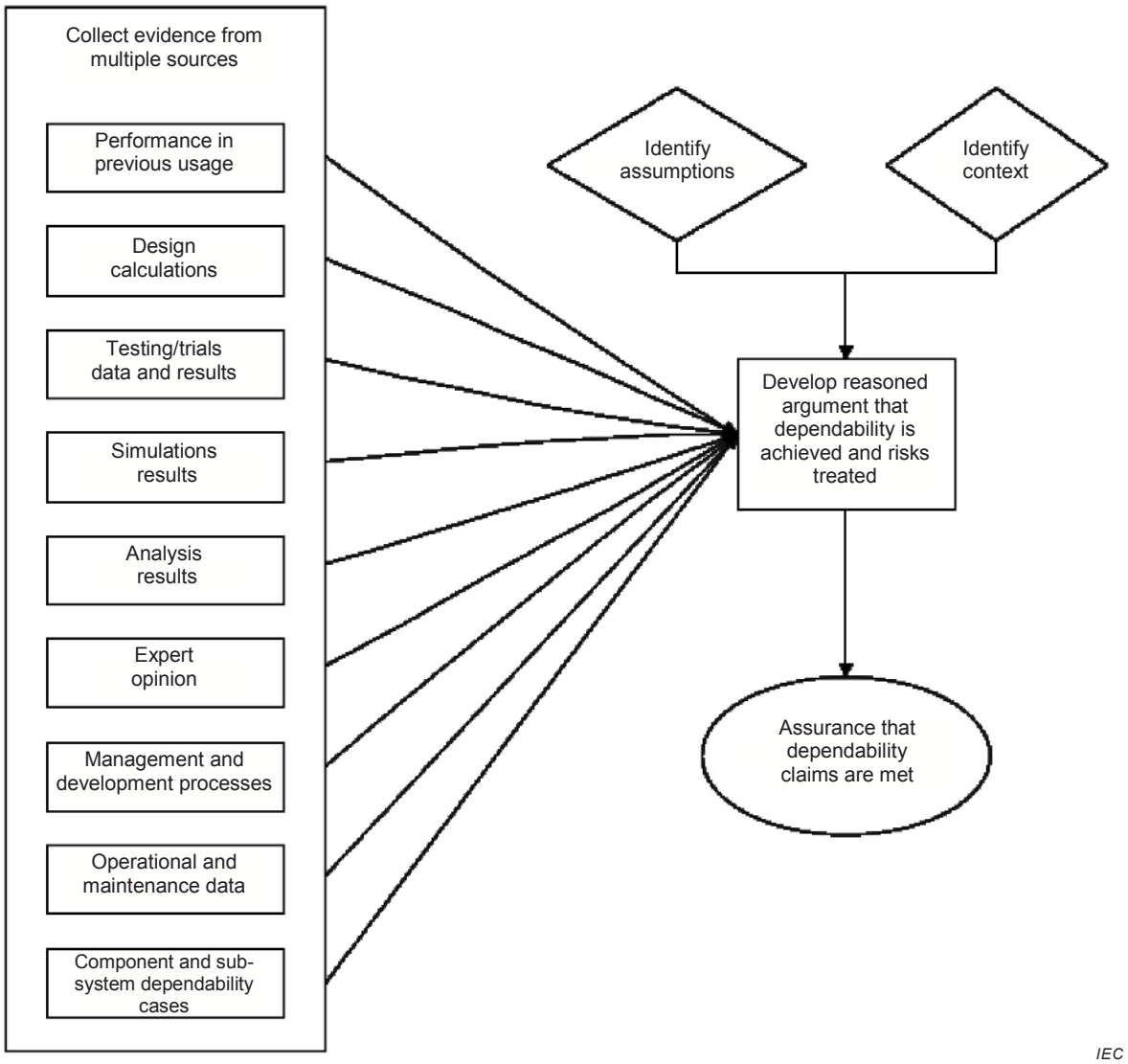

Figure 2 – The development of claims

Any assumptions necessary to make the argument should be identified and explicitly stated, along with the activities planned to validate them. These might include assumptions regarding the conditions of use, the environment in which the system is used or the nature and type of maintenance.

Arguments can fall into one of two categories:

a) arguments that all identified risks to the claim are eliminated or sufficiently treated, supported by evidence of successful treatments and by evidence that risk identification is comprehensive;

b) arguments that there are sufficient grounds for the claim, supported by evidence of truth of each and by evidence of adequacy.

The former requires that consideration is given to all significant sources of risks, areas of impacts, events (including changes in circumstances) and their causes and their potential consequences. The latter requires that the aspects covered by the evidence are sufficient to provide assurance of the claim.

It is also necessary to identify the context and background for which the argument is made as this identifies the limitations of the dependability case. The context includes the stakeholders who might be interested in the system, the objectives and performance requirements, the system being considered and any proposed limitations on the system's use.

Should any of the assumptions or context change, then the argument and claims in the dependability case will need to be reviewed.

During the implementation of the dependability plan, the key assumptions should be validated, where possible, effectively replacing each with substantiated evidence. Similarly, the contexts in which the argument is made should be validated to match the actual or intended application of the system and the dependability case.

From these sources of evidence and explicitly stated assumptions, a reasoned argument demonstrates how the dependability claims are substantiated. Documents and data relating to all of these make up the dependability case.

5.3 Using evidence in the dependability case

Evidence in the dependability case can be of two sorts. The first is direct evidence that the dependability requirements have been demonstrated. The second is evidence that activities designed to treat the risks that the dependability requirements are not met or demonstrated have been successful.

A wide range of sources of evidence should be used. These can include

a) performance in previous usage/operation,
b) design or other calculations,
c) test and trial data results,
d) simulation results (e.g. FEM or Monte Carlo),
e) results from analysis (e.g. FMECA and FTA) including predictions and modelling,
f) expert opinion, including previously recorded success of the supplier,
g) management and development processes including
   – correct implementation of best practice,
   – the management activities and systems processes followed,
h) operational and maintenance data,
i) dependability cases of components/subsystems provided by their suppliers.

It can also include evidence from activities and tasks carried out for purposes other than the implementation of the dependability plan, such as safety or logistic support analysis.

Before undertaking a dependability activity, its objectives should be fully understood, i.e. how does the activity help achieve dependability, how does it provide evidence for the dependability case, and what are the success criteria for the activity. The success criteria are applied to the records and outputs of the activity to judge if it has achieved its objectives. Evidence that the criteria are met (including the records and outputs) substantiates the claims that the objectives are achieved. Where applicable, the success criteria include that the risks have been adequately treated.

Quantified success criteria are preferred as determining success is simpler and less open to interpretation.

However, quantified success criteria cannot be produced for all activities. In such cases qualitative criteria based on the objectives of the activity should be defined and should include evidence that the activity, as well as the ouput of the activity, are appropriate and correct. For example, the success criteria for modelling are not simply that the predictions and modelling demonstrate compliance with requirements, but that the model itself is an adequate representation of the system, and that all system or system elements (e.g. software) have been included in the modelling. The model should also address the robustness of the design against variations in usage conditions and manufacturing conditions and manufacturing tolerances.

Assurance and evidence does not just result from the outputs of a dependability activity, but also from the timeliness of the activity and any actions which arise. Undertaking the activity at the appropriate time so that it influences the design of the system is very important and activities should be carried out in parallel with the design process. Therefore, the evidence from an analysis activity should include the documentation showing that the activities and actions have been implemented in a timely manner.

5.4 Evidence framework

The evidence framework presents the evidence used to demonstrate the claims and support the argument and is generally presented as a table. The evidence framework captures the current set of compliance and assurance activities (and their success or acceptance criteria) which demonstrate that dependability is achieved and that risks to dependability have been treated.

Figure 3 illustrates the steps to establish and develop the evidence framework. Each dependability case report should base its claims and argument for them on the latest status of the evidence framework.

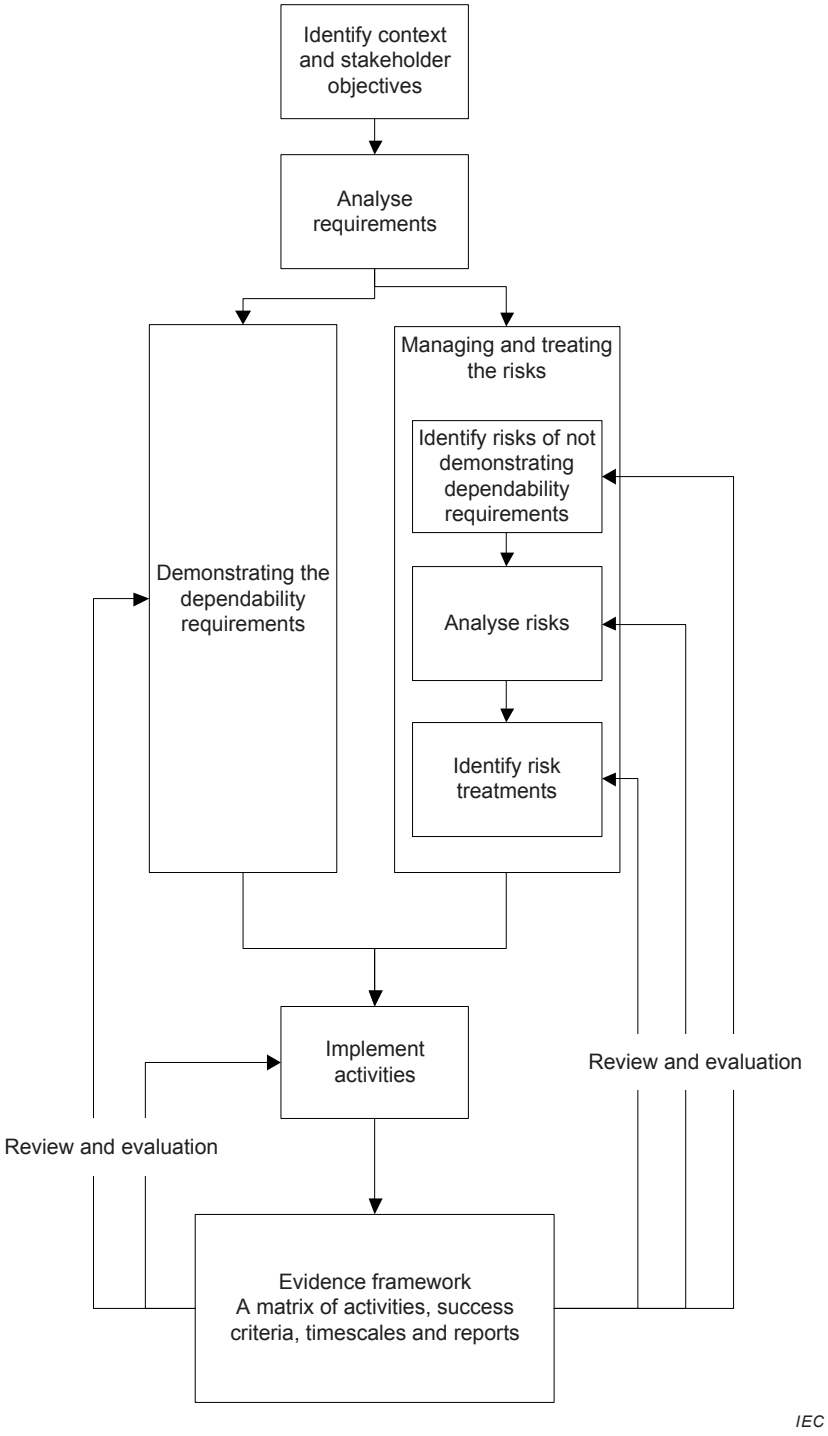

Figure 3 – Establishment and development of the evidence framework

The evidence framework should be tailored to the project. It will vary through the life cycle but should identify or contain

a) the dependability activities, including measurements and tests, which provide evidence for the dependability case,

b) the success or acceptance criteria for the evidence,

c) links to the risks that the activity is intended to treat or the claim which the activity supports (as applicable),

d) the dates/milestones when the activity should be complete and the evidence available,

e) references or links to the evidence actually provided,

f) confirmation of its acceptance (or rejection) (when applicable).

Annex A contains examples of evidence frameworks.

5.5 Dependability case report

In practice, the collation of all documentation into a single document is unmanageable, particularly where there are many and diverse sources of evidence. An acceptable solution is to present periodic updates to the dependability case as dependability case reports. The dependability case is then the body of accumulated dependability case reports which, in turn, refer to source evidence.

Dependability case reports are usually issued at pre-agreed points. They report on the evidence and conclusions drawn from work done so far (referring to papers and data sources where necessary), provide an assessment of overall dependability achievement/progress and a review and evaluation of the dependability activities. At the beginning of each stage, the supplier and customer should agree on the requirements to be satisfied at the end of that stage, i.e. the gate the project must pass before proceeding to the next stage. The agreement may include trade-offs between different competing requirements. The risks arising from this trade-off should be included in the evidence framework. Standards describing processes that could be used to reach robust agreements between customer and supplier are listed in the Bibliography.

When required by a contract, they can be used to provide sufficient detail for stakeholders or the customer to make a decision of whether to proceed from one stage of a project life cycle to the next. Annex B contains a description of the possible contents of a dependability case report.

The dependability case report can be presented as a narrative document but, if a more formal presentation of the argument is required, there are several techniques available which can be used to structure the argument and claims made from the evidence collected. The Bibliography provides informative references to some techniques.

6 Development of the dependability case

6.1 General

This standard primarily describes a project which follows the V-model life cycle where the supplier develops or proposes a system to meet the customer’s requirements and the customer manages it according to the changing needs until its retirement.

In projects using other project management processes, such as spiral models or SCRUM models, the requirements are defined as the project progresses and the guidance in this standard should be tailored to each project. However it is still important to agree on the requirements for the next stage and what is required by the end of that stage (e.g. a stable and functional product release).

The dependability case does not belong solely to the customer or supplier but is a joint body of evidence which is developed and added to by different parties at different life cycle stages.

Developing the dependability case enhances communication between the customer and the supplier. For example, a possible cause of failure to meet customer requirements is lack of understanding by the supplier of customer needs. Treating this risk requires the customer and supplier to communicate to reach a common understanding of requirements. Treating this risk early also minimizes costs.

6.2 Preparation of the dependability case

While the dependability case is most effective if started at the concept stage, it may be started at any life cycle stage. This subclause describes the activities which are required at whichever life cycle stage the dependability case is first developed. Subsequent subclauses describe how the dependability case might be developed throughout the project life cycle. For simplicity, it is written in the context of the project starting at the concept stage, where the supplier(s) might develop multiple solutions, one of which is selected by the customer and taken forward through to enhancement and retirement.

The development of the dependability case begins with the customer's activities to determine the dependability requirements and their measurement base. Normally, the way these requirements have to be measured is documented as part of the concept stage of a project. IEC 62347 and IEC 60300-3-4 give guidance on the specification of dependability.

The customer should include the dependability requirements, including availability, reliability, maintainability and supportability requirements, as part of the system specification that will also include performance and usage. Other requirements such as cost and risk profiles may also be specified.

Where necessary, references to other documents or evidence (such as the documents that detail the proposed arrangements for the management of risk, safety, supportability and environment) are also included. The customer should also supply the context for these requirements, from their operating profiles, the role of the project, etc., down to the terminology they employ. Similarly, the customer should clarify all assumptions they made in developing the requirements and expect those which are relevant or appropriate to dependability to be shared with the suppliers.

The customer may present these requirements, together with the context and the assumptions, in an initial dependability case report, with references to any pre-existing evidence, such as dependability performance of similar systems or subsystems. The customer might also identify risks to dependability and how they should be treated by either the supplier or customer. This should include information on how the customer will determine that the risks have been adequately treated.

On receipt of the dependability requirements or initial dependability case report from the customer, the supplier should analyse these dependability requirements and plan the activities to satisfy them. This analysis and planning will involve

a) gaining a full understanding of the requirements,
b) analysing requirements to define system dependability targets,
c) considering any existing evidence,
d) identifying risks (and transferring to the overall project-level risk register) and how they are to be treated.

The requirements that affect system dependability should be analysed to determine their impact at system and subsystem level as the results of these analyses form part of the dependability case. This analysis should include other aspects such as system operation, its environment and the human–machine interfaces, all of which have an impact on system dependability. To gain this understanding, the supplier should be involved in dialogue with the customer to ensure mutual understanding of all aspects. This dialogue results in a definitive statement of the customer’s requirement and all the operational and environmental conditions thereof. This statement gives confidence that the dependability requirements of the customer have been agreed and understood by both the customer and supplier (see 4.2). The customer and supplier should also agree how the risks are to be treated and how the customer will judge that the risks have been adequately treated.

From this, the supplier's dependability design targets and a measurement base are determined. These are design aims, possibly with a margin over the dependability requirement in order to reduce the risk that the requirement will not be met.

The dependability activities lead to an evidence framework and a dependability case. The planning of the dependability activities (to be included in the response to the customer) is based on the work required to demonstrate the achievement of dependability requirements. The objective of planning the activities is to provide confidence to the customer and supplier that the risk of failing to meet or demonstrate the achievement of dependability requirements is minimized, before committing resources.

However, different types of purchase or project can involve different combinations of life cycle stages and, depending upon the contractual arrangements, the dependability case may be started or completed at the end of any stage. For example, if a customer is buying an OTS system, the development might have been completed sometime earlier and the customer may prepare the dependability case that includes only the realization and utilization stages. Alternatively, the OTS system might provide its own dependability case, which includes the concept and development stages, which can be incorporated or referred to by many customers.

However, whichever stage the project begins at, the first dependability case report should include a full assessment of the requirements and the tasks and activities which will be undertaken.

6.3 Concept stage

At the concept stage, the customer should develop an outline set of requirements and may issue an outline dependability case report to the supplier. The customer should also identify risks to be included in the overall project risk register. Where there is a lengthy project, including a significant competitive development stage, then the customer might need to examine the outline requirements to ensure that the proposals from competing suppliers can be assessed for dependability using a common assessment methodology.

It is essential that all the dependability stakeholders are consulted at the concept stage to ensure that their requirements are fully captured. Expert advice and the use of dependability modelling techniques are probably necessary to validate that the requirements are suitable and sufficient.

It is likely that there will be considerable trade-off between different requirements. For this trade-off, the risks of not demonstrating compliance with the requirements may form a key part of the decision-making process, i.e. if compliance with the dependability requirements cannot be demonstrated, this might be a reason for the option's rejection. As part of the concept stage, the supplier or customer may move to a single preferred solution, or this might not occur until the development stage.

The supplier should analyse the requirements and develop one or more solutions. Risks might be identified at this stage that are common to any potential solution and that require specific and timely treatment. These risks might lead to an initial evidence framework that identifies required minimum assurance activities and these activities might, in turn, form part of the contractual requirements or scope of supply. However, in developing these solutions, the supplier may identify different risks to compliance with the dependability requirements for the different solutions. These should also be presented in the initial evidence framework.

The supplier should develop a preliminary set of dependability activities that will demonstrate the satisfaction of the dependability requirements and will treat the risks, based upon the initial evidence framework. This should be presented to the customer in the dependability plan which should outline the design philosophy and principal design features and then identify the differing risks for the proposed designs. In some instances, the risks could be determined using a checklist, but engineering judgement should be a significant input. These risks should

be included with other project risks into the overall project risk management plan. The risks and the plan for their management form part of the dependability case (see IEC 62198).

A dependability case report should be compiled at the end of this stage. It should discuss the development of the plan for providing assurance of dependability and document the justification for the proposed activities as well as outlining the proposed evidence to be collected. The objective of providing the customer with an early dependability case report is to demonstrate to the customer that dependability requirements will be met before resources are committed.

6.4 Development stage

At the development stage, the customer will generally provide a dependability case for a single preferred solution. It is possible that the dependability requirements will be different to those at the concept stage, due to the trade-off between different requirements, which will require the dependability case to be updated.

Through continued analysis of the dependability requirements, the supplier should decide upon a robust design philosophy for the preferred solution. The supplier develops, and places in the evidence framework, the detailed design of the preferred solution, explicit claims that the specific design will meet the requirements and an argument demonstrating how the claims will be substantiated. This should include ensuring that new risks identified while carrying out the activities are fed back to analysis and design at this stage in a timely manner and followed through.

If not completed in the concept stage, or if an update is required, the onus is on the supplier to take the initiative and propose dependability design targets and a measurement base. For example, the customer may specify an availability requirement but the supplier needs separate reliability and maintainability targets to develop the system.

At the development stage, the supplier should update the evidence framework as development progresses and activities are planned and implemented. The dependability case report compiled at the end of this stage should include a partially completed evidence framework consisting of the current and future dependability activities, their success criteria and the project milestone at which the evidence from these activities will be produced in order to be effective.

6.5 Realization stage

The dependability case in the realization stage is primarily concerned with developing and populating the dependability case as activities are completed and evidence becomes available. If the dependability case has been properly managed during the concept and development stages, significant changes would not be expected to the dependability requirements or risks which have previously been identified. However, new risks might be identified or updated treatments proposed as a result of the completed activities and the evidence produced.

The supplier should issue dependability case reports at agreed milestones throughout the realization stage, which should describe how the risks are being treated and provide the customer with increasing confidence that the requirements will be met. The customer’s acceptance of the dependability case reports will generally be one of the necessary conditions for interim payments to the supplier.

The customer should study the dependability case reports produced by the supplier. They should review the argument and the nature of evidence provided, including the activities undertaken to treat risks, and monitor the progressive achievement of dependability.

However if the customer finds the supplier’s progress unsatisfactory, this should be managed by the normal project procedures. The customer should also consider whether there are any

additional risks relevant to their particular context and update the dependability case accordingly.

At the end of the realization stage, if the customer is satisfied with the dependability case, this will indicate that the system is ready to be utilized.

6.6 Utilization stage

Once the system enters the utilization stage it is important that the dependability of the system be monitored and sustained. The dependability case should be updated to reflect the consequences of issues such as differences in the maintenance regime from that assumed, the way users interact with the system in practice or more detailed understanding of the operating environment.

The manager of the system when it is in use (whether supplier or customer) should review the argument, assumptions and contextual information on which the dependability case was based and check that all are still valid. This review may be held periodically or may be triggered by pre-defined events. The manager should review the register of risks and add new risks that could arise in use that may not have been considered by the supplier. Evidence from operational usage and/or testing and maintenance should be added to the dependability case. It is possible that more than one organization could use the system in different contexts and develop the dependability cases independently.

If the measured or achieved dependability differs significantly from that which was predicted, the possible reasons for this difference should be identified and corrective action undertaken to restore the levels of dependability identified in the requirement(s). If this is not feasible or justifiable, e.g. due to cost, the customer and supplier could agree to revise the requirements. If the change in requirements is significant, the customer and original supplier may then return to the concept stage to agree on revised requirements. Alternatively, the customer may initiate the enhancement stage to adapt the system to the changes. The customer and/or supplier should consider whether there are any additional risks relevant to the changes and update the dependability case accordingly.

At the end of the utilization stage the expectation is that the dependability case and evidence framework demonstrate that the dependability requirements have been met.

6.7 Enhancement stage

It is often the case that the system requires enhancement during the utilization stage. This might be by the customer, in which case the customer should develop the dependability case. Alternatively, it might involve contract action on a supplier. If this happens, the supplier should treat the enhancement as a new project, effectively restarting the dependability case from the concept or development stages, but using the previous dependability case as a baseline. The customer’s monitoring actions (see 6.5) and the results should also be captured in the dependability case and the dependability case managed accordingly.

6.8 Retirement stage

For some systems, the retirement stage may also require the dependability case to be updated if, for example, there are specific requirements for disposal and dismantling of the system. The same processes for managing the dependability case should be followed as for previous project stages.

It is also at this stage that the achieved dependability of the system can be measured. It is good practice to review the claims and evidence contained within the dependability case to determine whether these have been achieved. This may also provide lessons learnt for future projects.

The evidence frameworks and the dependability cases accumulated across successful projects may serve as a library of reusable elements for the organization so should be stored within the organization's knowledge management system.

7 Assessing the adequacy of evidence

The robustness of the dependability case in making dependability claims is dependent upon the adequacy of the evidence used. The customer should therefore review not only the argument and claims made in the dependability case but also consider the adequacy of the evidence upon which it is based.

The adequacy of evidence is primarily a function of its practical impact on the demonstration of dependability, the reduction of uncertainty and the treatment of the risks. Whilst it is not necessary to assess the adequacy of specific, detailed dependability activities 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 an effective dependability management system.

All relevant, available information on the dependability achievements and lessons learnt from a particular design should be used to provide assurance of dependability within the dependability case. It is not acceptable to ignore evidence which counters the argument being made.

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

a) the evidence as a whole is clearly derived from a properly planned dependability programme;
b) the links between any specific item of evidence, a dependability requirement, an activity in the dependability plan and identified risks are clear;
c) the evidence is derived from dependability activities carried out by competent people with adequate resources;
d) 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, it is important to seek traceable methods/techniques, assumptions and detailed results. Consequently, an open, honest dialogue between customer and supplier is important. Judgement is required to assess the evidence presented, including its visibility, traceability and quality in accordance with the criteria listed in this clause. Annex C provides a checklist of generic points which are not prescriptive, but which provide additional guidance on assessing the adequacy of evidence in appropriate circumstances.

Annex A
(informative)

Evidence framework

A.1 General

The evidence framework is defined in 5.4. Example column headings and contents are described as follows:

Column no.	Heading	Contents
1	Life cycle stage	Relevant stage in the project life cycle
2	Reference	Reference to the claim Cross-referenced to the project requirements specification or risk register
3	Claim description	Description of the claim supported Coordinated with the project requirements specification or risk register
4	Subclaim	A description of the subclaim Coordinated with the project requirements specification or risk register
5	Evidence required	Evidence needed to support the demonstration of the claim or treat the risks of not meeting the requirements (information, not deliverable reports)
6	Dependability activity	Activity 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		
7	Evidence	Deliverable document/contents
8	Time due	Time the evidence is due in order to be effective
Acceptance status		
9	Evidence	References to the latest evidence, including issue no. and date delivered

Column no.	Heading	Contents
10	Approval status	Whether approved or not. If rejected, include reasons and corrective action. If accepted, signature of approving authority and date of acceptance

Two examples of partial evidence frameworks are illustrated in Table A.1 and Table A.2. Each covers examples of claims and risks at various stages in the project life cycle, assuming the system involves substantial development activity and at different levels of detail.

While each row of the table is complete, neither example evidence framework examines all the expected claims or risks to be treated.

Therefore, when creating an evidence framework, the system should be considered in its own right and it is expected that the evidence framework will be substantially longer than the examples given here. However, the layout of the table may be used as a template.

A.2 Abbreviations used only in this annex

BIT	Built-in test
DRACAS	Data recording and corrective action system
HUMS	Health and usage monitoring system
ITEAP	Integrated test, evaluation and acceptance plan
PRAT	Production reliability acceptance test
OMD	Operational and maintenance demonstration
SMART	Specific, measurable, achievable, realistic, time-bound
TDP	Technology development plan

Table A.1 – Evidence framework for system "X"

"Evidence framework for system "X"						Issue:	Date:	Signature:	
Life cycle stage	**Ref**	**Claim**	**Subclaim**	**Evidence required**	**Dependability activity**	**Success/acceptance criteria**		**Acceptance status**	
						Evidence	**Time due/required**	**Ref, issue, date**	**Approval status**
Tender (for development)		The system achieves its specified reliability: 99,9 % over a 24 h duty cycle (requirement ref AAA)	Intrinsic reliability of solution components meets the requirements	Demonstration of intrinsic reliability by parts count prediction using part failure rates	Parts count reliability prediction using in-service experience of similar parts, defaulting to industry standard data sources, e.g. data from component or OTS suppliers	Parts count reliability prediction independently reviewed.	2 weeks prior to preliminary design review, update prior to critical design review	Report aa issue 01 dated zzz	Accepted
			Failure modes and criticality of solution(s) are fully understood and treated	Risk that critical failure modes and failure rates for single and double faults are missed so reliability does not meet the target (Risk ref BBB)	FMECA: this information will be provided by the design FMECA, conducted as design practice	FMECA independently reviewed	As parts count reliability prediction	Report bb Issue 02 dated yyy	Rejected. Critical failure modes not all managed. Redesign being undertaken
					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	Test results demonstrate requirements	2 weeks prior to critical design review	Not yet due	

"Evidence framework for system "X"						Issue:	Date:	Signature:	
Life cycle stage	**Ref**	**Claim**	**Subclaim**	**Evidence required**	**Dependability activity**	**Success/acceptance criteria**		**Acceptance status**	
						Evidence	**Time due/required**	**Ref, issue, date**	**Approval status**
Tender (for development) (cont.)			Solution performs as predicted in use	Demonstration of dependability during utilization	Develop proposals for monitoring and reporting of operational defects and maintenance performance through defect reporting via analysis of DRACAS database	Draft operational and maintenance demonstration plan available including acceptance criteria with regard to the 24 h duty cycle requirement	2 weeks prior to final design review.	Not yet due	
						Test results demonstrate requirements	1 year after entry into use	Not yet due	
		System BIT requirements are achieved (requirement ref CCC)	Testability design strategy tests all required functions	Risk that testability requirements are not verified resulting in either poor performance and/or customer not accepting item (risk ref DDD)	Review BIT design strategy in the light of the functional hierarchy developed in the FMECA (see Claim 1.1.1)	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	6 weeks prior to critical design review	Not yet due	
			Testability identifies critical failure modes	Risk that testability design strategy misses critical functions resulting in requirement not being achieved (risk ref EEE)	Extension of the FMECA to provide an evaluation of BIT coverage	BIT evaluation report shows that the system testability is consistent with BIT requirements for; Start-up. Continuous checks. Diagnostics. Location	6 weeks prior to final design review	Not yet due	

"Evidence framework for system "X"						Issue:	Date:	Signature:	
Life cycle stage	**Ref**	**Claim**	**Subclaim**	**Evidence required**	**Dependability activity**	**Success/acceptance criteria**		**Acceptance status**	
						Evidence	**Time due/required**	**Ref, issue, date**	**Approval status**
Tender (for development) (cont.)		The integration of latest technology and communications equipment into the design does not compromise the dependability of the complete system (requirement ref FFF)	Installation of new equipment does not restrict maintenance access to remainder of system	Risk that maintenance access is restricted is treated by technology demonstration plan (TDP) including dependability assessments (risk ref GGG)	Dependability predictions conducted to support the TDP	TDP dependability prediction report demonstrates that design is not compromised by new technology	6 weeks prior to critical design review	Not yet due	
			New technology systems do not produce excessive heat which impacts on performance of existing system	Risk that excessive heat is produced is treated by Technology demonstration plan (TDP) including assessment of heat loads and impact on existing system (risk ref HHH)	Dependability predictions conducted to support the TDP	TDP dependability prediction report demonstrates that design is not compromised by new technology	6 weeks prior to critical design review	Not yet due	
Development		Subsystem z possesses durability for required life (requirement III)	Wear out mechanisms are fully understood and managed	Risk that wear out is not understood by evaluation of expected life and determination of any changes necessary to achieve the requirement (risk ref JJJ)	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	3 months after contract award	Report dd issue 01 dated www	Accepted
					Accelerated life testing using the highly accelerated life test methodology	Accelerated life test report providing assurance for the final design meets the life requirement	6 months after receipt of test model(s)	Not yet due	

"Evidence framework for system "X"						Issue:	Date:	Signature:	
Life cycle stage	**Ref**	**Claim**	**Subclaim**	**Evidence required**	**Dependability activity**	**Success/acceptance criteria**		**Acceptance status**	
						Evidence	**Time due/required**	**Ref, issue, date**	**Approval status**
Realization		The chassis suffers no reduction in life during system assembly (as assembly activities include loading that is very different from when system is complete) (requirement ref KKK)	Stresses/fatigue during assembly do not reduce chassis life	Risk of excessive stress / fatigue is treated by 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. (risk ref LLL)	Evaluation of the load case	Report, including analysis and calculation records, showing acceptable stress margins. The report will highlight (any) areas of potential overstress and justify changes, if needed, to ensure adequate margins	3 months prior to completion of realization stage	Not yet due	
				Demonstration of manufacturing processes	Production reliability acceptance test (PRAT)	1) PRAT test plan. 2) PRAT test results assuring the integrity of the chassis for manufacture	1) PRAT plan required before start of production. 2) PRAT test results following completion of PRAT	Not yet due	
					Final quality inspection of deliverables	Quality inspection records demonstrating adequate quality	During production	Not yet due	

Table A.2 – Evidence framework for system Y

Evidence framework for system Y					Issue:	Date:		Signature:	
Life cycle stage	**Ref.**	**Claim**	**Sub-claim**	**Evidence required**	**Dependability activity**	**Success/acceptance criteria**		**Acceptance status**	
						Evidence	**Time due**	**Ref, Issue, date:**	**Approval status**
Concept		Reliability of item satisfies customer needs	Dependability requirements are correctly identified by customer and/or are complete	Risk that critical dependability system attributes have not been identified leading to missed requirements	Capability gap analysis. Operational analysis	Requirements document has been signed off by key stakeholders., agreeing completeness and appropriateness	Early in the concept stage, prior to initial business case submission	Report ee Issue 03 dated vvv	Accepted
			Dependability aspects are addressed within systems engineering, so that impact of dependability on capability is fully understood. Dependability requirements are SMART	Risk that sub-claim is not met is treated by: 1) development of utilization stage availability targets. 2) Adequate system numbers. 3) Initial dependability targets linked to utilization stage availability. 4) Assessment of the impact of dependability on operational effectiveness showing no adverse effects	Needs and numbers studies (with dependability input). Availability modelling	Document includes operation availability targets within the sustainability section and first cut dependability targets			

Evidence framework for system Y					Issue:	Date:		Signature:	
Life cycle stage	**Ref.**	**Claim**	**Sub-claim**	**Evidence required**	**Dependability activity**	**Success/acceptance criteria**		**Acceptance status**	
						Evidence	**Time due**	**Ref, Issue, date:**	**Approval status**
Concept (cont.)		Customer has properly managed dependability to achieve good dependability characteristics. Adequate and effective resources are in place	Downstream costs are optimized/ minimized due to effective dependability management	Risk that customer fails to realize the link between dependability and cost of ownership resulting in greater down stream costs	Dependability input into investment decision-making and life cycle cost modelling including the cost(including time) of delivering the required level of dependability	Plans clearly align with outturn of previous projects. Realistic estimates of funding and equipment numbers have been prepared and included in project execution plan by ensuring availability and reliability are included in these early studies as cost drivers. Team in place	Early in the concept stage, prior to initial business case submission	Project execution plan ref ff Issue 02 dated uuu	Accepted
			Programme meets timescale requirements of sponsor	Risk that the customer fails to consider the impact of the requirements on the need for complex or novel technology resulting in programme delays	Assessment of the technology risks including feasibility studies examining the maturity of the technology likely to be used in the solution options	1) Reports showing pull through from research. Formulation of technology demonstrator plans. 2) Input from industry through partnering teams		1) Report gg Issue 01 dated ttt .Report hh Issue 01 dated sss.2) Team mobilized	Report gg accepted. Report hh rejected and being rewritten
			Timescale risks are properly managed and minimized	Risk that customer fails to understand the key timescale risks resulting in low reliability and/or programme delays	Assessment of the timescale risks by Comparison with similar, related or historical projects	Analyses to show the timescales have been planned in accordance with the technology and technical risks. Accepted and agreed schedule		Schedule ii Issue 07 dated rrr	Accepted

Evidence framework for system Y					Issue:	Date:		Signature:	
Life cycle stage	**Ref.**	**Claim**	**Sub-claim**	**Evidence required**	**Dependability activity**	**Success/acceptance criteria**		**Acceptance status**	
						Evidence	**Time due**	**Ref, Issue, date:**	**Approval status**
Concept (cont.)			Assurance of dependability by supplier meets standards	Risk that customer fails to outline the strategy for assurance resulting in adequate evidence not being produced and customer dissatisfaction	An agreed dependability plan	A draft dependability plan outlining the elements, work and the strategy to treat the key risks. Statements of work for concept stage studies in initial business case. Plan includes customer's acceptance criteria	Early in the concept stage, prior to initial business case submission	Report jj draft C dated qqq	Accepted
Tender (for development)		Dependability supporting evidence is adequate and correct and meets the customer needs/expectation	Customer and supplier have communicated and agreed requirements and objectives	Risk that supplier does not understand customer's requirements leading to dependability supporting evidence being developed in an adhoc manner and failing to address the customer needs/expectation	Reliability predictions based on similar equipment failure rates, and any factors applied due to differences in duty cycle, usage, complexity, etc. leading to dependability requirements	Clear dependability requirements with the requisite evidence contained in the dependability case issued to the supplier.	Early in the development stage, prior to final business case submission	Not yet due	
					Details of utilization stage analysis and operational availability studies	Initial risk register			
Tender (for development) (cont.)		Customer selects the optimal solution from a dependability perspective so that dependability goals are	Selection mechanism includes dependability and has been rigorously and effectively	Risk that selection mechanism fails to rigorously address dependability so that dependability	Reliability estimates of concept options. Assessment studies allowing dependability estimates to be	Option selection reports showing evidence that the dependability has been factored into the selection process	In the development stage, prior to final business case submission	Not yet due	

Evidence framework for system Y					Issue:	Date:		Signature:	
Life cycle stage	**Ref.**	**Claim**	**Sub-claim**	**Evidence required**	**Dependability activity**	**Success/acceptance criteria**		**Acceptance status**	
						Evidence	**Time due**	**Ref, Issue, date:**	**Approval status**
		achieved	used	is not achieved	input along with other attributes into a structured option selection system				
Tender (for development) (cont.)				Risk that inadequate weighting is given to dependability in dependability assessment method so that other attributes are given undue weighting over dependability	Draft dependability assessment questions for tender marking scheme, ensuring dependability is given equal weighting to performance, time and cost	Final scores from the bid assessment, plus key risks and dependability achievement milestones necessary to contract for the production of dependability evidence are contained within the dependability case	In the development stage, prior to final business case submission		
				Risk that the technological risks associated with each option are not adequately assessed so that requirements are not met	Assessment of likely software complexity through measurements of the size and complexity of the software	Option selection reports include assessment of software dependability through life	In the development stage, prior to final business case submission	Not yet due	
					Project dependability design guidelines and definition of how these guidelines are to be contracted against	Stakeholder acceptance for the project dependability design guidelines has been obtained	In the development stage, prior to final business case submission	Not yet due	
Development		Supplier fully understands the intent of the	Supplier and customer have communicated	Risk that the supplier has not formally	Analysis of duty cycle, loads, temperature	Supplier's dependability case report demonstrates that the	Provided with the tender or early in the		

Evidence framework for system Y					Issue:	Date:		Signature:	
Life cycle stage	**Ref.**	**Claim**	**Sub-claim**	**Evidence required**	**Dependability activity**	**Success/acceptance criteria**		**Acceptance status**	
						Evidence	**Time due**	**Ref, Issue, date:**	**Approval status**
		requirements so that objectives are aligned with customer	and agreed the intent of the requirements, in particular with respect to the environmental constraints	addressed the impact of environmental constraints on dependability so that requirements are not met	levels, vibration levels. Analysis of the operational environment and required modes of operation Analysis of damage accumulation effects, dust, dirt ingress, moisture, etc.	environmental factors and duty cycle loads have been understood and will influence the design	realization stage		
		Supplier has recognized and treated the risks associated with dependability so that dependability requirements are met	Adequate risk management has taken place and has included dependability with project risks	Risk that supplier fails to involve dependability staff with formal risk identification resulting in risks not being identified and treated.	Identification of risks associated with dependability. Analysis of the strength of design of critical components against duty cycle loads	Customer review of supplier 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	Early in the design process to influence the design of prototype equipment	Not yet due	
				Risk that risk registers are not integrated leading to misalignment between dependability and project risks	Predictions and modelling to identify critical systems.				
Development (cont.)					Analysis of interface and integration issues				

Evidence framework for system Y					Issue:	Date:		Signature:	
Life cycle stage	**Ref.**	**Claim**	**Sub-claim**	**Evidence required**	**Dependability activity**	**Success/acceptance criteria**		**Acceptance status**	
						Evidence	**Time due**	**Ref, Issue, date:**	**Approval status**
						interface and integration issues are addressed and are not overlooked as causes of unreliability; - reliability modelling, predictions and allocations to determine criticality			
		OTS components perform as expected during development stage	Suitable OTS components used within the design	Demonstration of 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	Independently reviewed report.	Provided with the tender or early in the development stage	Not yet due	
						Option selection reports include realistic predictions for OTS sub-systems dependability			
		Testing is effective as test results can be properly sentenced	Design makes use of automated usage and fault reporting to record system condition and usage	Risk that events cannot be sentenced during testing, as all input parameters are not known, and hence dependability cannot be measured	HUMS to be implemented effectively and efficiently as part of the design process	Maintainability analysis report identifying functions covered by HUMS	Provided with the tender or early in the development stage	Not yet due	

Evidence framework for system Y					Issue:	Date:		Signature:	
Life cycle stage	**Ref.**	**Claim**	**Sub-claim**	**Evidence required**	**Dependability activity**	**Success/acceptance criteria**		**Acceptance status**	
						Evidence	**Time due**	**Ref, Issue, date:**	**Approval status**
Development (cont.)		The system achieves required dependability levels after the transition from development to utilization	The transition from development to utilization is properly managed and the required activities are undertaken	Risk that supplier expects that dependability issues will be addressed by the customer in utilization resulting in poor dependability and customer dissatisfaction	Identification of the risks and the planned dependability activities to treat those risks, along with the technical capability, resources and controls/success criteria to ensure it will happen	Supplier's dependability plan including: – clear dependability management and organizational structure; – systematic plan of activities for satisfying the dependability requirements set against the identified 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 plan; – planned dependability milestones for dependability achievement with periodic reviews	During proposals for project and during early development stage	Not yet due	
Development (continued)		Supplier carries out adequate	Test and evaluation	Demonstration of dependability by	Execute, monitor and review	Customer's acceptance of supplier's	During development	Not yet due	

Evidence framework for system Y					Issue:	Date:		Signature:	
Life cycle stage	**Ref.**	**Claim**	**Sub-claim**	**Evidence required**	**Dependability activity**	**Success/acceptance criteria**		**Acceptance status**	
						Evidence	**Time due**	**Ref, Issue, date:**	**Approval status**
		testing to provide sufficient evidence to demonstrate requirements to the satisfaction of the customer	criteria have been formally agreed between the supplier and the customer	design and test and evaluation data which provides engineering and statistical confidence that the pre-production prototype design has met the dependability requirements	dependability plan activities, amending where appropriate	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; – other test 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	prior to system acceptance and realization		
Development (cont.)		Reliability of OTS software packages is not affected when	The OTS interfaces are compatible with the	Demonstration that integration testing within the software	DRACAS report from the testing and development	DRACAS report shows evidence of: – design modifications leading to satisfactory	During development prior to system acceptance	Not yet due	

Evidence framework for system Y					Issue:	Date:		Signature:	
Life cycle stage	**Ref.**	**Claim**	**Sub-claim**	**Evidence required**	**Dependability activity**	**Success/acceptance criteria**		**Acceptance status**	
						Evidence	**Time due**	**Ref, Issue, date:**	**Approval status**
		integrated into the system	system software architecture	integration laboratory does not affect dependability results. Includes test analyse and fix process reported by formal DRACAS	activities	reliability growth; – input to dependability prediction reports to cover likely software failure rates cycles	and realization stage		
Realization		The system achieves required dependability levels after the transition from development to utilization	Supplier has accounted for and managed the scale of change between prototype and production system	Risk that the transition from development to utilization is badly managed by the supplier and activities are not undertaken due to lack of time resulting in poor initial dependability	Evidence that lessons learned from pre production prototype builds have influenced the production process	Supplier's 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;- capability indicators from Six Sigma processes	Preceding and during first off realization stage	Not yet due	
					Sufficient test and evaluation data to provide 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				
Realization (continued)					Mature production and quality processes alongside				

Evidence framework for system Y					Issue:	Date:		Signature:	
Life cycle stage	**Ref.**	**Claim**	**Sub-claim**	**Evidence required**	**Dependability activity**	**Success/acceptance criteria**		**Acceptance status**	
						Evidence	**Time due**	**Ref, Issue, date:**	**Approval status**
					pre-production prototype design				
					Procedures for the investigation and rectification of faults, failures and defects				
		Produced items are of acceptable quality.	Supplier has mature production facility and processes	Demonstration of consistent quality of manufacture (PRAT test plan)		PRAT batch test results.	At agreed points during realization stage	Not yet due	
			Supplier carries out suitable and sufficient monitoring	Demonstration of the implementation of effective quality procedures		Quality inspection records			
		OTS components perform as expected during realization	Assembly information for OTS equipment is suitable for application	Demonstration of consistent quality of assembly/ integration of OTS components through PRAT test plan		PRAT batch test results. Quality inspection records	At agreed points during realization stage	Not yet due	
				Demonstration of the implementation of effective quality procedures for assembly and integration					
Utilization		Change in use, environment and support is identified and well managed	Customer has specified system support requirements	Risk that dependability is degraded due to inadequate consideration of change in use,	Equipment usage and failure data along with the appropriate analysis to	Operational and maintenance demonstration (OMD) trial results. OMD dependability study results.	At the start and throughout utilization stage	Not yet due	

Evidence framework for system Y					Issue:	Date:		Signature:	
Life cycle stage	**Ref.**	**Claim**	**Sub-claim**	**Evidence required**	**Dependability activity**	**Success/acceptance criteria**		**Acceptance status**	
						Evidence	**Time due**	**Ref, Issue, date:**	**Approval status**
				support and environment	provide reliability estimates and failure trends. Identification of systematic failure modes and the introduction of modifications through post design services Data on repair costs and resources	OMD data collection and analysis			
Utilization/ retirement		Lessons are learnt from the project to prevent issues on future projects	System ownership and reporting responsibilities are defined by the customer	Risk that lessons learnt are not passed to future projects as they are not captured or disseminated by the customer resulting in problems repeating themselves	Full dossier of all elements of dependability work from concept through to utilization or retirement from regular lessons learnt activities	Early studies results.	On-going through to utilization and retirement	Not yet due	
			Customer's team is only demobilized once assurance and lessons learnt have been completed		Collation of all requirements documents, dependability data and reports into a corporate data repository	Mature dependability requirements			
Utilization/ retirement (cont.)					Production of a final lessons learnt report Providing insight into effective-ness of the plan	Extracts from through life management plan			

Evidence framework for system Y					Issue:	Date:		Signature:	
Life cycle stage	Ref.	Claim	Sub-claim	Evidence required	Dependability activity	Success/acceptance criteria		Acceptance status	
						Evidence	Time due	Ref, Issue, date:	Approval status
					and the final dependability estimates achieved				
						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			

Annex B
(informative)

General requirements for the dependability case report

B.1 General

This annex provides the headings and describes the content for sections within the dependability case report. It is not envisaged that this structure will be suitable for every project, but it is intended to provide guidance on the information that should be contained within the reports.

The dependability case report provides dependability evidence at a specific agreed milestone within the life cycle. The reports present an argument based on claims, which in turn is based on evidence and assumptions that the system will satisfy the dependability requirements. The report is not expected to contain all the evidence produced up to that milestone, but to summarize and act as a "signpost", indicating where the detailed evidence can be found.

This standard refers to dependability, which might be taken to imply that documentary evidence for reliability and maintainability will be summarized in a single report. If the evidence framework requires separate reports, or the customer 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.

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.

B.2 Elements required for the dependability case report

Each dependability case report should list and cross reference the requirements in the evidence framework, against which the evidence shall be judged, and be traceable to the original customer’s requirements.

The dependability case report should also outline the background, purpose and scope of the report detailing, for example:

a) an outline of the circumstances which led to the need for, and development of, the dependability case report;
b) the purpose of the dependability case report, i.e. why and for whom it has been produced;
c) the scope and boundary of the dependability case report;
d) what the report covers (and does not cover);
e) boundaries of responsibility with respect to managerial control and other stakeholders;
f) relationship with other reports, if applicable;
g) applicability and compliance with relevant regulations and standards.

B.3 Context and assumptions

B.3.1 Stakeholders

This clause describes the stakeholders interested in the system, their expectations and any requirements which are derived from them.

B.3.2 System description

The system description should contain the following items:

a) Physical 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 dependability case (see IEC 61078).

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) Users and required human machine interfaces – this should describe the people who will use the system and the interfaces they will have with the system.

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

h) 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.

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

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

B.3.3 Dependability requirements

This should reflect the customer's requirements and the supplier's understanding of those requirements and how they are to be measured. 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 the proposed design solution and developed into project target dependability.

B.3.4 Limitations on use

This section should define the boundaries on system use or the context in which the arguments are made which, if exceeded, mean that the dependability claims might not be valid. These limitations include the system's operating envelope, the environment and important maintenance activities.

B.3.5 Assumptions

All assumptions should be explicitly identified, either in the dependability case report or in a separate assumptions register. Where possible, activities to validate the assumptions should be identified and included in the evidence framework.

B.4 Risks

Through analysis of the dependability requirements, the supplier should identify the risks associated with the system not satisfying the dependability requirements, and how these risks will be, or have been, treated during the project. This information would normally be found in the evidence framework.

B.5 Dependability plan

The supplier should determine how they intend to meet and demonstrate the requirements and provide the necessary assurance. This section justifies the activities in the supplier's dependability plan and identifies the success criteria for these activities.

B.6 The evidence framework

This section should provide a complete overview of the evidence, whether during the development and realization stages or during system utilization. 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 customer and might be matched to payment milestones for control purposes.

B.7 Body of evidence

This should index the existing evidence. See 5.3 for examples of the types of evidence which might be included. Every item of evidence should be cross-referenced to the evidence framework and to the claims it demonstrates or the risks which it treats.

The body of evidence should also trace the history of reviews and updates of the dependability design philosophy, targets and plan, which keep these in line with the changing status of the original risks, as well as any new/emerging risks. The body of evidence should distinguish between the factual evidence and the arguments or inference drawn from the facts.

B.8 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.

B.9 Dependability claims and argument

This section contains the argument which supports the claims that the system satisfies each of the dependability requirements. This section should provide the reasoning why each of the requirements will be, or is being, met in utilization, based on the context, evidence and any assumptions.

All assumptions should be listed explicitly or an assumptions list referenced. At the start of the utilization stage, any remaining significant assumptions should be explicitly highlighted, along with any limitations on use which these may cause.

B.10 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. This includes referring back to the conclusions of the previous issues of the dependability case report and describing how the arguments have changed.

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.

The status of the dependability assumptions, evidence, argument, 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 treat the residual risks.

The recommendations should be based on current shortfalls in the evidence available and should propose changes, as appropriate, to the dependability design philosophy, targets and activities in order to maximize the progress towards providing assurance that the system satisfies each of the dependability requirements.

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 7 of this standard.

Checklist:

1) Are the objectives of the activity clearly defined?
2) Has the activity been undertaken in a systematic manner and is it complete?
3) Has the activity been undertaken at a time that allows influence on the design?
4) Does the activity properly reflect the usage and environment of the system and has this been documented?
5) Has the activity been undertaken to reflect the physical and functional boundaries of the system?
6) Are any assumptions recorded (e.g. inputs from other systems or services), and are they realistic and reasonable?
7) Is justification given for the activity method/technique used, and is it reasonable?
8) Who was consulted during the activity (e.g. user, maintainer, designer)? Was this level of consultation reasonable?
9) Are the activity recommendations clearly defined, and are they reasonable?
10) Does documentary evidence indicate that the recommendations have been implemented?
11) Have the activity results been progressively updated to reflect the latest design, and are these being used as an input to design reviews?

Bibliography

Documents for structuring arguments

Toulmin method – Toulmin, S., The Uses of Argument, 1958, 2nd edition, 2003

Goal Structuring Notation – GSN Community Standard

http://www.goalstructuringnotation.info/documents/GSN_Standard.pdf

Documents for reaching formal agreements

ISO/IEC 12207, *Systems and software engineering – Software life cycle processes*

ISO/IEC 15026, *Systems and software engineering – Systems and software assurance*

ISO/IEC 15288, *Systems and software engineering – System life cycle processes*

Documents for dependability

IEC 60300-3-1, *Dependability management – Part 3-1: Application guide – Analysis techniques for dependability – Guide on methodology*

IEC 60300-3-4, *Dependability management – Part 3-4: Application guide – Guide to the specification of dependability requirements*

IEC 61078, *Analysis techniques for dependability – Reliability block diagram and Boolean methods*

IEC 62347, *Guidance on system dependability specifications*

Documents for managing risks

IEC/ISO 31010, *Risk management – Risk assessment techniques*

IEC 62198, *Managing risk in projects – Application guidelines*

_____

This page deliberately left blank

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

Useful Contacts:

Customer Services
Tel: +44 845 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 845 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

bsi.

...making excellence a habit.™