IEC 62741

Edition 1.0 2015-02

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Demonstration of dependability requirements – The dependability case

Démonstration des exigences de sûreté de fonctionnement – Argumentaire dans le cadre de la sûreté de fonctionnement

IEC 62741:2015-02(en-fr)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
www.iec.ch

About the IEC
The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications
The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

IEC Catalogue - webstore.iec.ch/catalogue
The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

IEC publications search - www.iec.ch/searchpub
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and also once a month by email.

Electropedia - www.electropedia.org
The world's leading online dictionary of electronic and electrical terms containing more than 30 000 terms and definitions in English and French, with equivalent terms in 15 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
More than 60 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

IEC Customer Service Centre - webstore.iec.ch/csc
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: csc@iec.ch.

A propos de l'IEC
La Commission Electrotechnique Internationale (IEC) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications IEC
Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Catalogue IEC - webstore.iec.ch/catalogue
Application autonome pour consulter tous les renseignements bibliographiques sur les Normes internationales, Spécifications techniques, Rapports techniques et autres documents de l'IEC. Disponible pour PC, Mac OS, tablettes Android et iPad.

Recherche de publications IEC - www.iec.ch/searchpub
La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études,…). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

IEC Just Published - webstore.iec.ch/justpublished
Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et aussi une fois par mois par email.

Electropedia - www.electropedia.org
Le premier dictionnaire en ligne de termes électroniques et électriques. Il contient plus de 30 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans 15 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

Glossaire IEC - std.iec.ch/glossary
Plus de 60 000 entrées terminologiques électrotechniques, en anglais et en français, extraites des articles Termes et Définitions des publications IEC parues depuis 2002. Plus certaines entrées antérieures extraites des publications des CE 37, 77, 86 et CISPR de l'IEC.

Service Clients - webstore.iec.ch/csc
Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: csc@iec.ch.

IEC 62741

Edition 1.0 2015-02

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Demonstration of dependability requirements – The dependability case

Démonstration des exigences de sûreté de fonctionnement – Argumentaire dans le cadre de la sûreté de fonctionnement

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

ICS 03.120.01; 21.020

ISBN 978-2-8322-2247-8

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.

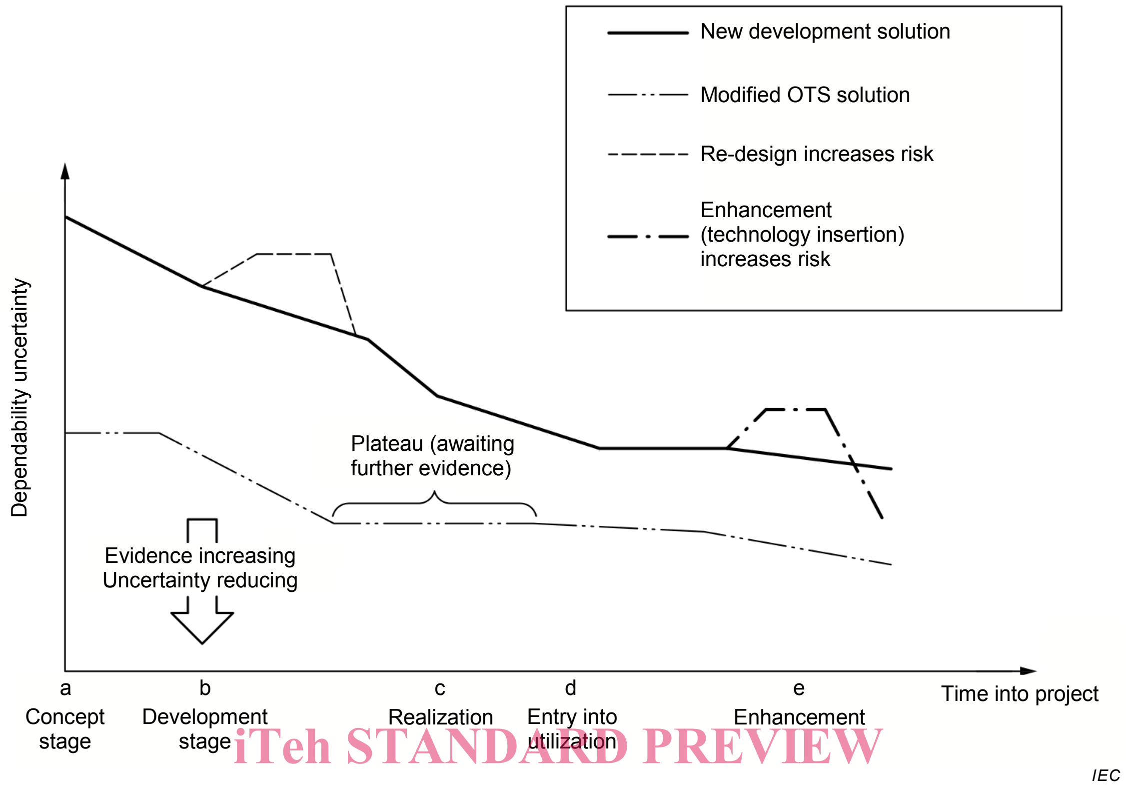

Figure 1 – Illustration of progressive assurance process

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.

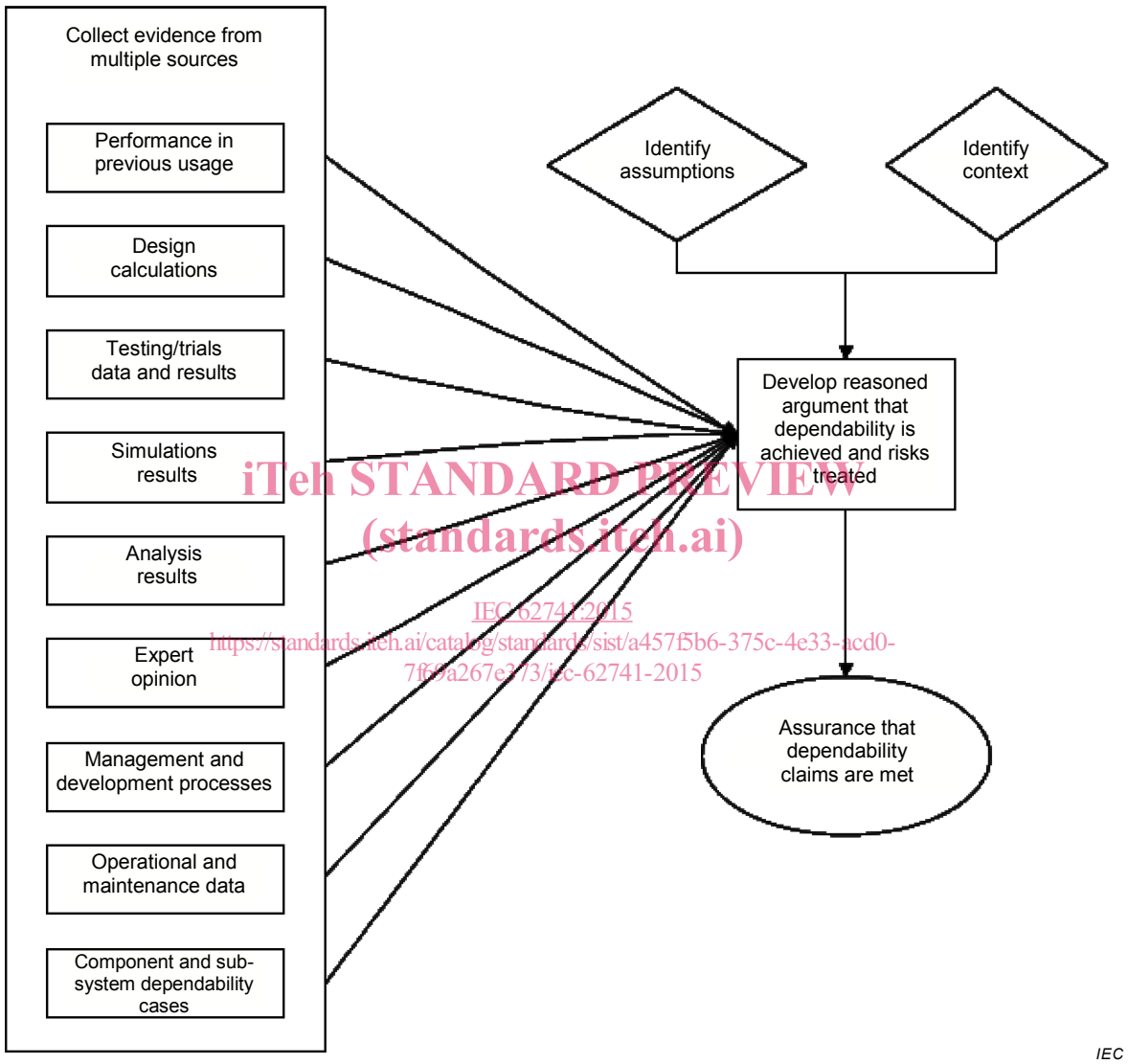

Figure 2 – The development of claims

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.