IEC 60300-3-4

Edition 2.0 2007-09

INTERNATIONAL STANDARD

NORME INTERNATIONALE

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

Gestion de la sûreté de fonctionnement –
Partie 3-4: Guide d'application – Spécification d'exigences de sûreté de fonctionnement

IEC 60300-3-4:2007

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland
Email: inmail@iec.ch
Web: 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.

- Catalogue of IEC publications: www.iec.ch/searchpub

The IEC on-line Catalogue enables you to search by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, withdrawn and replaced publications.

- IEC Just Published: www.iec.ch/online_news/justpub

Stay up to date on all new IEC publications. Just Published details twice a month all new publications released. Available on-line and also by email.

- Electropedia: www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 20 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary online.

- Customer Service Centre: www.iec.ch/webstore/custserv

If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:
Email: csc@iec.ch
Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00

A propos de la CEI

La Commission Electrotechnique Internationale (CEI) 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 CEI

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

- Catalogue des publications de la CEI: www.iec.ch/searchpub/cur_fut-f.htm

Le Catalogue en-ligne de la CEI vous permet d'effectuer des recherches en utilisant différents critères (numéro de référence, texte, comité d'études,…). Il donne aussi des informations sur les projets et les publications retirées ou remplacées.

- Just Published CEI: www.iec.ch/online_news/justpub

Restez informé sur les nouvelles publications de la CEI. Just Published détaille deux fois par mois les nouvelles publications parues. Disponible en-ligne et aussi par email.

- Electropedia: www.electropedia.org

Le premier dictionnaire en ligne au monde de termes électroniques et électriques. Il contient plus de 20 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International en ligne.

- Service Clients: www.iec.ch/webstore/custserv/custserv_entry-f.htm

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions, visitez le FAQ du Service clients ou contactez-nous:
Email: csc@iec.ch
Tél.: +41 22 919 02 11
Fax: +41 22 919 03 00

IEC 60300-3-4

Edition 2.0 2007-09

INTERNATIONAL STANDARD

NORME INTERNATIONALE

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

Gestion de la sûreté de fonctionnement –
Partie 3-4: Guide d'application – Spécification d'exigences de sûreté de fonctionnement

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

PRICE CODE
CODE PRIX W

ICS 03.100.40; 03.120.01

ISBN 2-8318-9308-9

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

DEPENDABILITY MANAGEMENT –

Part 3-4: Application guide – Guide to the specification of dependability requirements

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 provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with an IEC Publication.
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 60300-3-4 has been prepared by IEC technical committee 56: Dependability.

This second edition cancels and replaces the first edition published in 1996 and constitutes a technical revision.

The main changes from the previous edition are as follows:

– the concept of systems has been included and the need to specify the dependability of the system and not just the physical equipment has been stressed;
– the need for verification and validation of the requirement has been included;
– differentiation has been made between requirements, that can be measured and verified and validated, and goals, which cannot;
– the content on availability, maintainability and maintenance support has been updated and expanded to similar level of detail to reliability.

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

FDIS	Report on voting
56/1212/FDIS	56/1233/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.

A list of all parts of the IEC 60300 series, under the general title *Dependability management* can be found on the IEC website.

The committee has decided that the contents of this publication will remain unchanged until the maintenance result date indicated on the IEC web site 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

In many systems, reliability, maintainability and availability are essential performance characteristics. These characteristics, together with maintenance support performance, are known collectively as dependability.

In systems where any of the dependability characteristics are important, it is necessary that these characteristics should be defined and specified in the same way as other system characteristics such as technical performance, dimensions and mass.

The levels of reliability, maintainability, availability and maintenance support performance achieved by a system depend on the conditions under which the system is used and also on the mission profile of the system. When requirements for dependability characteristics are specified, it is necessary to define the conditions of storage, transportation, installation and use that will be applied to the system. It may be important to take account not only of the conditions under which the system will operate, but also of the maintenance policy and organization for maintenance support of the system.

In order to assess the values of the dependability characteristics achieved, it is necessary to use statistical methods.

Dependability characteristics may be specified, like other performance characteristics, in three different ways:

1) specifications written by the supplier;
2) specifications written by the purchaser;
3) specifications mutually agreed or written by the supplier and the purchaser.

This standard is applicable to all three types of specification.

This standard complements IEC 62347 which deals with the definitions of systems and their constituent elements and how to define these so that the dependability requirements of each element can be specified using this standard. The premise of IEC 62347 is to identify system requirements by functions from a system engineering perspective. It provides a process for transforming the purchaser's view on system applications into a technical view for engineering the system. IEC 62347 emphasises architectural and functional design for realisation of functions with appropriate selection of hardware, software and human elements to achieve the system dependability requirements relevant to the purchaser's needs.

DEPENDABILITY MANAGEMENT –

Part 3-4: Application guide – Guide to the specification of dependability requirements

1 Scope

This part of IEC 60300 gives guidance on specifying the required dependability characteristics in specifications, together with specifications of procedures and criteria for verification and validation.

The guidance provided includes the following:

– advice on specifying quantitative and qualitative reliability, maintainability, availability and maintenance support requirements;

– advice to purchasers of a system on how to ensure that the specified requirements will be fulfilled by suppliers;

– advice to suppliers to help them to meet purchaser requirements.

Other documents, such as legislation and governmental regulation may also place requirements on systems and these should be applied in addition to any specifications derived in accordance with this standard.

NOTE 1 Whilst mainly addressing system and equipment level reliability, many of the techniques described in the different parts of IEC 60300 may also be applied to products, items or at the component level. The term system is used throughout this standard.

NOTE 2 This standard does not give guidance on the management of dependability programmes or on the various activities necessary to fulfil stated availability, reliability, maintainability and maintenance support requirements. For this general guidance, see other standards.

NOTE 3 Safety and environment specifications are not directly considered in this guide. However, much of the guidance in this standard could also be applied to safety or environmental specification.

NOTE 4 Specifications for the dependability of a service are not considered in this guide. This includes the provision of a service such as those provided through Public-Private Partnership procurements.

2 Normative references

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

IEC 60050-191, *International Electrotechnical Vocabulary (IEV) – Chapter 191: Dependability and quality of service.*

IEC 60300-1, *Dependability management systems – Part 1: Dependability management systems*

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

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

IEC 60300-3-2, *Dependability management – Part 3-2: Application guide – Collection of dependability data from the field*

IEC 60300-3-3, *Dependability management – Part 3-3: Application guide – Life cycle costing*

IEC 60300-3-5, *Dependability management – Part 3-5: Application guide – Reliability test conditions and statistical test principles*

IEC 60300-3-10, *Dependability management – Part 3-10: Application guide – Maintainability*

IEC 60300-3-12, *Dependability management – Part 3-12: Application guide – Integrated logistic support*

IEC 60300-3-14, *Dependability management – Part 3-14: Application guide – Maintenance and maintenance support*

IEC 60605-4, *Equipment reliability testing – Part 4: Statistical procedures for exponential distribution – Point estimates, confidence intervals, prediction intervals and tolerance intervals*

IEC 60605-6, *Equipment reliability testing – Part 6: Tests for the validity and estimation of the constant failure rate and constant failure intensity*

IEC 60706-2, *Maintainability of equipment – Part 2: Maintainability requirements and studies during the design and development phase*

IEC 60706-3, *Maintainability of equipment – Part 3: Verification and collection, analysis and presentation of data*

IEC 60706-5, *Maintainability of equipment – Part 5: Diagnostic testing*

IEC 61014, *Programmes for reliability growth*

IEC 61025, *Fault tree analysis (FTA)*

IEC 61070, *Compliance test procedures for steady-state availability*

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

IEC 61123, *Reliability testing – Compliance test plans for success ratio*

IEC 61124, *Reliability testing – Compliance tests for constant failure rate and constant failure intensity*

IEC 61160, *Design review*

IEC 61164, *Reliability growth – Statistical test and estimation methods*

IEC 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

IEC 61649, *Goodness-of-fit tests, confidence intervals and lower confidence limits for Weibull distributed data*

IEC 61703, *Mathematical expressions for reliability, availability, maintainability and maintenance support terms*

IEC 61710, *Power law model – Goodness-of-fit tests and estimation methods*

IEC 61713, *Software dependability through the software life cycle processes – Application guide*

IEC 62198, *Project risk management – Application guidelines*

IEC 62308, *Equipment Reliability – Reliability assessment methods*

IEC 62347, *Guidance on system dependability specifications*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC 60050-191 and the following apply.

NOTE Definitions of "dependability", "availability (performance)", "reliability (performance)", "maintainability (performance)", "maintenance support", "failure", "fault", "item", "time to failure", and "operating time between failures" are given in IEC 60050-191.

3.1
verification
confirmation, through provision of objective evidence, that specified requirements have been fulfilled

[ISO 9000:2005, definition 3.8.4 modified]

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

NOTE 2 Example verification activities include:

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

– design reviews;

– tests and analysis performed on the designed systems to ensure that they perform according to their specification;

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

3.2
validation
confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled

[ISO 9000:2005, definition 3.8.5 modified]

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

4 General considerations for dependability specifications

4.1 The need for dependability

All systems exhibit some level of dependability, however often they might fail or require maintenance. However, if a system fails too often it might not be available to perform when required or it might cost too much to maintain. In addition, systems that fail repeatedly will get a bad reputation with the user and are unlikely to be bought again once a replacement is

required. On the other hand, designing and manufacturing systems with high levels of reliability can be costly and it may not be possible to produce such a system at an economical price. There is therefore a balance to be struck between low reliability systems that cost a lot to maintain and high reliability systems that may be expensive to design and construct. This is demonstrated by Figure 1, which shows the costs of design and operation for systems of different reliability.

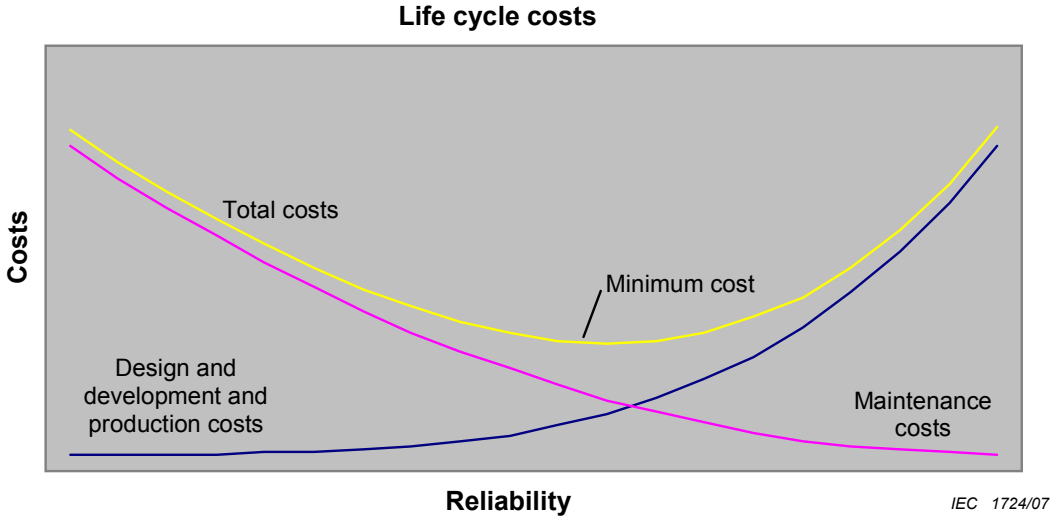

Figure 1 – Relationship between cost and reliability

Figure 1 shows that there is a level of reliability for which the costs over the lifetime of the system are minimized. If a system is Commercial Off The Shelf (COTS) (also known as off the shelf or commercially produced components) this minimum cost level will change as the design and development costs can be shared between many units. However, the optimum reliability for a system may be affected by other issues such as the safety requirements or system function and will not necessarily be the reliability corresponding to minimum life cycle costs.

It is probably true that systems produced by those organizations that do not actively manage dependability achieve levels of reliability much below the minimum life cycle cost point. An investment in dependability design and construction can therefore repay itself in terms of the combined development, manufacturing and operating costs for the system. IEC 60300-3-3 describes Life Cycle Costing and the relationships between dependability and cost.

Dependability includes a number of attributes that are specified differently. Within this standard, dependability has been considered under four headings, as follows:

– availability;
– reliability (R(t)), including mean time to failure (MTTF), mean operating time between failures (MTBF), Weibull or power law parameters;
– maintainability, including mean down time (MDT) and mean time to restoration (MTTR);
– maintenance support.

The dependability characteristics selected for specification should be related to the type and mission of the system, the intended application and the criticality of the required function. For example, only reliability requirements need to be specified if no maintenance actions are intended.

Availability performance requirements are generally specified for systems where down time could cause economic or other loss, through increased operating costs, or personnel injury or loss of service, for example, large systems, production plants, medical equipment, safety

equipment and military systems. Availability performance can be calculated from the system configuration, its subsystems and their reliability performance and maintainability performance requirements, if stated, and by taking into account the maintenance support performance.

Maintainability performance requirements should be specified for systems if the maintenance costs contribute significantly to life-cycle cost or if maintenance is important for the purchaser. Preventive and corrective maintenance requirements may be specified, if applicable.

NOTE The level of maintenance support is very often determined by the conditions of use and is not an intrinsic requirement of the system itself.

Clauses 6, 7, 8 and 9 contain further information on when each of the dependability characteristics would be the most appropriate.

The levels of dependability performance achieved by a system are strongly influenced by the conditions in which it is designed, developed, installed and operated. Dependability is therefore related to other attributes such as quality and the design and manufacturing process. The dependability specification therefore should be part of the total system specification and the interaction between the different attributes recognized and taken into account.

4.2 Requirements and goals

It is important to distinguish between formal requirements in a specification, and goals, as the method of acceptance is different.

A requirement is part of the specification that the purchaser considers is essential that the system meets and for which the supplier has to provide evidence. This evidence may be supplied before the system comes into service as part of the deliverables or once the system is in service, through the application of incentives and penalties for meeting the requirements.

A goal is not a requirement but is the purchaser's aspirations or aims and evidence of the achievement of the goal either need not or cannot be provided.

For high availability or reliability systems, it may not be practicable to provide formal evidence that the high level of availability or reliability has been achieved. The purchaser will need to provide both the high availability and reliability goals, for which evidence cannot be provided, and lower requirements for which evidence can be provided and make it clear which is which.

4.3 Systems

The specification of dependability should be at the system level. A system includes the equipment (both hardware and software) as well as the humans who operate and maintain the system and the procedures by which they operate and maintain it. The system also includes the environment in which the system operates, as shown in Figure 2.

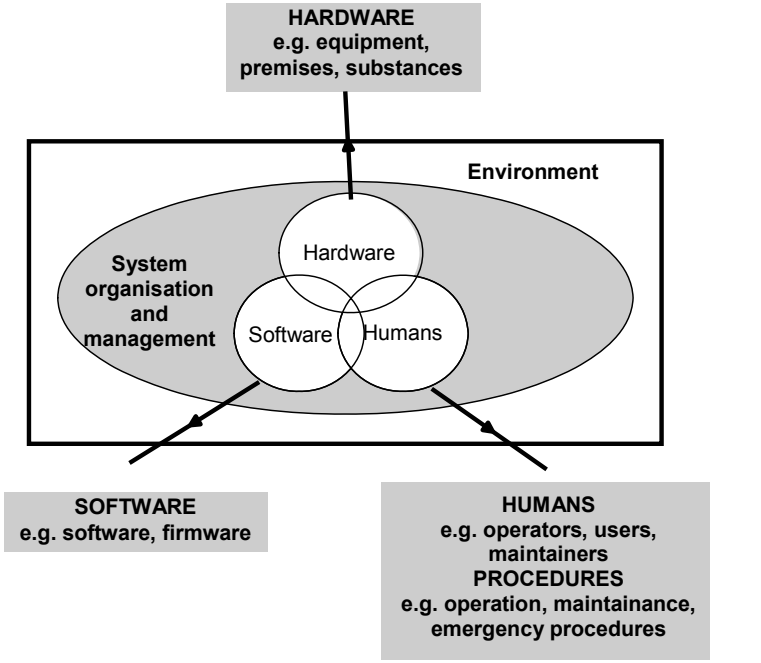

Figure 2 – System elements

Where, possible, all elements of a system should be included in a dependability specification as a change in any one can have a significant effect upon the achieved dependability of the system. For example, different operators of a system can misuse it or be more aggressive in their usage and lead to more failures and therefore achieve lower reliability. However, there may be instances where the supplier and purchaser have little or no control over subsequent maintenance procedures or skills, such as a system within a motor car once sold to a member of the public. The dependability requirements should recognise the particular circumstances of the system being specified.

In addition, the dependability requirements should be linked to the operational or use profile or the functional requirements of the system. The system should be defined in accordance with IEC 62347, which contains details of how to define a system, its elements and the criticality of each function so that the requirements for each element can be specified.

The dependability specification of a system should include the specification of the software and human elements as well as the requirements of the hardware. The guidance in this document may be applied to some aspects of the specification of software but specific guidance may be found in IEC 61713 and the different parts of IEC 61508.

Systems occur at many levels and any system may itself be made up of other systems, often referred to as a system of systems. For example, a bus is a system that includes the motor vehicle, the driver and the driving procedures. The motor vehicle is made up of subsystems that are themselves systems, for example the engine or gearbox, where the human input to the gearbox involves the operation of the gearlever. The subsystems are made up of components and equipment that can themselves be considered as systems and analysed accordingly. This includes considering the interaction of the humans who use the subsystem, how they do so and the manner in which different humans may subject the subsystem to different operational stresses, for example different drivers will drive differently and subject the gearbox to greater or lower loads.

The purchaser might set dependability requirements only at the highest level of system or might decide that it is important that one of the subsystems does not dominate the achieved reliability, and therefore also set requirements at lower levels. These lower level requirements have to be consistent with the top-level requirements and they have to be measurable and

achievable, or they will be goals and not requirements. For example, the contribution of the subsystem to the overall system dependability has to be estimated before the requirements can be apportioned to the subsystems. However, the apportionment to lower level subsystems is not straightforward other than in series systems where all subsystems have a constant failure rate. In other cases, such as systems with redundancy or where the failure rate changes with time, refer to standards such as IEC 61025 and IEC 61078. IEC 60300-3-1 and IEC 61703 give further guidance on the analysis of system dependability.

The type and nature of a system will affect the dependability specification. These include repairable and non-repairable systems and single use devices. Repairable systems cover those where failures can be repaired and the system returned to an operational state. Examples of non-repairable systems include sealed systems, COTS systems, systems where the cost of repair outweighs the cost of replacement, such as many consumer goods, and systems at remote locations where the skills and spares are not available for the time at risk. Single use devices include explosives, passenger air-bags and safety helmets.

Non-repairable systems have to be replaced rather than repaired and the maintainability and maintenance support requirements will be fundamentally different. Also, MTBF will not be a relevant measure for single use devices, where the correct measure would be reliability or alternatively the probability of premature activation. The purchaser has to ensure that the nature of the system and the effect that this can have upon the dependability requirements are identified before the specification is written.

4.4 Demonstration of achievement of requirements

4.4.1 Concept

There are two elements to any specification, the dependability performance requirements and the means by which the supplier has to demonstrate the achievement of the requirements to the purchaser. This means that the supplier has to provide sufficient evidence to the purchaser that the system meets its requirements to give the purchaser the confidence needed to pay the agreed price. Providing additional evidence costs money and is one element in the higher cost of higher reliability systems (see Figure 1) but, without these activities, there is the possibility that the system will not meet its requirements.

There are two main elements; verification and validation. These are defined in ISO 9000 and used for hardware as well as in the software industry as part of the software development process or “v-model” (see IEC 61508) and may be explained as follows. Verification is the process of providing evidence that the system, at any life cycle phase, meets its requirements from the previous life cycle phase(s). Validation is the process of providing evidence that the system meets the actual requirements, which might not always be reflected in the written specification. Both are essential elements.

The level of verification and validation required by the purchaser depends upon the confidence that the purchaser requires that the system will achieve the levels of dependability specified. If the purchaser is willing to maintain a system when it fails in use, then a lower level of evidence, and therefore confidence in the achieved dependability, may be acceptable. This is because the provision of evidence costs money and the purchaser may be willing to accept the risk that the system does not perform as required. The purchaser has to take a balanced decision on the risks that are acceptable when specifying verification and validation requirements (see IEC 62198 for further information on project risk management).

Verification and validation activities have to be planned and systematic in order to be effective. This requires the supplier to state the activities in advance and to obtain agreement from the purchaser, often through the contract. The dependability requirements should consider the various factors likely to affect the cost of dependability verification and validation. This includes the expected lifetime and disposal or recycling of the system.

For a long timescale procurement, activities might be planned many years before completion and, depending upon the contractual terms, the purchaser might have little control over them