

# INTERNATIONAL STANDARD

## NORME INTERNATIONALE

**Dependability management –  
Part 3-15: Application guide – Engineering of system dependability**

**Gestion de la sûreté de fonctionnement –  
Partie 3-15: Guide d'application – Ingénierie de la sûreté de fonctionnement des  
systèmes**



## THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2009 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester.

If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de la CEI ou du Comité national de la CEI du pays du demandeur.

Si vous avez des questions sur le copyright de la CEI ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de la CEI de votre pays de résidence.

IEC Central Office  
3, rue de Varembe  
CH-1211 Geneva 20  
Switzerland  
Email: [inmail@iec.ch](mailto:inmail@iec.ch)  
Web: [www.iec.ch](http://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](http://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 It also gives information on projects, withdrawn and replaced publications.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](http://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](http://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](http://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](mailto: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](http://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](http://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](http://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](http://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](mailto:csc@iec.ch)

Tél.: +41 22 919 02 11

Fax: +41 22 919 03 00

# INTERNATIONAL STANDARD

## NORME INTERNATIONALE

---

**Dependability management –  
Part 3-15: Application guide – Engineering of system dependability**

**Gestion de la sûreté de fonctionnement –  
Partie 3-15: Guide d'application – Ingénierie de la sûreté de fonctionnement des  
systèmes**

INTERNATIONAL  
ELECTROTECHNICAL  
COMMISSION

COMMISSION  
ELECTROTECHNIQUE  
INTERNATIONALE

PRICE CODE  
CODE PRIX

**XA**

ICS 03.120.01

ISBN 978-2-88910-099-6

## CONTENTS

|                                                                                                 |    |
|-------------------------------------------------------------------------------------------------|----|
| FOREWORD.....                                                                                   | 4  |
| INTRODUCTION.....                                                                               | 6  |
| 1 Scope.....                                                                                    | 7  |
| 2 Normative references .....                                                                    | 7  |
| 3 Terms and definitions .....                                                                   | 7  |
| 4 System dependability engineering and applications .....                                       | 8  |
| 4.1 Overview of system dependability engineering .....                                          | 8  |
| 4.2 System dependability attributes and performance characteristics .....                       | 9  |
| 5 Managing system dependability .....                                                           | 10 |
| 5.1 Dependability management .....                                                              | 10 |
| 5.2 System dependability projects .....                                                         | 10 |
| 5.3 Tailoring to meet project needs .....                                                       | 11 |
| 5.4 Dependability assurance .....                                                               | 11 |
| 6 Realization of system dependability.....                                                      | 11 |
| 6.1 Process for engineering dependability into systems.....                                     | 11 |
| 6.1.1 Purpose of dependability process .....                                                    | 11 |
| 6.1.2 System life cycle and processes .....                                                     | 11 |
| 6.1.3 Process applications through the system life cycle .....                                  | 12 |
| 6.2 Achievement of system dependability .....                                                   | 14 |
| 6.2.1 Purpose of system dependability achievements .....                                        | 14 |
| 6.2.2 Criteria for system dependability achievements .....                                      | 14 |
| 6.2.3 Methodology for system dependability achievements.....                                    | 15 |
| 6.2.4 Realization of system functions .....                                                     | 16 |
| 6.2.5 Approaches to determine achievement of system dependability.....                          | 17 |
| 6.2.6 Objective evidence of achievements .....                                                  | 18 |
| 6.3 Assessment of system dependability .....                                                    | 18 |
| 6.3.1 Purpose of system dependability assessments .....                                         | 18 |
| 6.3.2 Types of assessments .....                                                                | 18 |
| 6.3.3 Methodology for system dependability assessments.....                                     | 20 |
| 6.3.4 Assessment value and implications .....                                                   | 21 |
| 6.4 Measurement of system dependability .....                                                   | 21 |
| 6.4.1 Purpose of system dependability measurements .....                                        | 21 |
| 6.4.2 Classification of system dependability measurements.....                                  | 22 |
| 6.4.3 Sources of measurements .....                                                             | 23 |
| 6.4.4 Enabling systems for dependability measurements.....                                      | 23 |
| 6.4.5 Interpretation of dependability measurements.....                                         | 24 |
| Annex A (informative) System life cycle processes and applications .....                        | 25 |
| Annex B (informative) Methods and tools for system dependability development and assurance..... | 35 |
| Annex C (informative) Guidance on system application environment.....                           | 42 |
| Annex D (informative) Checklists for System Dependability Engineering.....                      | 47 |
| Bibliography.....                                                                               | 54 |
| Figure 1 – An overview of a system life cycle.....                                              | 12 |
| Figure 2 – An example of a process model .....                                                  |    |

|                                                                         |    |
|-------------------------------------------------------------------------|----|
| Figure A.1 – An overview of system life cycle processes.....            | 25 |
| Figure C.1 – Environmental requirements definition process .....        | 43 |
| Figure C.2 – Mapping system application environments to exposures ..... | 44 |

## INTERNATIONAL ELECTROTECHNICAL COMMISSION

**DEPENDABILITY MANAGEMENT –****Part 3-15: Application guide –  
Engineering of system dependability**

## 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 should 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 should 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 should not be held responsible for identifying any or all such patent rights.

International Standard IEC 60300-3-15 has been prepared by IEC technical committee 56: Dependability.

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

| FDIS         | Report on voting |
|--------------|------------------|
| 56/1315/FDIS | 56/1321/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

Systems are growing in complexity in today's application environments. System dependability has become an important performance attribute that affects the business strategies in system acquisition and the cost-effectiveness in system ownership and operations. The overall dependability of a system is the combined result of complex interactions of system elements, application environments, human-machine interfaces, deployment of support services and other influencing factors.

This part of IEC 60300 gives guidance on the engineering of the overall system to achieve its dependability objectives. The engineering approach in this standard represents the application of appropriate scientific knowledge and relevant technical disciplines for realizing the required dependability for the system of interest.

The four main aspects for engineering dependability concerning systems are addressed in terms of

- process,
- achievement,
- assessment, and
- measurement.

The engineering disciplines consist of technical processes that are applicable to the various stages of the system life cycle. Specific technical processes described in this part of IEC 60300 are supported by a sequence of relevant process activities to achieve the objectives of each system life cycle stage.

This part of IEC 60300 is applicable to generic systems with interacting system functions consisting of hardware, software and human elements to achieve system performance objectives. In many cases a function can be realized by commercial off-the-shelf products. A system can link to other systems to form a network. The boundaries separating a product from a system, and a system from a network, can be distinguished by defining the application of the entity. For example, a digital timer as a product can be used to synchronize the operation of a computer; the computer as a system can be linked with other computers in a business office for communications as a local area network. The application environment is applicable to all kinds of systems. Examples of applicable systems include control systems for power generation, fault-tolerant computing systems and systems for provision of maintenance support services.

Guidance on dependability engineering is provided for generic systems. It does not classify systems for special applications. The majority of systems in use are generally repairable throughout their life cycle operation for economic reasons and practical applications. Non-repairable systems such as communication satellites, remote sensing/monitoring equipment, and one-shot devices are considered as application-specific systems. They require further identification of specific application environment, operational conditions and additional information on unique performance characteristics to achieve their mission success objectives. Non-repairable subsystems and components are considered as throwaway items. The selection of applicable processes for engineering dependability into a specific system is carried out through the project tailoring and dependability management process.

This part of IEC 60300 forms part of the framework standards on system aspects of dependability to support IEC 60300-1 and IEC 60300-2 on dependability management. References are made to project management activities applicable to systems. They include identification of dependability elements and tasks relevant to the system and guidelines for dependability management reviews and tailoring of dependability projects.

## DEPENDABILITY MANAGEMENT –

### Part 3-15: Application guide – Engineering of system dependability

#### 1 Scope

This part of IEC 60300 provides guidance for an engineering system's dependability and describes a process for realization of system dependability through the system life cycle.

This standard is applicable to new system development and for enhancement of existing systems involving interactions of system functions consisting of hardware, software and human elements.

This standard also applies to providers of subsystems and suppliers of products that seek system information and criteria for system integration. Methods and tools are provided for system dependability assessment and verification of results for achievement of dependability objectives.

#### 2 Normative references

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

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

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

#### 3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

##### 3.1

##### **system**

set of interrelated items considered as a whole for a defined purpose, separated from other items

NOTE 1 A system is generally defined with the view of performing a definite function.

NOTE 2 The system is considered to be bound by an imaginary surface that intersects the links between the system and the environment and the other external systems.

NOTE 3 External resources (i.e. outside the system boundary) may be required for the system to operate.

NOTE 4 A system structure may be hierarchical, e.g. system, subsystem, component, etc.

##### 3.2

##### **subsystem**

system that is part of a more complex system

##### 3.3

##### **operating profile**

complete set of tasks to achieve a specific system objective

NOTE 1 Configurations and operating scenarios form part of the mode of system operation.

NOTE 2 An operating profile is the sequence of required tasks to be performed by the system to achieve its operational objective. The operating profile represents a specific operating scenario for the system in operation.

### 3.4 function

elementary operation performed by the system which, when combined with other elementary operations (system functions), enables the system to perform a task

[IEC 61069-1 :1991, 2.2.5] [1]<sup>1</sup>

### 3.5 element

combination of components that form the basic building block to perform a distinct function

NOTE 1 An element may comprise hardware, software, information and/or human components.

NOTE 2 For some systems, information and data are an important part of the system operations.

### 3.6 integrity

ability of a system to sustain its form, stability and robustness, and maintain its consistency in performance and use

## 4 System dependability engineering and applications

### 4.1 Overview of system dependability engineering

Dependability is the ability of a system to perform as and when required to meet specific objectives under given conditions of use. Dependability characteristics include availability and its inherent or external influencing factors, such as: reliability, fault tolerance, recoverability, integrity, security, maintainability, durability and maintenance support. The dependability of a system infers that the system is trustworthy and capable of performing the desirable service upon demand to satisfy user needs. The system objective, structure, properties, and influencing conditions affecting system dependability performance are described in IEC 62347 [2] which provides guidance for determination of relevant system functions for specifying system dependability.

There are four main aspects for engineering dependability into systems:

- a) **dependability process** – establishes the technical processes for engineering dependability into systems. The process consists of a sequence of activities implemented at each respective life cycle stage to achieve specific dependability objectives in system performance. The dependability process shall be fully integrated into the design and management processes;
- b) **dependability achievement** – implementation of the effective engineering effort and knowledge experience applied at appropriate system life cycle stages. The aim is for progressive accomplishment of dependability objectives of the constituent system functions suitable for subsystem realization and system integration (reliability growth);
- c) **dependability assessment** – evaluates the dependability attributes and determines their effectiveness when implemented into systems. The process identifies the specific dependability attributes to meet project needs and provides the methodology and rationale on how these attributes can be determined;
- d) **dependability measurement** – quantifies the dependability attributes for contracting, specification and assessment purposes. The process is to assign a quantitative value or number to designate a target entity representing a specific dependability characteristic.

<sup>1</sup> Figures in square brackets refer to the bibliography.

The aim is to express a statement of intent in quantifiable terms to facilitate mutual understanding of the issue involved and to serve as basis for negotiation in reaching agreements.

#### 4.2 System dependability attributes and performance characteristics

System dependability attributes are those specific dependability related features and time-dependent performance characteristics inherent in the system by design and construction. Some features, such as system performance characteristics can be quantified and measured. Other dependability features which are not quantifiable may present certain value or useful information pertinent to those attributes. These non-quantifiable features can be described in qualitative terms to establish its value for subjective dependability assessment. Both quantifiable and non-quantifiable features are important to describe the system dependability attributes. Examples of non-quantifiable features include product brand value, user friendly operation, and informative instructions. Examples of quantifiable performance characteristics include uptime duration, downtime frequency, mean-time-between-failures, and time for restoration from a degraded state back to normal system performance.

The main attributes of system dependability are as follows:

- a) **availability:** the ability of the system to be in a state to perform a required function when a demand is placed upon the system. Availability performance is characterized in terms of measures such as percentage uptime for the duration of system performance operation upon demand; outage frequency and downtime duration;
- b) **reliability:** the ability of the system to perform a required function for a given period of time under given conditions of use. Reliability performance is characterized in terms of measurements such as mean-time-between-failures and failure-free duration;
- c) **maintainability:** the ability of the system to be restored to a state in which it can provide a required function following a failure, or retained in such an up-state, under given conditions of use and maintenance. Maintainability performance is characterized in terms of measurements such as mean-time-to-restore and recovery time;
- d) **maintenance support:** ability of an organization to provide, when required, the resources required to maintain a system, under given conditions. Maintenance support performance is characterized in terms of measures such as utilization of maintenance resources, training needs, enabling tools and facilities, logistics delay time and turn-around time for spares provisioning.

There are other attributes related to dependability for specific system applications. They include but are not limited to:

- e) **recoverability:** ability of a system to be restored to a state in which it can perform a required function following a failure without repair of hardware or software. It is characterized in terms of measurements such as mean-time-to-recover;
- f) **testability:** ability of a system to be tested at designated maintenance levels for replace/repair action to determine fault coverage. It is characterized in terms of measurements such as percentage of test coverage;
- g) **service accessibility:** ability of a service to be obtained within specified tolerances and other given conditions when requested by the user. It is characterized in terms of measurements such as probability of access to a service;
- h) **service retainability:** ability of a service, once obtained, to continue to be provided under given conditions for a requested duration. It is characterized in terms of measurements such as probability of retention in time duration.

Recoverable performance is dependent on the design of system architecture, fault-tolerant and self-healing features incorporated into the system. Service performance is dependent on the properties of the system facilities, construction and infrastructure of resource deployment. The attributes of system performance in general are inherent in the system design. The performance attributes are derived from the capability of the system and the dependability feature of the system.

System performance characteristics are derived from time and incident measurements. An incident is an undesirable or unexpected event observed during system tests or in-service operation indicating that a failure might have occurred. All incidents should be recorded and investigated. This is to determine whether the incident is caused by a genuine failure, or it is due to human error or mistaken observation. A failure is a departure from the required performance functions of the system. However, at the time of observation, a failure may not cause complete cessation of the system functions, but may deteriorate system performance. The extent of deterioration before classification as failure should be defined and established for the measurements.

## **5 Managing system dependability**

### **5.1 Dependability management**

Dependability is a technical discipline and is managed by engineering principles and practices. IEC 60300-1 and IEC 60300-2 are used in this part of IEC 60300 for formulation of dependability management strategies and general application of technical approaches for implementation of dependability elements and tasks. Additional management processes are introduced to address system specific management issues. Dependability management involves project planning, resource allocation, dependability task assignments, monitoring and assurance, measurement of results, data analysis and continual improvement. Dependability activities should be conducted in conjunction with other technical disciplines to attain the needed synergistic effects and add values to the project outcomes. Project tailoring is emphasized for cost-effective management of system projects. Where applicable, life cycle cost analysis should be used for resource allocation and optimization for evaluation of acquisition and ownership costs.

### **5.2 System dependability projects**

Dependability is a key decision factor in project management. Dependability affects the cost of project implementation. It focuses on specific dependability application issues in project tasks that need effective resolutions. Dependability has extensive impact on the results in project deliveries to meet customer expectations. From a system engineering perspective, realization of dependability in systems is an important business decision issue that needs full integration of engineering and design with the management decision process. Managing obsolescence, project risk assessment, technical design trade-offs, life cycle costing, outsourcing and supply-chain coordination are some examples of dependability activities in systems engineering practices.

Not all projects involve complete new system development. Most systems are built by integration of subsystems and application of commercial-off-the-shelf products for realization of system functions. In major system development or for system enhancement projects, it may involve multiple developers of subsystems and subcontractors on supplies and services to achieve on-time project delivery of the system. In this respect, project management is essential for coordination of various project efforts. System dependability projects may involve specific dependability activities such as:

- a) adoption of new technology;
- b) development of dependability specifications for system and subsystems;
- c) dependability evaluation of commercial-off-the-shelf products for use in system functions;
- d) assessment of supplier's capability in fulfilment of dependability project requirements;
- e) assurance of dependability for system acceptance.

System dependability activities may occur at any stage of the system life cycle. Some dependability task assignments may demand special skills and training in specific technical disciplines such as software engineering, logistics support, and human reliability.

### 5.3 Tailoring to meet project needs

A system dependability project is initiated to resolve specific dependability issues of concern to the system. The purpose of tailoring is to manage the allocation of available project resources and select the appropriate methods for effective problem resolution. Examples of system dependability project activities appropriate for tailoring include:

- a) budget planning for allocation of dependability resources to meet project delivery targets;
- b) evaluation of alternative technologies for high reliability product acquisition;
- c) outsourcing of subsystem development to meet stringent criteria in software capability maturity model requirements where process monitoring is crucial;
- d) training time required to gain sufficient experience to use a new reliability analysis tool;
- e) selection of subcontractors for provision of on-site maintenance of critical systems for high availability performance expectations with no scheduled downtime permitted.

Guidelines for the tailoring process are described in IEC 60300-2.

### 5.4 Dependability assurance

Dependability assurance activities should form part of the quality assurance process for system dependability projects. This is to ensure that all planned and systematic activities implemented within the quality system, and demonstrated as needed, provide adequate confidence that the system and product quality requirements are fulfilled. Key activities involve project planning, technical and management responsibility assignment, verification of dependability assessment results, validation of dependability performance data for system acceptance, monitoring of dependability process effectiveness, failure reporting and data analysis for prompt corrective and preventive actions, documentation of relevant dependability information and maintenance of test records to support objective evidence, and management review to initiate process improvements. IEC 60300-2 provides additional information on selection of dependability program elements and tasks for tailoring of system dependability projects.

## 6 Realization of system dependability

### 6.1 Process for engineering dependability into systems

#### 6.1.1 Purpose of dependability process

Establishing a process is essential for successful management of project tasks and coordination of activities. The dependability process should be integrated into the technical processes to facilitate engineering dependability into the system. The dependability process provides specific inputs at major project decision points of the system life cycle to facilitate project implementation. These major decision points occur at the completion of critical project management phases for market identification, system development, product realization, system acceptance, in-service operation, enhancement and retirement. Dependability information is crucial at these major decision points to justify business investments.

#### 6.1.2 System life cycle and processes

The starting point for engineering dependability into a system should be at the earliest life cycle stage. The user should apply an effective engineering process at this life cycle stage.

The description of system life cycle stages can be viewed from a generic systems engineering perspective. There are other system life cycle descriptions. IEC 60300-2 describes the product life cycle phases from a project management view. ISO/IEC 15288 [3] provides a similar system life cycle description from an information technology and software engineering view. The guidance provided by this part of IEC 60300 is based on the concept of system life cycle stages, as described in Figure 1. System stages are precise technical transition points, whereas project phases may overlap by management discretions to reach major business

decisions. Project risk management as referred to in IEC 60300-2 applies throughout the life cycle processes.

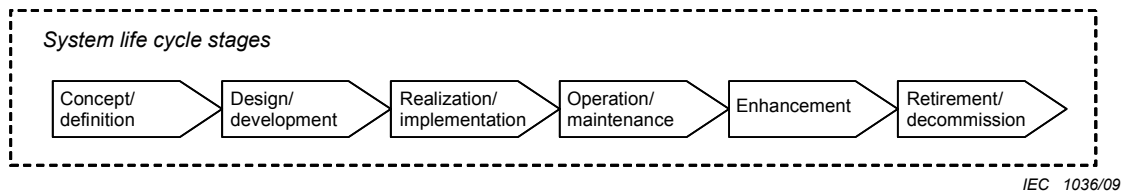


**Figure 1 – An overview of a system life cycle**

The technical processes for engineering consist of a sequence of process activities implemented at each respective life cycle stage to achieve the intended system performance and dependability objectives. Engineering dependability into a system is not completed in isolation. It is performed in conjunction with other technical disciplines (e.g. structural design) and supporting activities (e.g. quality assurance) for realization of system functions for their intended applications. Annex A describes a typical sequence of the system life cycle processes.

The key process activities in a system life cycle are as follows:

- a) requirements definition identifies the users' needs and constraints of system applications;
- b) requirements analysis transforms the users' view on system applications into a technical view for engineering the system and will include development of an operational use profile/timeline/design reference mission;
- c) architectural design synthesizes a solution that satisfies system requirements for operating scenarios by allocating the required system functions to hardware, software and human elements;
- d) functional design and evaluation determines the practical means for realizing the functions to facilitate design trade-off and optimization;
- e) system design documentation captures the system information, including dependability data, suitable for system design;
- f) system design and subsystem development creates the specified system and subsystem functions;
- g) realization produces the system and subsystem elements in hardware and software forms;
- h) integration assembles the system and subsystems consistent with the architectural design;
- i) verification confirms that the specified design requirements are fulfilled by the system;
- j) installation/transition establishes the system capability to provide the required performance service in a specified operational environment;
- k) validation/commissioning provide objective evidence that the system fulfils the functional requirements;
- l) operation engages the system to deliver its operational service;
- m) maintenance support sustains the system capability for operational service;
- n) enhancement improves the system performance with added features;
- o) retirement/decommissioning ends the existence of the system entity.

### 6.1.3 Process applications through the system life cycle

A process is an integrated set of interrelated or interacting activities that transforms inputs into outputs. Processes are used as reference models for functional organization (e.g. quality

management systems (QMS), project management), business transactions (e.g. acquisition, supply-chain agreement), and technical planning and implementation (e.g. product development, system assessments). This part of IEC 60300 focuses on the technical processes for engineering dependability into systems.

Figure 2 shows an example of a process model. In the context of engineering, the primary inputs usually consist of data providing a set of requirements, or the expressed needs of the customer. The outputs may consist of processed data describing a desired solution such as a specification, the fabrication of a product or the delivery of a service. There are other inputs associated with the process for controlling and enabling purposes. The process activities transform or convert the primary inputs to the desired outputs. This conversion is subject to the conditions set by the enabling mechanisms and associated influencing factors. Some influencing factors are controllable such as operating procedures for activating the process; others may be uncontrollable such as the weather conditions or sudden climate change. Enabling mechanisms such as methods and tools are essential for the conversion to take effects. This process model is used for implementing the technical processes described in this part of IEC 60300.

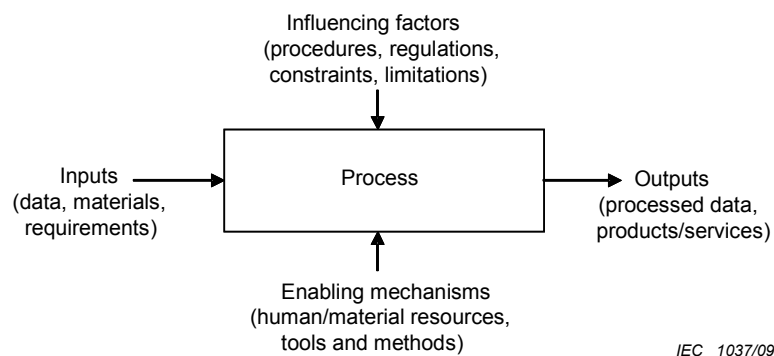


**Figure 2 – Example of a process model**

The technical processes serve two purposes:

- a) to perform engineering tasks and conduct re-engineering activities during system conception and development;
- b) to perform operation, maintenance and disposal activities with respect to the system.

The applications of technical processes are both recursive and iterative so as to complete the desired solution. This applies to all stages of the system life cycle. The relationships of the technical processes are independent of system size and structure. Process activities such as requirements definition, requirements analysis and architectural design are “top-down” technical approaches to engineer the desired solution (i.e. breaking the system down to its component elements); whereas integration and verification are “bottom-up” approaches to realize the system configuration and validate its performance (i.e. building the elements up to construct the system). The transition from “top-down” to “bottom-up” approaches during the implementation stage occurs at the completion of system installation where commissioning begins. This is known as the “V” model in engineering practice as described in ISO/IEC 15288 [3].

NOTE For further information on the “V” model refer to ISO/IEC/TR 15271 [4].

ISO/IEC 12207 [5] establishes a framework for software life cycle processes. It contains processes, activities and tasks that can be applied during the acquisition of a software product or service and during the supply, development, operation, maintenance and disposal of software products. ISO/IEC 12207 [5] can be used either alone or in conjunction with ISO/IEC 15288 [3].

Typical examples of process applications at each system life cycle stage can be found in Annex A. Knowledge of the system type and application environment is essential for tailoring the process application at the appropriate system life cycle stages in order to meet specific project needs.

## 6.2 Achievement of system dependability

### 6.2.1 Purpose of system dependability achievements

Achievement is the action of accomplishing an objective. It reflects the results brought about by successful problem resolution. The actions required for achieving system dependability can be accomplished by means of effective engineering effort and knowledge experience applied at appropriate system life cycle stages. The aim is for progressive accomplishment of dependability objectives of the constituent system functions leading to system integration. Achievement of system dependability is an important project objective that needs to be coordinated and demonstrated for system acceptance. System acceptance is usually a contractual agreement to meet customer requirements. The ultimate goal is to satisfy users' expectations of system performance.

### 6.2.2 Criteria for system dependability achievements

System dependability is achieved by successful incorporation of pertinent dependability attributes and related performance features into the system. The criteria for system dependability achievements should reflect:

- a) a sound understanding of system performance objectives;
- b) a sound understanding of operating conditions;
- c) the effective implementation of dependability principles into the operational infrastructure;
- d) the conditions of use;
- e) the application of appropriate processes for system realization;
- f) the utilization of knowledge and experience for cost-effective introduction of system services.

These criteria can be accomplished by focusing on key factors affecting dependability issues related to the system. The important criteria are identified which support process applications and realization of system objectives. Rationales are provided to clarify the significance of dependability implementation. These criteria should be considered in project planning and implementation. The user should tailor the appropriate dependability activities to meet specific project needs from a system life cycle perspective.

- 1) **dependability management policy** – this criterion influences the operational infrastructure, the allocation of appropriate resources, responsibility assignment for management accountability and dependability project leadership. The significance of dependability policy reflects a customer focus on dependability management strategy and commitments, collaborative effort, and systematic process approach towards effective application of dependability management principles as described in IEC 60300-1. The dependability management policy described in IEC 60300-1 applies throughout the engineering processes described in this part of IEC 60300;
- 2) **dependability knowledge base** – this criterion affects the accuracy of interpreting market needs, the adequacy of relevant information required for project initiation, the applications of available standards and specifications, the competitive leverage in contract negotiation and substantiation of dependability for objective evidence. The significance of dependability knowledge base lies in the market competitive advantage and technology leadership when dealing with new challenges in system dependability issues;
- 3) **design architecture** – this criterion affects the use of technologies for system applications, the selection of hardware, software, and human elements for realization of system functions, system integration and system in-service operation, and facilitating system enhancement and upgrade. Design architecture establishes a cohesive and

constructive framework for system integrity and realization. It facilitates capability enhancement, capacity expansion, cost-effective operation, and provision of quality of service. Appropriate technology utilization permits design trade-off by incorporation of advanced features and broadening the technical limits for applications;

- 4) **supply-chain cooperation** – this criterion affects make-buy decisions, outsourcing and subcontracting schemes, verification and validation procedures and documentations, and the monitoring and assurance processes. The significance of supply-chain management is based on purchaser-supplier cooperation and sharing of relevant information in the procurement and acquisition process. The supply-chain provides the necessary linkage for tracking important information. The impact on business is expediency in the administrative process, reduction in provisioning costs, and incentives for delivery of quality products and services;
- 5) **enabling systems** – this criterion affects the use of methods and tools, expediency of design throughputs, skills training needs, new product introduction and system deployment, maintenance and logistics support strategies. The significance of enabling systems is seen in the improvement of the design and delivery process and the effective utilization of methods and tools to expedite problem resolution. Enabling systems are not always technically complex requiring special skills for their comprehension and use. Some of the methodologies are simple checklists and instructions facilitating the operators and maintainers for on-site decisions to take proper actions. Further information on enabling systems is given in standard ISO/IEC 15288 [3];
- 6) **customer feedback and information management** – this criterion affects customer relations in terms of satisfaction and loyalty, provision of effective customer care services, accuracy in incident reporting, service data capture for analysis, effective implementation of corrective and preventive actions, establishment of system performance trends and records of dependability performance history. The significance of relevant feedback information is the ability to establish performance trends, identify critical areas requiring attention and provide objective evidence for verification and validation.

### 6.2.3 Methodology for system dependability achievements

The selection of applicable methods can proceed with the knowledge of criteria and the understanding of their significance for system dependability achievements. The objective is to utilize these methods to build dependability into the system. The application is aimed at incorporation of relevant dependability attributes into system functions.

The methodology for implementing dependability into system functions can be viewed from two perspectives:

- a) top-down approach to synthesize system dependability based on specified system requirements and market information to develop the system architecture;
- b) bottom-up approach to build dependability into system functions based on dependability design rules for simplification, fault tolerance, risk reduction and mitigation.

Both approaches involve the identification of dependability attributes and determination of their values. Dependability attributes are the fundamental measures for assessment and achievement of system dependability.

Dependability attributes that are relevant to system performance characteristics are time dependent. They can be quantified and derived from time and incident measurements. Examples include the percentage uptime for system availability performance, the probability of success of an operating system function with failure-free duration to demonstrate reliability, and the completion of system restoration within scheduled downtime to show expediency in maintenance support actions.

However, not all dependability attributes can easily be demonstrated due to time and cost constraints, technical limitations, or for other reasons related to the project. Examples include highly reliable complex systems, new systems with limited field deployment experience.

generic software systems for use in new application environment, and some commercial-off-the-shelf products with no performance reliability history. Other methods are needed to provide confidence for use and dependability assurance. It should be noted that system dependability attributes are stochastic or probabilistic in nature. They may encompass indirectly assessable features other than those performance characteristics that can be derived from direct measurements. Typical methods applicable include R&M case studies, simulated test cases, capability maturity models, and reliability growth programs.

Numbers and quantifiable values often need interpretation. A failure rate measurement may not be meaningful without proper reference to its context or explanation of the surrounding issues of concern. While the failure rate numbers may be used as indicators for comparison of alternative design options, the underlying assumptions are critical to support the rationale and justification. This allows application of statistical tools to determine inference bounds and confidence limits of potential risk exposures. In a business example, the mean-time-between-failures of a copying machine may not be too meaningful to the business owner, but the number of disposed void copies per month of machine usage would indicate the cost of wastage.

Annex B provides examples of applicable methods and tools to facilitate system dependability achievements. Knowledge of the system operating functions and its application environment described in Annex C is necessary for the selection of relevant methods and tools. Effective applications should focus on critical issues in solving technical problems. The limitations of these methods and tools for their specific applications should be noted to permit proper interpretation of results.

#### 6.2.4 Realization of system functions

System functions can be realized by using hardware, software, or human elements, or any of their combinations to achieve specific system performance objectives. The following describes the general issues related to the selection and application of these elements for successful dependability achievements.

- a) **Hardware element** – hardware is commonly used in system constructions. Hardware can consist of mechanical, electrical, electronic, optical, and other physical components. They are used in various configurations to realize the hardware functions. Most electronic products built today with hardware elements are relatively mature in technology applications. The design rules are well established. Electronic products exhibit consistency in production under controlled manufacturing process environment. Product quality and dependability can be ascertained by appropriate assurance programs. There are also ample 'experience' databases to support reliability performance of these hardware-based electronic products. However, some products with active electronic components are sensitive to varying application environments. The physics of failures of these components dominate the hardware failures and infant mortality phenomenon. Proper reliability design, packaging and screening can help significant reduction in early failures. Some hardware elements may wear-out due to operation or extensive use while others may have limited shelf-lives. These inherent reliability problems can be resolved by implementation of preventive and scheduled maintenance efforts. Hardware system structure is hierarchical. The maintenance support strategy can be deployed by proper functional design and packaging strategy of the lowest replaceable assembly or unit. This facilitates maintainability design and logistics support activities to improve system availability performance.
- b) **Software element** – software can consist of coded instructions, computer programs, established rules and procedures for system operation. Coded commands are used to instruct a software program for execution of system function for application. Software codes are difficult to test for coding errors unless it is run in actual computer operation. A software program error resulting in a system failure is due to the activation of a latent fault or "bug" within the software program. Software design disciplines are essential to minimize the potential of generating unintended errors in design. The approaches used include fault avoidance, fault removal and fault tolerance. They are formal methods in software design disciplines. Although software does not wear-out, its functions can deteriorate as a consequence of changes. Because the software is created in one form or

another by human origin, the design control disciplines are focused on the software design environment. Adopting an infrastructure using methodology such as the Capability Maturity Models as a framework for software development can facilitate the achievement of dependability in software functions. Software issues and versions for upgrades should be controlled by a system configuration management process to sustain interoperability of functions and enhance dependability in performance;

- c) **Human element** – human interactions with system operation can be viewed as part of the system functions or as an end user of the system. The role of the human in system performance can be beneficial with the human's ability to mitigate or control the on-going situations. However, most industrial incidents reported and major accidents studied can be traced back to human errors as the primary cause of system malfunction or disruption in performance service. Systems designed for human operation or use should incorporate human factors in the system design to minimize the risk of critical system failures, loss of properties, security violations or safety threats. Dependability can be achieved by application of human factors in design rules and simplification of tasks for human operation. The study of human factors involves a multi-disciplinary effort on gathering information about human capabilities and limitations for applications affecting human-system performance. The engineering aspects consist of the application of human factors information to the design of tools, machines, systems, tasks, jobs, and environment for safe, comfortable, and effective human use. Training and education are important prerequisites for any system operation requiring human interaction. Human factors standardization facilitates system integration, enhances interoperability of system elements, and improves serviceability and overall dependability performance.

Most system functions in today's electronic products use combined hardware and software elements in system designs. They offer a broad range of design features for diverse applications. Dependability of system functions is achieved by incorporation of design rules and established processes for applications. Design trade-off can be attained by proper combination of technologies suitable to meet specific application needs. Economic values can be gained through modular packaging and standardization for mass-scale production. System functions can be automated for self-checking to improve performance effectiveness by means of built-in-test or other monitoring schemes. Human intervention in system functions is only necessitated by safety and security regulations, or dictated by social and economic reasons. Annex D provides checklists for hardware, software, and human factor design applications.

#### 6.2.5 Approaches to determine achievement of system dependability

There are three generic approaches to determine that system dependability has been achieved. They serve different purposes with varying degree of engineering rigour. In practice, a combination of these approaches is likely to be used:

- a) **Demonstration** – this is achieved by means of actual system operation in an application environment over a scheduled time period to demonstrate dependability performance. Typical examples include:
- dependability performance history of systems in field operation;
  - formal reliability demonstration;
  - availability performance during warranty period.
- b) **Inference** – this is achieved by means of statistical methods using observed data of constituent system functions based on established criteria and assumptions to arrive at a numerical value representing system dependability attributes (characteristics / performance). Typical examples include:
- prediction of system of given configuration;
  - system simulation;
  - capability maturity models;
  - test case verification of system performance.

- c) **Progressive evidence** – this is achieved by progressive accomplishment of project milestones with auditable arguments to support objective evidence. Typical examples include:
- R&M case;
  - reliability growth program.

#### 6.2.6 Objective evidence of achievements

The following are key statements on system dependability characteristics for use as objective evidence to support system and product acceptance at applicable system life cycle stages. Objective evidence needs to be documented and authenticated for auditing and contracting purposes.

- a) a statement on system dependability attributes and operating environment to reflect user expectations in commercial specification or proposal based on market research information. This provides information to start project planning and develop system dependability specification;
- b) a statement on system performance characteristics in system dependability specification. This provides information for establishing dependability design objectives and system architecture;
- c) a statement on reliability and maintainability performance characteristics for each system function in functional design specification. This provides information for technology selection, make-buy decisions, and establishing procurement requirements;
- d) a statement on reliability and maintainability characteristics for system in-service operation and maintenance. This provides information for logistics support planning, contract maintenance, and special training needs;
- e) a statement on relevant dependability characteristics for product acceptance, verification compliance, and validation of system performance results. This forms the basis for fulfilment of contractual agreements for deliverable contract items;
- f) all dependability project reports containing dependability analysis data, test status and demonstration results. This provides information for project reviews, design changes, procedural updates, corrective and preventive actions for progressive improvement.

### 6.3 Assessment of system dependability

#### 6.3.1 Purpose of system dependability assessments

Assessment is an evaluation of the status or outcome of a specific dependability activity or issue. The purpose of assessment is to determine how a problem can be solved. The findings are used to support recommended actions with rationale and justification. The assessment process facilitates the identification of possible alternatives or options for resolution of the problem. This permits design trade-offs and preferred product selection. The assessment effort in system dependability should be tailored to meet specific project needs and for process enhancement.

#### 6.3.2 Types of assessments

Assessment can be objective or subjective. Objective assessment is by direct measurement of an entity to obtain the results. Subjective assessment is to assign a value on the nature, character, or quality of its findings. For example, to assess the quality of a software function in system application, we may gain insights on how the software is developed. Reviewing its design process to form a subjective opinion for appraisal could do this. The purpose is to ensure user confidence of the software's adequacy for application. We cannot be sure until we run the software in a computer system to ascertain its quality features in actual performance. This provides the crucial demonstration for objective evidence. In engineering practice, both objective and subjective assessments are used which complement each other in the evaluation process.

The following provides major project objectives associated with the assessment of system dependability at major decision points of the system life cycle:

- a) **market identification** – the objective is to identify the market needs to justify investments for new system development or enhancing an existing system for competition. Market analysis is essential to justify major investments involving resource commitments. Systems engineering activities involve capability and resource identification, evaluation of new technology for feasible application, competitive analysis and user expectation of system performance, the extent of maintenance support necessary to sustain new or enhanced service operation, time and cost constraints for market entry and regulatory and environmental impact on system introduction. Initial system structure and configuration should be considered to meet applicable system operating scenarios. System life cycle costs should be examined on a return-on-investments basis. Key dependability assessment to support market identification include:
- prediction of system dependability to meet anticipated market needs;
  - evaluation of new technology maturity suitable for system applications affecting dependability performance;
  - identification on critical dependability issues relating to serviceability impact and operability influence;
  - dependability capability evaluation of potential suppliers and subcontractors;
  - assurance of continuation of maintaining service, availability and safety until the system is fully retired.
- b) **system design and development** – the objective is to rationalize the system design approach and evaluate design alternatives and options. The selected design is followed by system development. This is a major commitment to both capital and resource investments. System engineering activities involve requirements analysis, architectural design configuration, functional design and technology evaluation, outsourcing of subcontract work and selection of suppliers, system realization and integration, qualification testing and verification, system installation and transition for the required operation services. Key dependability assessment to support design and development decision include:
- evaluation of system functions affecting dependability performance;
  - evaluation of system structure for reliability optimization of system configuration;
  - evaluation of access for maintenance;
  - system availability performance simulation and performance evaluation to determine critical system malfunction, failure mitigation and service support needs;
  - reliability verification and problem analysis for corrective actions;
  - evaluation of dependability programs of suppliers and subcontractors;
  - manufacturability assessment for production yield affecting reliability growth;
  - evaluation of reliability warranty incentives and logistics support requirements.
- c) **system realization and implementation** – the objective is to execute make-buy decisions for acquisition and deployment of subsystem elements, and to implement resource commitments for system construction and integration. Key dependability assessment to support system realization and implementation include:
- assessment of system elements and COTS products conformance to dependability requirements for subsystem integration;
  - assessment of subsystem conformance to dependability requirements;
  - assessment of quality assurance process;
  - evaluation of subsystem test performance results for system integration;
  - evaluation of system test performance results for preparation of system acceptance.
- d) **system acceptance for in-service operation** – the objective is to assure customer confidence for system acceptance. This involves the hand-over of responsibility to the customer for in-service operation. It initiates the warranty period to ensure system

performance meets the end users' expectations. Key dependability assessment to ensure system acceptance include:

- evaluation of system performance by introduction of field tracking and incident reporting schemes;
  - assess training needs and competency of customer operators and maintainers;
  - establishing a focal point for data collection and incident report analysis to determine dependability performance trends and criticality of system malfunction requiring immediate corrective actions;
  - evaluation of system maintenance service and logistics support effectiveness;
  - procedures for design change authorization and configuration management.
- e) **system enhancement** – the objective is to justify investment for enhancement, or upgrading of the existing system. This involves similar activities as for new system design and development for the enhancement part of the system. The legacy issues of the existing system shall be addressed to ensure interoperability and capability improvement of service. Key dependability assessment to support system enhancement decision includes:
- cost benefits analysis for change incorporation;
  - evaluation of dependability performance impact due to changes with added new features;
  - customer reaction to proposed changes;
  - risk and value assessments.
- f) **system retirement** – the objective is to retire the system from service. Key dependability assessment to support retirement decision include:
- evaluation of cost impact for termination of system service;
  - evaluation of regulatory and environmental impact for termination of system service.

### 6.3.3 Methodology for system dependability assessments

The assessment methodology addresses the implementation issues concerning processes, approaches and strategies.

The assessment methodology embraces two important processes:

- a) **verification** – the verification process is a method of confirming the assessment results. It should be conducted to support major decision points at each system life cycle stage.
- b) **validation** – the validation process provides objective evidence that the system meets the actual requirements and satisfies user expectations.

The approaches for assessment are often unique to suit various project implementation situations. They include a combination of the following approaches:

- 1) **analytical approach** – this involves activities such as design analysis, system performance simulation, standardization conformance, and compliance specification evaluation.
- 2) **experimental approach** – this involves activities such as performance testing and technical evaluation of system functions, physical assemblies, suppliers' products, subsystems integration, and the actual system acceptance.
- 3) **consultative approach** – this involves activities such as expert reviews, use of industry best practices, suppliers' consultation on product information, customer survey and user feedback, supply-chain participation, infrastructure development and enhancement.
- 4) **negotiated approach** – this involves activities such as establishing acceptable risk limits for system operating exposure to the environment, conditions for product deployment in specific regions, recycling of by-products and waste disposals, economic incentives and social benefits in contract agreements, and compliance to changing regulations.

The assessment strategies should focus on two main aspects in engineering dependability into systems:

- i) **application focus** – this relates to meeting project specific applications for compliance of contractual requirements. The essential assessment activities are focused on the evaluation and analysis of system dependability at major decision points of the applicable system life cycle. The methods and tools deployed for assessment are commonly used for product verification and system or subsystem validation.
- ii) **technology focus** – this relates to technology evaluation of design strategy and system support schemes to facilitate dependability performance achievements. The essential assessment activities are focused on evaluating the technology leverage that can be exploited for the system designs, and determining the viability of enabling systems to support continuity of system in-service operation. Issues concerning technology evolution and obsolescence should form part of the assessment strategies.

#### 6.3.4 Assessment value and implications

Assessment is a prerequisite and crucial input for decision-making in projects. The assessment effort should be rationalized for practical application. The resolution of the issues of concern should be completed within reasonable time limits to realize the expected value or benefits to the project. This would establish the needed confidence to support project decisions. The following key issues that exemplify the value of assessment are noted for illustration. Typical examples are shown to highlight their major implications to the project outcomes.

- a) Timing of assessment is crucial to provide meaningful results. The assessment value greatly diminishes when the assessment results are not available at the time needed to support major decisions. For example, a reliability prediction conducted during system design may provide valuable insights into the proper technology selection, architectural design structure, partitioning configuration, and choice of system elements and components for realizing system functions. A prediction done after design completion has limited value when the system is configured and ready for production.
- b) Justifying the cost benefits of the assessment prior to its initiation is prudent for project planning and effective management. For example, the “plan-do-check-act” process in quality management systems (QMS) is commonly used as basis for planning assessment activities. Investment analysis related to assessment is critical to justify major capital expenditures and new acquisitions.
- c) Ensuring the infrastructure support is adequate for implementation of assessment tools. This may involve technical procedure changes and cultural adjustments that would consume both time and effort. For example, migrating from the software capability maturity model process to the software capability maturity model integration process is a major endeavour for any corporation. Both technical resources and management culture would need adjustments to attain the industry recognized status and certification.
- d) Contingency planning is essential to avoid unexpected project outcomes or unscheduled delays. This may impact resource allocation and work redeployment, supply-chain distribution and delivery of supplier products, and affect the scheduled commitments for system commissioning and customer acceptance. For example, at major decision points, contingency plans should be included as part of the assessment process, such as identifying alternate suppliers in case of supplier disruption, the deployment of technical expertise to work on critical designs to meet stringent delivery targets, and exploring the means of viable financing for capital investments.

### 6.4 Measurement of system dependability

#### 6.4.1 Purpose of system dependability measurements

From an engineering perspective, system dependability measurements represent the process of assigning quantitative value to characterize the dependability attribute. The quantitative value is derived from observed or estimated data on time duration and the number of incident occurrences to reflect the dependability performance characteristics. The measurement process involves:

- a) identifying the type and objective of measurement under contractual, operational, or for specific conditions such as product evaluation requiring quantification of dependability attributes;
- b) determining the relevant data and the nature of the data sources for measurements;
- c) utilizing effective enabling systems to facilitate the measurement process such as deployment of data collection systems, failure reporting, analysis and corrective action systems, survey questionnaires, or other support schemes;
- d) interpreting the measurement results to establish performance trends, identify critical issues, and recommend management actions with rationales and justifications;
- e) documenting the measurement findings for record retention, quality audits, and objective evidence.
- f) ISO/IEC 15939 [6] defines a measurement process applicable to system and software engineering.

#### 6.4.2 Classification of system dependability measurements

There are four general classes of dependability measurements to meet specific project needs.

- a) **Measurement of inherent system dependability attributes** – the objective is to assign numerical figure-of-merits to represent the inherent dependability attributes of the system. This class of measurement is useful for comparison of dependability attributes of different design architectures and system configurations. The measurement process is conducted during system concept/definition stage to determine the inherent dependability performance capability of alternate options. The purpose is aimed at providing evidence of the system capability in meeting dependability objectives for proposal or contract inquiries. The numerical values can be stated in terms of probability of success, mean operating time between failures, life times or failure rates that quantify the system availability or reliability performance characteristics. The measurements are commonly carried out by prediction methods as described in IEC 60300-3-1 [7].
- b) **Measurement of system dependability for performance evaluation and in-service operation** – the objective is to assign a number to designate system dependability performance in actual operation. This class of measurement is useful for assessment of dependability attributes during design/development stage where products and subsystems are tested to verify the adequacy of performance. It is also used during the system operation/maintenance stage to determine compliance to established operational objectives for dependability achievements. The measurement process is conducted by progressive testing of products, subsystems and the integrated system for performance verification and validation, and by tracking performance status of the system in-service operation. The measurement data come from product qualification tests, suppliers test results on subsystems, acceptance testing, and field performance records and incident reports. The numerical values can be stated as reliability, failure probability, failure free time (time to first failure), lifetime, percentage uptime (availability), outage frequency and duration.
- c) **Measurement of system dependability for performance improvements** – the objective is to assign value to quantify and qualify the degree of customer satisfaction, or to determine the extent of customer value for performance improvements. This is an indirect measurement that helps to identify the impact of significant dependability attributes in system performance. This class of measurement is aimed at seeking direct user feedback on system performance, or to determine the value of service provision during system operation/maintenance stage. The measurement process is conducted by means of customer surveys, performance audits, value assessments, and direct contacts and dialogues with customers and suppliers. Customer satisfaction surveys are focused on identifying current issues of customer concerns. Quality function deployment is commonly utilized for performance value assessment to defining customer needs and translating them into appropriate technical requirements for actions in meeting those needs. The value assignment can be stated in a scale of 1 to 5 inclusive to indicate ratings such as from poor to excellent.

- d) **Measurement of system dependability for risk exposures** – the objective is to assign numerical values to indicate the extent of risk exposures when the system is used for safety and security applications. This is an indirect measurement to identify the criticality of the dependability attributes affecting system performance functions. This class of measurement is conducted during system concept/definition stage to identify critical system functions and elements for specific system operation or mission. The assessment process includes the determination of threat or harm by designation of its severity and frequency of occurrence. The classification of risks can be established qualitatively by a range of catastrophic, critical, major, minor or negligible events. Probabilistic values can be assigned to indicate the severity of the situation by a statement such as a critical failure occurring once in every 10 years. IEC 60300-3-9 [8] describes the technological risk assessment methods affecting the dependability attributes of system performance. A similar method is used in the IEC 61508 series [9] on safety-integrity levels for ranking safety functions (refer to IEC 61508-1 [10] for more details).

#### 6.4.3 Sources of measurements

Measurements of system dependability attributes can be ascertained by direct performance testing under simulated conditions or in actual operating environment where the relevant data can be collected. System dependability attributes can also be assessed by means of predictions based on field performance history of similar systems, or they can be derived from established reliability database with knowledge of the system configuration and the operating functions of its constituent system elements.

Measurement data related to dependability attributes can also come from other sources such as suppliers test programs, maintenance support data, warranty information, and customer surveys. It is important that the integrity of the data used for dependability assessment be validated for assurance purposes.

#### 6.4.4 Enabling systems for dependability measurements

Data integrity in dependability measurements is important to assure the accuracy, credibility and consistency of the data acquisition and collection process. It ensures that relevant data are used correctly in data analysis and permits proper interpretation of the analysis results. The system design and format should be simple and straightforward to capture relevant information needed. Automated data entries and interactive web-based information access would enhance expediency for system implementation. There are various supporting systems utilized in engineering practice to enable cost-effective data collection and facilitate dependability measurements. These systems are essential parts of the dependability management system infrastructure. For their specific supportive roles, these systems can be classified as enabling systems to facilitate engineering dependability into the system of interest. Typical enabling systems commonly used for data collection, incidents reporting, problem analysis and corrective action include:

- a) failure reporting, analysis and correction action system to capture non-conformance information and test failure data during system development, testing and integration;
- b) test yield data acquisition system to capture manufacturing anomalies to track production yield rates for problem identification and root-cause analysis during product assembly;
- c) incidents reporting during system in-service operation to capture incidents affecting the continuity of system performance service, report on-site maintenance actions, assign criticality of the incident, and record follow-up support requests and time required for resolution;
- d) spares provisioning system to capture spares consumption data and turn-around-time for spares replenishment, spares distribution, and stock reordering;
- e) information feedback system to capture customer complaints, suppliers concerns, and employee suggestions for infrastructure improvement, strategic planning, and problem resolution that add value to projects and organizational management.

#### 6.4.5 Interpretation of dependability measurements

The proper interpretation of measurement results is essential for prompt corrective and preventive actions to support cost-effective operation. The following examples show the importance of measured or analysed data when transcribed and interpreted for follow-up actions.

- a) The acquisition and collection of relevant data should provide value to meet current project needs. This infers proper planning and design of experiments. It takes time and effort to acquire data. If such data cannot be used to help resolve current problems, then it should not be collected. The objectivity of the measurement process should be clearly defined. For example, the collection of field performance data of old systems deployed many years ago that are no longer in production nor supported would not be too useful for the new system design using a different technology.
- b) The transcribed measurements and interpreted results should present logical conclusion for recommended actions. The measured data and captured information should permit further analysis if necessary to support the underlying rationales or arguments in reaching a logical decision to justify the recommended actions. It should be noted that different interpretation of dependability measurements may lead to diverse understanding by the recipients, usually someone who needs the information for making decisions. For example, an availability performance number of 99,999 7 % assigned to a switching system may be an appropriate number to use in probability calculation of system functions, but it would be difficult to devise a scheme for system availability demonstration.
- c) The dependability problems identified should address the criticality of the issues at hand to alert management actions. Such problems identified in a process of concern regarding dependability usually occur under situations that may cause significant safety or security impact if not promptly attended to. These dependability issues may have potential liability issues and risks exposure if not properly assessed at the time they occur. System in-service operation follows established operating procedures. System outage incidents are reported according to on-site assessment of their criticality. Some critical issues should be resolved immediately or within a limited time period. Other non-critical issues may be deferred to a later system update or maintenance enhancement. For example, a field modification of a system design to fix a temporary problem without proper design change authorization may create unknown long-term safety hazards. Temporary software patches to fix a localized problem without thorough investigation may lead to security violation or crashing the entire system operation. Dependability design may incorporate fault-tolerant protection features. Such protection features are no longer effective if they have been disarmed or disconnected due to a bypassing of access for temporary fixes without proper authorization. Interpretation process should identify and alert potential problem issues to avoid the reoccurrence of such incidents. Warning signs and labels placed in proper locations could draw attentions.

## Annex A (informative)

### System life cycle processes and applications

#### A.1 System life cycle processes

##### A.1.1 Description of system life cycle processes

Figure A.1 provides a logical sequence of process activities applicable to each stage of the life cycle for engineering dependability into the system.

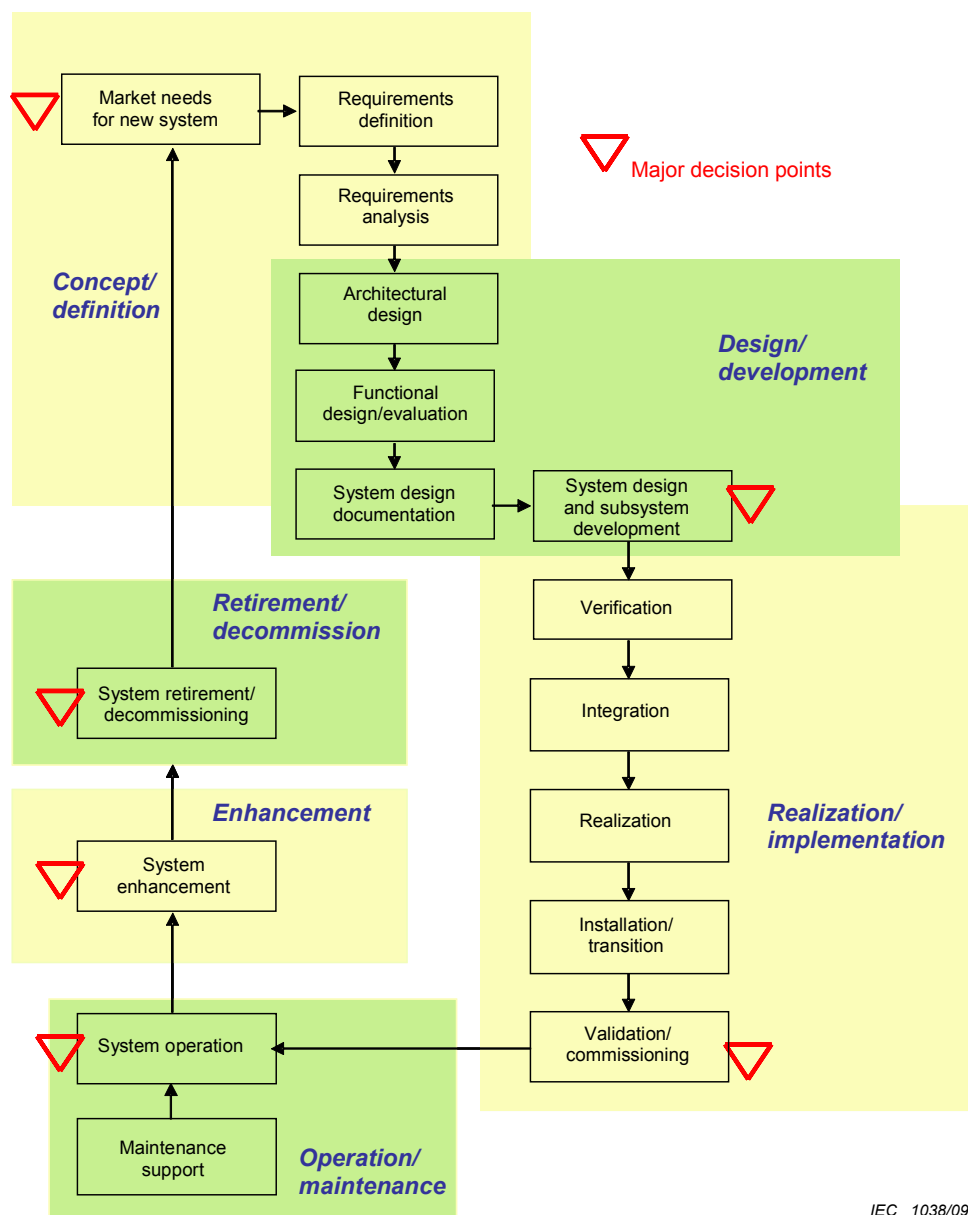


Figure A.1 – Overview of system life cycle processes

The first three stages of the system life cycle, i.e. concept/definition, design/development, and realization/implementation, before transition to operation/maintenance stage, overlap each other due to iteration of the processes. This indicates the need to provide continuity of workflow depending on the project needs. The extent of engineering effort crossing the arbitrarily defined boundaries of adjacent stages is dependent upon the project timeline and coordination activities. This can also be used to acquire sufficient system information to support the technical and business decision-making process. The following provides a brief description of each stage of the system life cycle:

- a) The **concept/definition** stage is to identify the market needs, define/identify the operational use environment/timeline, define preliminary system requirements and confirm feasible design solutions by producing technical specifications for the system design. Selection of design options is based on risk analysis, impact evaluation, and practical engineering approaches. The process activities involve requirements definition, requirements analysis, architectural design, and functional design/evaluation to provide high-level system specifications.
- b) The **design/development** stage is to plan and execute selected engineering design solutions for realization of system functions. This is transcribed into appropriate system development effort including engineering modelling, prototype construction, risk assessment, and interface identification of system and subsystem elements. Systematic evaluation of the integrated system functions is conducted to verify interoperability of system performance and interactions with external environments to validate final system configuration. Maintenance support planning, maintenance access, operation procedures, and assurance as well as support processes should be well established prior to system realization.
- c) The **realization/implementation** stage is to execute make-buy decisions for acquisition and deployment of subsystem elements. The realization efforts deal with activities such as technology applications, manufacturing, packaging and supplies sourcing to ensure the complete transformation from system design to the specified product or subsystem elements. The realized products or elements may comprise a combination of hardware and software functions. Implementation includes such activities as integration of system functions, verification of subsystems, and installation of the system. System acceptance procedures should be established with the customer for system trials in the actual operating environment prior to commissioning. Validation should be a part of the trial to provide objective evidence of conformance to system specification. It should be noted that verification and validation are activities that take place at each life cycle stage and not just at system integration as indicated in Figure 2.
- d) The **operation/maintenance** stage is used to deploy the system for delivery of service and to support system operational capability by means of maintenance. The process activities include operating and maintaining the system for service in accordance with system performance requirements, operators and maintainers training to maintain skills competency, customer interface to establish service relationship, and record keeping on system performance status and reporting failure incidents to initiate timely corrective and preventive actions. The system performance should be monitored and checked on a regular basis to ensure that reliability and quality of service objectives are met.
- e) The **enhancement** stage is to improve system performance with added features to meet growing user demands on the system. The process activities include software upgrade, hardware addition, skills training, simplifying procedures to improve operational efficiency, obsolescence management, organizational restructuring to increase expediency and customer value.
- f) **retirement/decommissioning** stage is to end the existence of the system entity. Upon termination of system service to the customer, the system may be disassembled, redeployed for other use, or disposed of where possible without affecting the environment. For complex systems, a strategy for decommissioning should be established to formalize planning and implementation of the decommissioning process to meet regulatory requirements. For consumer products regulatory rules concerning return and reuse or disposal may be in existence.

### A.1.2 Process activities for system life cycle stages

Figure A.1 also shows the linkage of process activities from stage to stage in a system life cycle. Major decision points are shown to indicate the start and end of the process activities at each stage where resource commitments are made to advance the technical processes. Relevant data are captured during the process activities. They provide the essential information for life cycle cost analysis and risk evaluation to support technical resolutions and business decisions.

The relevant data captured includes the key inputs necessary to initiate the process activities of each stage, the major dependability activities to be performed, the relevant influencing factors for consideration, and the outputs resulting from the process generated efforts. When possible, the priority and impact relevant to the process activities should be indicated. This provides useful information for risk assessment and life cycle costing. Where appropriate, the technical approaches and engineering methods used for the process activities should be identified.

## A.2 Examples of engineering process applications

### A.2.1 Process for the system concept/definition stage

Inputs:

- customer requirements, needs and wants;
- regulatory requirements related to health, safety, security, and environmental concerns;
- company policy on bid decisions;
- market intelligence and competitions.

#### *Key process activities*

#### *Dependability related activities*

| <i>Requirements definition</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>• Identify customer of the system, how the system is to be used, and for how long.</li> <li>• Identify system application environments.</li> <li>• Identify constraints related to potential system solutions.</li> <li>• Identify legacy issues related to interoperability with existing systems.</li> <li>• Establish system operating profile.</li> <li>• Document system specification.</li> <li>• Identify schedules and system deliverable targets.</li> <li>• Respond to customer RFP (request for proposal) if applicable.</li> </ul> | <ul style="list-style-type: none"> <li>• Identify dependability needs associated with the system applications.</li> <li>• Identify system availability and allowable outage downtimes acceptable by the customer</li> <li>• Identify technology constraints related to the scope and extent of achieving dependability objectives.</li> <li>• Gain knowledge of field performance history of existing or similar systems if available.</li> </ul> |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><i>Requirements analysis</i></p> <ul style="list-style-type: none"> <li>• Determine system boundaries, operating functions and performance characteristics from the set of defined system requirements.</li> <li>• Evaluate the constraints identified affecting architectural design.</li> <li>• Determine technical approaches and feasibility for system realization.</li> <li>• Determine technical and quality measures enabling system assessments.</li> <li>• Identify capability to undertake the system work.</li> <li>• Identify potential partnership and suppliers requirements.</li> </ul> | <ul style="list-style-type: none"> <li>• Determine operating scenario for dependability assessments.</li> <li>• Define system failures and performance degradation limits.</li> <li>• Identify risk exposures and criticality of system failures.</li> <li>• Determine the number of maintainers and their associated skill level required.</li> <li>• Analyse system structure and breakdown of system functions.</li> <li>• Analyse system availability contributed by functional configuration of architectural design.</li> <li>• Perform fault tree analysis to determine critical areas requiring design attention.</li> <li>• Conduct system level failure modes and effects and criticality analysis to support design alternatives and justifications.</li> <li>• Evaluate system availability and cost trade-off affecting design options.</li> <li>• Determine means for dependability assessments.</li> </ul> |
| <p><i>Architectural design</i></p> <ul style="list-style-type: none"> <li>• Determine appropriate logical architectural design options.</li> <li>• Establish system configuration.</li> <li>• Partition system functions.</li> <li>• Establish design criteria and interfaces.</li> <li>• Formulate make/buy decisions of system functions.</li> <li>• Select technologies for design and choice of hardware/software for realization of functions.</li> <li>• Formulate solution to meet system requirements.</li> <li>• Establish means for verification and integration of system functions.</li> </ul> | <ul style="list-style-type: none"> <li>• Establish plan for dependability evaluation.</li> <li>• Availability allocation of system functions.</li> <li>• Determine failure criteria of system functions.</li> <li>• Evaluate reliability of each partitioned function and recommend alternate design options if required.</li> <li>• Identify critical functions requiring attention.</li> <li>• Establish maintainability criteria for design.</li> <li>• Establish testability of system function for diagnostics and recommend maintenance actions.</li> </ul>                                                                                                                                                                                                                                                                                                                                                         |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>Functional design/evaluation</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <ul style="list-style-type: none"> <li>• Formalize the functional design process.</li> <li>• Identify design composition of hardware/software elements for each function.</li> <li>• Incorporate test functions for performance verification.</li> <li>• Establish human factors design criteria.</li> <li>• Establish environmental design criteria.</li> <li>• Establish ergonomics design criteria.</li> <li>• Establish EMC design criteria.</li> <li>• Establish safety, security and reliability design criteria.</li> <li>• Establish hardware design rules.</li> <li>• Establish software maturity design schemes.</li> <li>• Simulate system performance at the functional level to determine fault coverage and system recovery strategy.</li> <li>• Verify performance limits and interoperability of the functional design to meet architectural design requirements.</li> </ul> | <ul style="list-style-type: none"> <li>• Conduct reliability assessment.</li> <li>• Conduct maintainability evaluation.</li> <li>• Conduct functional level failure modes and effects and criticality analysis.</li> <li>• Conduct functional level design trade-off, fault tolerance and risk evaluation.</li> <li>• Establish maintenance and logistics support plan.</li> <li>• Establish process for supplier evaluation for quality assurance and reliability conformance.</li> <li>• Establish process for commercial off-the-shelf product evaluation and acceptance.</li> </ul> |
| <i>System design documentation</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <ul style="list-style-type: none"> <li>• Document system specifications.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | <ul style="list-style-type: none"> <li>• Incorporate dependability requirements in system specifications.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

Influencing factors for consideration:

- competitions;
- economic issues;
- technology issues;
- capability issues;
- environmental issues;
- legal issues;
- timing for investments issues.

Enabling mechanisms for process applications:

- human resources;
- financial resources;
- facilities;
- integrated design and implementation processes;
- assurance process.

Outputs:

- system specifications;
- systems design knowledge.

## **A.2.2 Process for the system design/development stage**

Inputs:

- system specifications;
- architectural design requirements;
- dependability plan.

| <i>Key process activities</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | <i>Dependability related activities</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>System design</b></p> <ul style="list-style-type: none"> <li>• Establish system design/development plan.</li> <li>• Specify system/subsystem interface requirements.</li> <li>• Establish linkage with interacting systems.</li> <li>• Establish human interface requirements.</li> <li>• Establish configuration management plan and design change procedures.</li> <li>• Establish physical dimensions and standardize assembly footprints.</li> <li>• Establish emission and susceptibility rules for facility construction, cabling and wiring inside and outside of buildings and equipment housing structures.</li> <li>• Reach agreements with suppliers for development and acquisition of hardware/software elements.</li> <li>• Initiate prototype construction of subsystems.</li> <li>• Establish system integration procedures.</li> <li>• Establish test plan and system acceptance criteria.</li> <li>• Establish system monitoring, diagnostic schemes, incidents reporting and data management system.</li> <li>• Establish training programs.</li> </ul> | <ul style="list-style-type: none"> <li>• Establish system dependability program.</li> <li>• Establish quality assurance program.</li> <li>• Formalize dependability requirements for system, subsystems and functions.</li> <li>• Establish suppliers' dependability programs.</li> <li>• Establish dependability acceptance criteria and reliability growth programs.</li> <li>• Establish system maintenance and logistics support program.</li> <li>• Establish failure reporting, analysis, data collection and feedback system.</li> <li>• Define human reliability criteria.</li> <li>• Define warranty conditions.</li> </ul> |
| <p><b>Subsystem development</b></p> <ul style="list-style-type: none"> <li>• Initiate in-house development for subsystems.</li> <li>• Initiate interface development for interoperability.</li> <li>• Monitor and collaborate with material outsourcing and contracting external development efforts.</li> <li>• Prepare production plan.</li> <li>• Prepare operation plan.</li> <li>• Prepare maintenance and logistics support plan.</li> <li>• Prepare packaging, handling, storage and transportation plan.</li> <li>• Prepare installation plan.</li> <li>• Prepare integration plan.</li> </ul> <p>NOTE The listed plans may be integrated as activities in the master project plan for ease of update and coordination of project activities.</p>                                                                                                                                                                                                                                                                                                                        | <ul style="list-style-type: none"> <li>• Implement subsystem dependability program.</li> <li>• Implement supplier's dependability program.</li> <li>• Develop spares provisioning program.</li> <li>• Develop software test and diagnostic program.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                       |

Influencing factors for consideration:

- availability and access to relevant skills resources;
- commitment targets for development schedules;
- project risks.

Enabling mechanisms for process applications:

- availability of specific tools required for development;
- training needs.

Outputs:

- system prototype;

- system and subsystem support requirements.

### A.2.3 Process for the system realization/implementation stage

Inputs:

- system prototype.

| <i>Key process activities</i>                                                                                                                                                                                                                                                                                                                                                                                                        | <i>Dependability related activities</i>                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Realization</b>                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                             |
| <ul style="list-style-type: none"> <li>• Carry out physical production of subsystems.</li> <li>• Realize construction of hardware/software elements.</li> <li>• Perform test evaluation of functions.</li> <li>• Carry out training of operators and maintainers.</li> <li>• Ensure test equipment and test facility are ready.</li> <li>• Ensure packaging, handling, storage and transportation instructions are ready.</li> </ul> | <ul style="list-style-type: none"> <li>• Implement system dependability program.</li> <li>• Implement quality assurance program.</li> <li>• Implement suppliers' dependability programs.</li> <li>• Implement system maintenance and logistics support program.</li> <li>• Implement failure reporting, analysis, data collection and feedback system.</li> </ul>                           |
| <b>Integration</b>                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                             |
| <ul style="list-style-type: none"> <li>• Execute integration plan.</li> <li>• Assemble and integrate system entity.</li> <li>• Prepare verification and validation plans and procedures.</li> <li>• Prepare system acceptance plan.</li> </ul>                                                                                                                                                                                       | <ul style="list-style-type: none"> <li>• Implement integration related system dependability program.</li> <li>• Implement integration related quality assurance program.</li> </ul>                                                                                                                                                                                                         |
| <b>Verification</b>                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                             |
| <ul style="list-style-type: none"> <li>• Implement verification plan.</li> <li>• Document verification test results.</li> <li>• Prepare system acceptance plan.</li> <li>• Check verification results against system acceptance plan</li> </ul>                                                                                                                                                                                      | <ul style="list-style-type: none"> <li>• Conduct subsystem dependability assessments</li> <li>• Document failure reports from verification tests.</li> <li>• Generate incident reports for recommended corrective/preventive actions.</li> <li>• Resolve anomalies found during verification.</li> </ul>                                                                                    |
| <b>Installation/transition</b>                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                             |
| <ul style="list-style-type: none"> <li>• Execute installation plan.</li> <li>• Document installation records and procedures.</li> <li>• Evaluate transition strategy for improvement.</li> </ul>                                                                                                                                                                                                                                     | <ul style="list-style-type: none"> <li>• Establish shared maintenance support and reporting schemes with customer maintainers on system installed on customer premises.</li> <li>• Monitor turn-around-time for system restoration and replenishment of spares.</li> <li>• Maintain adequate spares inventory on maintainer's/customer's site.</li> </ul>                                   |
| <b>Validation/commissioning</b>                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                             |
| <ul style="list-style-type: none"> <li>• Implement validation plan.</li> <li>• Document validation test results.</li> <li>• Execute system acceptance plan.</li> <li>• Implement warranty schemes if applicable.</li> <li>• Customer sign-off for system acceptance to initiate system operation.</li> </ul>                                                                                                                         | <ul style="list-style-type: none"> <li>• Validate that system performance fulfils the dependability requirements.</li> <li>• Document failure reports from validation tests.</li> <li>• Generate non-conformance reports for recommended corrective/preventive actions.</li> <li>• Resolve anomalies found during validation.</li> <li>• Resolve warranty issues with customers.</li> </ul> |

Influencing factors for consideration:

- transition management;
- commitment targets for system delivery schedule;

- warranty requirements and incentives.

Enabling mechanisms for process applications:

- project management;
- customer training.

Outputs:

- system operation for service;
- customer support.

#### **A.2.4 Process for the system operation/maintenance stage**

Inputs:

- system in full service operation.

| <i>Key process activities</i>                                                                                                                                                                                                                              | <i>Dependability related activities</i>                                                                                                                                                                                                                    |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Operation</b>                                                                                                                                                                                                                                           |                                                                                                                                                                                                                                                            |
| <ul style="list-style-type: none"> <li>• Implement operation strategy.</li> <li>• Monitor system performance.</li> <li>• Provide customer value.</li> </ul>                                                                                                | <ul style="list-style-type: none"> <li>• Implement reliability growth program.</li> <li>• Implement field data collection system.</li> <li>• Conduct customer satisfaction survey.</li> </ul>                                                              |
| <b>Maintenance</b>                                                                                                                                                                                                                                         |                                                                                                                                                                                                                                                            |
| <ul style="list-style-type: none"> <li>• Implement maintenance support strategy.</li> <li>• Monitor system maintenance efforts.</li> <li>• Provide customer care service.</li> <li>• Implement maintenance activities for adaptive corrections.</li> </ul> | <ul style="list-style-type: none"> <li>• Analyse failure trends.</li> <li>• Conduct root-cause analysis of problem areas.</li> <li>• Recommend design or procedural changes for continual improvement.</li> <li>• Determine quality of service.</li> </ul> |

Influencing factors for consideration:

- system service capacity;
- supply chain for spares provisioning;
- responsive maintenance actions.

Enabling mechanisms for process applications:

- project management;
- operators and maintainers training.

Outputs:

- dependable system performance;
- customer satisfaction results.

#### **A.2.5 Process for the system enhancement stage**

Inputs:

- new customer requirements;
- enhanced features.

| <i>Key process activities</i>                                                                                                                                                                                                                                                                  | <i>Dependability related activities</i>                                                                                                                                                                                                                                                                                                    |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Enhancement</b>                                                                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                            |
| <ul style="list-style-type: none"> <li>Identify new requirements.</li> <li>Establish enhancement strategy and plan.</li> <li>Evaluate the need for change and resulting benefits.</li> <li>Implement enhancement efforts.</li> <li>Implement activities for perfective corrections.</li> </ul> | <ul style="list-style-type: none"> <li>Evaluate impact on dependability performance due to changes with added new features.</li> <li>Conduct life cycle cost impact study for change incorporation.</li> <li>Conduct risk and value assessments.</li> <li>Conduct customer satisfaction survey resulting from change reactions.</li> </ul> |

Influencing factors for consideration:

- timing for change;
- return-on-investments.

Enabling mechanisms for process applications:

- change management;
- obsolescence management;
- customers “buy-in” or reaction to new service features incorporation.

Outputs:

- enhanced system performance;
- customer satisfaction results comparison before and after enhancement efforts.

#### **A.2.6 Process for the system retirement/decommission stage**

Inputs:

- status of aging system performance capability;
- competitiveness and marketability of existing operation service;
- increased maintenance and support costs.

| <i>Key process activities</i>                                                                                                                                                                                                                                                                                                           | <i>Dependability related activities</i>                                                                                                                                                                                                                                                |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Retirement/decommissioning</b>                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                        |
| <ul style="list-style-type: none"> <li>Execute system retirement/decommissioning plan.</li> <li>Implement reuse and redeployment strategy.</li> <li>Implement waste treatment on disposal items.</li> <li>Notify the customers on service termination.</li> <li>Provide information on new or alternative service provision.</li> </ul> | <ul style="list-style-type: none"> <li>Evaluate constraints on system deactivation and impact on removal of system from operation.</li> <li>Evaluate impact on environments of disposal items.</li> <li>Conduct customer satisfaction survey due to termination of service.</li> </ul> |

Influencing factors for consideration:

- timing for retirement;
- technology obsolescence;
- regulatory constraints;
- social impact due to termination of service.

Enabling mechanisms for process applications:

- project management.

Outputs:

- termination of service.

## **Annex B** (informative)

### **Methods and tools for system dependability development and assurance**

#### **B.1 General**

Methods and tools are useful aids for solving generic technical problems including engineering dependability into systems at various life cycle stages. There are numerous tools and a multitude of tool vendors in the market. Some of the tools are standard forms and simple checklists; others are complex interactive systems often requiring licensing agreements for database access and technical support. Methods and tools are commonly developed in-house based on past engineering experience, or they can be purchased from tool vendors to facilitate staff training and multiple project usage. The selection of the appropriate methods for technical solution should be at the discretion of the engineers or practitioners performing the dependability task. Since investments are involved in the choice of tools, the engineer or practitioner should consider the relevancy of the class of dependability engineering problems that need to be solved, the frequency of tool usage, the training effort required to effectively use the tool to achieve results, and the availability of alternative methods of using simpler techniques to solve the same problem with a simple tool set developed in-house. The following provide typical examples of general applications, hardware specific applications and software specific applications of methods and tools for engineering dependability into systems.

#### **B.2 General applications of methods and tools for engineering dependability into systems**

##### **B.2.1 Reliability and maintainability case**

The reliability and maintainability (R&M) case tool is used by a system acquirer to ensure that the R&M requirements of the purchaser are determined and understood by both the supplier and purchaser of a system. The tool also provides a means of achieving progressive assurance that the R&M requirements are being or will be satisfied throughout the life of the system.

The tool provides a framework for:

- a) the R&M case – a reasoned auditable argument to support the contention that a defined system satisfies the R&M requirements;
- b) the R&M case report – a summary or abstract of the R&M evidence and arguments from the R&M case to support programme milestones; and
- c) progressive assurance of R&M throughout the project milestones.

Reference document: DEF STAN 00-42 [11].

##### **B.2.2 Reliability growth programs**

Reliability growth programs are used for system reliability improvement during the system design/development stage. The objective of reliability growth is to realize the potential of system reliability targets by step-wise improvements using techniques in design analysis and reliability testing of the system modules or functions. The critical dependability activity is to identify and remove design weaknesses in the system for progressive reliability enhancement. Typical systems that would benefit from the application of reliability growth programs are those systems using novel architectural design techniques, new and unproven system components, and software intensive contents for incorporation in system operation.

reliability growth concept is to reduce the probability of failure occurrence due to design weaknesses via progressive design improvements of the system and its constituent functions throughout the design and development process. Reliability growth programs should be integrated into the system design and evaluation process to achieve cost-effective solutions. Reliability growth program is described in IEC 61014 [12]. The reliability growth models and estimation methods for reliability growth assessments based on failure data captured in the reliability growth program are described in IEC 61164 [13].

### **B.2.3 Configuration management**

The management of the various and successive system configurations is a major concern for dependability (i.e. maintenance support). This is due to the variety of interfaces generated through different configurations. The increasing demand for inter-changeability of components (hardware and software) and interoperability of systems has direct commercial relevance and implies specific attention to configuration management. This is particularly true for long-life systems with shorter life components, which may change frequently in technology over the life of the system. During system development, a sound configuration management system contributes significantly to effective dependability achievement. Configuration management is essential for system change controls and meaningful dependability assessments. Guidance on general configuration management is described in ISO 10007 [14].

### **B.2.4 Bayesian belief networks**

Bayesian belief networks (BBNs) are a powerful graphical formalism to support reasoning about uncertain events using diverse forms of evidence. They enable modelling of uncertainty and the combination of different types of evidence, including both subjective information based on expert judgement and 'hard' evidence from measurement. A BBN will accept as much or as little evidence as the user has available or wishes to enter, so it can make a prediction with missing or incomplete data. This methodology offers a useful approach to predicting dependability of a system at all life cycle stages when a mixture of indirect and direct dependability measurements is available.

There are numerous commercial Bayesian Network products available which facilitate the entry of data and setup of BBNs.

## **B.3 Hardware specific applications of methods and tools for engineering dependability into systems**

### **B.3.1 Reliability enhancement**

System reliability enhancement for hardware elements focuses on the inherent properties of the system functions and the influencing factors affecting the system reliability performance. The primary focus is on the technology used in system construction, the system operating environment, and the application of system functions to achieve system performance objectives. There are many classical reliability methods and techniques applicable for reliability assessments as described in IEC 60300-3-1. Reliability improvement can be achieved by proper incorporation of the recommended results with practical solutions based on relevant reliability assessment inputs. In most cases, design trade-off is necessary to determine the best solution. Some of these methods can be used for checks and balance to verify the analysis results of assessments done on the same hardware element.

Typical examples in the use of reliability methods and tools include:

- using reliability block diagram (RBD) to determine redundancy needs versus using a single higher reliability hardware element of new technology with a cost premium;
- using Markov analysis for reliability evaluation of complex system structures and complex maintenance strategies;
- using fault tree analysis (FTA) to identify critical failures in a system;