IEC 60300-3-15

Edition 1.0 2009-06

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

IEC 60300-3-15:2009

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

About the IEC

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

About IEC publications

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

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

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 It also gives information on projects, withdrawn and replaced publications.

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

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

- Electropedia: www.electropedia.org

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

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

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

A propos de la CEI

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

A propos des publications CEI

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

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

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

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

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

- Electropedia: www.electropedia.org

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

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

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

IEC 60300-3-15

Edition 1.0 2009-06

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

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][1]

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.

---

[1] 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.

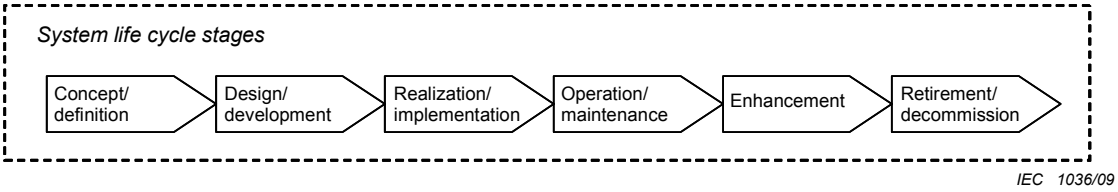

Figure 1 – An overview of a system life cycle

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.

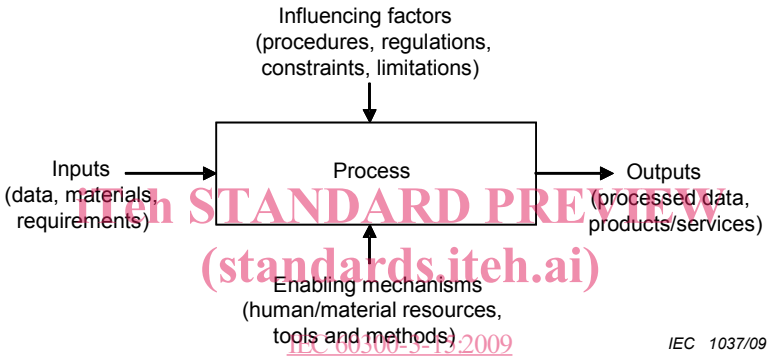

Figure 2 – Example of a process model

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].