

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Communication network dependability engineering

Ingénierie de la sûreté de fonctionnement des réseaux de communication



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
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 It also gives information on projects, withdrawn and replaced publications.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 61907

Edition 1.0 2009-12

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Communication network dependability engineering

Ingénierie de la sûreté de fonctionnement des réseaux de communication

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

PRICE CODE
CODE PRIX

XB

ICS 21.020; 33.040.40

ISBN 978-2-88910-584-7

CONTENTS

FOREWORD.....	4
INTRODUCTION.....	6
1 Scope.....	7
2 Normative references	7
3 Terms, definitions and abbreviations	7
3.1 Terms and definitions	7
3.2 Abbreviations	10
4 Overview of communication network dependability	10
4.1 Network dependability framework	10
4.2 Network life cycle and evolution process	11
5 Network dependability implementation.....	12
5.1 Dependability engineering applications.....	12
5.2 Network technology consideration	21
5.3 Network service functions consideration.....	22
5.4 Network performance consideration.....	23
5.5 Integrity of network data and information	26
5.6 Quality of service (QoS)	27
6 Network dependability assessment and measurement	30
6.1 Network dependability analysis	30
6.2 Network dependability fault insertion test	31
6.3 Measurement of network dependability attributes	32
6.4 Network dependability assessment methods	32
7 Quality of service measurement.....	34
7.1 QoS measurement overview.....	34
7.2 Generic user-oriented QoS parameters and requirements	35
Annex A (informative) Generic communication network model and related concepts	37
Annex B (informative) Network life cycle and evolution process	46
Annex C (informative) Criteria for establishing network security services	56
Bibliography.....	60
Figure A.1 – A generic communication network model	37
Figure A.2 – A process model on interactions of areas of influence.....	38
Figure A.3 – OSI reference model.....	39
Figure A.4 – QoS, dependability and network performance relationships	41
Figure B.1 – Network evolution process incorporated in the network life cycle stages	46
Table 1 – A matrix for capturing user's QoS data	36
Table A.1 – Examples of dependability influencing factors affecting network technology	42
Table A.2 – Examples of dependability influencing factors affecting network service functions.....	43
Table A.3 – Examples of dependability influencing factors affecting delivery of network performance	44
Table A.4 – Examples of dependability influencing factors affecting integrity of network data and information and provision of QoS	45



Table C.1 – Four basic types of vulnerability causes.....57

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMUNICATION NETWORK DEPENDABILITY ENGINEERING

FOREWORD

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

International Standard IEC 61907 has been prepared by IEC technical committee 56: Dependability.

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

FDIS	Report on voting
56/1339/FDIS	56/1350/RVD

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

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

The committee has decided that the contents of this publication will remain unchanged until the 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

Communication networks are today growing in complexity to meet diverse market demands and public communication needs; networks such as mobile phones, e-commerce, intranet and Internet services.

At the same time, communication technologies are developing rapidly to provide efficient network services and dependable performance needed in worldwide communications. The essential communication services such as information exchange, data processing and network connections enable public and private communications work to be carried out cost-effectively. Business and private sectors greatly depend on these communication services that have become pivotal in their daily routines. A key factor in ensuring network performance and network service functions is dependability.

Network dependability is the ability of a network to perform as and when required and to meet users' communication needs for continuous network performance and service operation. From a user's perspective, dependability infers that the provision of network service functions is trustworthy and capable of performing the desirable service upon demand. Network dependability is characterized by its performance attributes including availability of network performance and quality of service.

The network concept is an extension of the systems concept, addressing a common framework for the interaction of network elements and interoperability of service functions that together achieve specific communication objectives.

The network requires specific performance characteristics in order to deliver both its service functions and communication services. Network dependability engineering is a specific risk-based technical discipline intended to deal with the diverse applications and deployment of essential communication services. Unlike the system life cycle where system retirement exists, a network seldom reaches retirement. A network evolves with time to accommodate innovative feature applications and provision of continual communication service needs. The network life cycle is evolutionary and has to address technology convergence issues and renewal processes as well as characterize specific dependability attributes to meet network performance objectives. The need for network dependability standardization is essential to achieve cost-effective development and implementation of communication networks.

Communication network dependability provides important performance attributes for network equipment developers and suppliers, network integrators and providers of network service functions who are mainly concerned with global competitive environments. The primary reason is that dependability can seriously impact revenue generation and affect return-on-investments. Users of network service functions and communication services rely heavily on network functions and reliable services that guarantee network security and uninterrupted network connections for voice, video and data transmission.

This International Standard provides a generic framework for communication network dependability. The communication network includes telecommunications networks, Internet and intra-networks utilizing information technology. This standard describes the influence of dependability attributes and their impact on network performance. It provides the criteria and methodology for network technology designs, security service functions, dependability assessment and quality of service evaluation. This is to guide engineering and implementation processes for realization of network dependability performance objectives.

This standard constitutes part of a framework of standards on system aspects of dependability by extending the system dependability concepts of IEC 60300-3-15 for network applications, and to support IEC 60300-1 and IEC 60300-2 on dependability management. The network performance and communication services in this standard are referenced in the International Telecommunication Union Telecommunication standardization sector (ITU-T) series of recommendations.

COMMUNICATION NETWORK DEPENDABILITY ENGINEERING

1 Scope

This International Standard gives guidance on dependability engineering of communication networks. It establishes a generic framework for network dependability performance, provides a process for network dependability implementation, and presents criteria and methodology for network technology designs, performance evaluation, security consideration and quality of service measurement to achieve network dependability performance objectives.

This standard is applicable to network equipment developers and suppliers, network integrators and providers of network service functions for planning, evaluation and implementation of network dependability.

2 Normative references

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

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

IEC 60300-3-15, *Dependability management – Part 3-15: Application guide – Engineering of system dependability*

3 Terms, definitions and abbreviations

3.1 Terms and definitions

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

3.1.1

communication network

system of communication nodes and links that provides transmission of analog or digital signals

EXAMPLES Telecommunications networks, Internet, intranet, extranet, Wide Area Networks (WAN), Local Area Networks (LAN) and computer networking utilizing information technology.

NOTE 1 A network has its boundary. All nodes at the network boundary are called ends. In some applications, the term “node” is used instead of “end” as a communication access point to the network, as well as for interconnections between the transmission links.

NOTE 2 A “backbone” communication network consists of core network and high-speed transmission lines (national or international), connecting between major switching network nodes (interconnection of transmission lines) at various locations in a country or region.

3.1.2

(network) dependability

ability to perform as and when required to meet specified communication and operational requirements

3.1.3

(network) availability

ability to be in a state to perform as and when required, under given conditions, assuming that the necessary external resources are provided

NOTE 1 Availability depends on the combined characteristics of the reliability, maintainability, and recoverability of the item, and generally, on the maintenance support performance.

NOTE 2 Given conditions would include aspects that affect reliability, maintainability and maintenance support performance.

3.1.4

(network) reliability

ability to perform as required for a given time interval, under given conditions

NOTE 1 Given conditions would include aspects that affect reliability, such as: mode of operation, stress levels, environmental conditions.

NOTE 2 Reliability may be quantified using appropriate measures such as meantime to failure, or the probability of no failure within a specified period of time.

3.1.5

(network) maintainability

ability to be retained in, or restored to, a state in which it can perform as required under given conditions of use and maintenance

NOTE 1 "Given conditions of use" may include storage.

NOTE 2 "Given conditions of maintenance" include the procedures and resources to be used.

NOTE 3 Maintainability may be quantified using such measures as, mean time to restoration, or the probability of restoration within a specified period of time.

3.1.6

maintenance support

resources to conduct maintenance according to a given maintenance concept and policy

3.1.7

maintenance support performance

ability of an organization to complete specified network maintenance support upon demand under given conditions

NOTE The "given conditions" include those related to the maintenance organization, and to the conditions under which the item is used, maintained, and relevant maintenance policies and procedures.

3.1.8

(network) recoverability

ability to recover from a failure, without corrective maintenance

NOTE 1 The ability to recover may or may not require external actions.

NOTE 2 Recoverability may be quantified using such measures as, mean time to restoration, or the probability of restoration within a specified period of time.

3.1.9

(network) element

subsystem or component of a communication network

EXAMPLES Terminals, nodes, links and switches.

NOTE 1 A network element may involve human input to perform its service function.

NOTE 2 Network nodes and access points are connected by network links.

3.1.10**(network) link**

electrical, wireless or optical connection between network nodes

3.1.11**(network) performance**

ability to provide the service functions related to communications between users

[ITU Recommendation I.350]

NOTE Network dependability performance refers to the ability of the network to provide or demonstrate the dependability attributes in network operation to achieve network objectives and quality of service requirements.

3.1.12**(network) management**

application of organized processes and resources to manage the performance, configuration, accounting, fault, and security activities

3.1.13**(network) service function**

program or application that interacts with the network users or within the network infrastructure to transmit or exchange data and information in the network

NOTE A network service function may consist of hardware and software elements, and may involve human interactions for realizing a specific function.

3.1.14**network services**

provision of network service functions and communication services to the network users

NOTE 1 Communication services are the network services subscribed by the end-users.

NOTE 2 A bearer service is a communication service function that allows transmission of user-information signals between user-network interfaces.

3.1.15**quality of service**

collective effect of service performance that determines the degree of satisfaction of a user of the service

3.1.16**network failure**

loss of network ability to perform its function as required

NOTE The failure may be due to, for example, equipment failure, natural disasters or human-caused disturbance.

3.1.17**network fault**

state characterized by the inability of the network to perform its function as required

NOTE 1 In the context of network operation, a fault may be natural due to an abnormal condition, or malfunction resulting in a network element failure, or induced by external means such as fault insertion.

NOTE 2 A degraded state in network performance is a situation where one or more performance characteristics do not conform to requirements.

3.1.18**service provider**

organization that provides communication network services

EXAMPLES Telephone companies, data carriers, mobile services, Internet service providers, and cable television operators.

NOTE Network carrier or common carrier is an organization that transports a product or service using its facilities, or those of other carriers, and offers services to the general public. The term communication carrier refers to various telephone companies that provide local, long distance or value added services.

3.1.19

user

party that employs the services of a service provider for direct network access

NOTE 1 A user may be a source or recipient of user information, or both.

NOTE 2 In some circumstances, a user of a communication service is also known as a subscriber.

3.1.20

(network) integrity

ability to ensure that the data throughput contents are not contaminated, corrupted, lost or altered between transmission and reception

3.2 Abbreviations

E2E	End-to-End
FMEA	Failure Mode and Effects Analysis
FTA	Fault Tree Analysis
IP	Internet Protocol
ITU-T	International Telecommunication Union Telecommunication standardization sector
LAN	Local Area Network
NGN	Next Generation Network
OSI	Open Systems Interconnection
QoS	Quality of Service
RBD	Reliability Block Diagram
SLA	Service Level Agreement
TCP/IP	Transmission Control Protocol/Internet Protocol
WAN	Wide Area Network

4 Overview of communication network dependability

4.1 Network dependability framework

A communication network consists of network elements such as switches, transmitters, computers, telephones and other devices connected by communication facilities for exchanging information electronically. The connections can be permanent via cable or temporary by means of telephone or Internet links. The transmission medium can be physical (e.g. fibre optics) or wireless (e.g. satellite). It covers many technologies such as radio, television, telephone, data communication and computer networking utilizing information technology.

The nature of network operation is multi-faceted and ever expanding and evolving such as doing business on-line via the Internet. The infrastructure connecting different types of communication systems and interacting networks is extremely complex. The integration of disparate networks and systems demands evolving establishment of interfaces and protocols for interoperability to attain viable network connectivity and service performance. Enterprise marketing and e-commerce pressures often dictate development of new techniques that change the ground rules in business and service applications.

Network related activities are unique in assuring dependable performance and quality of service. The challenge is to provide network solutions that link network designs and service function applications to realize the relevant dependability attributes. Network dependability infers that the network performance is able to maintain information integrity and capable of delivering the network service functions to satisfy user expectations as well as the service provider's needs. The strategic framework is to select and implement appropriate network elements for the network configuration to achieve dependability and integrity in network performance.

Annex A presents a generic communication network model and related concepts.

Network dependability and network service functions are influenced by the dependability attributes relevant to their specific applications in various network life cycle stages. These dependability attributes include availability, reliability, maintainability, maintenance support performance, recoverability and integrity performance characteristics, incorporated in the network designs and implemented in the network service functions for network operation and maintenance.

The communication network dependability framework consists of six main interacting areas of influence:

- a) the application of dependability engineering;
- b) the utilization of network technology;
- c) the delivery of network performance;
- d) the deployment of network service functions;
- e) the integrity of network data and information;
- f) the provision of quality of service.

These six interacting areas of influence form the basis for network dependability management. Implementation of network dependability processes and methods are described in Clause 5.

4.2 Network life cycle and evolution process

A network evolves and changes with time to meet the dynamic network applications and network service needs in communications. The network evolution process is reflected in the system life cycle stages described in IEC 60300-3-15 and modified for network life cycle application to include the renewal process. The following presents the network life cycle stages:

- *concept/definition* stage to identify network operating scenario;
- *design/development* stage to determine technology applications and develop network service functions;
- *realization/integration* stage to realize network operation, verification and validation to assure network performance;
- *operation/maintenance* stage to sustain network operation and provision of network services;
- *enhancement* stage:

- to optimize and improve network performance by technology evolution and service functions convergence;
- to upgrade or renew continuing network services, and launch new features in network applications;
- *retirement/decommissioning* stage to discontinue obsolete service functions.

Annex B describes the network life cycle and evolution process.

5 Network dependability implementation

5.1 Dependability engineering applications

5.1.1 Management of network dependability

Dependability is a technical discipline that is managed by engineering principles and practices. The dependability management systems [1]¹ and guidelines [2] are used in this standard 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 network 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 necessary synergistic effects and add values to the project outcomes. Project tailoring is emphasized for cost-effective management of network projects. Where applicable, life cycle cost analysis [4] and risk assessment [11] should be used for resource allocation and optimization for evaluation of acquisition and ownership costs.

From a communication network management perspective, dependability management should be an integral part of the network management process with relevant dependability activities to support development and implementation of network service functions throughout the life cycle and network evolution. Network management is the execution of the set of management processes for planning, controlling, allocating, deploying, coordinating, maintaining and monitoring the resources of a network.

From an engineering perspective, a network can be viewed as a complex system consisting of multiple interconnecting systems. The technical processes in IEC 60300-3-15 are used to describe the network life cycle stages for project implementation. The network life cycle stages are modified to accommodate the process descriptions of network evolution and technology convergence, optimization and renewal, obsolescence and retirement. Network management process and dependability related activities for each network life cycle stage are presented in Annex B.

5.1.2 Network dependability attributes

The basic set of network dependability attributes is derived from a network performance perspective. Other attributes may be added for specific applications.

a) Availability

Network availability reflects the users' requirements from three aspects:

- the network has the ability to perform as and when required;
- the network service functions should not be affected by network faults;
- the network can recover as quickly as possible when a network fault affects its service functions.

b) Reliability

¹ Figures in square brackets refer to the Bibliography.

Network reliability can be improved by using redundancy technology and protection mechanisms. For a network with high reliability requirements, the protection of multipoint faults should be considered. The manifestation of faults becomes more critical for complex network operation, especially with the continued usage of obsolete equipment that may have compatibility problems.

c) *Maintainability*

Maintainability reflects the ease of restoring a network to an operating state following a fault, or from a degraded state of network performance operation. The incorporation of redundancy in design and fault management capability into the network can affect maintainability performance. For example, remote fault management where fault identification and corrective action are carried out by remote intervention, can shorten maintenance time.

d) *Maintenance support performance*

Maintenance support performance is dependent on the provision and management of resources to perform maintenance activities. Network dependability design requires an approach to reduce the complexity of network equipment for maintenance, easy access for active maintenance during network operation, standardized maintenance procedures, network fault identification and traceability, and perfected spare parts management system. This approach applies to hardware and software as well as to human functions for maintenance support performance and design consideration.

e) *Recoverability*

Recoverability in service performance is dependent on the design of network architecture, fault-tolerant protection mechanisms, access for maintenance and self-healing features incorporated into the network functions. The means of achieving restoration may be automatic or by external actions.

f) *Integrity*

Integrity infers that the network is stable and robust, and able to maintain consistency in performance and use. Network integrity provides security and protection for information transfer in network performance and service functions.

5.1.3 Network failures and faults

5.1.3.1 Network failure criteria

Network failure criteria should be established during the concept and definition stage and continually reviewed throughout the lifecycle of the network in order to permit classification and updating of network failures.

Failure criteria should be determined by the network service provider, based on industry standards and relevant data, including the network users' inputs, so that all conceivable conditions can be covered. This information is used in:

- specification of dependability requirements to the network equipment suppliers;
- reaching agreements (such as SLA) of the network dependability performance attributes with the users of the network services.

The following should be considered when establishing failure criteria.

- a) Network node and link failure: The failure of network nodes and links includes total failure and partial failure. Total failure is the loss of functionality of the entire network for a period of time. Partial failure is the loss of functionality of part of the network.
- b) Quality of service (QoS) degradation failure: Degradation failure is due to an unacceptable level of QoS in the provision of network service performance experienced by the users. Network service providers routinely gather QoS data through measurements and surveys to determine the level of QoS.

5.1.3.2 Network failure classification

Most network failures can be classified as to their probable causes so that failure analysis results can be categorized for network dependability improvement.

- *Facility-related network failure* – This is related to failures of individual network elements whose failure rate data can be used for predicting the corresponding node and link dependability parameters.
- *Traffic-related network failure* – This is related to the operation scenarios of network service traffic, which changes according to the network users' usage demands. Network design should consider users' usage demands and plan network traffic capacity to satisfy most operation scenarios to avoid network service performance degradation.
- *Disaster-related network failure* – This is related to failures that are man-made or caused by natural disaster. Sometimes the network facilities in the disaster area may be totally destroyed.
- *Security-related network failure* – This is related to network failures caused by insufficient security to prevent unauthorized intrusion, such as hacking, cyber attacks or sabotage activities.
- *Scheduled, activity-related network failure* – This is related to failures that occur during scheduled network maintenance activities, such as software upgrade causing the network to be temporarily out-of-service.
- *Human factor-related network failure* – This is related to failures due to human error, misused or negligence, such as network design errors, configuration errors, or mistakes in management of software versions.

5.1.3.3 Network fault conditions

A network failure represents an event in network operation and maintenance where the occurrence of an anomaly or malfunction in performance is experienced. A fault condition related to the failure occurrence describes the fault state or status of the fault condition observed. In practice, the cause of actual network failures is often unknown at its initial observation of incident reporting. The incident report captures the observed symptoms of the fault state or fault conditions on the network's inability to perform its function. The complexity of the network operations, the involvements of diverse service functions, and the time limitation to restore network services often prevent further investigation of the failure event situation. Priority under such fault conditions is to reroute, reboot and recover the failed service functions in order to restore normal network services. Network incident reporting should capture the failure symptom in order to initiate appropriate follow-up action and determine the cause of failure where practicable. Relevant information, captured by incident reporting during network operation and maintenance, provides an important source of failure data for implementing an effective network fault management system.

5.1.3.4 Network fault management system

The network fault management system is a network service support system. It facilitates the reporting of failure event data and capturing the observed fault conditions to support management and correction of network faults. The fault management system consists of a set of supporting functions to detect, isolate and also compensate, where applicable, environmental changes as well as correct network malfunctions. The system is designed and deployed to support network service restoration for tracing and identifying faults, performing diagnostics tests, correcting faults, activating alarms and reporting error conditions, maintaining error logs and providing error detection notifications (see 5.1.5.3). Network fault management system is an essential enabling mechanism to support network service functions.

5.1.4 Establishment of network dependability requirements

5.1.4.1 Network dependability requirements identification

Information gathering helps identify market needs of the new or upgraded network. The objective is to determine the commercial and technical requirements for network development and service enhancement. Information can come from various sources.

- a) *Information on upgrading an old network* – Network design could use the existing network as a basis for upgrade or enhancement, such as expansion of existing service facilities and capability to meet growing market needs. This would avoid extensive resource investments on building a completely new network. The enhancement incorporates new functional features and provides additional services and capacities to augment and complement the old network service functions.
- b) *Service functions and performance information* – These are the network service functions required by the network service provider; they include existing applications (e.g. telephone service) and new applications (e.g. internet service), as well as requirements for network performance, capacity and other network service features.
- c) *Customized information* – This type of information covers, for example, the requirements of end-users for customized services provided by the communication network. For example, users may ask for a videophone service.
- d) *User suggestions and complaints* – Useful suggestions and relevant complaints should be obtained from users concerning the existing network enabling solutions or improvement in the new network. Typical examples include conducting customer surveys and technical support feedback on user satisfaction.
- e) *Environmental factors* – The geographical environment in the network coverage area may pose special requirements for network design. For example, relevant information concerning locality, terrain, weather, and electric power supply.
- f) *Research Information* – Research studies often provide information on service planning, design and construction experience of similar networks and their dependability performance.
- g) *Commercial constraints* – Relevant information may provide useful data on network construction time limits, network service provider budgets as well as service level agreement and penalty clauses.
- h) *Regulatory constraints* – These could include laws or indications provided by national or international authorities to which operators are obliged to conform.

The information obtained from these various sources may require translation into more technical terms in order to conduct any further analysis.

5.1.4.2 Requirements analysis, allocation and review

Network dependability requirements analysis is the process to analyse the information collected from various sources from relevant information identified. The process converts the user needs into technical requirements for the network design to properly express the intent of identifying customer requirements. Dependability requirements form part of the technical requirements for resource allocation to the network elements for network specification and realization.

The following presents an approach for analysis of network dependability requirements.

a) Classification

This activity analyses the existing and future network service needs to determine the traffic flow, volume and load on network performance. The analysis summarizes and classifies the technical requirements into several categories, including dependability requirements on redundancy, fault-tolerance, fault detection and recovery, overload control, and maintenance and upgrade.

b) Breakdown

The breakdown of dependability requirements is achieved:

- by granularity: breakdown the requirements according to complexity and functions. This would permit reliability apportionment of specific functions to be realized in a single functional device or involving multiple network elements to achieve specific functional performance in the network;
- by layer: breakdown the requirements according to layers where the functions are necessary. Dependability requirements can be assigned to layer functions. The layer approach facilitates allocation of the dependability requirements to each network element used at that layer, defines the dependability functions that each network element should perform, and identifies the boundary and the interface of the network element.

c) Requirements integration

The dependability requirements obtained by various means and from various sources need to be integrated. Duplicated requirements are removed to avoid conflicts between contradictory requirements for overall dependability improvement, design trade-off and optimization.

d) Priority analysis

Priority analysis identifies the importance of requirements and determines their urgency for priority actions and implementation. It represents a systematic integrated process for priority development and assignment. A set of criteria should be established for priority ranking of the project tasks for assignment. Priority analysis should form part of the project plan for implementation. Risk and cost-benefits analysis should be conducted where appropriate in the priority analysis process.

e) Requirements review

Review information gathering, definition and others aspects to detect any errors or misinterpretations in the requirements analysis. This is to formalize the dependability specification which is used as basis for verification, test, acceptance and delivery.

5.1.4.3 Network operation profile

The application scenario presents an operational profile of the network. The objective of determining the network application scenario is to identify possible failures of the network service functions, the fault handling procedures and operations, and the interfaces of various network elements. The analysis approach should consider such factors as network topology, interfaces between network elements, and related network protocols.

The process for application scenario analysis should:

- determine the service function features;
- describe the networking application of the service features and depict the information to facilitate visual comprehension such as a networking diagram;
- describe the interfaces between the network elements involved with the service;
- determine the failure points on the network that are critical to the main network service functions and determine the failure modes and related operation scenarios;
- analyse the process flows of the related network elements based on the application scenarios for network operation to ensure that related failures and major functions can be recovered;
- determine a fair process for prioritizing different users and applications for a shared network.

5.1.5 Network dependability design consideration

5.1.5.1 Design incorporation of dependability attributes

Design incorporation of dependability attributes in networks for performance enhancements requires a systematic engineering approach for realization to achieve the desired level of

dependability objectives. Several critical factors influencing network performance are presented for network dependability design consideration.

5.1.5.2 Redundancy design

Redundancy design is an effective means to improve network dependability. It is often used in network dependability design applications. Both active redundancy and standby redundancy are employed as protection mechanisms for reliability improvement and backup storage services.

The redundancy design in a communication network is mainly the link redundancy design based on the network topology, and the redundancy design for critical network elements such as duplication of core memory in switching systems dual plane memory design. The former is viewed from the perspective of services and focuses on the protection for traffic channels. The latter is aimed at reliability enhancement and protection of network elements from malfunctions. The redundancy design scheme offers a protection mechanism which acts on service recovery in the event of a failure. The criticality of a network element for redundancy consideration is determined by its specific application in the network functions and its impact on loss or degradation of network services.

High availability can be reached also by geographical redundancy. This can be realized through system replication over two or more sites geographically separated to protect against site failure or site inaccessibility, due to any reasons, including externally caused destruction or damage such as earthquakes or fires.

5.1.5.3 Fault management

Fault management technology directly provides the means to attain the attributes of network dependability. It can be grouped into the following categories:

- *fault detection*: checking the operational status of network nodes and links, setting various network performance thresholds, and monitoring the changes of network performance to timely detect faults;
- *fault localization and diagnosis*: locating the fault and identifying its cause according to the collected information. For a fault that cannot be located directly, analysis can be made according to the relationship of the fault information to determine the specific location and cause of the fault;
- *fault isolation*: isolating the failed unit and preventing it from interfering with other working units;
- *fault recovery*: recovering network service functions by re-setting the unit or re-starting part of the unit in case of a fault. For a redundancy design unit, using protection switching or resource reallocation to avoid network service failure;
- *fault removal*: replacing the failed unit or correcting software fault by using the maintenance support system, including further in-depth analysis and follow-up recommendation for improvement actions and solution;
- *fault alarm*: setting an alarm to alert the network management system in the event of a network fault for immediate corrective action. Different alarms can be set to indicate different fault levels for priority actions. The network management system collects the related fault alarm information for fault localization and for further analysis;
- *fault prognosis*: analyzing and evaluating fault probabilities and likely consequences of faults by using methods such as trend analysis;
- *fault monitoring*: observing and checking the fault conditions to alert maintenance actions.

5.1.5.4 Data management

Network failure or outage breakdown could disrupt information traffic flow or cause data corruption. Loss of key data could result in the inability to restore network service functions or

affect economic losses to the network carriers. The following methods are commonly used to manage data in order to improve network dependability:

- storing duplicate data in different locations to protect the media of data storage from faults or damage;
- periodic backup to protect the key information and data. Important data should be protected by multiple backups and remote backup. The proper use of the backup and recovery mechanism can reduce downtime and improve performance;
- encryption, checksum, acknowledgment and re-transmission mechanism, and redundancy transmission mechanism can be used for the transmission of important service data via the network. For example, protection and assurance of financial data transmission for banking services to avoid the loss of packets;
- use of different media for storage of program data and information data;
- redundancy of important program data can be used to ensure normal running of the system even when the running software program is incorrectly modified;
- synchronization of information between the active and standby units of the redundancy system can be used to avoid data loss or abnormal behaviour during protection switching;
- protection, detection and verification of the program data during loading or transmission to ensure incorrect data are not recorded.

5.1.5.5 Network node and link factors

Network “ends” or terminations are connected to a network through network nodes and links. There are two common types of network configurations for dependability assessment:

- end-to-end (E2E) network dependability assessment;
- full-end network (a network with all the ends) dependability assessment.

A full-end network reflects the relationships between all the ends in the network. The full-end network dependability assessment is of general type of interest to the service providers. The E2E network dependability assessment is a special case of interest to the network users. The network dependability assessment methods are described in 6.4.

5.1.5.6 Environmental factors

Environmental factors could cause network interruption in various ways. For example, natural disasters, such as flood, earthquake, solar flares and typhoon, could all affect network operations. Network dependability design in terms of environmental factors should be considered. The impact of the environment on network dependability should be understood and appropriate preventive and corrective action plans should be formulated to sustain network dependability performance in case of disaster.

Natural disasters are accidental, but weather patterns are predictable. The primary impact on the network is reflected mainly on power fault of network equipment assuming that other network facilities are well protected under the conditions. This assumption simplifies the technical approach to a reasonable range for practical assessment. The assessment is based on the predicated power outage duration and frequency of each affected area where the network is located, and to initiate proper power protection and provide alternate power supply to minimize the impact of power outage on the operating equipment. It is essential to evaluate the percentage of the network service users affected by power outage and causing network disruptions in each area against the total number of users in the network. The downtime or unavailability of the network service functions resulting from power faults each year can be predicted.

5.1.5.7 Human factors

The impact of human factors on network downtime should be considered to evaluate human errors and process activity flow errors to provide the basis for dependability improvement.

a) Human factors consideration in scheduled network maintenance activities

Network upgrade and expansion are both scheduled network activities, which cause an office or the entire network to be temporarily out-of-service. A good upgrade/expansion plan and reasonable handling activity flow can reduce downtime. The prerequisite for the dependability assessment of such activities is to predict the average times of activities within the network plan year. The estimated downtime can be obtained by evaluating the technical plan and operation flow of the scheduled maintenance activities. The effect on network availability due to scheduled maintenance or upgrade can be evaluated by considering the percentage of the network service users affected.

b) Network configuration and operation

The statistics of incorrect network configuration and operation should be collected for prediction of human performance behaviour and evaluation of impact on network downtime. This is to identify the weakness in the network operation flow as the basis for reliability improvement.

c) Impact of external interference

Annual network service data has shown that network trunk links have been broken due to reasons such as human errors in construction, property damage due to accidents, vandalism on equipment and cable theft. The statistics of similar networks in past years can be used to predict the impact of external interference of the new network to determine network downtime due to human related causes.

5.1.5.8 Network design factors

From the perspective of network design, the factors influencing dependability assessment should focus on the following aspects.

a) Network protection mechanisms

The incorporation of protection mechanisms in network design is used to improve availability, reduce downtime, and enhance recovery performance. Protection mechanisms provide the necessary failure protection. Redundancies incorporated in the network designs for routing protocols, hot backup protocols, route binding protocols, and automatic protection switching protocols are all network failure protection mechanisms. The protection mechanisms usually consist of hardware/software functions and are subject to random or systemic failures. Dependability assessment to evaluate the consequences of failure in the protection mechanisms should be considered in network design.

b) Traffic burst

Traffic burst is the existence of traffic “bottleneck” situation in network performance. Traffic burst causes unstable performance. Traffic study provides the necessary information on the traffic flow pattern and the probability distribution over time. For normal operation, the traffic burst can be expected and sometimes may be predictable, e.g. peak load at certain days or hours, or sometimes may be unpredictable, e.g. due to external events like weather, accidents etc. The network is normally designed for a finite capacity limit and service functions have capacity thresholds that would affect access and connection if exceeded. The traffic burst impact on performance can be assessed by creating a topology model and dividing the network into layers and areas from top down, and then by finding the network traffic “bottleneck” for each service from the bottom up, hence predicting the range of the services that are affected.

c) Maintenance access

Maintenance access is an important factor for consideration in network design. In provision of network services, it is common industry practice to perform maintenance activities without interruption of network operation. The maintenance activities may require on-site physical access to the network equipment or remote access to the network function for software update. To facilitate physical access, network design should consider site location, site accessibility, service environment to perform the maintenance tasks, maintainability design of network equipment requiring the service, and logistic support requirements to support maintenance activities. To facilitate remote access, network design should consider appropriate protocol for network link interface, security, and

intervention, assurance process for network protection, and backup systems for network survivability.

5.1.6 Network dependability simulation

Network dependability simulation is a process to study and analyse the existing or planned network dependability. The simulation is based on network dependability modelling and network failure research study. The purpose is to find solutions for network dependability improvement. Network dependability simulation should consider both the static structure of a network, and the dynamic behaviour of the network nodes and link connections.

The static structure of a network refers to its topological connections. Analysis of the static structure should clarify the connections of the network elements and their hierarchical and structural relationships.

Dynamic behaviour of a network refers to the failure probability of each element and connection over time, functional interaction of various elements, behaviour of related elements after failures, and their impact on users. The analysis of dynamic network behaviour should focus on:

- various network services (for example, voice and data);
- failures of various network layers (for example, physical layer failure, network layer failure, and service layer failure);
- weighting the impacts of various failures (for example, the impact of a failure affects a number of users, the service interruption duration, and the types of network services);
- failure detection and location probability of the network node and link connection;
- probability of successful switching between network elements;
- recovery time after a failure.

5.1.7 Network dependability evaluation

Network dependability evaluation is the process to verify the network conception, in meeting the dependability objectives. It includes:

- identifying the purpose of evaluation and assessment objects: A network consists of many sub-networks. Any two network nodes can be linked by connection between them to form the smallest network. Therefore, the boundary of the network needs to be made clear before dependability evaluation commences. The type of equipment used and the links involved in the network should be determined for appropriate dependability design evaluation;
- defining failures: Network elements experience many intermediate performance situations from normal operation to network failure. To simplify the assessment process where possible and applicable, a suitable network failure definition or failure classification should be established. The situation at which the performance of a network element is functioning within the threshold is deemed acceptable. When the functioning exceeds the threshold, it is considered unacceptable and represents a failure (see 5.1.3);
- creating a relevant dependability model: Establishing the relationships between various network elements to formulate a network dependability model should be based on the network topology, service features and network layers;
- obtaining relevant data of all network elements and links suitable for dependability assessment: The dependability data consists of failure and downtime information collected during network operation. The data can be obtained by performance test or from on-site data collection;
- performing the evaluation and analysis: Using the dependability model and data to perform analysis to obtain quantitative results of the dependability attributes pertaining to the network performance characteristics;

- interpreting the evaluation results for recommendation of follow-up actions: The analysis results should be interpreted in terms of predicted network performance, design alternatives and practical improvements;
- conducting formal verification and validation processes where applicable for network dependability evaluation.

Network dependability assessment and measurement are described in Clause 6.

5.2 Network technology consideration

5.2.1 Network architecture

Communication network architecture can be represented hierarchically by vertical layers and horizontal partitioning. The hierarchy forms the structure of the network architecture. The network boundaries are used to identify access points and separate connections of sub-networks.

a) Horizontal partitioning

The horizontal partitioning can be divided into customer premises network, access network and core network:

- customer premises network, connected between a user terminal and a User-to-Network Interface, enables a user to access the network conveniently, such as the cabling system at home or in the office;
- access network can be an entity network between a User-to-Network Interface and a service node interface for transportation purposes;
- core network can consist of broadband high-speed “backbone” transport network, which provides the main connections and large switching nodes.

The closer the device connection to the core network, the more concentrated the traffic becomes. This results in the need for higher capacity transmission medium to accommodate the increased traffic and utilizing more complex systems to process the network information. Hence the devices deployed for use closer to the core network can have greater impact on the network service functions. High reliability performance is necessary for dependability. The horizontal partitioning is shown in the generic communication network model in Figure A.1.

b) Vertical hierarchy

The vertical hierarchy can be grouped into the bottom layer for transport functions and the top layer for application service functions. The groupings of the two separate layer blocks are known in the network architecture as strata of functionality. They are defined below:

- *transport stratum*: to provide transparent transfer of data between hosts and provide for end-to-end connection, error recovery, flow control, and ensuring complete data transfer;
- *service stratum*: to provide users with various communication services and end users with information applications.

In addition, the supporting networks ensure the smooth operation of networks for accomplishing the monitoring and control functions. Supporting networks include signalling network, synchronization network, and communication management network.

Network dependability analysis should consider the relevant influences of the layers affecting network performance. The dependability of a network service concerns not only the transport equipment and the routing of bearer service, but also the application service equipment used for the network functions. The impact of supporting networks should also be evaluated.

Clause A.3 provides a brief description of the Open System Interconnection (OSI) reference model and the layers associated with communication network. The groupings of blocks representing the service stratum and the transport stratum are shown in Figure A.3.

5.2.2 Topology

Communication network consists of terminals, network nodes and transport links. The network topology reflects the connection from a network configuration perspective. Network topology is the arrangement or mapping of the network nodes connected to each other by links, which may be physical or logical connections. Physical topology is the mapping of the network nodes and their connections such as cabling to connect separate network equipment. Logical topology is the signal paths for data travel between nodes. The signal paths have multiple logical connections and may take alternate routes for data travel to reach its destination.

Under the support of different network technologies, networks may come in different topological forms, such as *star* type, *mesh* type, *tree* type, and *ring* type which represent the shape of network topology. Typical examples of network topology applications include a central dispatch communication network representing a *star* type configuration, a distributive switching network representing a *mesh* type configuration for connecting telephone subscribers, a *tree* type configuration for multimedia delivery, and a ring type configuration for fast optical network protection. Topology of network describes the active or operating path(s) of service transporting on the network, along with the backup path(s) and protection mechanism, and reflects the ability of service access and transportation. Some network analysis methods on network dependability, such as network vulnerability analysis and network survivability analysis, are applied from the perspective of network connectivity. They describe the impact of the network topology on network dependability. In the modelling and assessment of network dependability, the topological form of the network should be considered. A parallel topology in conjunction with a failure protection switching mechanism can improve availability in network performance.

5.2.3 Interconnection

Network users, devices, links and other entities connect with one another to form a network. The interconnection is an important feature of the network, reflecting the requirements of network for equipment interfaces. The interconnection can be permanent (e.g. cable) or temporary (e.g. telephone session connection), the transmission media can be fixed (e.g. optical fibre) or wireless (e.g. radio waves).

The reliability of interconnection has a great impact on network dependability. Interconnection reliability improvement should consider both hardware, such as adopting high reliability devices and fail-safe designs, and software, such as running a protection switching protocol on the equipment interconnection interface to support redundancy schemes.

5.3 Network service functions consideration

5.3.1 Network service function provisions

Network service functions refer to programs or applications that interact with the network end-users to transmit or exchange data and information in the network. With the development of network technologies, especially the advancement in mobile network technologies, more services can be provided on modern networks. Examples of such service offerings include telephone, facsimile, web-browsing, e-mail, e-business, and video-on-demand. A mix of voice, video, and data by Internet, intranet and extranet can be accessed and delivered at the same network. Different types of network services require different traffic performance.

These diverse network service functions reflect the users' demands on the network. The high serviceability of a network is generally expected in the network service provision. The development of dependability requirements for network service functions should consider the access capability, the retention of service connections, and the user experience of the service.

5.3.2 Network policy

Network policy is the rules and regulations designated by the network service provider for compliance during network operation. Proper execution of the network policy, which defines

the management scheme for allocation of internal and external resources in the network business, can achieve cost-effective network operations. For example, a good routing policy can improve network transport efficiency; the application of traffic policy can adjust network utilization and improve network performance; and a QoS policy can define traffic priority according to network service and user attributes, and using various methods and processes to guarantee QoS.

Network policy reflects the mutual control and checking relationships between various layers of the network. Effective network dependability management requires reasonable support of network policy to achieve the highest cost-efficient ratio for return-on-investment.

5.3.3 Network end-users

Network end-user can be a person or an application using the network service function, as opposed to those who develop, provide or support the network operation. End-users interacting with the network are not concerned about the network structure and compositions. Their views on network service functions are different from the service providers' point of view.

Network dependability reflecting the end-users' viewpoints include:

- end-users' network dependability requirements;
- service provider's offerings of network dependability (or planned/targeted network dependability);
- dependability achieved or delivered by the service provider;
- dependability perceived/experienced by the end-users.

End-users' dependability needs are the primary source of information for establishing dependability requirements. The existing and future end-users' activity profile and network usage should be considered. The end-users' needs should be well understood when designing a network.

5.3.4 Network security

Network security is vital in business transactions and protection of personal privacy. This is due to the explosive growth in communications and networking via the Internet and the dependency of computer use for exchange of information. Various methods have been developed to protect sensitive data from unauthorized access, accidental disclosure, or security threats. Such methods include authentication, encoding and encryption of data and messages, virus detection and firewall protection to prevent network-based attacks.

There are three main aspects of information security for consideration besides physical security for network protection:

- attacks due to any actions compromising the information owned by an organization or a person;
- mechanism that is designed to detect, prevent or recover from a security attack;
- service that enhances the security protection of data processing and information transfer via the network.

Annex C provides criteria for establishing network security services.

5.4 Network performance consideration

5.4.1 Traffic

Traffic refers to the overall communication network usage and transaction of information at any given point in time. The information consists of messages, records, and data. Network performance related to traffic issues is generally known as trafficability performance.

Trafficability performance is the ability to meet traffic demand and handling capacity of the network.

The requirements for traffic volume have increased significantly with the growing needs for communications and entertainment. In a global environment, there are increasingly more communication carriers in competition to deliver data, voice and video services on a single bearer network to reduce operating expenditure. This trend demands cost-effective processing of network traffic that affects dependability in network performance.

a) Capacity

Network planning and design should consider future network growth, analyze the requirements of the anticipated network service functions related to traffic flow capacity, and the impact of bursting traffic for cost-effective network capacity utilization and flow control optimization. A network capacity with proper redundancy can achieve favourable network service access capability and accommodate anticipated growth and future development in communication traffic needs.

b) Congestion control

The instability of traffic flow over time is reflected in that a large amount of traffic could travel through the network at the same time during a short period. This is known as “traffic burst”, where the “bottleneck” or limitation of network resources will emerge. For example, when the capacity of a network segment is inadequate, the traffic is congested, and the processing capability of a network element is queued causing a “bottleneck” situation. This would result in the access denial of some new network services, the telephone sessions delayed, and the quality of sustaining network services degraded. Modern networks bear multiple services in a more effective manner by using the statistical multiplexing technology.

The congestion control technology includes techniques such as congestion detection, access control, committed access rate, discarding strategy, queuing, and bandwidth management. Congestion control acts in different ways for different network services. Congestion causes network unavailability in service provision. Dependability issues related to congestion control should be considered in network reliability assessment.

c) Traffic performance

The quality of traffic flow is quantitatively reflected in the network traffic performance parameters. For example, in Internet Protocol (IP) transport network, the packet transfer delay, delay variation, loss ratio, would affect the quality of traffic performance. When network transfer performance is degraded to a certain degree or threshold, some normal services can no longer be provided.

5.4.2 Transmission

There are various means to transfer voice, video, data or other information over a communication network. Transmission performance reflects the capability of communication network that transfers relevant services in normal operation. The performance is related to the type and quality of transmission medium and the intensity of signal to noise ratio. This would affect network dependability.

a) Synchronization

Synchronization is the process that ensures the signal sending equipment and the signal receiving equipment work in perfect alignment for reliable transmission of data. The synchronization network is an important supporting network. When analyzing the dependability of a communication network, analysis and evaluation of clock fault, timing error, and associated risks should be performed. Both the impact of clock fault on the communication network and the correctness and dependability of the clock network itself should be considered.

b) Transmission integrity

Transmission integrity is the ability of the signals, consisting of information and data, carried by the communication network, to have minimal errors during transport. It can be measured by parameters such as bit error ratio and error free seconds ratio, etc. High

quality transport media as well as rapid and reasonable fault switching protection and re-transmission mechanism should be used to significantly improve signal integrity. Transmission integrity would affect dependability performance.

c) Connection quality

Connection between networks is the basis for delivering communication functionality. Connection quality reflects the capability of network link to transport information. The evaluation of link transport quality should consider the level of noise and interference, and the speed of transmission. The evaluation is applicable to both fixed connection and propagation of radio signals. Connection quality would affect dependability performance.

5.4.3 Robustness

Robustness reflects the adaptability of a network to conditions of abnormalities. Network dependability design and implementation could improve robustness in network performance and enhance mission or safety critical features incorporated in network safety operation.

a) Reliability

Reliability forms the basis of a robust network. Within cost constraints, the use of highly reliable network devices, high quality network links, and “bug-free” software would help achieve sustainable reliability in practice.

b) Survivability

Survivability refers to the capability of a network to recovery within acceptable performance limits upon encountering incidents or faults. This would permit the network to continue delivering normal network functions. Acceptable performance limits are determined from the network service provider’s service level agreement (SLA) to meet QoS requirements (see Clause 7). The frequency and duration of adverse situations in specific service areas often dictate the extent of network design and operation to maintain survivability. Consideration should be given in network design to focus on dependability to improve network survivability and recoverability, especially when safety issues are involved.

c) Fault tolerance

Fault tolerance reflects the capability of the network to perform in the presence of faults. That is, the network continues to work upon experiencing internal fault, reflecting its sustainable transport capability for providing the services. Generally, fault tolerance of a network can be achieved with redundancy design, and the incorporation of network fault management system for network operation. For example, when a fault is found, the standby unit will take over the operating functions of the active unit immediately to assure sustainable processing of services.

5.4.4 Serviceability

Serviceability reflects the delivery of network dependability of service to the end-users. Higher serviceability improves availability, provides integrity of service without excessive impairments, and reduces service costs. Serviceability can be described using the following performance criteria.

a) Service accessibility

Service accessibility is the ability of a network service to be accessed by the user, under given conditions, for a given period of time. For connection-oriented services, it refers to the ability to establish connection. Accessibility can be measured in terms of service access delay, network access capability, and service access control capability. The evaluation of accessibility should consider the user’s network accessibility such as establishing connection of the physical circuit, and the ability to establish service connection or service receiving capability such as establishing connection for high layer call control.

b) Service retainability

Service retainability is the ability of a network service, once obtained, to continue to be provided under given conditions for a requested duration. It reflects the reliability of the service.

service traffic continual transmission, let alone with traffic accessing or disengaging of the network. The provision of an end-to-end service involves multiple network devices and links. Retainability requires network dependability support to maintain stable operation. Network design redundancy and fault management are generally accepted practice to improve fault tolerance for service retainability.

c) Service integrity

Service integrity is the delivery of information and data by the network without excessive impairment. Service integrity relates to the transfer of information and data known as throughput. The impairment is generally caused by noise, time/speed variation, and partial distortion during transmission.

d) Disengagement

Disengagement concerns the network devices and links involved in the end-to-end communication of a user as well as network resources (including bandwidth, channel or resources related to upper-layer protocols) to be released when the communication connection or session is closed. A highly dependable network could ensure the reliability and accuracy of disengagement. This would avoid long-term seizure of resources, abnormal charging and other problems. Disengagement is a characteristic affecting service accessibility and service retainability in network serviceability.

5.4.5 Operability

Operability can be viewed from two aspects.

- a) From the user's perspective, operability refers to the ability of a service to be successfully and easily operated by a user. For example, the operability for a user to gain network access or the operability for a user to dial a number. Service providers can provide users with reliable connection for ease of use to improve the reliability of user operations.
- b) From the service provider's perspective, operability refers to the ability of the network to be successfully and easily operated by the communication carrier, including service delivery and network management. By improving the network operability for ease-of-use with user-centred design and protection of abnormal operation, the faults caused by operation can be greatly reduced, hence improving dependability.

5.5 Integrity of network data and information

5.5.1 Credibility of network data throughput

The need for data integrity is identified through market survey of service provider needs and user requirements related to the accuracy and protection of information when using the network services. The information represents an independent entity carried by the communication network from input to output. Integrity reflects the credibility of the information, transformed as data throughput in the network operation. Data throughput is the amount of digital data per time unit that is delivered over a physical or logical link, or that is passing through a network node in a communication network. Credibility is the ability of the network service functions to recognize the extent of correct inputs to permit authorized access. The network elements and the responsible service functions transform the user inputs into the outputs for the intended recipients. The integrity characteristic of network dependability is the ability of the network to provide a secured passage for protection of the data throughput contents. Integrity is the assurance process for the network service functions to ensure that the data throughput contents are not contaminated, corrupted, or altered in transforming the inputs into outputs.

Achieving integrity is dependent upon the mechanisms implemented in the network elements and the service functions designed to detect and prevent incorrect transition of data flow between the network processing functions. It also depends on the mechanisms used to verify the accuracy and authenticity of data inputs and outputs. Integrity in this context is deterministic and some aspects can be quantified. An example is the authorization of access to an automatic teller machine for cash withdrawal. The machine validates that the credit card and personal identification is genuine and permits the cash withdrawal. In such case, the integrity of a distributed automatic teller machine network can be assessed quantitatively.

based on influencing conditions such as access denial frequency, user population and usage, the volume of business transactions and crime rates in the area. The integrity indication from a user's view point could be assessed qualitatively that the automatic teller machine is efficient, convenient, working sometimes, or broken.

5.5.2 Network control of data impairment

Integrity also refers to the processing of the transmission signal information as data throughput in a network operating environment without excessive impairment. Integrity can be understood from the knowledge of network hierarchies. The lack of integrity or inadequate data control at the bottom layer is reflected in the transmission damage due to the quality of the transmission media. The integrity of the packet carrier layer can be measured in packet drop ratio and error packet ratio. The integrity of the service layer is reflected in the integrity of information data.

- *Service data*: a service provided by the network. Once the user has obtained a specific service, the network should ensure that the service is free of excessive impairment. Service interruption and outage reflect such impairment. The integrity of service data can be improved by adopting redundancy design and accelerating protection switching in the event of faults. Service data include service control data and service media data.
- *Program data*: a program is a set of coded instructions for the running of network software. Program reliability should stress abnormal modification, such as write protection of program memory and provision of a checking mechanism. This is to enhance the integrity of software program data.
- *Information data*: supporting information for running the network software, such as user information and transmission control protocols connection information. The integrity of such information should be considered for network reliability design. In redundancy design, information backup should be incorporated into the network to avoid impairment.

5.6 Quality of service (QoS)

5.6.1 QoS objectives

In the context of network dependability, QoS deals with the effects of network performance to determine the level of quality in the service provision. QoS is defined by the SLA.

The level of quality is the degree of satisfaction represented by QoS. Dependability is a quality attribute. It assures the continuity of service against failures and denial of service access and disengagement, and the transfer of user information against loss or interruption.

QoS is a generic term derived from a set of indicators. It is assessed by the service providers to determine the performance value of the network to ensure their return-on-investment and to improve their service offerings. QoS is also perceived by the users (subscribers of communication services) to ascertain the value of the service they are paying for.

The applications of QoS include:

- determining the QoS and network performance relationships in the network dependability framework;
- identifying the performance attributes and factors influencing the outcome of QoS;
- establishing measurable and observable parameters relevant to QoS;
- identifying the process and methodology for QoS assessment.

5.6.2 Service level agreement for provision of QoS

A service level agreement is a formal agreement between two or more parties. This is a common business practice for business partners in the provision of network service functions. The agreement for provision of QoS includes statements on performance, billing, service delivery, and legal and economic issues.

There are two parts in the agreement.

a) General agreement

The general agreement provides a statement of purpose of the agreement and the partnerships involved.

The purpose of the agreement is

- to define the service levels that all interested parties have to guarantee for customer satisfaction;
- to assist the user, service provider, network provider in exchanging information with suitable quality of service and network performance;
- to provide a basis for measurements and parameters for realization of the service level agreement;
- to stipulate penalties in case of SLA breach for contract termination and dissolution.

The scope of the agreement should describe the provision of the services and their target performance.

A statement of confidentiality should be stated specifying the treatment of the agreement, the sharing of information, and the obligations of the parties involved.

A review process should be incorporated in the agreement to state the frequency and the format for review.

The general agreement should be signed by the designated authorities representing the parties involved.

b) Specific agreement on provision of quality of service

The specific agreement provides details of the specific quality of service agreement of an individual party involved.

The contents of the specific agreement on provision of quality of service should include:

- interface description to set the boundary of the individual party involved at interaction points for the purpose of exchanging information with the service provider who is controlling all the interaction points;
- business interface information: composed of interaction points located between the user and the service provider for specific quality of service agreement functions, performance reporting, and reaction patterns to indicate the agreed level of quality of service provided;
- technical interface information: composed of interaction points exchange service specific information to permit measurements of quality of service achieved;
- traffic patterns description and measurement schemes;
- quality of service parameters and objectives specific to this agreement;
- quantitative and qualitative measures of QoS requirements such as availability performance and other relevant dependability characteristics;
- penalty statement on terms and conditions specific to SLA breach for contract termination and dissolution.

5.6.3 QoS and network performance relationships

QoS is derived from the results of network performance through established relationships. QoS is determined by a set of criteria of importance to the service providers as well as to the users of the network services. These criteria can be translated into performance parameters. Network performance may represent the performance of an individual network element, or the network as a whole. Network performance influences the outcome of the QoS.

The users of a network service are generally interested in QoS for end-to-end service such as completing a telephone call or the successful messaging on the Internet. The quality performance of interest to the users is the assurance at the service access point.

The service providers are more interested in the efficiency and effectiveness of the network performance associated with system development, network planning, and operation and maintenance. The interest on quality of the service providers is at network connection points.

A network may have several service providers working together to complete the entire network services. For multiple network provider environments, there may be different levels of QoS involved in the network services. In practice the users may experience a variety of QoS ranges. Hence minimum performance levels for each service, and also for the network connection elements should be established to conform to the respective service level agreement applicable to each service provider.

The communication process consists of key service functions:

- the *access* function permits the user to gain access to the network resources to start the communication process;
- the *user information transfer* function provides the end-to-end exchange of information;
- the *disengagement* function covers the ending of a communication process.

The relevant service quality criteria related to the communication process include:

- *speed* to indicate the time interval used to perform the function;
- *accuracy* to denote the degree of correctness of the function performed;
- *availability* to assure the degree of certainty of the function performed.

From this set of primary performance parameters and outage thresholds, a combination of the QoS requirements can be determined (see Clause 7). The derived performance parameters can be represented by a quantifiable function or functions for the purpose of performance measurements.

5.6.4 QoS and dependability relationships

The link to QoS is the identification of dependability as a quality attribute for serviceability contribution in delivering dependability of service to the end-users. Dependability characteristics include availability performance and its influencing factors such as reliability, maintainability and maintenance support. Availability is a network performance parameter affecting the outcome of QoS. Hence the relationships between QoS and dependability can be linked.

Dependability covers a broad range of technologies and influences the provision of QoS. The applications of dependability engineering facilitate the realization of reliable products, simplify the maintenance processes, and provide cost-effective logistic support strategies. Dependability adds values to QoS in network performance. The following illustrate some examples of the QoS and dependability relationships.

- The queuing process is used in dependability applications for stochastic analysis of process flow and congestion delays. The queuing technique is employed at the network transport layer to determine the types of network service affecting QoS. The QoS relationship with dependability can be linked in determining the optimum routing architecture and recovery mechanisms for network technology application.
- The network policy in service provision employs various schemes to guarantee QoS. The integrated logistic support strategy is a dependability process to optimize availability performance and enhance maintenance support effort that affects provision of network service functions. The QoS relationship with dependability can be linked by improved availability performance through cost-effective provision of network services.
- The robustness in network performance requires dependable access (*accessibility*) and retention (*retainability*) for network connections. Dependability techniques utilizing redundancy design would improve network performance influencing the outcome of QoS.

- Dependability engineering applications can be viewed as an enabling mechanism to enhance network performance and provide effective network service functions which affect the outcome of QoS. Dependability influences the delivery of QoS.

The mapping of QoS, dependability, and network performance with the identification of key dependability influencing factors is shown in Figure A.4.

QoS measurement is described in Clause 7.

6 Network dependability assessment and measurement

6.1 Network dependability analysis

6.1.1 Objective of network dependability analysis

Network dependability analysis is aimed at improving the network design and operation flow. The analysis provides a means to identify various networking alternatives for selection of an optimal range best suited for determining the network dependability requirements and for resource planning and allocation.

6.1.2 Network dependability analysis process

6.1.2.1 General method for network dependability analysis

Network dependability analysis should identify and determine the characteristics of all the functions associated with the realization of network performance. For each identified function, the analysis should consider the faults of various network nodes and physical links in the network that can affect different network services. They include network service functions affected by the operating environment, hardware and software, maintenance support, human errors, and network design. The assessment should validate the practicality of technology used in the network for dependability improvement.

Network dependability analysis should include the following:

- a) the analysis should consider the application or use environment and evaluate the risks involved from nature and human factors influences;
- b) the network boundary should be identified to determine all the network nodes and links;
- c) a set of network failure classification (see 5.1.3.2) should be established to facilitate identification of possible fault conditions by the network service provider, network operator and network users. The type of failures classified should be measurable under established conditions. Network performance levels can be defined as the probabilities of fulfilling the network functions. Performance levels can be measured and determined for evaluation over a period of time.

6.1.2.2 Other methods for consideration

- a) Qualitative analysis method
 - Consider the network services and the network design architecture, determine the modes, mechanisms, causes, and effects of the network failure, and define the fault severities. Based on the network service functions, fault severities are defined in various levels in terms of the scope, duration, and degree of the impact produced by the faults on the services and in terms of the service experience of the users;
 - Analyze the detection and repair time necessary for the fault to be identified, the isolation methods that can be used, and the repair methods;
 - Determine the possibility of avoiding faults, and the strategy and dependability technologies that can be used to reduce the probability or impact of faults.
- b) Quantitative analysis method
 - Create network models with the help of network dependability simulation;

- Collect relevant data for the network model;
- Analyze and evaluate network dependability by using applicable network dependability analysis methods.

c) Use of classical reliability analysis methods

Classical reliability analysis methods [3] are often used for network dependability analysis. Some methods are standardized such as Failure Mode and Effects Analysis (FMEA) [7], Fault Tree Analysis (FTA) [8], Reliability Block Diagram (RBD) [9] and Markov techniques [10].

6.2 Network dependability fault insertion test

6.2.1 Objectives of fault insertion test

The network fault insertion test is performed for verification of network performance for the following purposes:

- testing to verify the network dependability conforms to the requirements of the network service provider, and to determine that the network design objective is met by simulating the actual operating scenario of the network;
- detecting the weaknesses and potential problems in the network dependability design, and timely revising and optimizing the network design before the network is officially put into service;
- obtaining relevant dependability data for evaluation.

The network dependability fault insertion test should be comprehensive but remain practical. Consideration should be given to faults resulting from equipment failures, environmental effects and human mishaps under normal network operation. Relevant experienced information should be used to design the test cases to reflect the causes of the faults. The faults are injected to the network under test for simulation. This is done by accelerating the occurrence of the faults to determine mitigation or solution.

6.2.2 Fault insertion test process

The network fault insertion test needs detailed planning. The test process should:

- a) analyze the layers, topology, services provided, expected traffic distribution and network service paths of the network under test according to the network dependability design requirements. A test strategy should be developed and test cases should be derived from on-site experience data;
- b) plan various resources including human resources, arrange test environment and time schedule. Build the test environment according to the expected service scenario, test and configure the traffic simulation tool and fault insertion tool as necessary, and prepare the test plan. Familiarize with the test environment and the use of various instruments and tools necessary for the test;
- c) execute the test cases and record the test results. Observe all the related network elements and service paths during the test. Determine the scope and extent of impact of the fault on the network service functions, the service recovery time, and the tolerance capability of the network;
- d) maintain detailed records of the failures and anomalies detected during the test. Assess the situation as to how the malfunctions occur, their consequences, residing equipment, failure classification, severities, and expected correction dates;
- e) collate the test records and analyse the test results to validate dependability conformance. Finalize the test report and recommend improvement where applicable with supporting rationale.

6.3 Measurement of network dependability attributes

6.3.1 Objectives of measurement of network dependability attributes

Measurements of network dependability attributes provide powerful insights into network dependability performance. They are used to evaluate the outage frequency and downtime duration delivered to the user during network operation. The goal is to reduce both the frequency and duration of outages and their associated cost and impact causing customer dissatisfaction.

6.3.2 Process for measurement of network dependability attributes

Network dependability attribute measurements include outage frequency and downtime. These measurements provide statistics from equipment providers and service providers reflecting their respective experiences. The criteria for incident reporting, the classification of faults, and the measurement parameters and recording procedures should be established and documented prior to the measurement process.

The following are typical network dependability attribute measurements captured for incident reporting:

- network outage downtime frequency;
- network outage downtime duration;
- network service impact related to the numbers of subscribers affected for each outage occurrence;
- network service restoration or recovery time;
- network failure classification (see 5.1.3.2) traceable to specific failure category.

From these set of measurements, specific network dependability attributes can be determined.

- *Availability* can be determined from relevant network performance data collected on up-time and down-time. The steady-state network availability may be expressed as the ratio of the mean up-time to the sum of the mean up-time and mean down-time.
- *Reliability* for a network link or node can be determined by measurement or estimation of failure probability or failure rate of the network link or node.
- *Maintainability* denotes the time necessary for maintenance, which may include the time for technical and logistic delays. Maintenance actions can be preventive or corrective. Maintainability can be expressed as the probability that a given maintenance action, performed under stated conditions and using stated procedures and resources, can be carried out within a stated time interval.
- *Maintenance support performance* can be determined from information related to the provision and management of resources to perform the maintenance tasks. Maintenance support performance is the ability of an organization to complete a maintenance action upon demand and under given conditions.
- *Recoverability* of a network can be determined by measurement of the time required to achieve restoration. This represents the duration from the time of a detected network fault to the time the network is restored for normal operation. This is generally expressed as time to restoration or time to recovery. Recoverability applies to the recovery from complete or partial failure of a network or from a degraded state of network operation.

6.4 Network dependability assessment methods

6.4.1 E2E network dependability assessment

a) Objectives of E2E network dependability assessment

E2E network dependability assessment is the process of evaluating the network dependability characteristics on end-to-end services from the perspective of network users. Dependability characteristics include availability and influencing factors affecting network

performance. To assess E2E network dependability, the typical service scenarios relevant to the network topology and service paths should be analysed. The E2E dependability assessment covers various scenarios. This would facilitate determining the improvement areas.

b) Typical process for E2E network dependability assessment

- Identify typical service scenarios for the analysis. For example, a typical scenario could be a user turning on a cell phone to register into network.
- Establish the functional structure of the E2E network topological configuration pertaining to a specific scenario for analysis. Determine the path of the service data in the service application. The creation and maintenance of an E2E service is related to both the equipment involved in the service data path and the control equipment. The path of the control signaling should be considered in addition to the media service data path.
- List the failure mode, and conduct failure mode and effects analysis based on the E2E service path. The result can be used for network optimization.
- Develop failure models to predict network path availability to support design decisions. Techniques such as RBD or Markov technique can be used.
- Construct the RBD for the entire E2E network from top down to represent the network structure layer by layer for the sub-networks and lower modules where applicable.
- Some sub-networks such as core network are often designed with the dual-plane redundant structure for high reliability configuration. Redundancy should be reflected in constructing the RBD.
- On the entire E2E path, there are service layer equipment, control layer equipment, and bearer layer equipment and links. Top-down analysis approach is commonly used to calculate the network availability.
- Influencing factors inherent and external to the applicable E2E network should be documented. Constraints and limitations affecting the functional configuration of the E2E network performance should be noted. Design trade-offs and alternate solutions should be investigated.
- The complete E2E network dependability assessment results including breakdowns of sub-networks and lower level modules of the entire E2E network configuration for each service scenario should be documented.

6.4.2 Full-end network dependability assessment

a) Objectives of full-end network dependability assessment

Full-end network dependability assessment is the process of evaluating the network dependability characteristics of the entire network from the network operator or the network service provider perspective. Unlike E2E dependability assessment, full-end network dependability assessment does not focus on the E2E service path in specific scenarios, but on the overall operation status of the network. Full-end network dependability design considers all the equipment and links of the entire network including the network protection mechanism. This is to improve the network design for best cost-effect ratio.

b) Typical process for full-end network dependability assessment

- Analyse typical service functions. For example, a typical service function could be setting up a video conference call or transmitting voice over the Internet.
- Conduct failure mode and effects analysis, and evaluate the effects of failure mode impacts on affecting the percentage of users in the service area, frequency and duration, and repair actions. The result can be used for network optimization.
- Develop failure models to predict the full-end network availability using RBD or similar methods to identify the network functions based on a top-down and layer-by-layer approach. Where applicable, experienced network failure data should be used.

- The relationships between various network functions in the RBD representing the network elements such as sub-networks, modules, and units according to the network configuration and protection switching mechanism can be established.
- A weighted method is used to evaluate the contribution of each network node or link failure to the whole network failures. The weighted ratio which reflects the contribution of the node or link failure to the whole network failures can be determined. For example, the traffic capacity of a network user impacting the individual node or link failure contributes to the whole network failures due to traffic capacity affecting all the users.
- The full-end network downtime can be determined by summation of the weighted failure contributions. A common industry practice is to interpret network downtime on an annual basis to reflect overall network dependability performance.
- The results of the full-end network dependability assessment including frequency of downtime occurrences, inherent and external influencing factors should be recorded.

7 Quality of service measurement

7.1 QoS measurement overview

QoS is used to determine the degree of satisfaction of the network service performance. QoS can be viewed from four perspectives.

- *User's QoS requirements* – This is the statement of the level of quality of a particular service required or preferred by the user. The level of quality may be expressed by the user in technical or non-technical language.
- *Service provider's offering of QoS* – This is the statement of the level of quality expected to be offered to the user by the service provider. The level of quality is expressed by values assigned to QoS parameters as per SLA.
- *QoS achieved or delivered* – This is a statement of the level of quality achieved or delivered by the service provider. The level of quality is expressed by values assigned to the parameters as per SLA.
- *User survey rating of QoS* – This is a statement expressing the level of quality experienced or perceived by the users at large from customer satisfaction survey results. The level of quality represents the degree of user satisfaction.

QoS measurement utilizes a set of service quality criteria for assessment of network service functions. The QoS measurements provide subjective appraisal as well as quantitative performance values.

The network service functions include key performance issues, or parameters of concerns by the network users and the network service providers. Network service functions can be related to:

- *service management* (i.e. sales contract management, management of service support, maintenance activities, and provisioning of services) for qualitative or subjective appraisal;
- *connection quality* (i.e. network connection access, information transfer, and disconnection or disengagement of network) for quantitative assessment;
- *billing* to determine the transaction cost in doing business;
- *network service management by customer* (i.e. configuring network devices, provisioning of services, and managing faults associated with customer/user applications).

The service quality criteria include:

- *speed* (i.e. the speed with which a service function or the provision of the service is carried out);

- *accuracy* (i.e. the correctness and completeness in carrying out the service function with respect to a reference or specified level);
- *availability* (i.e. service upon demand for accessing and using the service function);
- *reliability* (i.e. performance of service function without impairment or failure over a specified time period);
- *security* (i.e. the confidentiality with which the service function is carried out by the service provider to the user);
- *simplicity* (i.e. the ease in the application of the service function);
- *flexibility* (i.e. the options available in the provision of service functions to accommodate special requirements).

The importance of the service quality criteria varies with the provision and performance of network service functions to meet diverse users' needs. The QoS measurement should reflect the importance of the service functions from an application perspective [14].

7.2 Generic user-oriented QoS parameters and requirements

QoS parameters can be obtained from the list of network service functions and the set of service quality criteria considered important to the user [14]. The user's QoS requirements can be captured by using a matrix table representing the selected service functions in a vertical column against a horizontal row of important service quality criteria. The individual cells in this matrix table facilitate the capture of the relevant QoS requirements.

Table 1 presents an example of a matrix for capturing the QoS requirements. The service functions selected include access, user information transfer, and disengagement representing the identified service function of connection quality of specific interest to dependability engineering. The service quality criteria of importance to the user are speed, accuracy, and availability. The data captured in the matrix provide useful information on the user's QoS requirements of specific interest to dependability design implementation.

The QoS requirements are used to help dimension the parameters of the communication carrier network through the relationship:

$$\text{QoS requirements} > \text{Required network performance} > \text{Required network parameters}$$

Dependability plays an important role in ensuring network performance and delivery of QoS to the users or customers.

Table 1 – A matrix for capturing user's QoS data

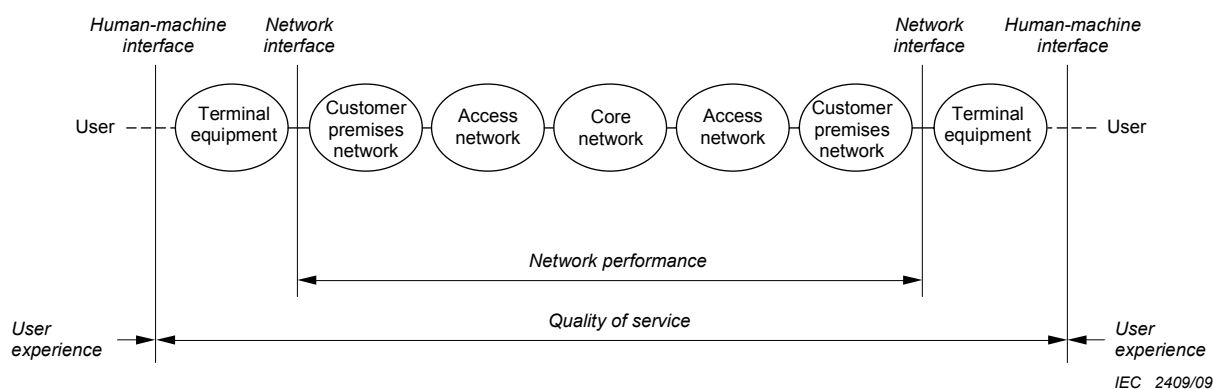
Service quality criterion	Speed	Accuracy	Availability
Connection service function			
Access	• Access delay	• Incorrect access probability	• Access denial probability • Access failure probability
User information transfer	• User information transfer delay • User information rate • User information transfer time/speed-variation	• User information error probability • Extra user information delivery probability • User information mis-delivery probability	• User information loss probability • User information transfer cut-off probability • User information transfer interruption probability • User information transfer interruption duration
Disengagement	• Disengagement delay	• Incorrect disengagement probability	• Disengagement denial probability • Disengagement failure probability

Annex A (informative)

Generic communication network model and related concepts

A.1 Generic communication network model

A generic communication network model is shown in Figure A.1. It identifies the connection points, network access boundaries, network interfaces, and the flow of information path. Network performance reflects the performance contributions of the core network, access network and customer premises network. QoS is viewed by the service provider as the performance value of the network configuration pertaining to the provision of network service functions to satisfy its customers. QoS is perceived by the user as user experience for end-to-end network connection services. Terminal equipment such as a computer facilitates the user access to the network.



User experience	Quality of service	Network performance
User oriented	User oriented	Service provider oriented
User behaviour attribute	Service attribute	Connection/flow element attribute
Focus on user-expected effects	Focus on user-observable effects	Focus on planning, design, operation and maintenance
User subject	Between or at service access points	End-to-end or network elements capabilities

Key

Terminal equipment – user equipment connected to the network user interface such as a personal computer

Customer premises network – customer premises network (e.g. a customer based network providing communications and control interface functions between the users or subscribers and the public information networks)

Access network – a network providing connections for users or subscribers access to their immediate service provider for connections to the “backbone” communications network

Core network – a “backbone” communications network consisting of high-speed transmission lines or media (national or international) connecting between major switching networks (points) at various locations in a country or region

Figure A.1 – A generic communication network model