IEC 61907

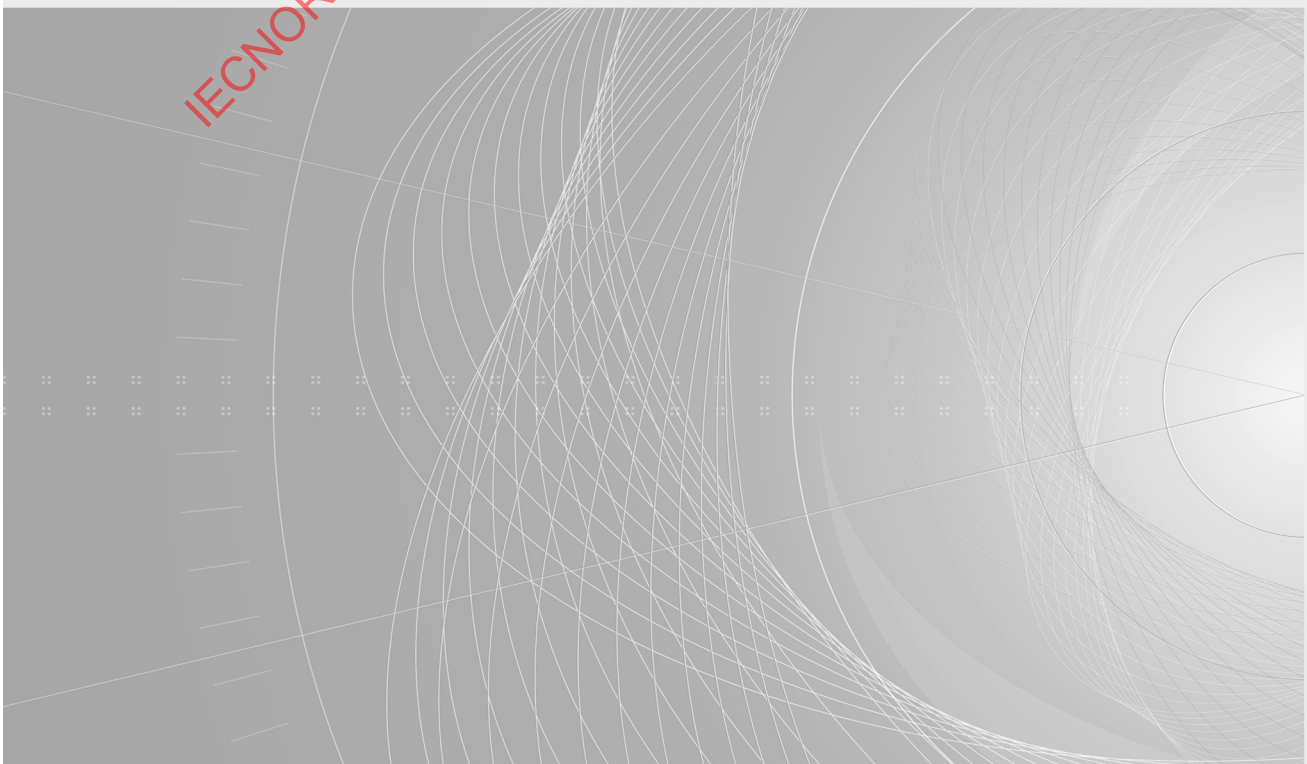
Edition 1.0 2009-12

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Communication network dependability engineering

Ingénierie de la sûreté de fonctionnement des réseaux de communication



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

About the IEC

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

About IEC publications

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

- Catalogue of IEC publications: www.iec.ch/searchpub
The IEC on-line Catalogue enables you to search by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, withdrawn and replaced publications.
- IEC Just Published: www.iec.ch/online_news/justpub
Stay up to date on all new IEC publications. Just Published details twice a month all new publications released. Available on-line and also by email.
- Electropedia: www.electropedia.org
The world's leading online dictionary of electronic and electrical terms containing more than 20 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary online.
- Customer Service Centre: www.iec.ch/webstore/custserv
If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:
Email: csc@iec.ch
Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00

A propos de la CEI

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

A propos des publications CEI

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

- Catalogue des publications de la CEI: www.iec.ch/searchpub/cur_fut-f.htm
Le Catalogue en-ligne de la CEI vous permet d'effectuer des recherches en utilisant différents critères (numéro de référence, texte, comité d'études,…). Il donne aussi des informations sur les projets et les publications retirées ou remplacées.
- Just Published CEI: www.iec.ch/online_news/justpub
Restez informé sur les nouvelles publications de la CEI. Just Published détaille deux fois par mois les nouvelles publications parues. Disponible en-ligne et aussi par email.
- Electropedia: www.electropedia.org
Le premier dictionnaire en ligne au monde de termes électroniques et électriques. Il contient plus de 20 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International en ligne.
- Service Clients: www.iec.ch/webstore/custserv/custserv_entry-f.htm
Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions, visitez le FAQ du Service clients ou contactez-nous:
Email: csc@iec.ch
Tél.: +41 22 919 02 11
Fax: +41 22 919 03 00

IEC 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

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 network

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 for

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

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:

QoS requirements > Required network performance > 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

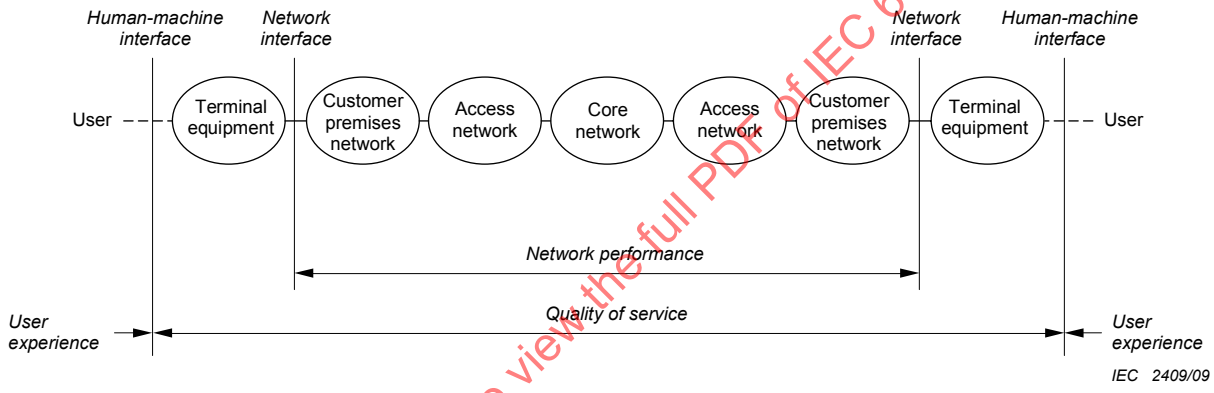
Service quality criterion Connection service function	Speed	Accuracy	Availability
Access	• Access delay	• Incorrect access probability	• Access denial probability • Access failure probability
User information transfer	• User information transfer delay • User information rate • User information transfer 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

A.2 Interactions of network dependability framework areas of influence

The concept of communication network dependability framework can be viewed from the interactions of areas of influence which consist of:

(1) the application of *dependability engineering*;

(2) the utilization of *network technology*;

(3) the delivery of *network performance*;

(4) the deployment of *network service functions*;

(5) the *integrity* of network data and information;

(6) the provision of *quality of service*.

The interactions of areas of influence are shown in Figure A.2 utilizing a process model to illustrate the relationships.

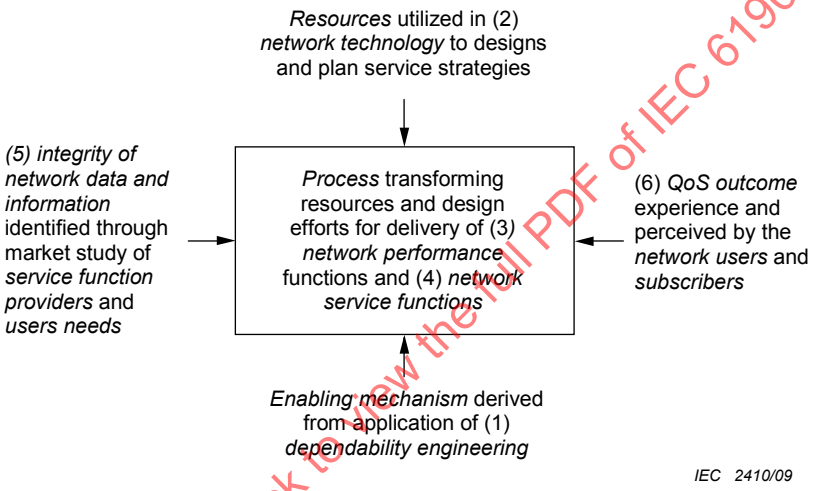


Figure A.2 – A process model on interactions of areas of influence

A.3 Communication network reference models

A.3.1 OSI reference model

A.3.1.1 General

The OSI reference model, which describes the various layers associated with a communication network, is presented in Figure A.3. The OSI reference model is a joint ISO and ITU-T standard for computer networks and communication protocols [12].

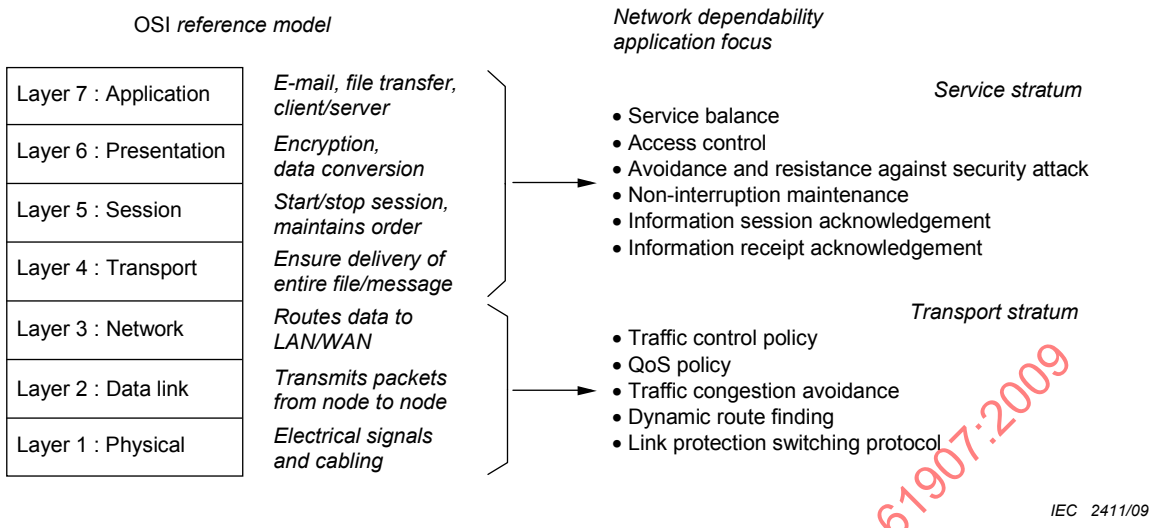


Figure A.3 – OSI reference model

A.3.1.2 Upper layers of OSI reference model

Layers 7 through 4 comprise the upper layers of the OSI protocol stack which are geared to the type of application rather than the lower layers designed to move packets. A packet is a block of data transmitted or sent over a network.

- **Application layer 7:** defines the language and syntax that programs use to communicate with other programs. Common functions at layer 7 are opening, closing, reading and writing files, transferring files and e-mail messages, executing remote jobs and obtaining directory information about network resources.
- **Presentation layer 6:** negotiates and manages the way that data are represented and encoded when data are transmitted between different types of computer systems. Layer 6 is also used for encryption and decryption.
- **Session layer 5:** provides coordination of the communications in an orderly manner, determining one-way or two-way communications and manages the dialog between both parties. Layer 5 provides marking on the significant parts of the transmitted data with checkpoints to allow for fast recovery in the event of a connection failure. (Note: in practice, Layer 5 is often not used. The services within this layer are sometimes incorporated into the Transport Layer 4.)
- **Transport layer 4:** is responsible for overall end-to-end validity and integrity of the transmission.

NOTE OSI transport services include layers 1 through 4 collectively responsible for delivering a complete message or file from sending to receiving station without error.

A.3.1.3 Lower layers of OSI reference model

Layers 3 through 1 are responsible for moving packets from the sending station to the receiving station.

- **Network layer 3**: establishes the route between the sender and receiver across switching points, which are typically routers.
- **Data link layer 2**: is responsible for node to node validity and integrity of the transmission.
- **Physical layer 1**: is responsible for passing bits onto and receiving them from the connecting medium and deals with the electrical and mechanical characteristics of the signals and signalling methods.

A.3.2 Next generation network reference model

The next generation network (NGN) architecture [18] is represented by two distinct blocks separating the upper and lower OSI layers to provide the network service functions and the network transport functions. These blocks are known in the NGN architecture as strata of functionality. The transport functions reside in the *transport stratum* and the service functions related to applications reside in the *service stratum*. The NGN strata of functionality are shown in Figure A.3 indicating the grouping of layer blocks.

The *service stratum* provides the user functions that transfer service-related data and the functions that control and manage service resources and network services. The service function enables user services and applications.

The *transport stratum* provides the user functions that transfer data and the functions that control and manage transport resources to carry such data between terminating entities. The transport functions provide connectivity.

A.3.3 Transmission Control Protocol/Internet Protocol (TCP/IP) model

The TCP/IP is a protocol for communication between computers, used as a standard for transmitting data over networks and as the basis for standard Internet protocols. The TCP/IP is a 4 layer stack consisting of the application layer, transport layer, network layer (Internet layer), and the link layer (network interface layer).

A.4 QoS, dependability, and network performance relationships

Figure A.4 shows the QoS, dependability, and network performance relationships. It presents a framework for mapping the relationships to reflect current network operations, including the provision network services of voice, data, and video as well as Internet and Web services.

The *QoS layer* on the top showing the quality of service characteristics is separated from the bottom *network performance layer* representing the contributions of various performances and attributes. *Dependability* attributes are influencing the serviceability to QoS by delivering *dependability of service* and contributing to network performance in *dependability performance*. The connections of the three circles indicate that there are three distinct technical domains in network operations. Dependability as a technical discipline influences the provision of QoS to satisfy user expectations and fosters the achievement of effective network performance to meet SLA requirements. The overall network performance affects the achievement of QoS.

QoS is dependent on the provision of network services, security of service, and serviceability in delivering dependability of service in network operations to facilitate user communications. Key QoS characteristics include accessibility and retainability of the network functions, maintenance support of network services from the network operator and user perspectives, and integrity and security of the data throughput of the network operations reflecting the user satisfaction.

Dependability of service is a key contributing factor in serviceability to QoS to meet user satisfaction. The delivery of *dependability of service* deals with the processes of successful performance achievements of service accessibility, service retainability, and service integrity to establish E2E network service connections.

The *dependability performance* characteristics consist of *availability, reliability, maintainability, recoverability, integrity,* and *maintenance support.* These characteristics influence network capability performance, trafficability performance, and network security performance. They act in collaboration as enabling agents to guide efficient network management for planning, administration, monitoring and control processes, and effective implementation of network fault management systems and customer care services.

The application of dependability engineering in network architecture construction and network element designs would influence the effective harnessing of technologies to achieve the network performance objectives. Network service performance could be improved by implementation of appropriate process simplification, hardware reduction, software upgrades, maintenance support strategies [5] and logistic support schemes [6] to maximize the benefits of resource allocation and operational effectiveness. Dependability also provides a forward looking prediction method to project network performance trends based on continual improvement process. Dependability and related technical disciplines when properly applied in network service functions would generate user confidence and customer satisfaction.

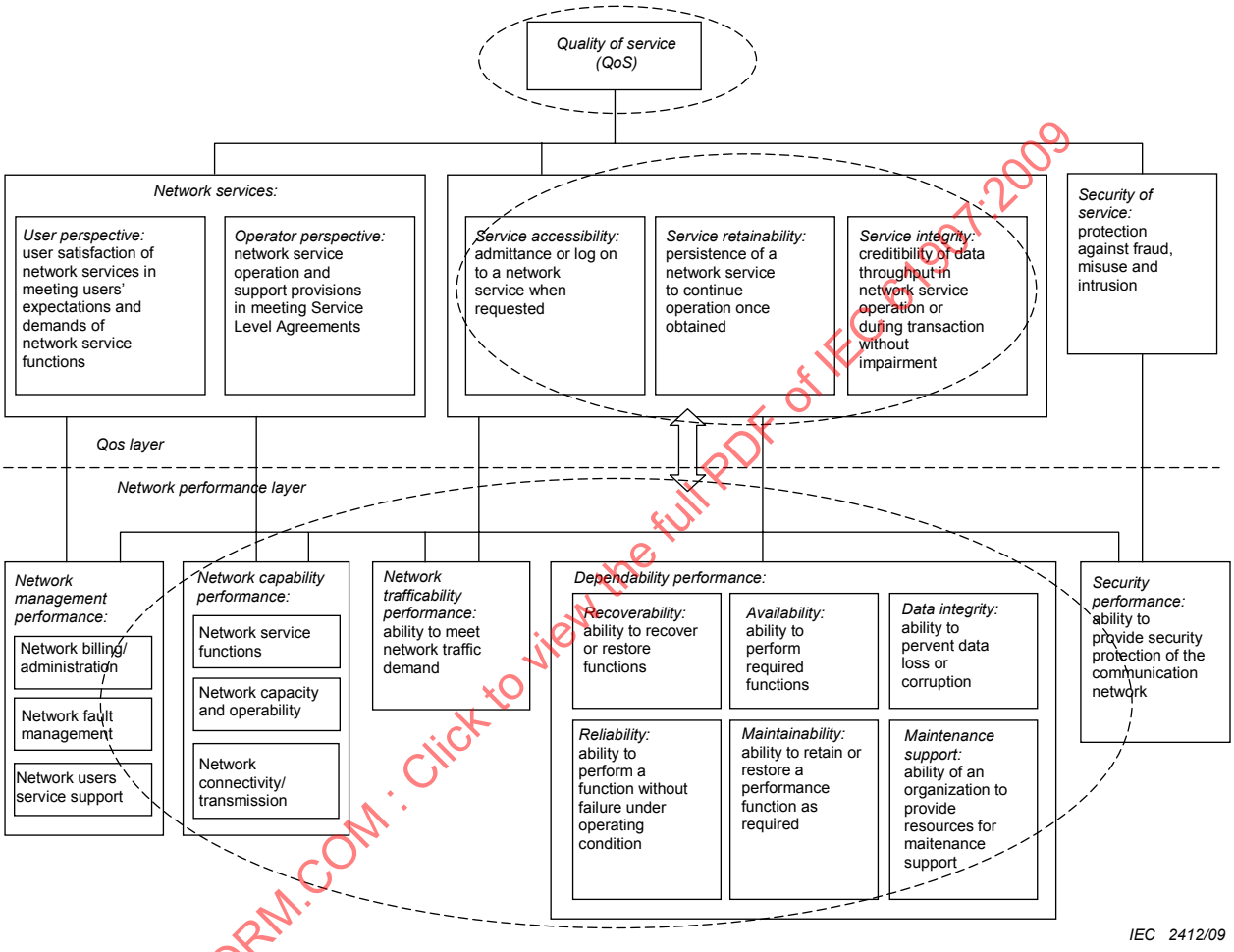


Figure A.4 – QoS, dependability and network performance relationships

A.5 Dependability influencing factors

Dependability influencing factors affecting the collaboration of network dependability framework areas of influence are shown in Tables A.1 to A.4.

Table A.1 – Examples of dependability influencing factors affecting network technology

	Utilization of network technology (5.2)		
Dependability application (5.1)	**Architecture**	**Topology**	**Inter-connection**
Management process	Focus on core network reliability	Focus on topology selection to meet network performance needs	Focus on interconnection strategy
Attributes assignment	Reliability of different network layers	Reliability of functional service traffic path	Reliability of network interface and connection
Requirements determination	Reliability target of different network layers	Network connectivity performance targets	Reliability target of network interface and connection
Design implementation	Reliability mechanism of network elements on different layers	Redundancy and protection switching	Fail-safe designs and fault tolerant systems
Evaluation approach	Network simulation and assessment	Network survivability analysis	E2E test

Table A.2 – Examples of dependability influencing factors affecting network service functions

	Deployment of network service functions (5.3)			
Dependability application (5.1)	**Service provisions**	**Network policy**	**End-user needs and expectations**	**Network security**
Management process	Focus on access capability and retention of all services	Focus on coordination of network policies and cost-effective network operation	Focus on delivery of quality of service and customer satisfaction	Focus on information security and protection systems
Attributes assignment	Maintainability and maintenance support performance of network service functions	Network dependability objectives	Accessibility, retainability and recoverability	Accessibility, retainability and recoverability
Requirements determination	Serviceability and recovery of different services	Dependability of network performance and operation scenarios	Fulfillment of service requirements to different users	Security mechanism for protection and recovery
Design implementation	Reliability of access, retention and recovery of network service functions	Network dependability performance	Network dependability performance	Redundancy and protection control mechanism
Evaluation approach	E2E test	Network policy compliance	User survey and feedback analysis	Security check and protection confirmation

Table A.3 – Examples of dependability influencing factors affecting delivery of network performance

	Delivery of network performance (5.4)				
Dependability application (5.1)	**Traffic**	**Transmission**	**Robustness**	**Serviceability**	**Operability**
Management process	Focus on capacity, traffic performance and congestion control	Focus on type and quality of transmission medium	Focus on network dependability objectives	Focus on network service support for cost-effective availability performance	Focus on ease of operation
Attributes assignment	Availability performance	Reliability of synchronization, transmission integrity, and connection quality	Reliability, survivability, and fault tolerance	Accessibility, retainability and disengagement	Reliability, maintainability and maintenance support performance
Requirements determination	Capacity and performance	Reliability requirements of transmitted information, integrity and quality	Adaptability of a network to conditions of abnormalities	Supportability of a network to services	Reliability, maintainability and maintenance support performance
Design implementation	Cost-effective processing of network traffic	Transmission mechanism and connection quality	Reliability, redundancy and recovery methods	Network service function controllability and fault tolerance	Reliability, maintainability and maintenance support performance
Evaluation approach	E2E test	E2E test	E2E test	E2E test	E2E test

Table A.4 – Examples of dependability influencing factors affecting integrity of network data and information and provision of QoS

	Integrity of network data and information (5.5)	Provision of Quality of Service (5.6)	
Dependability application (5.1)		**Service level agreement compliant**	**User perception**
Management process	Focus on provision of data and information without excessive impairment	Focus on level of service	Assurance of user confidence
Attributes assignment	Integrity of data transmission	Availability performance	Network availability and data integrity
Requirements determination	Quality of transmission media	Accuracy, speed and dependability	Focus on level of service
Design implementation	Redundancy design, information backup, data protection	Access, information transfer, disengagement	Availability and recoverability
Evaluation approach	Transmission quality, packet drop ratio, packet error ratio	E2E test	User survey and feedback analysis

Annex B
(informative)

Network life cycle and evolution process

B.1 Overview of network evolution process

A communication network provides specific communication services to a broad range of network users and involves various service providers in the provision of network service functions. Networks are complicated and unique, and evolve with time to meet market needs and user requirements. Figure B.1 shows the network evolution process incorporated in the network life cycle stages. The disconnection of the enhancement stage to the retirement stage in the network life cycle emphasizes the evolution process through optimization and continuous network renewal prior to discontinuation of obsolete service functions.

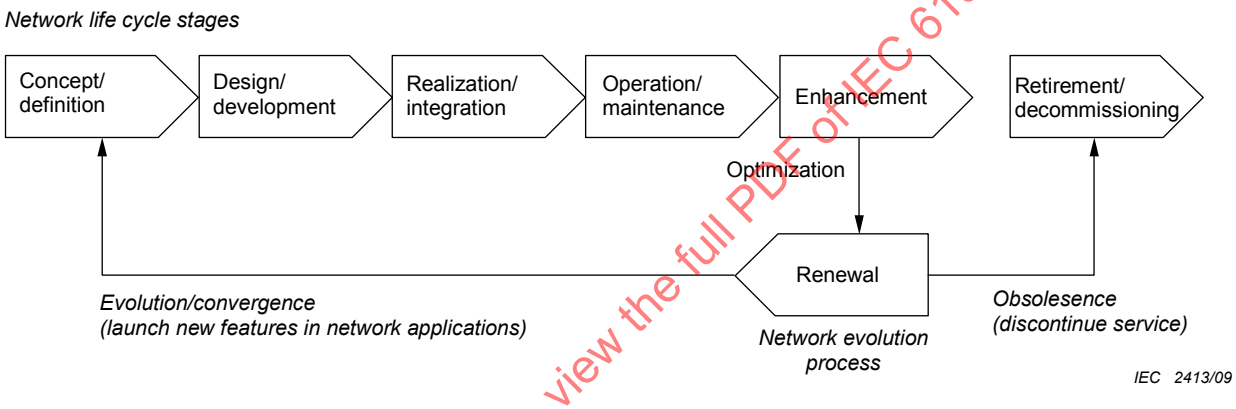


Figure B.1 – Network evolution process incorporated in the network life cycle stages

B.2 Network life cycle stages

B.2.1 Concept/definition

The *concept/definition* stage is the initial stage of network creation. A network can be a completely "new" network or one that is based on an existing "old" network; noting that most network planning starts with some premise for practical and economic reasons.

Activities at this stage include the identification on the types and needs of network users to confirm the market study results, the determination of the network elements and equipment sites, and the relevant regulatory requirements to establish a communication network business.

The business goals and investment objectives should be well researched and analysed to establish a viable business plan. Business partnerships, ownership responsibilities, and service success criteria should be formalized to reach mutual understanding and agreement. Potential client base should be cultivated and the network service functions promoted to attract new service subscribers.

Dependability plan should be prepared as part of the network project plan to establish quantitative network dependability performance targets and acceptance criteria.

From a management perspective, quality policy and dependability performance commitments should be documented to guide development of network service functions. Operational

guidelines should be established, functional responsibilities should be assigned and risk management practices should be initiated for service provision to begin business operation.

B.2.2 Design/development

The *design/development* stage commences with the design of network architecture, identifying the network elements appropriate for designing the required service functions, determining the resources needed to sustain network capacity operation and service function capability requirements. The goal at this stage is to seek a reasonable baseline network structure to accommodate anticipated network growth with time, ascertain the minimum investment risk, and strive to achieve optimal cost-performance ratio.

Activities at this stage include analysis of current and future development of existing network technologies, evaluate cost efficiency for product realization, divide network hierarchy conforming to network architecture and network topology schemes, determine the access and boundary connection relationships, analyse the traffic characteristics, load and behaviour of each service function to determine network performance requirements, prepare network resource management scheme, select network protocols including routing protocol and protection switching protocol, design network prototype, conduct design verification and validation and plan scheduled network development activities.

The network design objective is to realize a robust network structure for dependability performance. Dependability assessment results should form a major input for justification of design changes and improvement recommendations. Management review should validate technical achievements and evaluate cost and time constraints, as well as business risks and major capital investments for full scale development, network realization and construction.

B.2.3 Realization/integration

The *realization/integration* stage is to construct the network to meet business objectives and service function performance expectation.

Activities at this stage include verification and validation of equipment installation, connections and operability for network performance, initiation of quality program for assurance process, product acceptance and non-conformity follow-up on procedures, dependability evaluation of products integrated into the network including commercial-off-the-shelf products. Civil works and facility installations should be inspected and certified for health and safety occupation and conformance to regulatory requirements. Network maintenance and logistic support process should be established for training programs.

Dependability activities include verification of the physical and functional conformance of the network elements and their connectivity prior to end-to-end network performance testing.

Management review should focus on operational plan to assure network service readiness. Service providers and users training and liaison should form part of the marketing strategy for promotion of network services.

Activities on commissioning of the network for acceptance include tests to verify network service functions, validate network performance and evaluate the ability of the network to bear anticipated traffic load for provision of network services. The dependability activity of this stage is to test the dependability related functions such as protection switching verification, and to perform the network failure insertion tests to verify the redundancy design and fault management capability of the network.

Upon acceptance of the verification results, the network is turned over to the customer (a network owner/service provider) for service operation. There may be a warranty period during commissioning prior to customer final acceptance. The warranty duration and conditions for acceptance are in accordance to the contract agreements between the network developer and the customer.

B.2.4 Operation/maintenance

The *operation/optimization* stage is to deploy network service functions for provision of network services.

Activities at this stage include network operation and maintenance to support user access and connection for information exchange. The dependability activity at this stage is to ensure that the operational performance of the network meets the user dependability objectives. Billing process is activated for revenue generation from provision of network services. Network operation is sustained over a long period of time and maintains a level of cost-effective network services. The operation may extend to the enhancement stage for implementation of optimization process to improve performance efficiency.

B.2.5 Enhancement

The *enhancement* stage optimizes and improves the network performance by technology evolution and service functions convergence, upgrade or renew continuing network services, and launch new features in network applications.

a) Optimization

The network evolves with time to accommodate technology advancements and incorporate new service features. This is necessary for the service provider to improve the efficiency of service functions for return-on-investments and respond to market demands by introducing new features offerings to the users. The optimization effort is imminent with the change of times and adjustments to social needs. From a technical operation perspective, the following aspects should be considered:

- aging occurs gradually with some network hardware. Hardware becomes obsolete due to increased maintenance costs for upkeep of outdated technologies. Some existing service functions are no longer attractive to the users who may seek alternate network services and new features offerings. This would impact significant decrease in revenue generation due to loss of subscribers.
- network software is updated continuously to optimize network performance and improve dependability. This is necessary to sustain network growth and new features incorporation for continual improvement of network performance. However, there is a limit to the extent of optimization effort to sustain status quo operation in view of technical and economic reasons.
- service degradation often occurs when network service functions remain stagnant when optimization work has reached its limits. From a user's viewpoint, the network performance appears to be inefficient causing access and connection problems and the perception of mistrust. This would impact user's decision to seek alternate network services.

b) Renewal

Network evolution is a continuous renewal process to achieve service excellence to sustain a viable and competitive network business. The renewal process is driven by technology advancement responding to market demands for new service features. The renewal process often leads to the expansion of service capability as well as capacity to accommodate a broad range of new and renewed attractive features. For efficient service operation, combination and convergence of new and existing services in packages or in bundle offerings are often feasible in rendering value-added renewal services. For example, the fixed-mobile convergence is the way to converge mobile and fixed network. The service providers can offer the converged services to the end-users irrespective of their location, access technology, and terminal. This is an attractive service function feature that offers convenience to the users. Network renewal always launches new features in network applications.

B.2.6 Retirement/decommissioning

The *retirement/decommissioning* stage is to discontinue obsolete service functions. Obsolescence occurs when a service function is no longer offered or supported. Obsolete equipment and hardware are generally removed and disposed of in accordance with regulatory and environmental requirements. Obsolete software is deleted. When a service function is no longer offered or discontinued, a replacement or alternate service function should be readily put into operation to provide continuity of normal network service functions.

B.3 Network management process and dependability related activities

B.3.1 Network management and process activities

Network management deals with the effective implementation of organized processes for managing the performance, configuration, accounting, faults, and security activities of the network infrastructure. The objectives of network management are aimed at maximizing the return-on-investments through planning and control, allocation and deployment, coordination and monitoring of the available network resources. Network infrastructure and network service functions are constructed by architectural design, functional configuration, and technology deployment utilizing hardware, software, and human resources for realization of the necessary service functions. For communication network the linkages of QoS to dependability and network performance functions are described in A.4. The dependability influencing factors affecting the collaboration of network dependability framework areas of influence are shown in A.5. The various process activities associated with the achievement of network service functions are influenced by timely implementation of dependability related activities for network enhancement and life cycle applications. The management objectives of the network service functions [16] are noted as follows:

- *performance management*: measure and make available various aspects of network performance so that inter-network performance can be maintained at an acceptable level; activities include performance quality assurance, monitoring, control and analysis;
- *configuration management*: monitor network and system configuration information so that the effects on network operation of various versions of hardware and software elements can be tracked and managed; activities include network planning and engineering, installation, service planning and negotiation, provisioning, status and control;
- *accounting management*: measure network utilization parameters so that individual or group use of the network can be regulated appropriately to minimize network problems and maximize network access to all users based on apportionment of network resource capacities; activities include usage measurement, tariff and pricing, collections and finance, enterprise control;
- *fault management*: detect, log, notify users of fault condition causing network downtime or unacceptable network degradation, and where possible, automatically fix the network problems to ensure normal network performance; activities include assurance of reliability, availability and survivability, alarm surveillance, fault localization and correction, testing and trouble administration;
- *security management*: control access to network resources according to local guidelines so that the network cannot be sabotaged, intentionally or unintentionally, and sensitive information cannot be accessed by those without appropriate authorization; activities include prevention, detection, containment and recovery, security administration.

Key process activities associated with the achievement of network service functions are summarized in B.3.2 for each network life cycle stage.

B.3.2 Process activities for network life cycle stages

B.3.2.1 Process activities for network concept/definition stage

Inputs

- Customer requirements, needs and wants
- Business plan, investment goals and constraints
- Market intelligence and competitions
- Regulatory requirements

Key process activities	*Dependability related activities*
• Conduct market survey. • Identify customers of the network. • Identify network application environments. • Identify regulations on provision of network services. • Identify service level agreements and QoS requirements. • Identify interoperability requirements with interacting networks and interfaces. • Establish network boundary and operating profile. • Perform network service requirements analysis. • Establish network architecture. • Identify configuration options and technology selection to meet network service objectives. • Evaluate capability of network service functions. • Evaluate feasibility of design options for practical implementation of network service functions. • Review business plan. • Formulate project plan. • Develop network design specifications.	• Identify dependability needs associated with the network applications. • Identify network availability and allowable outage downtimes acceptable by the customers and in applicable regulations. • Identify technology constraints related to the scope and extent of achieving network dependability objectives. • Determine operating scenario for dependability assessments. • Define network failures and performance degradation limits. • Identify risk exposures and criticality of network faults. • Analyse network structure and breakdown of network service functions. • Analyse network availability contributed by functional configuration and design architecture. • Perform fault tree analysis to determine critical areas requiring design attention. • Conduct high level failure modes and effects and criticality analysis to support design justifications. • Evaluate network availability and cost trade-off affecting design options. • Determine means for dependability assessments of network service functions. • Conduct reliability and maintainability assessment. • Establish maintenance and logistic support plan. • Establish process for supplier evaluation for quality assurance and reliability conformance. • Establish process for off-the-shelf product evaluation and acceptance. • Develop dependability plan.

Influencing factors for consideration

- Competitions
- Economic issues
- Technology issues
- Capability issues
- Human resources

- Financial resources
- Facilities
- Assurance process

Outputs

- Network design specifications
- Dependability plan

B.3.2.2 Process activities for network design/development stage

Inputs

- Network design specifications
- Network configuration and design requirements
- Network dependability requirements

Key process activities	*Dependability related activities*
• Design network architecture. • Identify network elements for design of the required network service functions. • Determine resource requirements for planned network capacity operation. • Determine the capability of network service functions to sustain growth potential. • Evaluate design options. • Establish network configuration. • Update project plan and schedule for network development. • Monitor material outsourcing. • Collaborate with external contract development efforts. • Establish network operation and maintenance and logistic support requirements. • Develop network realization plan and implementation requirements.	• Establish network dependability program. • Establish quality assurance program. • Formalize dependability requirements for development of network service functions. • Establish suppliers' dependability programs. • Establish dependability acceptance criteria and reliability growth programs. • Establish failure reporting, analysis, data collection and feedback system. • Develop network dependability assessment plan for verification and validation of network service functions.

Influencing factors for consideration

- Availability of relevant skills resources
- Development schedules
- Project risks
- Training needs

Outputs

- Network realization plan and implementation requirements

B.3.2.3 Process activities for network realization/implementation stage

Inputs

- Network realization plan and implementation requirements

Key process activities	*Dependability related activities*
• Acquire network equipment and components. • Construct civil works and install network facilities. • Develop verification and validation plans and procedures. • Test and evaluate network elements. • Test and evaluate network service functions. • Test and evaluate for network integration and network performance verification. • Conduct training of network operators and maintainers. • Develop network acceptance plan. • Develop network operation and maintenance procedures. • Implement warranty schemes if applicable. • Process customer sign-off for network acceptance to initiate network operation.	• Implement network dependability program. • Implement quality assurance program. • Implement suppliers' dependability programs. • Implement network maintenance and logistic support program. • Implement failure reporting, analysis, data collection and feedback system. • Monitor network failures and corrective/preventive actions for network verification and validation.

Influencing factors for consideration

- Transition management
- Network delivery schedule
- Warranty requirements
- Customer acceptance criteria
- Customer training

Outputs

- Network performance operation and maintenance service procedures
- Customer support procedures

B.3.2.4 Process activities for network operation/maintenance stage

Inputs

- Network performance operation and maintenance service procedures

Key process activities	*Dependability related activities*
• Implement operation plan. • Monitor network performance. • Implement maintenance support strategy. • Monitor network maintenance support efforts. • Provide customer care service.	• Implement reliability growth program. • Implement field data collection system. • Conduct customer satisfaction survey. • Analyse failure trends. • Conduct root-cause analysis of problem areas. • Recommend design and procedure changes for network service improvement. • Determine quality of service.

Influencing factors for consideration

- Network service capacity
- Responsive maintenance actions
- Operators' and maintainers' training

Outputs

- Network performance records
- Quality of service data
- Customer satisfaction results

B.3.2.5 Process activities for network enhancement stage

B.3.2.5.1 Process activities for network optimization

Inputs

- Market survey inputs
- Customer satisfaction results
- Quality of service data
- Network performance records

Key process activities	*Dependability related activities*
• Identify market and customer needs to improve efficiency of network service functions. • Identify areas of technology obsolescence. • Identify increased maintenance cost burden. • Review adequacy of current level of network service performance. • Evaluate the need for change and resulting change benefits. • Implement enhancement efforts through optimization.	• Evaluate network dependability objectives to sustain acceptable level of performance efficiency. • Determine adequacy of network performance to meet customer service requirements. • Conduct impact study on network optimization and service improvement. • Conduct risk and value assessments. • Conduct customer satisfaction survey resulting from change reactions.

Influencing factors for consideration

- Timing for change implementation
- Return-on-investments
- Change management
- Obsolescence management

Outputs

- Customer satisfaction results comparison before and after enhancement efforts

B.3.2.5.2 Process activities for network renewal

Inputs

- Market survey inputs
- Network performance records
- New customer requirements

Key process activities	*Dependability related activities*
• Identify new service functions and feature improvement needed to sustain market competition. • Identify opportunity for technology convergence. • Evaluate the need for change and resulting change benefits. • Implement enhancement efforts through renewal process.	• Evaluate impact on dependability performance due to changes with added new features. • Conduct cost impact study for change incorporation. • Conduct risk and value assessments. • Conduct customer satisfaction survey resulting from change reactions.

Influencing factors for consideration

- Timing for change implementation
- Return-on-investments
- Change management
- Obsolescence management

Outputs

- Enhanced network performance with incorporation of new service features

B.3.2.6 Process activities for network retirement/decommissioning stage

Inputs

- Status of aging network performance capability
- Competitiveness and marketability of existing network services
- Increased network maintenance and support costs
- Business plan updates

Key process activities	*Dependability related activities*
• Identify areas of obsolescence and candidates for retirement. • Evaluate cost impact on network service termination. • Notify customers on specific network service termination. • Inform customers on new or alternative service provision.	• Evaluate constraints on retirement/decommissioning process. • Evaluate impact on environments of disposal items. • Conduct customer satisfaction survey on termination of specific network service and introduction of new service features.

Influencing factors for consideration

- Timing for retirement
- Technology obsolescence

- Regulatory constraints
- Social impact due to termination of service

Outputs

- Termination of specific network service

Annex C
(informative)

Criteria for establishing network security services

C.1 Network security service objectives

The network security service objectives are aimed at preventing unauthorized network access or intrusion and protection from security attacks without the loss or revelation of secured information.

The provision of network security services should take into consideration:

- the threats involved in network security attacks;
- the planning of the security service functions for network protection;
- the vulnerabilities of network security provisions;
- the implementation of network security layers.

C.2 Threats to network security

In the provision of network services the normal flow of information originating from a legitimate source should reach the designated destination. This normal flow of information can be disrupted when the network is being attacked, exposed to security breaches, or experiencing other threats.

The network security threats consist of four main categories:

- *interruption*: an asset of the network is destroyed or becomes unavailable or unusable. This is an attack on network availability;
- *interception*: an unauthorized party gains access to an asset of the network. This is an attack on confidentiality;
- *modification*: an unauthorized party not only gains access to an asset of the network, but also tampers with the asset. This is an attack on integrity;
- *fabrication*: an unauthorized party inserts counterfeit objects into an asset of the network. This is an attack on authenticity.

C.3 Network security service functions

Security services are intended to counter the attacks or threats to the network. The network security services deploy one or more security mechanisms utilizing security algorithms to provide the following security service functions for network protection purposes:

- confidentiality;
- authentication;
- integrity;
- non-repudiation;
- access control;
- availability.

Confidentiality is the protection of transmitted data from passive attacks such as release of data contents. Confidentiality also includes protection of traffic flow through the network from

unauthorized analysis where the attacker may gain access to observe the traffic characteristics, such as source and destination, on a communication facility.

Authentication is to assure that the communication is authentic. The authentication function assures that the connections initiated between legitimate parties are authentic and not interfered with by unauthorized transmission or reception.

Integrity is to assure that messages are received, as sent, with no duplication, insertion, modification, reordering, relays or destruction of data.

Non-repudiation prevents either the sender or the receiver from denying a transmitted message.

Access control is the ability to limit and control the access to host network and applications via communication links. This is to assure access rights to the network by means of identification and authentication for controlling purpose.

Availability is the provision of continuity of service upon demand without denial of service due to security service reasons.

The incorporation of automated recovery mechanisms in network service functions and data is an important service feature that may prevent serious consequences in devastating situations such as loss of information, data corruption, and server crashes.

C.4 Vulnerability

Vulnerability is a flaw in the security system and an exposure to the network. When a specific vulnerability is exploited, the target of vulnerability may affect a person or an organization as the victim of the attack. The vulnerability may also affect the security system or the network. In some cases, the response time to an attack is instantaneous or within seconds such as a worm entering into the security system via an email message to create havoc. In other cases, the response time to an attack may take months or years such as breaking the encryption codes or circumventing the security protection policy of an organization.

There are four basic types of vulnerability causes as shown in Table C.1.

Table C.1 – Four basic types of vulnerability causes

Target of vulnerability →	1) Affects a person or an organization	2) Affects the security system or the network
Response time to an attack is		
– instantaneous	a) social engineering	c) logic error
– over a period of time	b) policy oversight	d) weakness

a) **Social engineering:** area of exposure to attack directly against the security policy of an organization such as an internal worker committing sabotage or the deliberate planned destruction of the organization's intellectual properties. "Social engineering" is a term related to the modern day cyber phenomenon. It is used in the security business to describe the practice of obtaining confidential information by manipulation of legitimate users.

b) **Policy oversight:** flaw in the planning of a security system such as inadequate software backup and duplicate files for data protection.

c) **Logic error:** software fault inherent in the system design such as a poorly written software code that allows unwanted or uncontrolled access.

d) **Weakness**: design flaw that could lead to a security breach such as breaking the encryption irrespective how well it is designed at first (eventually the attacker will find a way to break-in).

Since computers are used extensively for control of security systems, the vulnerabilities to computers have the following attributes:

- *fault*: describing how the vulnerability has become a mistake and created the problem;
- *severity*: describing the degree of compromise such as gaining security administrator access to certain files not normally granted to the regular user;
- *authentication*: describing the intruder's successful registration with the host computer with proof of identity before exploiting the vulnerability of the system;
- *tactic*: describing the issue of who is exploiting who in terms of location and access to a valid account for entry to the security system;
- *consequences*: describing the outcome and the mechanics behind the access promotion showing how a small amount of access can lead to far greater compromises.

Network security protects the network infrastructure from exposure to attacks by deploying appropriate defence at all possible entry points of attacks before they spread to other parts of the network. It is a preventive measure which attempts to protect individual computers and other shared resources connected by the network.

Computer security is the means and measures of self-defence taken to protect individual computers connected to a network. A computer whose security is compromised is likely to infect other computers connected to a potentially unsecured network.

C.5 Layers of network security

There are six layers of network security that can be used to manage security systems to prevent exposures and vulnerabilities. The combination and application of these layers provides increased security for the network.

The foundation of the first layer of network security is the work performed by the *network administrators* who understand the operating systems and know how to lock down specific systems to allow only the ports and processes through that need to get through. On-going training of network administrators is essential to stay ahead of network knowledge from exploits and virus attacks.

The second layer of network security is the *physical security* to protect the network assets from "social engineering" manipulation. A typical example is to gain access to a security system by calling the help desk on forgotten password and requesting change to a temporary or new password. Physical security includes access control and identification of legitimate users, and implementation of good organizational practices in security policies.

The third layer is *monitoring*. Most attacks involve repeated attempts to access the security system. By monitoring the system logs on a regular basis, it is possible to identify certain patterns in the log files. There are software programs available for monitoring the log files to identify and alert suspicious patterns of attempts to gain access to the security system.

The fourth layer is the *software* put on the servers for applications. Every piece of software should be tested and evaluated with appropriate security procedures before loading onto the servers for assurance purposes.

The fifth layer is the deployment of *security tools* for protection and preventive measures. Security tools include, but not limited to firewalls, intrusion detection software, and proxies (i.e. an intermediary function within the network to ensure security, administrate control and caching service).

The sixth layer is *security auditing*. This provides regular checking and examination of the security system against new exploits since network security is a continuous on-going process. A security audit should test every aspect of the network security system. This should be done on a regular basis due to new software installation, system upgrade, changing user base, and revision of security policies.

Bibliography

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

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

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

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

[5] IEC 60300-3-11, *Dependability management – Part 3-11: Application guide – Reliability centred maintenance*

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

[7] IEC 60812, *Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)*

[8] IEC 61025, *Fault tree analysis (FTA)*

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

[10] IEC 61165, *Application of Markov techniques*

[11] IEC 62198, *Project risk management – Application guidelines*

[12] ISO 7498-1, *Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model*

[13] ITU-T Recommendation E.800, *Definitions of terms related to quality of service*

[14] ITU-T Recommendation G.1000, *Communications quality of service: A framework and definitions*

[15] ITU-T Recommendation I.350, *General aspects of quality of service and network performance in digital networks, including ISDNs*

[16] ITU-T Recommendation M.3400, *TMN management functions*

[17] ITU-T Recommendation X.140, *General quality of service parameters for communication via public data networks*

[18] ITU-T Recommendation Y.2011, *General principles and general reference model for Next Generation Networks*

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

INGÉNIERIE DE LA SÛRETÉ DE FONCTIONNEMENT DES RÉSEAUX DE COMMUNICATION

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (CEI) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de la CEI). La CEI a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, la CEI – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de la CEI"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec la CEI, participent également aux travaux. La CEI collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de la CEI concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de la CEI intéressés sont représentés dans chaque comité d'études.
3) Les Publications de la CEI se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de la CEI. Tous les efforts raisonnables sont entrepris afin que la CEI s'assure de l'exactitude du contenu technique de ses publications; la CEI ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de la CEI s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de la CEI dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de la CEI et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) La CEI elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de la CEI. La CEI n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à la CEI, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de la CEI, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de la CEI ou de toute autre Publication de la CEI, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de la CEI peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. La CEI ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et de ne pas avoir signalé leur existence.

La Norme internationale CEI 61907 a été établie par le comité d'études 56 de la CEI: Sûreté de fonctionnement.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
56/1339/FDIS	56/1350/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation de cette norme.

Cette publication a été rédigée selon les Directives ISO/CEI, Partie 2.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de maintenance indiquée sur le site web de la CEI sous http://webstore.iec.ch dans les données relatives à la publication recherchée. A cette date, la publication sera

- reconduite,
- supprimée,
- remplacée par une édition révisée, ou
- amendée.

INTRODUCTION

La complexité des réseaux de communication est aujourd'hui en croissance constante afin de répondre aux demandes du marché et du public dans des domaines technologiques aussi divers que la téléphonie mobile, le commerce électronique, les services intranet et Internet.

En même temps, les technologies de la communication se développent rapidement pour fournir des services en réseau efficaces et une sûreté de fonctionnement nécessaire aux communications à l'échelle mondiale. Les services de communication essentiels tels que les échanges d'informations, le traitement des données et les connexions réseau permettent aux réseaux de communication publics et privés d'être effectués à un coût acceptable. Les domaines commerciaux et privés dépendent pour une large part de ces services de communication qui sont devenus d'usage courant. La sûreté de fonctionnement est l'un des facteurs clés pour assurer la performance des réseaux et des fonctions de service en réseau.

La sûreté de fonctionnement d'un réseau se définit par son aptitude à fonctionner correctement et au moment voulu, de manière à répondre aux besoins de communication des utilisateurs par un fonctionnement permanent du réseau et des services. Du point de vue de l'utilisateur, la sûreté de fonctionnement suppose la fourniture de fonctions de service en réseau fiables et la capacité à réaliser le service souhaité sur demande. La sûreté de fonctionnement du réseau se caractérise par ses attributs de performance comprenant la disponibilité de la performance du réseau et la qualité de service.

Le concept de réseau est une extension des concepts de systèmes qui couvrent un ensemble d'interactions d'éléments de réseau et d'interopérabilité de fonctions de service qui permettent ensemble la réalisation d'objectifs de communication précis.

Pour remplir ses fonctions de service et assurer les services de communication, le réseau requiert des caractéristiques de performance spécifiques. L'ingénierie de la sûreté de fonctionnement des réseaux est une discipline technique spécifique basée sur les risques et qui traite des diverses applications et du déploiement des services de communication essentiels. Contrairement à la notion de cycle de vie d'un système qui sous-entend qu'il y a tôt ou tard une mise hors service définitive du système, un réseau atteint rarement ce stade final. Un réseau évolue avec le temps pour intégrer des applications innovantes et les dispositions nécessaires pour des services de communication ininterrompus. Le cycle de vie d'un réseau est évolutif et il doit répondre aux nécessités de convergence technologique et de processus de renouvellement, et de ce fait, il est caractérisé par des attributs spécifiques de sûreté de fonctionnement destinés à répondre à des objectifs de performance du réseau. La normalisation en matière de sûreté de fonctionnement est essentielle pour développer et mettre en œuvre des réseaux de communication de manière rentable.

La sûreté de fonctionnement d'un réseau de communication apporte d'importants attributs de performance qui, dans un environnement de concurrence globale, sont d'un intérêt primordial pour les développeurs, les fournisseurs d'équipements de réseaux, les intégrateurs de réseaux ainsi que pour les prestataires de fonctions de service de réseau. Ceci résulte principalement du fait que la sûreté de fonctionnement peut avoir un impact déterminant sur les revenus générés et affecter le retour sur investissement. Les utilisateurs des fonctions de service et des services de communication sont particulièrement concernés par la sûreté de fonctionnement des fonctions du réseau et par les dispositions de service fiables qui doivent être capables d'assurer la sécurité du réseau et des connexions ininterrompues pour la transmission de la voix, de l'image et des données.

La présente Norme internationale fournit un cadre général permettant de définir la sûreté de fonctionnement des réseaux de communication. Les réseaux de communication comprennent des réseaux de télécommunications ainsi que des réseaux Internet et intranet utilisant les technologies de l'information. La présente norme décrit l'influence des attributs de la sûreté de fonctionnement et leur impact sur la performance des réseaux. Elle définit les critères et la méthodologie pour les conceptions des technologies des réseaux, les fonctions des services de sécurité, l'évaluation de la sûreté de fonctionnement et l'évaluation de la qualité de

service. Ces éléments sont destinés à servir de base à l'ingénierie et à la mise en œuvre des processus permettant d'atteindre les objectifs en matière de sûreté de fonctionnement des réseaux.

La présente norme fait partie d'un ensemble de normes relatives aux aspects systémiques de la sûreté de fonctionnement, elle étend les concepts de sûreté de fonctionnement telle que définie dans la CEI 60300-3-15 à des applications réseau et permet de prendre en charge la gestion de la sûreté de fonctionnement telle que définie dans les CEI 60300-1 et CEI 60300-2. Dans la présente norme, la performance du réseau et les services de communication renvoient à la série de recommandations du secteur de la normalisation des télécommunications de l'Union Internationale des Télécommunications (UIT-T).

INGÉNIERIE DE LA SÛRETÉ DE FONCTIONNEMENT DES RÉSEAUX DE COMMUNICATION

1 Domaine d'application

La présente Norme Internationale fournit des lignes directrices relatives à l'ingénierie de la sûreté de fonctionnement des réseaux de communication. Elle définit un cadre général pour garantir la sûreté de fonctionnement des réseaux, fournit un processus de mise en œuvre de la sûreté de fonctionnement des réseaux, présente des critères et une méthodologie de conception technologique des réseaux, d'évaluation de la performance, ainsi que des considérations d'ordre sécuritaire et de mesure de la qualité de service nécessaires à la réalisation des objectifs de sûreté de fonctionnement des réseaux.

La présente norme s'adresse aux développeurs et fournisseurs d'équipements réseau, aux intégrateurs de réseau et aux fournisseurs de prestations de services de réseau afin de leur permettre de planifier, d'évaluer et de mettre en œuvre la sûreté de fonctionnement des réseaux.

2 Références normatives

Les documents de référence suivants sont indispensables pour l'application du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

CEI 60050-191, *Vocabulaire électrotechnique international – Chapitre 191: Sûreté de fonctionnement et qualité de service*

CEI 60300-3-15, *Gestion de la sûreté de fonctionnement – Partie 3-15: Guide d'application – Ingénierie de la sûreté de fonctionnement des systèmes*

3 Termes, définitions et abréviations

3.1 Termes et définitions

Pour les besoins du présent document, les termes et définitions donnés dans la CEI 60050-191, ainsi que les suivants s'appliquent.

3.1.1
réseau de communication
système constitué de nœuds et de liaisons de communication assurant la transmission des signaux analogiques ou numériques

EXEMPLES Les réseaux de télécommunications, l'Internet, l'intranet, l'extranet, les réseaux étendus (WAN), les réseaux locaux (d'entreprise) (RLE) et les réseaux informatiques utilisant les technologies de l'information.

NOTE 1 Un réseau comporte sa propre frontière. L'ensemble des nœuds situés au niveau de la frontière d'un réseau s'appellent des terminaux. Dans certaines applications, le terme «nœud» est utilisé à la place du terme «terminal» comme point d'accès de communication au réseau, ainsi que pour désigner les interconnexions entre les liaisons de transmission.

NOTE 2 Un réseau de communication «fédérateur» est constitué d'un réseau central et de lignes de transmission à grande vitesse (nationales ou internationales) reliant entre eux des nœuds de réseaux de commutation importants (interconnexion de lignes de transmission) en divers lieux d'un pays ou d'une région.

3.1.2
sûreté de fonctionnement (d'un réseau)
aptitude d'un réseau à être en état de fonctionner de la manière requise et au moment voulu afin de répondre à des exigences spécifiques relatives à la communication et au fonctionnement

3.1.3
disponibilité (d'un réseau)
aptitude à être en état de fonctionner de la manière requise et au moment voulu, dans des conditions données, en supposant que la fourniture des ressources extérieures nécessaires soit assurée

NOTE 1 La disponibilité dépend à la fois des caractéristiques de fiabilité, de maintenabilité et de capacité de restauration du réseau et en général, de l'aptitude de soutien logistique à la maintenance.

NOTE 2 L'expression «dans des conditions données» peut inclure des aspects pouvant affecter la fiabilité, la maintenabilité et l'aptitude de soutien logistique à la maintenance.

3.1.4
fiabilité (d'un réseau)
aptitude à fonctionner de la manière requise, pendant un intervalle de temps donné, dans des conditions données

NOTE 1 L'expression «dans des conditions données» peut inclure des aspects pouvant affecter la fiabilité, tels que: le mode de fonctionnement, les niveaux de contrainte, les conditions d'environnement.

NOTE 2 La fiabilité peut être quantifiée au moyen de mesures appropriées telles que la durée moyenne avant défaillance ou la probabilité de ne pas connaître de défaillance au cours d'une durée spécifiée.

3.1.5
maintenabilité (d'un réseau)
aptitude à être maintenu ou ramené à un état lui permettant de fonctionner de la manière requise, dans des conditions données d'utilisation et de maintenance

NOTE 1 L'expression «conditions données d'utilisation» peut comprendre le stockage.

NOTE 2 L'expression «conditions données de maintenance» comprend les modes opératoires et les ressources à utiliser.

NOTE 3 La maintenabilité peut être quantifiée en utilisant des mesures telles que la durée moyenne nécessaire à la restauration ou la probabilité de restauration au cours d'une durée spécifiée.

3.1.6
soutien logistique à la maintenance
ressources utilisées afin d'effectuer la maintenance selon des concepts et une stratégie de maintenance

3.1.7
aptitude de soutien logistique à la maintenance
aptitude d'un organisme à réaliser, sur demande et dans des conditions données, une action de maintenance spécifiée sur le réseau

NOTE L'expression «conditions données» inclut les conditions d'organisation de la maintenance, les conditions d'utilisation et de maintenance de l'élément, ainsi que les stratégies et procédures de maintenance correspondantes.

3.1.8
capacité de restauration (d'un réseau)
aptitude à recouvrer, sans maintenance corrective, l'état de fonctionnement après une défaillance

NOTE 1 L'aptitude à restaurer peut ou non nécessiter des actions externes.

NOTE 2 La capacité de restauration peut être quantifiée en utilisant des mesures telles que la durée moyenne nécessaire à la restauration ou la probabilité de restauration au cours d'une durée spécifiée.

3.1.9
élément (d'un réseau)
sous-système ou composant d'un réseau de communication

EXEMPLES Les terminaux, les nœuds, les liaisons et les commutateurs.

NOTE 1 Un élément de réseau peut nécessiter une intervention humaine pour réaliser ses fonctions de service.

NOTE 2 Les nœuds, ainsi que les points d'accès au réseau, sont liés par des liaisons de réseau.

3.1.10
liaison (d'un réseau)
connexion électrique, sans fil ou optique entre les nœuds d'un réseau

3.1.11
performance (d'un réseau)
aptitude à fournir les fonctions de service relatives aux communications entre utilisateurs

[Recommandation I.350 de l'UIT]

NOTE L'aptitude de sûreté de fonctionnement d'un réseau fait référence à l'aptitude du réseau à fournir ou à démontrer que les attributs de sûreté de fonctionnement du réseau satisfont aux objectifs définis pour le réseau et aux exigences relatives à la qualité de service.

3.1.12
gestion (d'un réseau)
mise en œuvre de processus et de ressources organisés pour gérer la performance, la configuration, la comptabilité, les pannes et les activités de sécurité

3.1.13
fonction de service (d'un réseau)
programme ou application qui interagit avec les utilisateurs du réseau ou au sein de l'infrastructure de réseau pour transmettre ou échanger des données et des informations sur le réseau

NOTE Une fonction de service d'un réseau peut être constituée d'éléments matériels et logiciels et peut impliquer des interventions humaines pour exécuter une fonction spécifique.

3.1.14
services de réseau
ensemble des fonctions de service et de communication de réseau fournies aux utilisateurs du réseau

NOTE 1 Les services de communication sont les services de réseau auxquels ont souscrit les utilisateurs finaux.

NOTE 2 Un service support est une fonction de service de communication qui permet de transmettre des signaux d'informations utilisateurs entre des interfaces utilisateur-réseau.

3.1.15
qualité de service
effet collectif de la performance d'un service qui détermine le degré de satisfaction d'un utilisateur du service

3.1.16
défaillance d'un réseau
perte de l'aptitude d'un réseau à remplir sa fonction

NOTE La défaillance peut être due, par exemple, à une panne d'équipement, une catastrophe naturelle ou à des perturbations d'origine humaine.

3.1.17
panne d'un réseau
état caractérisé par l'inaptitude du réseau à remplir sa fonction

NOTE 1 Dans le contexte du fonctionnement d'un réseau, une panne peut être naturelle, due à une cause anormale ou à un dysfonctionnement donnant lieu à une défaillance d'un élément du réseau, ou induite de l'extérieur, comme par exemple une panne provoquée par insertion d'un défaut.

NOTE 2 Un état dégradé de la performance d'un réseau est une situation dans laquelle une ou plusieurs caractéristiques de performance ne sont pas conformes aux exigences.

3.1.18
prestataire
fournisseur de service
organisation qui fournit des services de réseaux de communication

EXEMPLES Les opérateurs téléphoniques, les prestataires de services de transport de données, les opérateurs de téléphonie mobile, les fournisseurs d'accès Internet et les câblo-opérateurs.

NOTE Un opérateur de réseau ou, tout simplement, un opérateur est une entité qui transporte un produit ou un service en utilisant ses propres installations ou celles d'autres opérateurs et propose des services au grand public. Le terme opérateur de télécommunications fait référence à divers opérateurs téléphoniques qui fournissent des services locaux, interurbains ou à valeur ajoutée.

3.1.19
utilisateur
personne physique ou morale qui utilise les services d'un fournisseur de services afin d'accéder directement à un réseau

NOTE 1 Un utilisateur peut être à l'origine ou le destinataire des informations utilisateur, ou les deux à la fois.

NOTE 2 Dans certains cas, l'utilisateur d'un service de télécommunication est également appelé abonné.

3.1.20
intégrité (d'un réseau)
aptitude à garantir que le contenu du flux de données n'est pas contaminé, corrompu, perdu ou altéré entre l'émission et la réception

3.2 Abréviations

E2E de bout en bout[1]

AMDE analyse des modes de défaillance et de leurs effets

AAP analyse par arbre de panne

IP protocole Internet[2]

UIT-T secteur de la normalisation des télécommunications de l'Union Internationale des Télécommunications

RLE réseau local (d'entreprise)

NGN réseau de nouvelle génération[3]

---

1 E2E = *End-to-End*.

2 IP = *Internet Protocol*.

3 NGN = *Next Generation Network*.

OSI interconnexion de systèmes ouverts[4]

QS qualité de service

BDF bloc-diagramme de fiabilité

SLA accord sur le niveau de service[5]

TCP/IP protocole de commande de transmission/protocole Internet[6]

WAN réseau étendu[7]

4 Aperçu de la sûreté de fonctionnement d'un réseau de communication

4.1 Cadre général de la sûreté de fonctionnement d'un réseau

Un réseau de communication est constitué d'éléments de réseau tels que des commutateurs, des émetteurs, des ordinateurs, des téléphones et autres dispositifs connectés par des moyens de communication permettant l'échange électronique d'informations. Les connexions peuvent être permanentes au moyen de câbles ou temporaires au moyen de liaisons téléphoniques ou Internet. Le support de transmission peut être physique (par exemple des fibres optiques) ou sans fil (par exemple le satellite). Un réseau de communication couvre de nombreuses technologies telles que les radiofréquences, la télévision, la téléphonie, la communication de données et la mise en réseau d'ordinateurs utilisant les technologies de l'information.

La nature du fonctionnement d'un réseau comporte des facettes multiples, toujours en expansion et en évolution, comme par exemple les échanges commerciaux en ligne sur Internet. L'infrastructure qui permet de relier différents types de systèmes de communication et de réseaux en interaction est extrêmement complexe. L'intégration de réseaux et de systèmes disparates nécessite sans cesse la mise en place d'interfaces et de protocoles d'interopérabilité permettant de réaliser une connectivité de réseau fiable et une performance optimale des services. Les pressions imposées par les techniques de marketing et le commerce en ligne des entreprises conduisent souvent l'élaboration de nouvelles techniques qui modifient les règles fondamentales de fonctionnement des applications commerciales et de service.

Les activités en relation avec un réseau jouent un rôle primordial dans l'assurance des performances et de la qualité de service du réseau. L'enjeu est de fournir des solutions en réseau qui lient les conceptions de réseau et les applications de fonctions de service et permettent d'atteindre les attributs pertinents de sûreté de fonctionnement. La sûreté de fonctionnement d'un réseau implique que la performance du réseau soit capable d'assurer l'intégrité des informations et de fournir les fonctions de services du réseau qui satisfont à la fois les attentes de l'utilisateur et les besoins des fournisseurs de services. Le principe stratégique consiste à choisir et à mettre en œuvre des éléments de réseau appropriés à la configuration du réseau, de manière à obtenir la sûreté de fonctionnement et l'intégrité nécessaires à la performance du réseau.

L'Annexe A présente un modèle général de réseau de communication ainsi que les concepts correspondants.

---

4 OSI = *Open Systems Interconnection.*

5 SLA = *Service Level Agreement.*

6 TCP/IP = *Transmission Control Protocol/Internet Protocol.*

7 WAN = *Wide Area Network.*

La sûreté de fonctionnement d'un réseau et les fonctions de services du réseau sont influencées par les critères de sûreté de fonctionnement correspondant à leurs applications spécifiques au cours des diverses étapes du cycle de vie du réseau. Ces attributs de sûreté de fonctionnement comprennent la disponibilité, la fiabilité, la maintenabilité, l'aptitude de soutien logistique à la maintenance, la capacité de restauration et l'intégrité, ainsi que des caractéristiques de performance intégrées dans la conception des réseaux et la mise en œuvre de leurs fonctions de service en vue de garantir de façon optimale le fonctionnement et la maintenance du réseau.

Le cadre général de la sûreté de fonctionnement d'un réseau de communication comporte six principaux domaines d'influence interagissant entre eux:

a) l'application de la sûreté de fonctionnement;

b) l'utilisation de la technologie réseau;

c) la fourniture de la performance requise pour le réseau;

d) le déploiement des fonctions de service du réseau;

e) l'intégrité des données et informations du réseau;

f) la fourniture d'une qualité de service appropriée.

Ces six domaines d'influence interagissant entre eux constituent la base même de la gestion de la sûreté de fonctionnement d'un réseau. L'Article 5 décrit la mise en œuvre des processus et des méthodes de sûreté de fonctionnement des réseaux.

4.2 Cycle de vie et processus d'évolution d'un réseau

Un réseau évolue dans le temps afin de répondre aux applications de réseau dynamiques et aux besoins de services de réseau nécessaires à la communication. Le processus d'évolution d'un réseau est reflété par les étapes du cycle de vie du système décrites dans la CEI 60300-3-15 et modifiées pour application au cycle de vie d'un réseau de manière à tenir compte du processus de renouvellement. Les étapes du cycle de vie d'un réseau sont présentées ci-après:

– étape *concept/définition* destinée à identifier le scénario opérationnel du réseau;

– étape *conception/développement* destinée à déterminer les applications technologiques et à développer les fonctions de service du réseau;

– étape *réalisation/intégration* permettant de réaliser le fonctionnement, la vérification et la validation du réseau pour s'assurer de sa performance;

– étape *exploitation/maintenance* prenant en charge le fonctionnement opérationnel du réseau et la fourniture des services du réseau;

– étape d'*amélioration:*

  – pour optimiser et accroître les performances d'un réseau grâce à la convergence des évolutions technologiques et des fonctions de service;

  – pour mettre à jour ou renouveler en permanence des services du réseau, et pour initier de nouvelles fonctionnalités d'applications réseau;

– étape *retrait du service/déclassement* pour arrêter la fourniture de fonctions de service obsolètes.

L'Annexe B décrit le cycle de vie et le processus d'évolution d'un réseau.

5 Mise en œuvre de la sûreté de fonctionnement d'un réseau

5.1 Applications de l'ingénierie de la sûreté de fonctionnement

5.1.1 Gestion de la sûreté de fonctionnement d'un réseau

La sûreté de fonctionnement est une discipline technique gérée par des principes et des pratiques d'ingénierie. Les systèmes [1][8] ainsi que les lignes directrices [2] relatifs à la gestion de la sûreté de fonctionnement sont utilisés dans la présente norme pour la formulation des stratégies de gestion de la sûreté de fonctionnement et pour l'application générale d'approches techniques permettant de mettre en œuvre les éléments et les tâches liés à la sûreté de fonctionnement. Des processus de gestion supplémentaires sont introduits afin de couvrir les aspects de la gestion spécifiques aux réseaux. La gestion de la sûreté de fonctionnement implique des activités telles que la planification de projets, l'attribution de ressources, l'affectation de tâches de sûreté de fonctionnement, la surveillance et la sécurisation, la mesure des résultats, l'analyse des données et l'amélioration continue. Il convient de mener les activités de sûreté de fonctionnement conjointement à d'autres disciplines techniques pour obtenir les effets synergiques nécessaires et valoriser les résultats du projet. L'accent est notamment mis sur l'ajustement du projet pour une gestion économique des projets de réseaux. Le cas échéant, il est recommandé d'effectuer l'analyse du coût global [4] et l'évaluation des risques [11] pour attribuer et optimiser les ressources, ainsi que pour évaluer des coûts d'évaluation et de possession.

Du point de vue de la gestion d'un réseau de communication, il convient que la gestion de la sûreté de fonctionnement fasse partie intégrante du processus de gestion du réseau, avec des activités pertinentes de sûreté de fonctionnement destinées à soutenir le développement et la mise en œuvre de fonctions de services du réseau pendant toute la durée du cycle de vie et d'évolution du réseau. La gestion du réseau consiste à appliquer l'ensemble des processus de gestion pour planifier, maîtriser, attribuer, déployer, coordonner, maintenir et surveiller les ressources d'un réseau.

D'un point de vue technique, un réseau peut être perçu comme un système complexe constitué de plusieurs systèmes interconnectés. Les processus techniques décrits dans la CEI 60300-3-15 sont utilisés pour décrire les différentes étapes du cycle de vie d'un réseau afin de permettre la mise en œuvre du projet correspondant. Les étapes du cycle de vie d'un réseau sont modifiées pour tenir compte du descriptif des processus d'évolution du réseau et de la convergence technologique, de l'optimisation et du renouvellement, de l'obsolescence et de la mise hors service. Les processus de gestion du réseau et les activités liées à la sûreté de fonctionnement, pour chaque étape du cycle de vie d'un réseau, sont présentés en Annexe B.

5.1.2 Attributs de la sûreté de fonctionnement d'un réseau

L'ensemble de base des attributs de la sûreté de fonctionnement découle des performances attendues du réseau. Il est admis que d'autres attributs soient intégrés pour des applications spécifiques.

a) Disponibilité

La disponibilité du réseau reflète les exigences des utilisateurs selon trois aspects:

– le réseau est capable de fonctionner de la manière requise et au moment voulu;

– il convient que les fonctions de service du réseau ne soient pas affectées par des pannes du réseau;

– le réseau peut être restauré aussi rapidement que possible lorsqu'une panne affecte ses fonctions de service.

8 Les chiffres entre crochets carrés réfèrent à la bibliographie.

b) Fiabilité

La fiabilité du réseau peut être améliorée en utilisant des techniques de redondance et des mécanismes de protection. Pour un réseau ayant des exigences de fiabilité élevées, il convient d'envisager une protection contre les pannes se manifestant en plusieurs points. La manifestation de pannes devient plus critique pour le fonctionnement d'un réseau complexe, notamment lorsqu'on continue à utiliser des équipements obsolètes qui peuvent poser des problèmes de compatibilité.

c) Maintenabilité

La maintenabilité reflète la facilité avec laquelle l'état opérationnel d'un réseau est rétabli à la suite d'une panne ou suite à un état dégradé de la performance du réseau. L'intégration au réseau d'une redondance conceptuelle et d'une capacité de gestion des pannes peut affecter son aptitude de maintenabilité. Par exemple, une gestion à distance des pannes, avec identification des pannes et des mesures correctives réalisées par une intervention à distance, peut réduire les délais de maintenance.

d) Aptitude de soutien logistique à la maintenance

L'aptitude de soutien logistique à la maintenance dépend de la fourniture et de la gestion des ressources utilisées pour mener les activités de maintenance. La conception de la sûreté de fonctionnement d'un réseau nécessite une approche permettant de réduire la complexité des équipements du réseau en termes de maintenance, un accès aisé pour une maintenance active pendant le fonctionnement du réseau, des procédures de maintenance normalisées, une identification et une traçabilité des pannes du réseau et un système perfectionné de gestion des pièces de rechange. Cette approche s'applique aux matériels et aux logiciels ainsi qu'aux fonctions humaines d'aptitude de soutien à la maintenance et à des considérations relevant de la conception proprement dite.

e) Capacité de restauration

La capacité de restauration de la performance des services dépend de la conception de l'architecture du réseau, des mécanismes de protection tolérants aux pannes, de l'accès à des fins de maintenance et de fonctionnalités d'auto-régénération intégrées parmi les fonctions du réseau. Les moyens d'obtenir la restauration peuvent être automatiques ou dépendre d'interventions extérieures.

f) Intégrité

L'intégrité implique stabilité et robustesse du réseau et elle doit être capable de maintenir une qualité homogène de performance et d'utilisation. L'intégrité du réseau assure la sécurité et la protection des transferts d'informations en termes de performance du réseau et de fonctions de service.

5.1.3 Défaillances et pannes d'un réseau

5.1.3.1 Critères de défaillance d'un réseau

Il convient de déterminer les critères de défaillance d'un réseau lors de l'étape de conception et de définition et que ces critères soient révisés en permanence tout au long du cycle de vie du réseau, afin de permettre le classement, et la mise à jour des défaillances du réseau.

Il convient que les critères de défaillance soient établis par le fournisseur de services du réseau, sur la base de normes industrielles et de données pertinentes, tenant compte des informations fournies par les utilisateurs du réseau, afin de pouvoir définir toutes les conditions envisageables. Ces informations sont utilisées pour:

– la spécification des exigences de sûreté de fonctionnement applicables aux fournisseurs d'équipements de réseau;

– la conclusion d'accords (tel que le SLA) avec les utilisateurs des services du réseau en matière d'attributs de performance de sûreté de fonctionnement du réseau.

Il convient de tenir compte des éléments suivants lors de la définition des critères de défaillance:

a) La défaillance au niveau des nœuds et des liaisons du réseau: La défaillance des nœuds et des liaisons du réseau comprend les défaillances totales et partielles. La défaillance totale définit une perte de la fonctionnalité de l'ensemble du réseau pendant une durée donnée. La défaillance partielle définit la perte de fonctionnalité d'une partie du réseau.

b) La défaillance due à une dégradation de la qualité de service (QS): La défaillance par dégradation résulte d'un niveau inacceptable de la QS en termes d'aptitude à la fourniture de services du réseau constatée par les utilisateurs. En général, les fournisseurs de services du réseau collectent des données de QS par le biais de mesures et d'études permettant d'en déterminer le niveau.

5.1.3.2 Classement des défaillances d'un réseau

La plupart des défaillances d'un réseau peuvent être classées de manière à identifier leurs causes probables et de ranger par catégorie les résultats des analyses de défaillance, dans le but d'améliorer la sûreté de fonctionnement du réseau.

– *Défaillance d'un réseau liée aux installations* – Il s'agit de la défaillance d'éléments individuels d'un réseau dont les taux de défaillance peuvent être utilisés pour prédire les paramètres de sûreté de fonctionnement du nœud et de la liaison correspondants.

– *Défaillance d'un réseau liée au trafic* – Cette défaillance correspond à des scénarios d'exploitation liés aux variations du trafic des services du réseau en fonction du taux d'utilisation par les utilisateurs. Il convient que la conception du réseau tienne compte des demandes d'utilisation des utilisateurs et planifie la capacité de trafic du réseau, de manière à répondre à la plupart des scénarios d'exploitation et à éviter ainsi une dégradation de la performance des services du réseau.

– *Défaillance d'un réseau liée à une catastrophe* – Il s'agit d'une défaillance du réseau due à un sinistre d'origine humaine ou naturelle. Dans certains cas, les installations du réseau dans la zone du sinistre peuvent être entièrement détruites.

– *Défaillance d'un réseau liée à la sécurité* – Il s'agit d'une défaillance du réseau due à une sécurité insuffisante en termes de prévention d'intrusions comme par exemple le piratage, les cyber-attaques ou les actes de sabotage.

– *Défaillance d'un réseau liée à des activités planifiées* – Il s'agit d'une défaillance qui a lieu lors d'activités prévues de maintenance du réseau, comme par exemple la mise à niveau de logiciels entraînant une mise hors-service temporaire du réseau.

– *Défaillance d'un réseau liée à des facteurs humains* – Il s'agit d'une défaillance du réseau due à des erreurs, à des mauvaises utilisations ou à des négligences humaines, telles que les erreurs de conception ou de configuration de réseau ou encore les erreurs dans la gestion des versions de logiciels.

5.1.3.3 Etats de panne d'un réseau

Une panne de réseau est un événement survenant au cours de l'exploitation et de la maintenance du réseau et révélant une anomalie ou un dysfonctionnement en termes de performance. Un état de panne provoqué par une défaillance décrit l'état de dérangement ou le statut observé. Dans la pratique, les causes des pannes réelles d'un réseau sont souvent inconnues lors de l'observation initiale du compte-rendu d'incident indiquant les symptômes observés de l'état ou des conditions de panne quant à l'incapacité du réseau à remplir sa fonction. La complexité de fonctionnement des réseaux, l'utilisation de fonctions de service diverses, ainsi que les délais limités de rétablissement des services du réseau empêchent souvent d'approfondir les causes réelles de l'événement de défaillance. La priorité dans des situations de panne est de réacheminer, réinitialiser et rétablir les fonctions de service défaillantes afin de rétablir des services de réseau normaux. Il convient que les comptes-rendus d'incidents de réseau décrivent les symptômes de la défaillance afin de lancer des mesures de suivi appropriées et déterminer, dans toute la mesure du possible, la cause de la défaillance. Des informations pertinentes, recueillies grâce aux comptes-rendus d'incidents au cours du fonctionnement et de la maintenance du réseau, constituent des sources importantes de données de défaillance permettant la mise en œuvre efficace d'un système de gestion des pannes du réseau.

5.1.3.4 Système de gestion des pannes d'un réseau

Le système de gestion des pannes d'un réseau est un système de soutien des services de réseau facilitant l'élaboration de comptes-rendus de données d'évènements de défaillance et la détection des états de panne observés afin de permettre la gestion et la correction des pannes du réseau. Le système de gestion des défaillances est constitué d'un ensemble de fonctions de soutien destinées à détecter, isoler, et le cas échéant compenser, les modifications d'environnement et à corriger les dysfonctionnements du réseau. Le système est conçu et déployé pour prendre en charge la restauration des services du réseau pour la traçabilité et l'identification des pannes, la réalisation d'essais de diagnostic, la correction des pannes, l'activation d'alarmes et l'élaboration de rapports de conditions d'erreurs, le maintien de journaux d'erreurs et la notification des erreurs détectées (voir 5.1.5.3). Le système de gestion des pannes du réseau est un mécanisme de validation essentiel permettant de soutenir les fonctions de service du réseau.

5.1.4 Détermination des exigences relatives à la sûreté de fonctionnement d'un réseau

5.1.4.1 Identification des exigences de sûreté de fonctionnement d'un réseau

La collecte des informations permet d'identifier les besoins du marché en réseaux, qu'ils soient nouveaux ou mis à niveau. L'objectif est de définir les exigences commerciales et techniques pour le développement du réseau et l'amélioration du service. Les informations peuvent provenir de sources diverses.

a) *Informations relatives à la mise à niveau d'un réseau ancien* – Pour concevoir un réseau, il est possible d'utiliser le réseau existant comme base de mise à niveau ou d'amélioration, comme par exemple l'extension d'installations de service existantes et l'aptitude à répondre aux besoins croissants du marché. Ceci peut permettre d'éviter des investissements importants en termes de ressources pour construire un réseau totalement nouveau. L'amélioration intègre de nouvelles fonctionnalités et fournit des services ainsi que des capacités supplémentaires qui renforcent et complètent les fonctions de service de l'ancien réseau.

b) *Fonctions de service et informations relatives à la performance* – Il s'agit des fonctions de service du réseau exigées par le fournisseur de service du réseau; elles comprennent les applications existantes (comme par exemple le service téléphonique) et de nouvelles applications (comme par exemple le service Internet), ainsi que des exigences relatives à la performance du réseau, à la capacité et à d'autres caractéristiques des services de réseau.

c) *Informations «sur-mesure»* – Ce type d'informations fait état, par exemple, des exigences des utilisateurs finaux qui demandent des services sur-mesure fournis par le réseau de communication. Il est admis par exemple que des utilisateurs demandent des fonctions de visiophonie comme service adapté ou spécial.

d) *Suggestions et réclamations des utilisateurs* – Il convient d'obtenir des utilisateurs des suggestions utiles et des réclamations pertinentes concernant le réseau existant qui permettront de définir des solutions ou des améliorations pour le nouveau réseau. Il convient par exemple de mener des enquêtes auprès des clients et d'obtenir des retours d'informations techniques quant à la satisfaction des utilisateurs.

e) *Facteurs liés à l'environnement* – L'environnement géographique de la zone de couverture du réseau peut nécessiter une prise en charge particulière pour la conception du réseau. Par exemple, des informations pertinentes quant à la situation géographique, au relief, aux conditions climatiques et à l'alimentation électrique peuvent être requises.

f) *Informations obtenues à partir de recherches* – Les recherches et études fournissent souvent des informations sur la planification des services; sur les retours d'expériences de conception et de construction de réseaux similaires et sur leur aptitude en termes de sûreté de fonctionnement.

g) *Contraintes commerciales* – Des informations pertinentes peuvent fournir des données utiles sur les délais de construction du réseau, le budget du fournisseur de services de réseau ainsi que sur les accords de niveaux de services et les clauses de pénalité.

h) *Contraintes réglementaires* – Ce sont par exemple les lois ou les indications fournies par les autorités nationales ou internationales auxquelles les opérateurs doivent se conformer.

Les informations obtenues de ces diverses sources peuvent nécessiter une transposition en des termes plus techniques pour analyses ultérieures.

5.1.4.2 Analyse, affectation et révision des exigences

L'analyse des exigences en matière de sûreté de fonctionnement d'un réseau correspond au processus d'analyse des informations recueillies à partir de diverses sources et identifiées comme étant pertinentes. Ce processus convertit les besoins des utilisateurs en exigences techniques afin que le réseau soit conçu de manière à exprimer correctement l'intention d'identifier les demandes des clients. Les exigences relatives à la sûreté de fonctionnement font partie des exigences techniques qui permettent d'attribuer des ressources aux éléments du réseau, de spécifier et de réaliser le réseau proprement dit.

Une approche de l'analyse des exigences relatives à la sûreté de fonctionnement d'un réseau est présentée ci-après.

a) Classement

Cette activité analyse les besoins présents et futurs d'un service de réseau afin de déterminer les effets de l'écoulement du trafic, de son volume et de sa charge sur la performance du réseau. L'analyse récapitule et classe les exigences techniques en plusieurs catégories, telles que les exigences relatives à la sûreté de fonctionnement en termes de redondance, de tolérance aux pannes, de détection des pannes et de restauration, de maîtrise des surcharges, de maintenance et de mise à niveau.

b) Décomposition

Les exigences relatives à la sûreté de fonctionnement sont décomposées:

– par granularité: décomposition des exigences selon leur complexité et leurs fonctions. Ceci peut permettre une ventilation de la fiabilité de fonctions spécifiques en un seul dispositif fonctionnel ou impliquant plusieurs éléments de réseau de manière à obtenir une performance fonctionnelle spécifique du réseau;

– par couche: les exigences sont réparties par couches où les fonctions sont nécessaires. Les exigences relatives à la sûreté de fonctionnement peuvent être allouées en fonction des couches. L'approche par couches facilite l'affectation des exigences relatives à la sûreté de fonctionnement à chaque élément de réseau utilisé au niveau de ladite couche; elle définit les fonctions de sûreté de fonctionnement qu'il convient d'appliquer à chaque élément du réseau et identifie les frontières et l'interface de l'élément réseau.

c) Intégration des exigences

Il est nécessaire d'intégrer les exigences relatives à la sûreté de fonctionnement obtenues par divers moyens et à partir de sources diverses. Les exigences en doublon sont retirées afin d'éviter les conflits entre exigences contradictoires et d'améliorer ainsi la sûreté de fonctionnement globale, arbitrer et afin d'optimiser la conception.

d) Analyse des priorités

L'analyse des priorités identifie l'importance des exigences et détermine leur urgence en termes d'actions et de mise en œuvre prioritaires. Il s'agit d'un processus intégré systématique pour le développement et l'attribution des priorités. Il convient d'établir un ensemble de critères de classement par priorités pour les tâches du projet à affecter. Il est recommandé de faire en sorte que l'analyse des priorités fasse partie du plan du projet de mise en œuvre. Il convient, le cas échéant, d'effectuer une analyse des risques et une analyse coûts-avantages dans le cadre du processus d'analyse des priorités.

e) Révision des exigences

Il s'agit de revoir les informations collectées, leur définition et autres aspects afin de déceler les éventuelles erreurs ou erreurs d'interprétation dans l'analyse des exigences.

Ceci est destiné à formaliser la spécification de sûreté de fonctionnement utilisée comme base pour la vérification, l'analyse, l'acceptation et la livraison.

5.1.4.3 Profil de fonctionnement d'un réseau

Le scénario de l'application présente un profil opérationnel du réseau. La détermination du scénario d'application du réseau a pour objectif d'identifier les défaillances possibles au niveau des fonctions de service du réseau, les procédures et opérations de traitement des pannes ainsi que les interfaces des divers éléments du réseau. Il convient que l'approche analytique tienne compte des facteurs tels que la topologie du réseau, les interfaces entre éléments du réseau et les protocoles de réseau correspondants.

Il convient que le processus d'analyse du scénario d'application:

– détermine les caractéristiques des fonctions de service;
– décrive l'application de la mise en réseau des fonctionnalités des services et fournisse des informations permettant de mieux comprendre visuellement le réseau, comme par exemple un diagramme;
– décrive les interfaces entre les éléments du réseau impliqués dans le service;
– détermine, sur le réseau, les points de défaillance critiques des principales fonctions de service du réseau et détermine les modes de défaillance ainsi que les scénarios opérationnels correspondants;
– analyse les flux de processus des éléments de réseau concernés, en s'appuyant sur des scénarios d'application pour le fonctionnement du réseau afin de garantir une restauration des fonctions majeures en cas de défaillance;
– détermine un processus pour établir un ordre de priorité équitable des différents utilisateurs et des applications dans le cadre d'un réseau partagé.

5.1.5 Considérations relatives à la conception de la sûreté de fonctionnement d'un réseau

5.1.5.1 Intégration des paramètres de sûreté de fonctionnement dans la conception

L'intégration des paramètres de sûreté de fonctionnement dans la conception, afin d'améliorer la performance d'un réseau, nécessite une approche technique systématique permettant d'atteindre les objectifs requis en matière de sûreté de fonctionnement. Les performances d'un réseau sont affectées par plusieurs facteurs critiques présentés en termes de conception de la sûreté de fonctionnement d'un réseau.

5.1.5.2 Conception redondante

La conception redondante permet d'améliorer efficacement la sûreté de fonctionnement d'un réseau. Elle est fréquemment utilisée dans la conception de la sûreté de fonctionnement d'un réseau. Les mécanismes de protection utilisés pour améliorer la fiabilité et les services d'enregistrement et de sauvegarde emploient à la fois la redondance active et la redondance passive.

Dans un réseau de communication, la conception redondante consiste principalement en une redondance des liaisons basée sur la topologie du réseau et, pour des éléments importants du réseau, elle consiste par exemple en une duplication de la mémoire centrale lors de la conception de la mémoire à double face des systèmes de commutation. La première forme de redondance est perçue du point de vue des services et s'intéresse à la protection des canaux de trafic. La seconde vise à renforcer la fiabilité et à protéger les éléments du réseau contre les dysfonctionnements. Le schéma de conception redondante offre un mécanisme de protection qui agit sur la restauration des services en cas de défaillance. Du point de vue de la redondance, la criticité d'un élément du réseau est déterminée par son application spécifique dans les fonctions du réseau et par son impact sur la perte ou la dégradation des services de réseau.

Il est également possible d'atteindre un niveau de disponibilité élevé grâce à la redondance géographique. Celle-ci est réalisée par réplication du système sur deux ou plusieurs sites géographiquement séparés afin d'assurer une protection contre les défaillances ou l'inaccessibilité d'un site donné, quelle qu'en soit la raison, y compris les dégâts ou dommages induits par des causes externes comme par exemple les tremblements de terre ou les incendies.

5.1.5.3 Gestion des pannes

La technologie de gestion des pannes fournit directement les moyens nécessaires à l'atteinte des attributs de sûreté de fonctionnement d'un réseau. La gestion des pannes peut être groupée en différentes catégories:

– *détection des pannes*: vérification de l'état opérationnel des nœuds et des liaisons du réseau, réglage de différents seuils de performance du réseau et surveillance des variations de la performance du réseau afin de détecter les pannes en temps opportun;

– *localisation et diagnostic des pannes*: localisation de la panne et identification de sa cause en fonction des informations recueillies. Pour une panne ne pouvant pas directement être localisée, il est possible d'effectuer une analyse en fonction des corrélations entre les informations relatives à la panne afin de déterminer l'emplacement spécifique et la cause de la panne;

– *isolement des pannes*: isolement de l'unité défaillante pour éviter toute interférence avec d'autres unités en service;

– *rétablissement des fonctions de service du réseau*: rétablissement des fonctions de services de réseau en réinitialisant l'unité ou en redémarrant une partie de l'unité en cas de panne. Pour une conception redondante de l'unité, utiliser la commutation de protection ou réaffecter les ressources pour éviter une défaillance des services de réseau;

– *élimination des pannes*: remplacement de l'unité défaillante ou correction du défaut logiciel en utilisant le système de soutien de maintenance, y compris une analyse approfondie et les recommandations de suivi pour des actions et des solutions d'amélioration;

– *alarme sur panne*: établissement d'une alarme pour avertir le système de gestion du réseau en cas de panne du réseau pour qu'une mesure corrective immédiate puisse être prise. Différentes alarmes peuvent être établies pour indiquer différents niveaux de panne et définir la priorité des interventions. Le système de gestion du réseau recueille les informations relatives aux alarmes sur pannes pour localiser les pannes et procéder aux analyses ultérieures;

– *prévision des pannes*: analyse et évaluation des probabilités de panne ainsi que des conséquences probables des pannes en utilisant des méthodes telles que l'analyse des tendances;

– *suivi des pannes:* observation et contrôle des états de pannes pour diligenter des actions de maintenance.

5.1.5.4 Gestion des données

Les défaillances du réseau ou les pannes donnant lieu à une indisponibilité peuvent interrompre le flux du trafic d'informations ou entraîner une corruption des données. La perte de données-clés peut empêcher la restauration des fonctions de service du réseau ou entraîner des pertes matérielles pour les opérateurs. Les méthodes décrites ci-après sont généralement utilisées pour gérer des données afin d'améliorer la sûreté de fonctionnement des réseaux:

– l'archivage de données dupliquées en des lieux différents afin de protéger les supports d'enregistrement des données contre d'éventuels dégâts ou dommages;

– la sauvegarde périodique afin de protéger les informations et les données-clés. Il convient de protéger les données importantes par des sauvegardes multiples et une sauvegarde en un lieu situé à distance. L'utilisation correcte du mécanisme de sauvegarde et de récupération peut réduire le temps d'arrêt et améliorer la performance;

– le chiffrement, les sommes de contrôle, les mécanismes d'accusés de réception et de réémission, ainsi que les mécanismes d'émission redondante peuvent être utilisés pour transmettre sur le réseau des données de service importantes. Par exemple, la protection et l'assurance de transmission de données financières pour les services bancaires afin d'éviter la perte de paquets de données;
– l'utilisation de supports différents pour l'archivage de données de programmes et d'informations;
– la redondance de données de programme importantes peut être utilisée pour assurer un fonctionnement normal du système, même lorsque le programme du logiciel exécuté est altéré;
– la synchronisation des informations entre unités actives et passives du système redondant peut être utilisée pour éviter les pertes de données ou un comportement anormal lors de la commutation de protection;
– la protection, la détection et la vérification des données du programme pendant le chargement ou la transmission pour s'assurer que les données incorrectes ne sont pas enregistrées.

5.1.5.5 Facteurs relatifs aux éléments et aux liaisons du réseau

Les «terminaux» ou «points de terminaison» du réseau sont reliés au réseau au moyen de nœuds et de liaisons de réseau. Pour évaluer la sûreté de fonctionnement, il existe deux types communs de configurations de réseau:

– l'évaluation de la sûreté de fonctionnement du réseau de bout en bout (E2E);
– l'évaluation de la sûreté de fonctionnement d'un réseau avec toutes ses terminaisons (tous ses terminaux).

Cette dernière évaluation reflète les rapports existant entre toutes les terminaisons du réseau. L'évaluation de la sûreté de fonctionnement d'un réseau avec toutes ses terminaisons est d'un intérêt d'ordre général pour les fournisseurs de services. Elle est propre à chaque utilisateur du réseau. Les méthodes d'évaluation de la sûreté de fonctionnement des réseaux sont décrites en 6.4.

5.1.5.6 Facteurs liés à l'environnement

Les facteurs liés à l'environnement peuvent entraîner l'interruption du réseau de diverses manières. Par exemple, des catastrophes naturelles telles que les inondations, les séismes, les éruptions solaires et les typhons peuvent tous affecter le fonctionnement d'un réseau. Il convient de tenir compte des facteurs liés à l'environnement lors de la conception de la sûreté de fonctionnement d'un réseau. Il convient de bien appréhender l'impact de l'environnement sur la sûreté de fonctionnement du réseau et de formuler des plans appropriés d'actions préventives et correctives pour maintenir, en cas de sinistre, l'aptitude de sûreté de fonctionnement du réseau.

Les catastrophes naturelles sont accidentelles alors que les conditions atmosphériques sont prévisibles. Le principal impact sur le réseau est en premier lieu reflété par des pannes d'alimentation des équipements du réseau en supposant que les autres installations du réseau sont bien protégées contre de telles conditions. Cette hypothèse simplifie l'approche technique qui est ramenée à une étendue raisonnable d'évaluations pratiques. L'évaluation est fondée sur la durée prévue d'interruption de l'alimentation et sa fréquence en chaque zone concernée du réseau; elle est utilisée pour assurer une protection adéquate de l'alimentation et fournit une source alternative de manière à réduire l'impact de l'interruption d'alimentation sur les équipements opérationnels. Il est essentiel d'évaluer le pourcentage d'utilisateurs des services de réseau affectés par la panne d'alimentation ayant entraîné des interruptions du réseau, dans chaque zone, par rapport au nombre total d'utilisateurs du réseau. L'arrêt ou l'indisponibilité des fonctions de service du réseau résultant de ces pannes d'alimentation peut être prévu annuellement.

5.1.5.7 Facteurs humains

Il convient de tenir compte de l'impact des facteurs humains sur le temps d'arrêt du réseau afin d'évaluer les erreurs humaines et les erreurs de flux d'activités du processus et de les utiliser comme base d'amélioration de la sûreté de fonctionnement.

a) La prise en compte des facteurs humains dans des activités de maintenance systématique du réseau

La mise à niveau et l'extension d'un réseau sont des activités programmées qui peuvent entraîner une mise hors-service temporaire d'une organisation ou de l'ensemble du réseau. Un plan correct de mise à niveau/extension et un flux raisonnable des activités correspondantes peuvent réduire de manière significative les temps d'arrêt. La condition préalable de l'évaluation de la sûreté de fonctionnement liée à ces activités est de prévoir la durée moyenne des activités dans le cadre du plan annuel de gestion du réseau. Le temps d'arrêt estimé peut être obtenu en évaluant le plan technique et le flux opérationnel des activités de maintenance programmées. L'effet de la maintenance programmée ou des mises à niveau sur la disponibilité du réseau peut être évalué en tenant compte du pourcentage des utilisateurs de services de réseau affectés.

b) Configuration et fonctionnement du réseau

Il convient de recueillir des données statistiques sur les configurations et fonctionnements incorrects du réseau afin de prédire les incidences des erreurs humaines et d'en évaluer l'impact sur le temps d'arrêt du réseau. Ceci permet d'identifier les faiblesses du flux opérationnel du réseau et de les utiliser comme base pour améliorer la fiabilité.

c) Impact des interférences externes

Les données annuelles concernant les services de réseau ont montré que des liaisons principales de réseaux ont été interrompues du fait d'erreurs humaines de construction, de dommages aux infrastructures dus à des accidents, à des actes de vandalisme sur les équipements et à des vols de câbles. Les données statistiques des années précédentes concernant des réseaux similaires peuvent être utilisées pour prévoir l'impact des interférences externes sur le nouveau réseau afin de déterminer le temps d'arrêt dû à des causes humaines.

5.1.5.8 Facteurs de conception des réseaux

Du point de vue de la conception des réseaux, il convient que les facteurs affectant l'évaluation de la sûreté de fonctionnement s'intéressent aux aspects suivants.

a) Les mécanismes de protection du réseau

L'intégration des mécanismes de protection dans la conception du réseau est utilisée pour améliorer la disponibilité, réduire les temps d'arrêt et renforcer l'aptitude de restauration. Les mécanismes de protection assurent la protection nécessaire contre les défaillances. Les redondances intégrées dans les conceptions de réseaux pour ce qui concerne les protocoles d'acheminement, les protocoles de sauvegarde à chaud, les protocoles de rattachement d'itinéraires et les protocoles de commutation automatique, sont tous des mécanismes de protection contre les défaillances du réseau. Les mécanismes de protection sont en général constitués de fonctions matérielles et logicielles et sont sujets à des défaillances aléatoires ou systématiques. Il convient d'envisager, lors de la conception du réseau, une évaluation de la sûreté de fonctionnement en tenant compte des conséquences des défaillances des mécanismes de protection.

b) Pointes de trafic

Les pointes de trafic correspondent à des situations de «goulots d'étranglement» du trafic qui affectent la performance du réseau. Les pointes de trafic peuvent entraîner une instabilité des performances. Des études du trafic fournissent les informations nécessaires sur la structure des flux de trafic et sa loi de probabilité dans le temps. En fonctionnement normal, on peut s'attendre à des pointes de trafic et parfois les prévoir; par exemple une pointe de charge apparaissant certains jours ou à certaines heures, du fait d'éléments externes tels que des intempéries, des accidents, etc. En général, le réseau est conçu pour avoir une limite de capacité finie et les fonctions de service ont des seuils de capacité qui risquent d'affecter l'accès et la connexion s'ils sont dépassés. L'impact des

pointes de trafic sur la performance peut être évalué en élaborant un modèle de topologie et en divisant le réseau en couches et en zones de du haut vers le bas, pour ensuite déceler les «goulots d'étranglement» du trafic réseau pour chaque service du bas vers le haut, ce qui permet de prédire la gamme de services qui est touchée.

c) Accès de maintenance

L'accès de maintenance est un facteur important qu'il convient de prendre en compte pour la conception du réseau. En matière de fourniture de services de réseau, il est commun dans ce secteur d'effectuer des opérations de maintenance sans interrompre le fonctionnement du réseau. Les activités de maintenance peuvent nécessiter un accès physique sur site aux équipements du réseau ou un accès distant à la fonction réseau de mise à jour des logiciels. Pour faciliter l'accès physique, il convient que la conception du réseau tienne compte de l'emplacement du site, de son accessibilité et de l'environnement de service pour les tâches de maintenance, de la maintenabilité des équipements de réseau nécessitant le service et des exigences de soutien logistique aux activités de maintenance. Pour faciliter l'accès à distance, il convient que la conception du réseau envisage l'utilisation d'un protocole approprié pour l'interface de liaison du réseau, la sécurité des informations, le processus de vérification de la protection du réseau et les systèmes de sauvegarde pour assurer la pérennité du réseau.

5.1.6 Simulation de la sûreté de fonctionnement d'un réseau

La simulation de la sûreté de fonctionnement d'un réseau est un processus utilisé pour étudier et analyser la sûreté de fonctionnement existante ou prévue de ce réseau. La simulation est basée sur une modélisation de la sûreté de fonctionnement du réseau et une étude des défaillances du réseau. Le but est de trouver des solutions permettant d'améliorer la sûreté de fonctionnement du réseau. Il convient que la simulation de la sûreté de fonctionnement du réseau tienne compte à la fois de la structure statique du réseau et du comportement dynamique de ses nœuds et des connexions de ses liaisons.

La structure statique d'un réseau fait référence à ses connexions topologiques. Il convient d'analyser la structure statique afin de mieux appréhender les connexions des éléments du réseau ainsi que leurs relations hiérarchiques et structurelles.

Le comportement dynamique d'un réseau renvoie à la probabilité de défaillance de chaque élément et connexion dans le temps, à l'interaction fonctionnelle des divers éléments, au comportement d'éléments corrélés après défaillance et à leur impact sur les utilisateurs. Il convient que l'analyse du comportement dynamique d'un réseau s'intéresse aux éléments suivants:

– les divers services de réseau (par exemple, voix et données);
– les défaillances des différentes couches du réseau (par exemple défaillance de la couche physique, défaillance de la couche réseau et défaillance de la couche service);
– la pondération de l'impact des différentes défaillances (par exemple l'impact d'une défaillance affecte un certain nombre d'utilisateurs, la durée de l'interruption du service ainsi que les types de services de réseau);
– la détection des défaillances et la probabilité de localisation des nœuds et de la connexion des liaisons du réseau;
– la probabilité de succès de la commutation entre éléments du réseau;
– le délai de restauration après une défaillance.

5.1.7 Evaluation de la sûreté de fonctionnement d'un réseau

L'évaluation de la sûreté de fonctionnement du réseau définit le processus permettant de vérifier que la conception du réseau satisfait aux objectifs de sûreté de fonctionnement. Cette évaluation comprend:

– l'identification de l'objectif de l'évaluation et des objets à évaluer: Un réseau est constitué de plusieurs sous-réseaux. Deux nœuds de réseau quelconques peuvent être reliés entre eux par une connexion de sorte qu'ils constituent le plus petit réseau. Par conséquent, il

est nécessaire de bien définir les frontières du réseau avant de commencer l'évaluation de la sûreté de fonctionnement. Il convient de déterminer le type d'équipements utilisés et les liaisons impliquées dans le réseau pour une évaluation appropriée de la conception de la sûreté de fonctionnement;

– la définition des défaillances: Les éléments du réseau sont confrontés à de nombreuses situations intermédiaires impliquant leurs performances entre le fonctionnement normal et la défaillance du réseau. Pour simplifier le processus d'évaluation dans toute la mesure du possible et le cas échéant, il convient d'établir une définition adaptée de la défaillance réseau ou un classement des défaillances. Une situation est considérée acceptable si la performance d'un élément de réseau s'inscrit dans les limites de ce seuil; elle est considérée inacceptable et constitue donc une défaillance dans le cas contraire (voir 5.1.3);
– l'élaboration d'un modèle de sûreté de fonctionnement pertinent: Il convient de s'appuyer sur la topologie du réseau, sur les fonctionnalités des services et sur les couches du réseau pour établir les relations entre divers éléments de réseau, de manière à formuler un modèle de sûreté de fonctionnement du réseau;
– la collecte de données relatives à l'ensemble des éléments et liaisons du réseau, pertinentes en matière d'évaluation de la sûreté de fonctionnement. Ces données sont constituées d'informations relatives aux défaillances et au temps d'arrêt recueillies pendant le fonctionnement du réseau. Elles peuvent être obtenues par des essais de performance ou être recueillies sur site;
– la réalisation de l'évaluation et de l'analyse: Sur la base du modèle de sûreté de fonctionnement et des données, des analyses sont effectuées pour obtenir des résultats quantitatifs des paramètres de sûreté de fonctionnement relatifs aux caractéristiques des performances du réseau;
– l'interprétation des résultats de l'évaluation pour émettre des recommandations et lancer des actions de suivi: Il convient d'interpréter les résultats de l'analyse en termes de performance prévue du réseau, d'alternative de conception et d'améliorations pratiques;
– le cas échéant, la mise en œuvre de processus formels de vérification et de validation pour l'évaluation de la sûreté de fonctionnement du réseau.

L'Article 6 décrit l'évaluation et les mesures de sûreté de fonctionnement d'un réseau.

5.2 Prise en compte des aspects technologiques du réseau

5.2.1 Architecture du réseau

L'architecture d'un réseau de communication peut être représentée de manière hiérarchique par des couches verticales et un découpage horizontal. Cette hiérarchie constitue la structure de l'architecture du réseau. Les frontières du réseau sont utilisées pour identifier les points d'accès et les connexions individuelles des sous-réseaux.

a) Découpage horizontal

L'architecture du réseau peut être découpée horizontalement en réseau de locaux d'abonnés, réseau d'accès et réseau fédérateur:

– le réseau de locaux d'abonnés, connecté entre un terminal utilisateur et une interface utilisateur-réseau, permet à un utilisateur d'accéder en toute commodité au réseau; il s'agit par exemple du système de câblage utilisé dans les habitations ou les bureaux;
– le réseau d'accès peut être un réseau d'entités, entre une interface utilisateur-réseau et une interface de nœud de services utilisée à des fins de transport;
– le réseau fédérateur peut être constitué d'un réseau de transport «fédérateur» à large bande et à grande vitesse, qui fournit les principales connexions et les grands nœuds de commutation.

Plus la connexion du périphérique est proche du réseau fédérateur et plus le trafic est concentré. De ce fait, il est nécessaire de disposer d'un support de transmission de grande capacité pour prendre en charge l'augmentation du trafic et d'utiliser des systèmes plus complexes pour traiter les informations du réseau. Par conséquent, les périphériques

déployés pour utilisation à proximité du réseau fédérateur peuvent avoir un impact plus important sur les fonctions de service de réseau. Du point de vue de la sûreté de fonctionnement, il est nécessaire de disposer de performances de fiabilité plus élevées. Le découpage horizontal est illustré sur le modèle général de réseau de communication en Figure A.1.

b) Hiérarchie verticale

La hiérarchie verticale peut être groupée dans la couche inférieure pour les fonctions de transport et dans la couche supérieure pour les fonctions de services d'application. Les regroupements des deux blocs de couches séparées sont appelés strates de fonctionnalités en architecture réseau. Elles sont définies ci-après:

– *strate de transport*: elle assure un transfert en toute transparence des données entre serveurs ainsi que la connexion de bout en bout, la restauration après un état d'erreur et le contrôle de flux; elle réalise également un transfert complet des données;

– *strate de service:* elle fournit aux utilisateurs divers services de communication et aux utilisateurs finaux des applications informatiques.

En outre, les réseaux de soutien assurent le fonctionnement fluide du réseau en exécutant les fonctions de suivi et de contrôle. Les réseaux de soutien comprennent un réseau de signalisation, un réseau de synchronisation et un réseau de gestion des communications.

Il convient que l'analyse de la sûreté de fonctionnement du réseau tienne compte des influences des couches sur la performance du réseau. La sûreté de fonctionnement d'un service de réseau concerne non seulement les équipements de transport et l'acheminement du service support, mais également les équipements de services applicatifs utilisés pour les fonctions de réseau. Il est également recommandé d'évaluer l'impact des réseaux de soutien.

L'Article A.3 fournit une description concise du modèle de référence OSI et des couches associées au réseau de communication. Les regroupements en blocs représentant la strate de service et la strate de transport sont représentés en Figure A.3.

5.2.2 Topologie

Un réseau de communication est constitué de terminaux, de nœuds de réseau et de liaisons de transport. La topologie du réseau reflète la connexion du point de vue de la configuration du réseau. La topologie d'un réseau est la disposition ou la cartographie des nœuds du réseau reliés entre eux par des liens; il peut s'agir de connexions physiques ou logiques. La topologie physique constitue la cartographie des nœuds du réseau et de leurs connexions, comme par exemple le câblage entre des équipements réseau séparés. La topologie logique représente les trajets des signaux correspondant aux déplacements des données entre nœuds. Les trajets des signaux ont de multiples connexions logiques et peuvent prendre des routes alternatives de transfert de données pour atteindre leur destination.

Il existe plusieurs types de technologies de réseau correspondant à des formes topologiques différentes comme par exemple le réseau *en étoile*, le réseau *maillé*, le réseau *arborescent* et le réseau *annulaire,* désignés en fonction de cette forme topologique. Les exemples types d'applications de topologies réseaux sont par exemple les réseaux de communication à répartition centralisée qui ont une configuration de type *en étoile*, les réseaux de commutation distributive qui ont une configuration de type *maillé* et permettent de relier des abonnés du téléphone, les configurations de type *arborescent* pour la livraison de services multimédia et les réseaux de type *annulaire* pour assurer la protection de réseaux optiques rapides. La topologie du réseau décrit le ou les cheminements actifs ou opérationnels de transport de services sur le réseau, ainsi que le ou les cheminements de secours et les mécanismes de protection; elle reflète également les capacités d'accès au service et de transport. Certaines méthodes d'analyse de la sûreté de fonctionnement du réseau, telles que l'analyse de la vulnérabilité du réseau et l'analyse de la pérennité du réseau, sont appliquées du point de vue de la connectivité du réseau. Elles permettent de décrire l'impact de la topologie du réseau sur sa sûreté de fonctionnement. Il convient de tenir compte de la forme topologique du réseau pour la modélisation et l'évaluation de la sûreté de fonctionnement. Une topologie parallèle associée à un mécanisme de commutation pour la protection contre les défaillances peut améliorer la disponibilité, et de ce fait, la performance du réseau.

5.2.3 Interconnexions

Les utilisateurs du réseau, de périphériques et de liaisons, ainsi que d'autres entités, se connectent entre eux de manière à constituer un réseau. L'interconnexion est une caractéristique importante du réseau et reflète les exigences du réseau en matière d'interfaces équipements. L'interconnexion peut être permanente (par exemple câblée) ou temporaire (par exemple une liaison téléphonique); les supports de transmission peuvent être fixes (par exemple par fibres optiques) ou sans fil (par exemple hertziens).

La fiabilité de l'interconnexion a un impact important sur la sûreté de fonctionnement du réseau. Il convient d'améliorer la fiabilité des interconnexions, tant du point de vue matériel comme par exemple en adoptant des périphériques d'un niveau de fiabilité élevée et de conception à sécurité intrinsèque que logiciel comme par exemple l'exécution d'un protocole de commutation de protection sur l'interface d'interconnexion des équipements pour permettre la prise en charge de la redondance.

5.3 Prise en compte des fonctions de service du réseau

5.3.1 Fourniture des fonctions de service du réseau

Les fonctions de service du réseau renvoient à des programmes ou à des applications qui interagissent avec les utilisateurs finaux du réseau pour transmettre ou échanger des données et des informations sur le réseau. Le développement des technologies réseau et notamment les progrès des technologies de réseaux mobiles, permet de fournir un plus grand nombre de services sur les réseaux modernes. Des exemples de ces offres de services sont le téléphone, la télécopie, la navigation par Internet, le courrier électronique, le commerce électronique et la vidéo à la demande. Il est possible d'accéder à une combinaison d'informations et de les délivrer sur le même réseau: voix, images, et données via les réseaux de type Internet, intranet et extranet. Les différents types de services de réseau nécessitent des qualités de trafic différentes.

Ces diverses fonctions de service de réseau reflètent les demandes des utilisateurs du réseau. Les utilisateurs attendent généralement une aptitude à l'emploi élevée en matière de fourniture de services de réseau. Il convient que les exigences relatives à la sûreté de fonctionnement des fonctions de service de réseau soient élaborées en tenant compte de la capacité d'accès, du maintien des connexions de service et de la perception du service par l'utilisateur.

5.3.2 Stratégie du réseau

La stratégie du réseau est constituée des règles et règlementations précisées par le fournisseur de services de réseau pour assurer la conformité aux exigences pendant le fonctionnement du réseau. Une mise en œuvre appropriée de la stratégie du réseau, définissant le système particulier de gestion pour l'affectation des ressources internes et externes aux activités du réseau, permet une exploitation rentable du réseau. Par exemple, une stratégie d'acheminement correcte peut améliorer l'efficacité de transport du réseau; si elle est correctement appliquée, la stratégie de gestion de trafic permet de réguler l'utilisation du réseau et d'améliorer sa performance; de même, une stratégie QS peut définir les priorités de trafic en fonction du service de réseau et des caractéristiques des utilisateurs, en utilisant diverses méthodes et différents processus pour garantir la QS requise.

La stratégie du réseau reflète le contrôle mutuel et la vérification des relations entre les différentes couches du réseau. Une gestion efficace de la sûreté de fonctionnement du réseau nécessite une prise en charge raisonnable de la stratégie du réseau afin d'obtenir le rapport coût-efficacité le plus élevé en termes de retour sur investissement.

5.3.3 Utilisateurs finaux du réseau

L'utilisateur final du réseau peut être une personne ou une application qui utilise la fonction de service du réseau, par opposition à ceux qui développent, fournissent ou prennent en

charge l'exploitation du réseau. Les utilisateurs finaux qui interagissent avec le réseau ne sont pas concernés par la structure et la composition du réseau. Leurs points de vue sur les fonctions de service du réseau sont différents de ceux des fournisseurs de services.

Du point de vue des utilisateurs finaux, la sûreté de fonctionnement d'un réseau comprend:

– les exigences des utilisateurs finaux en matière de sûreté de fonctionnement du réseau;
– les offres des fournisseurs de services en termes de sûreté de fonctionnement du réseau (ou sûreté de fonctionnement du réseau prévue/cible);
– la sûreté de fonctionnement réalisée ou livrée par le fournisseur de services;
– la sûreté de fonctionnement perçue/constatée par les utilisateurs finaux.

Les besoins des utilisateurs finaux en matière de sûreté de fonctionnement sont la principale source d'information pour l'établissement des exigences de sûreté de fonctionnement. Il est recommandé de tenir compte du profil d'activité des utilisateurs finaux existants et futurs, ainsi que de l'usage qu'ils font du réseau. Lors de la conception d'un réseau, il convient de bien comprendre les besoins des utilisateurs finaux.

5.3.4 Sécurité du réseau

La sécurité d'un réseau est primordiale pour les transactions commerciales, ainsi que pour la protection de la vie privée. Ceci est rendu nécessaire par l'extraordinaire croissance en matière de communications et de mise en réseau via Internet ainsi que par la dépendance vis-à-vis de l'informatique dans l'échange d'informations. Il a été développé diverses méthodes pour protéger les données sensibles contre tout accès non autorisé, la divulgation accidentelle d'informations ou les menaces à la sécurité. Ces méthodes comprennent l'authentification, le codage et le chiffrement des données et des messages, la détection de virus et l'utilisation de pare-feu pour prévenir les attaques liées au réseau.

Outre la sécurité physique des réseaux, trois principaux aspects de la sécurité de l'information doivent être pris en compte:

– les attaques dues à d'éventuelles actions portant atteinte à l'intégrité des informations appartenant à une personne physique ou morale;
– les mécanismes conçus pour détecter, prévenir ou récupérer à la suite d'une attaque compromettant la sécurité;
– les services qui améliorent la sécurité du traitement des données et du transfert des informations sur le réseau.

L'Annexe C fournit des critères d'établissement de services de sécurité réseau.

5.4 Prise en compte de la performance du réseau

5.4.1 Trafic

Le terme trafic fait référence à l'utilisation globale du réseau de communication et aux transactions d'informations à un moment donné. Ces informations sont constituées de messages, d'enregistrements et de données. La performance du réseau en fonction des aspects relatifs au trafic est généralement appelée aptitude à la traficabilité. Elle définit l'aptitude à répondre à une demande de trafic tout en gérant la performance du réseau.

Les exigences en termes de volume de trafic ont notablement augmenté au fur et à mesure de la croissance des besoins en matière de communications et de loisirs. Dans un environnement globalisé, il y a de plus en plus d'opérateurs de communication en concurrence pour fournir les services de données, de voix et d'image sur un unique réseau support afin de réduire les dépenses d'exploitation. Cette tendance exige un traitement rentable du trafic réseau qui affecte l'aptitude de sûreté de fonctionnement des réseaux.

a) Capacité

Il convient que la planification de la conception du réseau tienne compte de la croissance future du réseau, qu'elle analyse par anticipation les exigences des fonctions de service du réseau en termes de capacité de flux de trafic ainsi que l'impact de l'explosion du trafic pour une utilisation rentable de la capacité du réseau et une maîtrise optimisée du flux. Une capacité réseau disposant de la redondance requise peut atteindre une capacité avantageuse d'accès aux services de réseau et prendre en charge la croissance prévue et les développements futurs des besoins du trafic des communications.

b) Maîtrise des encombrements

L'instabilité du flux de trafic dans le temps se reflète par la présence simultanée d'une importante quantité de trafic sur le réseau, au cours d'une courte période. Cette situation est connue sous l'expression «pointe de trafic» au cours de laquelle apparaîtraient les phénomènes de «goulot d'étranglement» ou de restriction des ressources du réseau. Lorsque par exemple la capacité d'un segment du réseau est inadaptée, le trafic est encombré et la capacité de traitement d'un élément du réseau est mise en file d'attente, ce qui entraîne une situation de «goulot d'étranglement». Ceci peut donner lieu à un refus d'accès de certains services de réseau nouveaux, à un retard des communications téléphoniques et à une dégradation de la qualité de prise en charge des services de réseau. Les réseaux modernes peuvent prendre en charge des services multiples de manière plus efficace grâce à l'utilisation de la technologie du multiplexage statistique.

La maîtrise des encombrements utilise des techniques telles que la détection des encombrements, le contrôle d'accès, le tarif d'accès effectué, la stratégie du rejet sélectif, la mise en file d'attente et la gestion de largeur de bande. La maîtrise des encombrements agit de différentes manières selon les divers services de réseau. L'engorgement entraîne une indisponibilité de fourniture des services de réseau. Il convient de tenir compte des questions de sûreté de fonctionnement liées à la maîtrise des encombrements lors de l'évaluation de la fiabilité du réseau.

c) Capacité d'écoulement du trafic

La qualité d'écoulement du trafic est quantitativement reflétée par les paramètres de performance du trafic réseau. Par exemple, sur un réseau de transport utilisant le protocole IP, le délai de transfert des paquets, la variation de ces délais et le taux de perte, peuvent affecter la qualité d'écoulement du trafic. Lorsque l'aptitude de transfert d'un réseau s'est dégradée jusqu'à un certain degré ou seuil, certains services ordinaires ne peuvent plus être fournis.

5.4.2 Transmission

Il existe différents moyens de transférer la voix, les images, les données ou autres informations sur un réseau de communication. La qualité de transmission reflète la capacité du réseau de communication à transférer les services pertinents en fonctionnement normal. Les performances correspondantes sont liées au type et à la qualité du support de transmission ainsi qu'à l'intensité du rapport signal-bruit. Ces éléments peuvent affecter la sûreté de fonctionnement du réseau.

a) Synchronisation

La synchronisation définit le processus assurant que l'équipement qui envoie le signal et l'équipement qui le reçoit fonctionnent en parfait alignement pour une transmission fiable des données. Le réseau de synchronisation est un réseau support important. Lorsqu'il s'agit d'analyser la sûreté de fonctionnement d'un réseau de communication, il convient d'effectuer l'analyse et l'évaluation des défauts d'horloge, des erreurs de synchronisation et des risques correspondants. Il convient de tenir compte à la fois de l'impact du défaut d'horloge sur le réseau de communication et de l'exactitude et de la sûreté de fonctionnement du réseau d'horloge proprement dit.

b) Intégrité de la transmission

L'intégrité de la transmission est l'aptitude des signaux, constitués d'informations et de données transportées par le réseau de communication, à avoir un nombre minimal d'erreurs pendant le transport. Cette intégrité peut être mesurée par des paramètres tels que le taux d'erreur sur les bits et le taux de secondes sans erreur, etc. Il convient d'utiliser des supports de transport de haute qualité ainsi qu'une protection rapide et raisonnable par commutation sur défaut, ainsi qu'un mécanisme de retransmission pour

améliorer de manière notable l'intégrité des signaux. L'intégrité de la transmission peut affecter l'aptitude de sûreté de fonctionnement.

c) Qualité de la connexion

La connexion entre réseaux constitue la base même de la fourniture d'une fonctionnalité de communication. La qualité de la connexion reflète la capacité de la liaison réseau à transporter les informations. Il convient que l'évaluation de la qualité de transport de liaison tienne compte du niveau de bruit et des perturbations ainsi que de la vitesse de transmission. L'évaluation s'applique tant aux connexions fixes qu'à la propagation de signaux radioélectriques. La qualité de la connexion peut affecter la performance de sûreté de fonctionnement.

5.4.3 Robustesse

La robustesse reflète l'aptitude d'adaptation d'un réseau dans des conditions anormales. La conception et la mise en place de la sûreté de fonctionnement d'un réseau peut non seulement améliorer la robustesse de sa performance mais aussi améliorer ses importantes fonctions de mission ou de sécurité intégrées lors du fonctionnement du réseau en toute sécurité.

a) Fiabilité

La fiabilité est à la base de la robustesse d'un réseau. En tenant compte des contraintes de coûts, l'utilisation de périphériques réseau de haute fiabilité, de liaisons réseau de haute qualité et de logiciels «exempts de bogues» permettrait dans la pratique d'obtenir une fiabilité durable.

b) Pérennité

La pérennité fait référence à l'aptitude d'un réseau à récupérer, dans les limites de performance acceptables, à la suite d'incidents ou de pannes. Ceci peut permettre au réseau de continuer à fournir des fonctions de réseau normales. Les limites de performance acceptables sont déterminées à partir de l'accord sur le niveau de service (SLA) du fournisseur de services de réseau afin de satisfaire aux exigences de QS (voir l'Article 7). La fréquence et la durée des situations indésirables, dans des zones de service spécifiques, nécessitent souvent d'étendre la conception et le fonctionnement du réseau pour maintenir la pérennité. Il convient que la conception du réseau tienne compte de la sûreté de fonctionnement de manière à améliorer la pérennité et la capacité de restauration du réseau, surtout lorsque la sécurité est en jeu.

c) Tolérance aux pannes

La tolérance aux pannes reflète l'aptitude du réseau à fonctionner lorsque des pannes surviennent. En d'autres termes, le réseau continue à fonctionner en cas de panne interne, reflétant ainsi son aptitude à assurer un transport durable et à fournir les services prévus. En général, la tolérance aux pannes d'un réseau peut être obtenue grâce à une conception redondante et à l'intégration d'un système de gestion des pannes du réseau. Par exemple, lorsqu'une panne est décelée, l'unité passive prend immédiatement en charge les fonctions opérationnelles de l'unité active pour assurer un traitement durable des services.

5.4.4 Aptitude à l'emploi

L'aptitude à l'emploi reflète la capacité à délivrer la sûreté de fonctionnement d'un réseau du service aux utilisateurs finaux. Une aptitude à l'emploi élevée améliore la disponibilité, fournit une intégrité de service sans défaillance supplémentaire, et réduit les coûts de service. L'aptitude à l'emploi peut être décrite au moyen des critères de performance suivants.

a) L'accessibilité aux services

L'accessibilité au service désigne la facilité d'accès à un service de réseau par l'utilisateur, dans des conditions données et pendant une durée donnée. Pour les services en mode connexion, ceci fait référence à l'aptitude à établir la connexion. L'accessibilité peut être mesurée en termes de délais d'accès au service, d'aptitude d'accès au réseau et de capacité de contrôle d'accès au service. Il convient que l'évaluation de l'accessibilité tienne compte de l'accessibilité au réseau par l'utilisateur, comme par exemple

l'établissement de la connexion du circuit physique, et de l'aptitude à établir la connexion de service ou à recevoir le service comme dans le cas de l'établissement d'une connexion pour un contrôle d'appel de couche supérieure.

b) La continuité des services

La continuité des services désigne l'aptitude d'un service de réseau, une fois établi, à continuer à être fourni dans des conditions données et pendant la durée requise. Elle reflète la fiabilité de transmission continue du trafic de service, avec une certaine autonomie d'accès au trafic ou de libération du réseau. La fourniture d'un service de bout en bout implique de nombreux périphériques et liaisons réseau. La continuité nécessite un soutien de la sûreté de fonctionnement du réseau pour maintenir un fonctionnement stable. Une conception redondante du réseau et une gestion efficace des pannes sont des pratiques généralement acceptées pour améliorer la tolérance aux pannes de manière à assurer la continuité des services.

c) L'intégrité des services

L'intégrité des services désigne la capacité du réseau à délivrer les informations et les données sans dégradation excessive. Elle est liée au transfert des informations et des données appelé débit. La dégradation est généralement causée par des bruits, une variation temps/vitesse, et par une déformation partielle durant la transmission.

d) Libération

La libération concerne les périphériques et liaisons de réseau impliqués dans la communication de bout en bout d'un utilisateur donné ainsi que les ressources réseau (y compris la largeur de bande, le canal ou les ressources relatives aux protocoles de couche supérieure) qui doivent être libérés lorsque la connexion ou la session de communication est fermée. Un réseau ayant une sûreté de fonctionnement élevée peut assurer la fiabilité et la justesse de cette libération. Ceci permettrait d'éviter une mainmise de longue durée sur les ressources, des surcharges anormales et d'autres problèmes encore. La libération est une caractéristique affectant l'accessibilité et la continuité des services dans l'aptitude à l'emploi d'un réseau.

5.4.5 Opérabilité

L'opérabilité peut être perçue de deux points de vue différents.

a) Du point de vue de l'utilisateur, elle fait référence à l'aptitude d'un service à être exploité avec succès et facilité. Par exemple, l'opérabilité permet à un utilisateur d'accéder à un réseau ou de composer un numéro. Les fournisseurs de services peuvent offrir aux utilisateurs une connexion fiable en termes de facilité d'utilisation, afin d'améliorer la fiabilité des opérations de l'utilisateur.

b) Du point de vue du fournisseur de services, l'opérabilité fait référence à l'aptitude du réseau à être exploité avec succès et avec facilité par l'opérateur de communication, ce qui comporte la livraison du service et la gestion du réseau. En améliorant l'opérabilité du réseau en termes de facilité d'utilisation, avec une conception orientée utilisateur et une protection contre tout fonctionnement anormal, les pannes dues à l'exploitation peuvent être notablement réduites, ce qui renforce la sûreté de fonctionnement.

5.5 Intégrité des données et informations du réseau

5.5.1 Crédibilité du débit de données du réseau

Les besoins en termes d'intégrité des données sont identifiés par des études de marché s'intéressant aux besoins du fournisseur de services et aux exigences de l'utilisateur pour ce qui concerne l'exactitude et la protection des informations liées à l'utilisation des services de réseau. Les informations constituent une entité indépendante transportée par le réseau de communication du point d'entrée au point de sortie. L'intégrité reflète la crédibilité des informations, transformées en flux de données pendant le fonctionnement du réseau. Le débit de flux de données est la quantité de données numériques par unité de temps qui est livrée sur une liaison physique ou logique ou qui passe par un nœud de réseau dans un réseau de communication. La crédibilité est l'aptitude des fonctions de service du réseau à reconnaître la quantité d'entrées correctes pour autoriser l'accès. Les éléments du réseau et les fonctions

de service qui en sont chargés transforment les entrées de l'utilisateur en sorties à l'attention des destinataires prévus. La caractéristique d'intégrité de la sûreté de fonctionnement d'un réseau est l'aptitude du réseau à assurer le passage des données en toute sécurité de manière à protéger le contenu du flux de données. L'intégrité est le processus de vérification des fonctions de service du réseau utilisé pour s'assurer que le contenu du flux de données n'est pas contaminé, corrompu ou altéré lorsque les entrées sont transformées en sorties.

L'obtention de l'intégrité nécessaire dépend des mécanismes mis en œuvre dans les éléments de réseau et les fonctions de service conçues pour détecter et prévenir un transfert incorrect du flux de données entre les fonctions de traitement du réseau. L'intégrité dépend également des mécanismes utilisés pour vérifier la justesse et l'authenticité des entrées et des sorties de données. Dans ce contexte, l'intégrité est déterminante et il est possible d'en quantifier certains aspects. Prenons par exemple l'autorisation d'accès à un distributeur automatique de billets. La machine valide le fait que la carte de crédit et l'identifiant personnel sont authentiques et permet de retirer de l'argent. Dans ce cas, l'intégrité d'un réseau de distributeur automatique de billets peut être évaluée quantitativement sur la base de conditions d'influence telles que la fréquence de refus d'accès, la population d'utilisateurs et l'usage, le volume de transactions commerciales et les taux de criminalité dans le voisinage. L'indication de l'intégrité du point de vue de l'utilisateur peut être évaluée qualitativement sachant que le distributeur automatique est efficace, commode, qu'il fonctionne quelquefois ou qu'il est en panne.

5.5.2 Maîtrise de la dégradation des données par le réseau

L'intégrité fait également référence au traitement des informations de signaux de transmission, comme par exemple le débit de données sans dégradation excessive présent dans l'environnement d'exploitation d'un réseau. L'intégrité est bien perçue si l'on connaît les différentes hiérarchies des réseaux. Le manque d'intégrité ou la maîtrise inadaptée des données de la couche inférieure est reflété par la dégradation de la transmission résultant de la qualité des supports de transmission. L'intégrité de la couche de transport de paquets peut être mesurée en termes de taux d'abandon de paquets et de taux d'erreurs de paquets. L'intégrité de la couche service s'exprime par l'intégrité des données d'information.

– *Données de service*: service fourni par le réseau. Une fois que l'utilisateur a obtenu un service spécifique, il convient que le réseau s'assure que ce service est exempt de toute dégradation excessive. Cette dégradation est reflétée par l'interruption et l'arrêt du service. L'intégrité des données de service peut être améliorée en adoptant une conception redondante et en accélérant la commutation de protection en cas de panne. Les données de service comprennent les données de contrôle de service et les données de supports de service.
– *Données de programme*: un programme est un ensemble d'instructions codées permettant l'exécution du logiciel réseau. Il convient que la fiabilité du programme mette l'accent sur toutes les modifications anormales, comme par exemple une mémoire programme protégée en écriture et la fourniture d'un mécanisme de vérification. Ceci permet d'améliorer l'intégrité des données du programme logiciel.
– *Données d'information*: informations de support permettant le fonctionnement du logiciel réseau telles que les informations utilisateur et les informations de connexion des protocoles de contrôle de la transmission. Il convient que la conception de la fiabilité du réseau tienne compte de l'intégrité de ces informations. Dans le cas d'une conception redondante, il est recommandé que le réseau comporte une sauvegarde des informations pour éviter leur dégradation.

5.6 Qualité de service (QS)

5.6.1 Objectifs de la QS

Dans le contexte de la sûreté de fonctionnement des réseaux, la QS traite des effets de la performance du réseau pour déterminer le niveau de qualité de la fourniture de service. La QS est définie par le SLA.

Le niveau de qualité est le degré de satisfaction que représente la QS. La sûreté de fonctionnement est un attribut de la qualité. Elle assure non seulement la continuité du service en le protégeant contre les défaillances, le refus d'accès au service et la libération des ressources, mais aussi le transfert des informations utilisateur en les protégeant contre toutes pertes ou interruptions.

QS fait référence à un terme générique dérivé d'un ensemble d'indicateurs. Elle est évaluée par les fournisseurs de services afin de déterminer la valeur de performance d'un réseau qui permet de garantir leur retour sur investissement et d'améliorer leur offre de services. La QS est également perçue par les utilisateurs (abonnés des services de communication) pour vérifier la valeur du service qu'ils paient.

Les applications de QS comprennent:

– la détermination des relations existantes entre la QS et la performance du réseau dans le cadre de la sûreté de fonctionnement du réseau;
– l'identification des attributs et des facteurs de performance qui influencent la QS résultante;
– l'établissement de paramètres et de critères de la QS mesurables et observables;
– l'identification du processus et de la méthodologie d'évaluation de la QS.

5.6.2 Accord sur le niveau de service pour la fourniture de la QS requise

Un accord sur le niveau de service est un accord formel entre deux ou plusieurs parties. Il s'agit d'une pratique commerciale commune en matière de fourniture des fonctions de services de réseau. L'accord concernant la fourniture de la QS requise inclut des déclarations relatives à la performance, à la facturation, à la livraison des services ainsi que des questions d'ordre juridique et économique.

L'accord est constitué de deux parties.

a) L'accord cadre

L'accord cadre constitue une déclaration des objectifs de l'accord et définit les partenaires concernés.

L'accord a pour objectif de:

– définir les niveaux de service que toutes les parties concernées doivent garantir pour la satisfaction des utilisateurs;
– aider les utilisateurs, les fournisseurs de services et les fournisseurs de réseau à échanger des informations avec une qualité de service et une performance du réseau appropriées;
– fournir une base de mesure ainsi que des paramètres permettant d'exécuter l'accord sur le niveau de service;
– stipuler les pénalités en cas de violation du SLA menant à la résiliation et à la rupture du contrat.

Il convient que l'objectif de l'accord décrive la fourniture des services et la performance envisagée.

Il convient que l'accord inclue une clause de confidentialité précisant la manière dont son contenu doit être traité, le partage des informations et les obligations des parties impliquées.

Il convient que l'accord prévoie un processus de revue indiquant la fréquence et les modalités de la revue.

Il convient que l'accord cadre soit signé par les autorités désignées à cet effet et représentant les parties impliquées.

b) L'accord spécifique sur la fourniture de la qualité de service

L'accord spécifique donne une description détaillée de la qualité de service particulière à fournir à une partie donnée.

Il convient que l'accord spécifique sur la qualité de service fournie comprenne:

– une description de l'interface de manière à établir la frontière des responsabilités de chaque partie impliquée en des points d'interaction pour l'échange d'informations avec le fournisseur de services qui contrôle tous les points d'interaction;

– des informations concernant l'interface commerciale: constituées de points d'interaction placés entre l'utilisateur et le fournisseur de services pour des fonctions spécifiques de l'accord de qualité de service, des comptes-rendus de performance et des schémas de réaction afin d'indiquer le niveau convenu de qualité de service fournie;

– des informations concernant l'interface technique: elle est constituée de points d'interaction pour l'échange d'informations de service spécifiques permettant de mesurer la qualité des services réalisés;

– une description des configurations de trafic et des schémas de mesure correspondants;

– les paramètres et objectifs de qualité de service spécifiques à l'accord;

– les mesures quantitatives et qualitatives des exigences relatives à la QS telles que les performances de disponibilité ou autres caractéristiques concernant la sûreté de fonctionnement;

– la déclaration des pénalités selon les termes et conditions spécifiques à la violation du SLA menant à la résiliation et à la rupture du contrat.

5.6.3 Rapports entre QS et performance du réseau

La QS résulte, par des relations établies, de la performance du réseau. La QS est déterminée par un ensemble de critères importants pour les fournisseurs de services ainsi que pour les utilisateurs des services de réseau. Ces critères peuvent être traduits en paramètres de performance. La performance du réseau peut représenter la performance d'un élément particulier du réseau ou du réseau dans son ensemble. La performance du réseau affecte la QS.

Les utilisateurs d'un service de réseau sont généralement concernés par la QS pour un service de bout en bout, comme par exemple pour mener à bien un appel téléphonique ou l'émission de messages sur Internet. Pour les utilisateurs, la performance est la garantie de la fourniture au point d'accès au service.

Les fournisseurs de services sont davantage concernés par l'efficacité et le rendement de la performance du réseau, associés au développement des systèmes, à la planification du réseau ainsi qu'à l'exploitation et à la maintenance. Les fournisseurs de services sont concernés par la qualité aux points de connexion du réseau.

Un réseau peut comporter plusieurs fournisseurs de services collaborant entre eux pour fournir l'ensemble des services de réseau. Dans des environnements comportant de multiples fournisseurs de services, il peut y avoir différents niveaux de QS. Dans la pratique, les utilisateurs peuvent être confrontés à diverses plages de QS. Il convient donc d'établir des niveaux minimaux de performance pour chaque service, ainsi que pour les éléments de connexion du réseau pour se conformer à l'accord correspondant sur le niveau de service, applicable à chaque fournisseur de service.

Le processus de communication comporte les fonctions de services clés présentées ci-après:

– la fonction «accès» permet à l'utilisateur d'accéder aux ressources du réseau pour lancer le processus de communication;

– la fonction «transfert des informations utilisateurs» assure l'échange d'informations d'un bout à l'autre;

– la fonction «libération» concerne l'achèvement du processus de communication.

Les critères pertinents de qualité de service liés au processus de communication sont les suivants:

– la *vitesse* qui indique l'intervalle de temps nécessaire pour réaliser la fonction;
– l'*exactitude* qui marque le degré de conformité de la fonction réalisée;
– la *disponibilité* qui définit le degré de certitude de la fonction réalisée.

A partir de cet ensemble de paramètres de performance de base et des seuils d'indisponibilité, il est possible de déterminer une combinaison d'exigences QS (voir l'Article 7). Les paramètres de performance résultants peuvent être représentés par une ou plusieurs fonctions quantifiables à des fins de mesure de la performance.

5.6.4 Rapports entre QS et sûreté de fonctionnement du réseau

Le lien avec la QS est l'identification de la sûreté de fonctionnement comme un attribut de la qualité pour contribuer à l'aptitude à l'emploi afin de fournir la sûreté de fonctionnement du service aux utilisateurs finaux. Les caractéristiques de sûreté de fonctionnement comprennent la disponibilité et ses facteurs d'influence tels que la fiabilité, la maintenabilité et le soutien à la maintenance. La disponibilité est un paramètre de performance d'un réseau qui affecte la QS résultante. Il est de ce fait possible de lier la QS et la sûreté de fonctionnement.

La sûreté de fonctionnement couvre une large gamme de technologies et influence la QS fournie. Les applications utilisées dans l'ingénierie de la sûreté de fonctionnement facilitent l'obtention de produits fiables, simplifient les processus de maintenance et fournissent des stratégies de soutien logistique rentables. La sûreté de fonctionnement apporte à la QS une valeur ajoutée en termes de performance du réseau. Quelques exemples de la relation existant entre la QS et la sûreté de fonctionnement sont présentés ci-après.

– Le processus de mise en file d'attente est utilisé dans les applications relatives à la sûreté de fonctionnement pour l'analyse stochastique du flux du processus et les délais d'encombrement. La technique de la file d'attente est utilisée au niveau de la couche de transport du réseau afin de déterminer les types de services de réseau qui affectent la QS. Il est possible d'établir une relation entre QS et sûreté de fonctionnement pour déterminer l'architecture optimale d'acheminement et les mécanismes de restauration à utiliser dans les applications de technologies de réseau.
– La stratégie réseau en matière de fourniture de services utilise divers schémas pour garantir la QS. La stratégie du soutien logistique intégré est un processus de sûreté de fonctionnement utilisé pour optimiser la disponibilité et améliorer le soutien à la maintenance qui affecte la fourniture des fonctions de services de réseau. Il est possible de relier la QS à la sûreté de fonctionnement en améliorant la disponibilité grâce à la fourniture de services de réseau rentables.
– La robustesse de la performance du réseau nécessite un accès sûr (*accessibilité*) et une *continuité* des connexions de réseau. Les techniques de sûreté de fonctionnement utilisant une conception redondante peuvent améliorer la performance du réseau qui affecte directement la QS.
– Les mécanismes d'ingénierie de la sûreté de fonctionnement peut être perçue comme un mécanisme de validation qui permet d'améliorer la performance du réseau et fournit des fonctions de services de réseau efficaces, ce qui affecte également la QS. La sûreté de fonctionnement influence la QS fournie.

La mise en correspondance de la QS, de la sûreté de fonctionnement et de la performance du réseau, avec identification des principaux facteurs d'influence de la sûreté de fonctionnement, est illustrée en Figure A.4.

La mesure de la QS est décrite à l'Article 7.

6 Évaluation et mesure de la sûreté de fonctionnement d'un réseau

6.1 Analyse de la sûreté de fonctionnement d'un réseau

6.1.1 Objectif de l'analyse de la sûreté de fonctionnement d'un réseau

L'analyse de la sûreté de fonctionnement d'un réseau a pour but d'améliorer la conception du réseau et le flux opérationnel. L'analyse permet d'identifier diverses alternatives de mise en réseau pour sélectionner la gamme optimale la mieux adaptée à la détermination des exigences de sûreté de fonctionnement du réseau ainsi que pour la planification et l'affectation des ressources.

6.1.2 Processus d'analyse de la sûreté de fonctionnement d'un réseau

6.1.2.1 Méthode générale d'analyse de la sûreté de fonctionnement d'un réseau

Il convient que l'analyse de la sûreté de fonctionnement d'un réseau identifie et détermine les caractéristiques de toutes les fonctions associées à l'obtention de la performance du réseau. Pour chacune des fonctions identifiées, il est recommandé que l'analyse tienne compte des pannes au niveau de divers nœuds du réseau et des liaisons physiques pouvant affecter les différents services de réseau. Ils englobent les fonctions de service de réseau affectées par l'environnement d'exploitation, le matériel et le logiciel, le soutien à la maintenance, les erreurs humaines et la conception du réseau. Il convient que l'évaluation valide la faisabilité de la technologie utilisée dans le réseau pour améliorer la sûreté de fonctionnement.

Il convient que l'analyse de la sûreté de fonctionnement d'un réseau inclue les éléments suivants:

a) il est recommandé que l'analyse tienne compte de l'environnement d'application ou d'utilisation et évalue les risques induits par des facteurs naturels et humains;

b) il convient d'identifier les frontières du réseau afin de déterminer tous les nœuds et toutes les liaisons du réseau;

c) il convient d'établir un classement des défaillances du réseau (voir 5.1.3.2) pour faciliter l'identification des éventuels états de panne par les fournisseurs de services de réseau, les opérateurs de réseau et les utilisateurs. Il convient que le type de défaillance ainsi classé soit mesurable dans des conditions établies. Les niveaux de performance du réseau peuvent être définis en termes de probabilités d'exécution des fonctions du réseau. Les niveaux de performance peuvent être mesurés et déterminés pour évaluation sur une durée donnée.

6.1.2.2 Autres méthodes envisageables

a) Méthode d'analyse qualitative

- Elle tient compte des services de réseau et de l'architecture de conception du réseau; elle détermine les modes, les mécanismes, les causes et les effets de la défaillance du réseau et définit les degrés de gravité des pannes. En se fondant sur les fonctions des services de réseau, les gravités des pannes sont classées par niveaux, en termes de portée, de durée et de degré de l'impact des pannes sur les services ainsi qu'en termes de satisfaction des utilisateurs du service;
- Elle analyse le temps nécessaire à la détection et à la réparation de la panne identifiée ainsi que les méthodes d'isolement et de réparation qui pouvant être utilisées;
- Elle détermine la possibilité d'éviter les pannes ainsi que la stratégie et les techniques de sûreté de fonctionnement utilisables pour réduire la probabilité ou l'impact des défaillances.

b) Méthode d'analyse quantitative

- Elle élabore des modèles de réseaux à l'aide d'une simulation de la sûreté de fonctionnement du réseau;

– Elle recueille des données pertinentes pour le modèle réseau;

– Elle analyse et évalue la sûreté de fonctionnement du réseau en utilisant les méthodes pertinentes d'analyse de la sûreté de fonctionnement du réseau.

c) Utilisation de méthodes classiques d'analyse de la fiabilité

Les méthodes classiques d'analyse de la fiabilité [3] sont souvent utilisées pour l'analyse de la sûreté de fonctionnement des réseaux. Certaines de ces méthodes sont normalisées: analyse des modes de défaillance et de leurs effets (AMDE) [7], analyse par arbre de panne (AAP) [8], bloc-diagramme de fiabilité (BDF) [9] et techniques de Markov [10].

6.2 Vérification de la sûreté de fonctionnement d'un réseau par insertion de défauts

6.2.1 Objectifs de l'insertion de défauts

L'insertion de défauts est utilisée pour vérifier la performance du réseau dans le but de:

– s'assurer que la sûreté de fonctionnement du réseau est conforme aux exigences du fournisseur de services de réseau et déterminer que l'objectif de conception du réseau est atteint en simulant le scénario de fonctionnement réel du réseau;

– détecter les faiblesses et problèmes éventuels de conception de la sûreté de fonctionnement du réseau, et ainsi pouvoir réviser et optimiser en temps opportun la conception du réseau avant qu'il ne soit officiellement mis en service;

– obtenir des données pertinentes de sûreté de fonctionnement et les évaluer.

Il convient que la vérification de la sûreté de fonctionnement du réseau par l'insertion de défauts soit globale mais demeure réalisable dans la pratique. Il convient de tenir compte des pannes résultant de défaillances des équipements, des effets de l'environnement et des accidents provoqués par l'homme dans des conditions normales de fonctionnement du réseau. Il est recommandé d'utiliser des retours d'information pertinents pour concevoir les essais élémentaires, de manière à refléter les causes des pannes. Les défauts sont injectés au réseau soumis à l'essai à des fins de simulation. Ceci est obtenu en accélérant l'apparition des pannes afin de déterminer les solutions permettant de les atténuer ou d'y remédier.

6.2.2 Processus de vérification par insertion de défauts

La vérification par insertion de défauts sur le réseau nécessite une planification précise. Il convient que le processus d'essai:

a) analyse des couches, de la topologie, les services fournis, la répartition du trafic prévue et les cheminements de services du réseau soumis à l'essai conformément aux exigences de conception de la sûreté de fonctionnement du réseau. Il convient d'élaborer une stratégie d'essai et que les essais élémentaires soient déduits des données d'expériences obtenues sur le terrain;

b) planifier les diverses ressources, y compris les ressources humaines, mettre en place l'environnement d'essai et le programme d'exécution. L'environnement d'essai doit être construit en fonction du scénario de service prévu. L'outil de simulation du trafic et l'outil d'insertion des défauts doivent être soumis aux essais et configurés conformément aux exigences; un plan d'essai doit être élaboré. Il est important de se familiariser avec l'environnement d'essai et avec l'utilisation des divers instruments et outils nécessaires à l'essai;

c) exécuter les tests unitaires et enregistrer les résultats. Observer tous les éléments de réseau et cheminements de service concernés pendant l'essai. Déterminer la portée et l'étendue de l'impact du défaut sur les fonctions de service du réseau, le délai de restauration des services et l'aptitude de tolérance aux pannes du réseau;

d) conserver les enregistrements détaillés des défaillances et anomalies détectées au cours de l'essai. Evaluer la situation quant à la manière dont les dysfonctionnements ont lieu, quant à leurs conséquences, quant aux équipements résidents et quant au classement des défaillances ainsi que par rapport à leur gravité et aux dates des actions de correction prévues;

e) rassembler les enregistrements d'essais et analyser les résultats de manière à valider la conformité de la sûreté de fonctionnement. Finaliser le rapport d'essai et recommander le cas échéant des améliorations en les justifiant.

6.3 Mesure des attributs de sûreté de fonctionnement d'un réseau

6.3.1 Objectifs de la mesure des attributs de sûreté de fonctionnement d'un réseau

Les mesures d'attributs de sûreté de fonctionnement d'un réseau fournissent des informations importantes sur l'aptitude de sûreté de fonctionnement du réseau. Elles sont utilisées pour évaluer la fréquence d'indisponibilité et les temps d'arrêt constatés par les utilisateurs pendant le fonctionnement du réseau. L'objectif est de réduire à la fois la fréquence et la durée des indisponibilités ainsi que les coûts et impacts associés qui génèrent un mécontentement des utilisateurs.

6.3.2 Processus de mesure des attributs de sûreté de fonctionnement d'un réseau

La mesure des attributs de sûreté de fonctionnement du réseau comprend la fréquence d'indisponibilité et le temps d'arrêt. Ces mesures fournissent des données statistiques provenant des fournisseurs d'équipements et de services reflétant leurs expériences respectives. Il convient de définir et de documenter les critères de comptes-rendus d'incidents, un classement des pannes ainsi que les paramètres de mesure et les procédures d'enregistrement, avant d'entamer le processus de mesure.

Les mesures-types d'attributs de sûreté de fonctionnement du réseau nécessaires à l'élaboration des comptes-rendus sont présentées ci-après:

– la fréquence d'interruption du réseau;
– la durée d'interruption du réseau;
– l'impact des services du réseau par rapport au nombre d'abonnés affecté lors de chaque interruption;
– le temps nécessaire à la récupération ou à la restauration des services du réseau;
– la classification des défaillances du réseau (voir 5.1.3.2) provenant d'une catégorie de défaillances spécifique.

Il est possible de déterminer à partir de ces ensembles de mesures, des attributs spécifiques de sûreté de fonctionnement d'un réseau.

– La *disponibilité* peut être déterminée à partir de données pertinentes de performance du réseau recueillies au cours de périodes de disponibilité et d'indisponibilité. La disponibilité du réseau en régime établi peut être exprimée comme étant le rapport du temps moyen de disponibilité sur la somme de temps moyen de disponibilité et du temps moyen d'indisponibilité.
– La *fiabilité* d'une liaison ou d'un nœud réseau peut être déterminée en mesurant ou en estimant la probabilité ou le taux de survenue d'une défaillance au niveau de la liaison ou du nœud du réseau.
– La *maintenabilité* désigne le temps nécessaire à la maintenance, ce qui peut inclure les délais techniques et logistiques. Les actions de maintenance peuvent être préventives ou correctives. La maintenabilité peut être exprimée comme étant la probabilité qu'une action de maintenance donnée, réalisée dans des conditions établies et utilisant des modes opératoires et des ressources définis, puisse être réalisée dans un intervalle de temps déclaré.
– L'*aptitude de soutien logistique à la maintenance* peut être déterminée à partir d'informations concernant la fourniture et la gestion des ressources nécessaires à la réalisation des tâches de maintenance. Elle est également définie comme l'aptitude d'une organisation donnée à réaliser une action de maintenance sur demande et dans des conditions données.

– La *capacité de restauration* d'un réseau peut être déterminée en mesurant la durée nécessaire pour obtenir le rétablissement du réseau. Cette durée est comptée depuis le moment où une panne du réseau est détectée jusqu'au moment où le fonctionnement normal du réseau est rétabli. Elle s'exprime généralement en temps de panne ou de durée nécessaire au rétablissement. La capacité de restauration s'applique à la restauration à partir d'une défaillance totale ou partielle d'un réseau ou à partir d'un état de fonctionnement dégradé d'un réseau.

6.4 Méthodes d'évaluation de la sûreté de fonctionnement d'un réseau

6.4.1 Evaluation de la sûreté de fonctionnement E2E d'un réseau

a) Objectifs de l'évaluation de la sûreté de fonctionnement E2E d'un réseau

L'évaluation de la sûreté de fonctionnement E2E d'un réseau définit le processus d'évaluation des caractéristiques de sûreté de fonctionnement du réseau pour des services de bout en bout, du point de vue des utilisateurs du réseau. Les caractéristiques de sûreté de fonctionnement incluent la disponibilité et les facteurs d'influence qui affectent la performance du réseau. Il convient d'analyser les scénarios de services types en fonction de la topologie du réseau ainsi que des cheminements de service pour évaluer la sûreté de fonctionnement E2E d'un réseau. L'évaluation de la sûreté de fonctionnement E2E comporte divers scénarios. Leur mise en œuvre peut faciliter la détermination des domaines d'amélioration.

b) Processus-type d'évaluation de la sûreté de fonctionnement E2E d'un réseau

– Identifier pour analyse les scénarios-types de services. Par exemple, un scénario-type peut être un utilisateur mettant sous tension un téléphone cellulaire pour s'inscrire dans un réseau.

– Etablir pour analyse la structure fonctionnelle de la configuration topologique du réseau E2E correspondant à un scénario spécifique. Déterminer le cheminement des données de service dans l'application. La création et la maintenance d'un service E2E sont liées à la fois aux équipements impliqués dans le cheminement de données de service et aux équipements de contrôle. Outre le cheminement des données de service des supports, il convient de tenir compte du cheminement de la signalisation de contrôle.

– Répertorier les modes de défaillance et effectuer une analyse des modes de défaillance et de leurs effets sur la base du cheminement de service E2E. Le résultat peut être utilisé pour optimiser le réseau.

– Elaborer des modèles de défaillance pour prédire la disponibilité du réseau, afin de conforter les choix de conception. Des techniques telles que le bloc-diagramme de fiabilité BDF ou la technique de Markov peuvent être utilisées.

– Le BDF doit être construit pour l'ensemble du réseau E2E, du haut vers le bas, de manière à représenter la structure du réseau couche par couche, pour les sous-réseaux et le cas échéant les modules inférieurs.

– Certains sous-réseaux, comme par exemple les réseaux centraux, sont souvent conçus avec une structure redondante à double plan de contrôle fournissant une configuration de haute fiabilité. Il convient que l'élaboration du bloc-diagramme BDF reflète cette redondance.

– Il existe sur l'ensemble du cheminement E2E des équipements appartenant aux couches de service, aux couches de contrôle et aux couches support, ainsi que des liaisons. Une analyse du haut vers le bas (dite descendante) est communément utilisée pour calculer la disponibilité d'un réseau.

– Il convient de documenter les facteurs d'influence inhérents et externes au réseau E2E concerné. Il est recommandé de noter les contraintes et limites qui affectent la configuration fonctionnelle en termes de performance du réseau E2E. Il convient d'étudier d'éventuels compromis de conception et solutions alternatives.

– Il convient de documenter l'ensemble des résultats de l'évaluation de la sûreté de fonctionnement E2E d'un réseau, y compris les décompositions en sous-réseaux et les modules de niveau inférieur de la totalité de la configuration E2E du réseau, pour chaque scénario de service.

6.4.2 Evaluation de la sûreté de fonctionnement d'un réseau et de l'ensemble de ses terminaisons

a) Objectifs de l'évaluation de la sûreté de fonctionnement de l'ensemble des terminaisons d'un réseau

L'évaluation de la sûreté de fonctionnement de l'ensemble des terminaisons du réseau désigne le processus qui permet d'évaluer les caractéristiques de sûreté de fonctionnement de l'ensemble du réseau, du point de vue des opérateurs de réseau ou des fournisseurs de services de réseau. Contrairement à l'évaluation de la sûreté de fonctionnement E2E, celle-ci ne s'intéresse pas au cheminement de service E2E dans des scénarios spécifiques, mais à l'état global de fonctionnement du réseau. La conception de la sûreté de fonctionnement de l'ensemble des terminaisons d'un réseau tient compte de tous les équipements et liaisons du réseau complet, y compris le mécanisme de protection du réseau. Ceci permet d'améliorer la conception du réseau et d'obtenir un meilleur rapport coût-efficacité.

b) Processus-type d'évaluation de la sûreté de fonctionnement E2E de l'ensemble des terminaisons d'un réseau

- Analyse des fonctions de service types. Par exemple, une fonction de services-types peut être la fonction d'établissement d'un appel en vidéoconférence ou l'émission d'une voix via Internet.
- Réalisation d'une analyse des modes de défaillance et de leurs effets et évaluation des effets des impacts des modes de défaillance sur le pourcentage d'utilisateurs dans la zone de service, la fréquence et la durée ainsi que les mesures de réparation. Le résultat peut être utilisé pour optimiser le réseau.
- Elaboration de modèles de défaillance pour prédire la disponibilité du réseau et de toutes ses terminaisons, au moyen de la méthode BDF ou autre méthode similaire pour identifier les fonctions réseau sur la base d'une approche descendante et par couches. Le cas échéant, il convient d'utiliser les données relatives aux précédentes défaillances du réseau.
- Il est possible d'établir les relations existantes entre les différentes fonctions réseau dans le diagramme BDF représentant les éléments du réseau tels que les sous-réseaux, les modules et les unités en fonction de la configuration du réseau et du mécanisme de commutation de protection.
- Une méthode de pondération est utilisée pour évaluer la contribution de chaque défaillance d'un nœud de réseau ou d'une liaison à l'ensemble des défaillances du réseau. Le rapport pondéré qui reflète la contribution de la défaillance du nœud ou de la liaison à l'ensemble des défaillances du réseau peut alors être déterminé. Par exemple, l'impact de la capacité d'écoulement du trafic d'un utilisateur du réseau sur la défaillance d'un nœud ou d'une liaison individuel contribue à l'ensemble des défaillances du réseau car la capacité d'écoulement du trafic affecte tous les utilisateurs.
- Le temps d'arrêt du réseau et de l'ensemble de ses terminaisons peut être déterminé en additionnant les contributions des défaillances pondérées. Il est commun dans ce domaine d'interpréter le temps d'arrêt du réseau sur une base annuelle, de manière à refléter l'aptitude globale de sûreté de fonctionnement d'un réseau.
- Il convient d'enregistrer les résultats de l'évaluation de la sûreté de fonctionnement du réseau dans son ensemble, y compris la fréquence des temps d'arrêt et les facteurs d'influence inhérents et extérieurs.

7 Mesures de la qualité de service

7.1 Aperçu des mesures de la qualité de service

La QS est utilisée pour déterminer le degré de satisfaction relatif à la performance du service du réseau. La QS peut être perçue de quatre points de vue différents.

– *Exigences QS de l'utilisateur* – Il s'agit d'une déclaration du niveau de qualité d'un service particulier requis ou souhaité par l'utilisateur. Le niveau de qualité peut être exprimé par l'utilisateur en termes techniques ou non techniques.

– *Offre de QS par le fournisseur de services* – Il s'agit d'une déclaration du niveau de qualité que le fournisseur de services souhaite offrir à l'utilisateur. Le niveau de qualité est exprimé par des valeurs attribuées à des paramètres QS conformément au SLA.

– *QS réalisée ou fournie* – Il s'agit d'une déclaration du niveau de qualité réalisé ou fourni par le fournisseur de service. Le niveau de qualité est exprimé par des valeurs attribuées aux paramètres conformément au SLA.

– *Notation de la QS sur la base d'enquêtes utilisateurs* – Il s'agit d'une déclaration exprimant le niveau de qualité constaté ou perçu par les utilisateurs dans leur ensemble à partir des résultats d'une enquête de satisfaction des clients. Le niveau de qualité représente le degré de satisfaction de l'utilisateur.

Les mesures de la QS utilisent un ensemble de critères de qualité de service permettant d'évaluer les fonctions de services de réseau. Les mesures de la QS donnent une appréciation subjective ainsi que des valeurs quantitatives de performance.

Les fonctions de service du réseau incluent des questions-clés de performance ou des paramètres d'intérêt pour les utilisateurs et les fournisseurs de services de réseau. Les fonctions de service de réseau peuvent être corrélées:

– *à la gestion de service* (par exemple la gestion des contrats de vente, la gestion de la logistique de soutien des services, les activités de maintenance et la fourniture des services) pour une appréciation qualitative ou subjective;

– *à la qualité de la connexion* (par exemple l'accès de la connexion au réseau, le transfert d'informations et la déconnexion ou la libération du réseau) pour une évaluation quantitative;

– *à la facturation* pour déterminer le coût de la transaction dans l'activité commerciale;

– *à la gestion du service du réseau par le client* (par exemple la configuration des dispositifs du réseau, la fourniture des services, ainsi que la gestion des pannes associées aux applications client/utilisateur).

Les critères de qualité de service comprennent:

– *la vitesse* (par exemple la vitesse à laquelle une fonction de service ou la fourniture du service est réalisée);

– *l'exactitude* (c'est-à-dire le caractère correct et complet de la réalisation de la fonction de service par rapport à une référence ou à un niveau spécifié);

– *la disponibilité* (par exemple service à la demande pour accès et utilisation de la fonction de service);

– *la fiabilité* (par exemple la performance de la fonction de service sans dégradation ou défaillance pendant une période spécifiée);

– *la sécurité* (par exemple la confidentialité avec laquelle le fournisseur de services réalise la fonction de service pour l'utilisateur);

– *la simplicité* (c'est-à-dire la facilité d'utilisation de la fonction de service);

– *la souplesse* (c'est-à-dire par exemple les options disponibles dans la fourniture des fonctions de service pour prendre en charge des exigences particulières).

L'importance des critères de qualité de service varie selon la fourniture et la performance des fonctions de service de réseau, de manière à répondre aux besoins des divers utilisateurs. Il convient que la mesure de la QS reflète l'importance des fonctions de service du point de vue applicatif [14].

7.2 Paramètres et exigences générales de la QS orientée utilisateurs

Les paramètres de la QS peuvent être obtenus à partir de la liste des fonctions de service de réseau et de l'ensemble des critères de qualité des services que l'utilisateur considère importants [14]. Les exigences de l'utilisateur relatives à la QS peuvent être saisies sur un tableau matriciel représentant dans une colonne verticale les fonctions de service sélectionnées et dans une rangée horizontale les critères importants de qualité de service. Les cellules individuelles de ce tableau matriciel facilitent la saisie des exigences pertinentes relatives à la QS.

Le Tableau 1 donne un exemple de matrice de saisie des exigences relatives à la QS. Les fonctions de service sélectionnées incluent l'accès, le transfert des informations de l'utilisateur et la libération représentant la fonction de service identifiée comme étant la qualité de la connexion qui revêt un intérêt spécifique en matière d'ingénierie de la sûreté de fonctionnement. Les critères de qualité de service importants pour l'utilisateur sont la vitesse, l'exactitude et la disponibilité. Les données saisies dans la matrice fournissent des informations utiles sur les exigences QS de l'utilisateur qui revêtent un intérêt particulier pour la mise en œuvre de la conception de la sûreté de fonctionnement.

Les exigences relatives à la QS sont utilisées comme aide au dimensionnement des paramètres du réseau de l'opérateur de communication grâce à la relation:

> *Exigences relatives à la QS > Performance du réseau requise > Paramètres de réseau requis*

La sûreté de fonctionnement joue un rôle important en matière de garantie de performance du réseau et de fourniture de la QS requise aux utilisateurs ou aux clients.

Tableau 1 – Matrice de saisie des données QS des utilisateurs

Critère de qualité de service Fonction de service connexion	Vitesse	Exactitude	Disponibilité
Accès	• Délais d'accès	• Probabilité d'accès incorrect	• Probabilité de refus d'accès • Probabilité de défaillance de l'accès
Transfert des informations utilisateur	• Délais de transfert des informations utilisateur • Débit d'informations utilisateur • Variation temps/vitesse lors du transfert des informations utilisateur	• Probabilité d'erreurs des informations utilisateur • Probabilité de livraison d'informations utilisateur supplémentaires • Probabilité d'erreurs de livraison d'informations utilisateur	• Probabilité de perte des informations utilisateur • Probabilité de coupure de transfert des informations utilisateur • Probabilité d'interruption de transfert des informations utilisateur • Durée de l'interruption de transfert des informations utilisateur
Libération	• Délais de libération	• Probabilité de libération incorrecte	• Probabilité de refus de libération • Probabilité de défaillance de la libération