IEC 62673

Edition 1.0 2013-06

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Methodology for communication network dependability assessment and assurance

Méthodologie pour l'évaluation et l'assurance de la sûreté de fonctionnement d'un réseau de communication

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
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.

Useful links:

IEC publications search - www.iec.ch/searchpub

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It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

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

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 30 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary (IEV) on-line.

Customer Service Centre - webstore.iec.ch/csc

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: csc@iec.ch.

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.

Liens utiles:

Recherche de publications CEI - www.iec.ch/searchpub

La recherche avancée vous permet de trouver des publications CEI en utilisant différents critères (numéro de référence, texte, comité d'études,…).
Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

Just Published CEI - webstore.iec.ch/justpublished

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

Electropedia - www.electropedia.org

Le premier dictionnaire en ligne au monde de termes électroniques et électriques. Il contient plus de 30 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (VEI) en ligne.

Service Clients - webstore.iec.ch/csc

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: csc@iec.ch.

IEC 62673

Edition 1.0 2013-06

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Methodology for communication network dependability assessment and assurance

Méthodologie pour l'évaluation et l'assurance de la sûreté de fonctionnement d'un réseau de communication

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

PRICE CODE
CODE PRIX

W

ICS 03.120.01

ISBN 978-2-83220-871-7

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

METHODOLOGY FOR COMMUNICATION NETWORK DEPENDABILITY ASSESSMENT AND ASSURANCE

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 62673 has been prepared by IEC technical committee 56: Dependability.

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

FDIS	Report on voting
56/1507/FDIS	56/1514/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 stability 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.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

Communication network dependability is highly influenced by the design and implementation of the network service functions, which aim to achieve user satisfaction in service performance.

Network evolution, service growth and functional renewal in communications have long been challenges to the providers of network services, not just for the broad range of services now in existence, but also for those service-related activities experienced by the end-users.

To sustain viable business in network services, it is prudent for the communications industry to provide the

– needed network service functions,
– adequate network capacity and performance capability,
– security of service,
– quality of service, and
– dependability of service.

This International Standard addresses one of the most important issues concerning the assessment and delivery of dependability of service to ensure network service performance. It also addresses the network dependability assurance strategies and methodology applications for enhancing and sustaining network operation.

This International Standard describes a generic methodology for dependability assessment and assurance of communication networks. It also provides relevant assessment and assurance methods to support communication networks for dependability engineering application, such as those conforming to IEC 61907 and ITU-T [1] Recommendations concerning dependability.

It presents an approach for network dependability analysis and evaluation that ensures dependable network design for effective implementation.

The objective of this standard is to achieve a cost-effective solution for realizing the network dependability performance and to assure the benefits from the network dependability of service operation.

---

1 ITU-T: International Telecommunications Union – Telecommunications.

METHODOLOGY FOR COMMUNICATION NETWORK DEPENDABILITY ASSESSMENT AND ASSURANCE

1 Scope

This International Standard describes a generic methodology for dependability assessment and assurance of communication networks from a network life cycle perspective. It presents the network dependability assessment strategies and methodology for analysis of network topology, evaluation of dependability of service paths, and optimization of network configurations in order to achieve network dependability performance and dependability of service. It also addresses the network dependability assurance strategies and methodology for application of network health check, network outage control and test case management to enhance and sustain dependability performance in network service operation.

This standard is applicable to network service providers, network designers and developers, and network maintainers and operators for assurance of network dependability performance and assessment of dependability of service.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. 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 (IEV) – Chapter 191: Dependability and quality of service*

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

IEC 61907, *Communication network dependability engineering*

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 IEC 61907, as well as the following, apply.

3.1.1
communication network
system of communication nodes and links that provides transmission of analogue and digital signals

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

Note 1 to entry: 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 to entry: 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
dependability
network dependability
ability to perform as and when required to meet specified communication and operational requirements

3.1.3
availability
network availability
ability to be in a state to perform as required

Note 1 to entry: Availability depends upon the combined characteristics of the reliability, recoverability and maintainability of the network and on the maintenance support performance.

Note 2 to entry: Availability may be quantified using appropriate performance measures.

3.1.4
reliability
network reliability
ability to perform as required, without failure, for a given time interval, under given conditions

Note 1 to entry: The time interval duration may be expressed in units appropriate to the network concerned.

Note 2 to entry: Reliability of a network depends upon the combined characteristics of the reliability, recoverability, maintainability and maintenance support performance of the constituent network elements.

Note 3 to entry: Given conditions include aspects that affect reliability, such as: mode of operation, stress levels, environmental conditions, and maintenance.

Note 4 to entry: Reliability may be quantified using appropriate performance measures.

3.1.5
maintainability
network maintainability
ability to be retained in, or restored to a state to perform as required under given conditions of use and maintenance

Note 1 to entry: Given conditions include aspects that affect maintainability, such as: location for maintenance, accessibility, maintenance procedures and maintenance resources.

Note 2 to entry: Maintainability may be quantified using appropriate performance measures.

3.1.6
maintenance support
network maintenance support
provision of resources to maintain a network

Note 1 to entry: Resources include human resources, support equipment, materials and spare parts, maintenance facilities, documentation, information and maintenance information systems.

3.1.7
maintenance support performance
network maintenance support performance
effectiveness of an organization in respect of maintenance support for the network

Note 1 to entry: Maintenance support performance may be quantified using appropriate measures.

3.1.8
recoverability
network recoverability
ability to recover from a failure, without corrective maintenance

Note 1 to entry: The ability to recover may or may not require external actions.

Note 2 to entry: Recoverability may be quantified using such measures as the probability of recovery within a specified time interval.

3.1.9
element
network element
subsystem or component of a communication network

EXAMPLES Terminals, nodes and switches.

Note 1 to entry: A network element may involve human input to perform its service function.

Note 2 to entry: Network elements are connected by network links.

3.1.10
link
network link
electrical, wireless or optical connection between network nodes

3.1.11
performance
network performance
ability to provide the service functions related to communications between users

[SOURCE: ITU-T Recommendation I.350:1988][1][2]

3.1.12
management
network management
application of organized processes and resources to manage the performance, configuration, accounting, fault, and security activities

3.1.13
service function
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 1 to entry: 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 to entry: Communication services are the network services subscribed by the end-users.

Note 2 to entry: 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 ability of a network to perform as required

---

2 References in square brackets refer to the Bibliography.

Note 1 to entry: The network failure may be due to, for example, equipment failure, natural disasters or human-caused disturbance.

3.1.17
network fault
state of inability of a network to perform as required, for internal reason

Note 1 to entry: In the context of network operation, a fault may be natural due to an abnormal condition, or malfunction resulting from a network element failure, or induced by external means such as fault injection.

Note 2 to entry: 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 service providers, Internet service providers and cable television operators.

Note 1 to entry: A 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 to entry: A user may be a source or recipient of user information, or both.

Note 2 to entry: In some circumstances, a user of a communication service is also known as a subscriber.

3.1.20
integrity
network integrity
ability to ensure that the data contents are not contaminated, corrupted, lost or altered between transmission and reception

Note 1 to entry: Throughput is the rate of successful message delivery over a communication channel of a network service.

3.1.21
dependability performance
network dependability performance
ability to provide or demonstrate the performance characteristics of dependability in network operation to achieve network service objectives

Note 1 to entry: In the context of this standard, network dependability performance refers to the provision of full-end network services.

Note 2 to entry: A full-end network service is the provision of service connectivity established for all transmission and reception ends of a communication network.

3.1.22
dependability of service
network dependability of service
effect of providing the required dependability performance for user communications services

Note 1 to entry: In the context of this standard, network dependability of service refers to the provision of end-to-end (E2E) network services.

Note 2 to entry: An end-to-end network service is the provision of service connectivity established between the transmission and reception ends of a communication network.

3.1.23
security of service
network security of service
effect of providing the required security for user communications services

3.1.24
service path
network service path
connecting path by network links and nodes to establish user communications services

3.1.25
service flow
network service flow
flow of information and data through the service path

3.1.26
service scenario
operational situation in communication network for provision of network service functions and user service applications

3.1.27
network outage
state of the network being unable to perform its primary function

3.2 Abbreviations

E2E	End-to-End
FRACAS	Failure Reporting, Analysis, Corrective Action System
FRU	Field Return Unit
HAZOP	Hazard and operability studies
MTTR	Mean Time to Restoration of Node/link
ND	Network Dependability
NFIT	Network Fault Insertion Test
NFMECA	Network Failure Modes, Effects and Criticality Analysis
OAMP	Operations, Administration, Maintenance, and Provisioning
OSI	Open System Interconnection
QoS	Quality of Service
RBD	Reliability Block Diagram
SLB	Service Logic Block

4 Overview of network dependability methodology

4.1 Need for network dependability methods

A communication network is a system of systems that interacts with other networks to achieve multiple service performance objectives. A communication network is complex and its constituent systems are constantly changing and evolving. Appropriate methodology and technical approaches are needed for dependability assessment and assurance of the network.

From a network dependability assessment perspective, the classical dependability techniques for analysis and evaluation have a limited scope in network application. Existing dependability methods are often unsuitable for modelling complex network topology and difficult for analysis of multiple network configurations and network service paths to provide confidence in the evaluation results. Selective methods such as SLB, NFMECA, and network simulation suitable for network dependability analysis and evaluation can provide effective network solutions.

They have become the essential processes to ensure sustainable network services and dependability performance.

A common approach for assurance of network dependability performance and dependability of service is to construct reliable network structure, establish effective routing schemes, provide efficient fault management and network maintenance support, and gather performance data and user feedback for network service evaluation and improvement. The process involves analysis of network service functions for cost-effective implementation, and evaluates value-added network service features for dependability of service enhancement. This approach, though adequate for system life cycle assessment of hardware and software network elements to ascertain dependability performance, is inadequate to deal with routing connectivity of user services in network operation. The traditional assurance approach lacks the responsiveness to react to the market dynamics of adaptive network configurations. This affects the network service objectives to ensure network dependability performance and to guarantee dependability of service in a highly competitive global network business.

There are many dependability methods developed over the years but only a selective few provide efficient methodology appropriate for effective network dependability performance and dependability of service applications. This observation is noted due to the complex nature of network evolution; the innovative topology for development of advanced network service functions, and the unique techniques required for practical dependability methodology applications. Whereas there are many factors that could influence the dependability performance in the network life cycle, the most significant impact would be during the early stages in concept/definition, design/development, and realization/integration. New additions to the existing network would involve scenario analysis of the legacy system during the concept/definition stage prior to investments in subsequent design/development and realization/integration stages. The extent of operation/maintenance, enhancement/renewal and retirement needs should be included in the scenario analysis of the legacy system. Network dependability performance and dependability of service should be continuously monitored, analysed and evaluated for optimization of network operations and provision of revenue generating network services. The network dependability assurance strategies and methodology applications are key contributing factors to enhance and sustain continued provision of network services from a viable business perspective.

4.2 Network dependability objectives

The capability of a network to provide users' communication for continual and uninterrupted service operation is highly dependent on its dependability performance. Dependability implies that the provision of network service functions is trustworthy and capable of performing the desirable service upon demand. To achieve network performance and assure network dependability of service, it is essential to utilize relevant methods for assessment of network dependability. This standard supports the engineering requirements for network design and process implementation, and provides relevant dependability methodology for analysis and evaluation of communication networks. The technical framework of IEC 60300-3-15 on system aspects of dependability and the requirements of IEC 61907 on network dependability engineering apply to this standard. Terms related to communications quality of service are referenced in ITU-T Recommendation G.1000 [2].

In the development and implementation of communication networks, there are several important influencing factors that concern the network operators and service providers to sustain a viable business. They include:

- network service functions to satisfy user needs;
- network performance capability to meet service demands;
- security of service;
- quality of service (QoS) [3];
- dependability of service.

In the assessment and assurance of network dependability, it should be noted that

a) the network functional parameters such as transmission capacity and performance connectivity will degrade with time due to failures and this will affect network dependability;

b) the robustness of the network to resist service performance violation due to external intrusion and outage interruption will affect critical network infrastructure protection.

4.3 Network service scenarios

There are two network service scenarios of interest to network dependability.

a) Dependability of service of the end-users' connections for end-to-end (E2E) network services (see Clause A.2) – the objective is to determine the network dependability performance characteristics on E2E network services from the perspective of network end-users. The E2E network service is an essential service to meet end-user needs based on the performance capability of a full-end network in service operation. In the E2E network service scenario, the dependability of service is reliant on the routing schemes and the capability of the network performance associated with the specific service paths selected for the E2E connections. Dependability of service is experienced by the end-users and reflects customer demands and user satisfaction.

b) Dependability performance of the entire network for full-end network services (see Clause B.2) – the objective is to determine the network dependability performance characteristics of the entire network from the network operator or the network service provider perspective. A full-end network can operate in a service scenario where the service provider has full control of a private network and has the responsibility to provide network dependability performance adequate for the network services. The full-end network can also operate in a service scenario with multiple service providers each controlling a designated segment of the entire network as in a public switching network. The network operator is responsible for the overall network service performance. Individual service providers are responsible for their contributions of network service performance under the network service level agreements with the network operator in provision of QoS.

The two network service scenarios associated with E2E and full-end network service operations are interdependent and complementary. It should be noted that without dependability performance capability, adequate user services could not be achieved or guaranteed; and without user satisfaction of dependability of service, the service provider would experience difficulty in sustaining user service demands and could lose subscriptions; hence affecting network service revenue generation. Relevant network user feedback information gathered and network performance data analysed from these two network service scenarios would facilitate resource planning and control of QoS provision to subscribers or users and maintain dependability of overall network services.

Network dependability performance and dependability of service reflect the network service scenarios and operation environments in doing business. This is achieved by means of dependability assessment to ensure dependability performance during network development and dependability assurance to sustain dependability of service during network operation.

The strategies for network dependability assessment and dependability assurance are outlined in 4.4 and 4.5. The dependability methodology and methods for network applications are provided in Clause 5.

4.4 Network dependability assessment strategies

Dependability assessment is an appraisal process to determine the status of network performance for delivery of dependability of service. The following describes the network dependability assessment strategies relevant to the network service scenarios.

a) E2E network dependability assessment strategy

The E2E network dependability is influenced by the network topology, the routing schemes and the selection of service paths to achieve user service connections. To assess E2E network dependability, the routing service paths associated with the service scenarios should be analysed. All the equipment and links of each service path should be evaluated

for achievement and delivery of dependability of service. The E2E network dependability assessment covers various network service scenarios in public and private networks.

The assessment strategy for E2E network should consider a technical approach for evaluation of dependability of service. This is due to the multiple service paths that need to be analysed for optimization of dependability of service. The complex nature of the network configuration demands a unique modelling technique and methodology consisting of Service Logic Block (SLB) diagrams (see Clause A.3) to facilitate E2E network dependability of service evaluation.

b) Full-end network dependability assessment strategy

A full-end network operating in a service scenario consists of numerous interacting networks offering various service functions by multiple service providers. Provision of network dependability performance is the collaborative efforts of these service providers under service level agreements for delivery of QoS. The service function reliability of the full-end network can be modelled by the RBD [4] or similar methods. Full-end network dependability assessment can only be practically ascertained after network service implementation by means of field performance survey and customer satisfaction feedback to obtain relevant network performance data. This is due to the complex nature of network evolution where new service functions are continuously being added for performance enhancement and termination of obsolete or unprofitable network services. The public switching network is an example where network dependability performance can be assessed by analysis and evaluation of the reported frequency of user service outages and the outage duration and customer complaints on service impact. The assessment outputs include the categorization of network outages associated with the identified failure causes and their resulting service impact to the network subscribers or users.

A full-end network can be a private network and owned by a single network operator who has full control for provision of the network services. A secured data network consisting of automated teller machines to provide distributed banking services is an example of a private network. To assess the dependability performance of the full-end private network, all the network elements and their relationships should be determined and all relevant dependability performance characteristics evaluated for conformance to established network service performance criteria. The technical processes for network dependability assessment are analysed and evaluated as a system with boundary conditions. For new network development, the network life cycle process should be followed and the dependability engineering activities conducted according to the recommended guidelines from IEC 61907. For network enhancement and renewal projects, it is essential to take into consideration the legacy issues of existing network configurations to optimize renewed network performance. Network performance statistics from field operation should be collected and analysed to validate performance adequacy in meeting network service objectives.

4.5 Network dependability assurance strategies

The network dependability assurance strategies are planned activities engaging systematic processes to ensure achievement of network dependability in performance and delivery of customer focused dependability of service. The network dependability assurance strategies reflect the relevant technical domains in network specific applications. They collaborate with network performance management and the routine network maintenance and support activities by providing specific dependability engineering effort. The network specific dependability assurance strategies are summarized from a network operation viewpoint.

a) Delivery of dependability of service to end-users

There are two separate strategic issues concerning the delivery of dependability of service: one is concerning the service contributions from the delivery mechanism of network equipment functions and interoperability in service operation; the other relates to the service delivery of data information as throughput by utilizing the delivery mechanism of the network configuration. The application specific strategies focus on the delivery mechanism and the data integrity.

b) Ensuring data integrity

The data integrity is the foundation for credible information generation and data transmission through the network service paths that represent the delivery mechanism of the network configuration. The data specific strategy is focused on the network dependability performance and the ability to prevent data loss, corruption or security exposure.

c) Enhancement of network performance functions and support processes

The network performance functions and support processes would tend to degrade if not adequately maintained and regularly updated. This would result in gradual degradation in network performance leading to frequent network outages and increased service downtime durations; hence affecting network operation and QoS. The network maintenance support strategy for dependability assurance is to promote continuous improvement to optimize network functions and simplify procedures for network support processes. The technical focus is to enhance critical network performance related dependability characteristics such as recoverability, availability, reliability, maintainability, and maintenance support. Continuous network improvement is essential to sustain viable network service operations and to ensure the satisfaction of end users. The assurance strategy provides corrective and preventive measures to avoid recurrence of network operation problems.

5 Network dependability methodology applications

5.1 Network life cycle process

5.1.1 Life cycle process applications

The applications of network life cycle process involve a series of dependability activities to achieve its performance objectives. The network life cycle stages include concept/definition, design/development, realization/integration, operation/maintenance, enhancement/renewal, and retirement. The relevant application methods for network dependability analysis and evaluation are identified. The objective is to ensure that network dependability requirements are met through judicious applications of relevant methods for assurance of network dependability performance to achieve the required dependability of service.

Individual networks differ from one another due to boundary and service conditions. The network operational scenario relevant to the provision of essential network services should be established. Relevant analysis and evaluation methods should be identified in early network concept design to maximize dependability performance benefits. This process helps assure dependability of service achievement from the network services and the user satisfaction perspectives. The technical approach and process flows are described herein to facilitate methodology applications. Relevant input and output requirements should be identified for network service analysis. Timely response to data collection, analysis and interpretation of evaluation results, and risk assessment as part of the dependability assurance process should form the basis for recommending network dependability improvement.

5.1.2 Risk assessment process applications

Risk assessment [5, 6] is the overall process of risk identification, risk analysis, and risk evaluation. A risk assessment provides an understanding of the risk involvement, risk causes and consequences, which are useful inputs to decision making during the life cycle stages of a network project. The information derived from a risk assessment process can provide significant contributions to important business and project decisions, including where major resource commitments are made. The information is used to support analysis of business impact associated with risks and benefits. Business impact analysis should be performed in conjunction with the service scenario analysis to address investment risks and recovery plans to avert potential loss or damage of critical network functions.

Project specific dependability engineering activities often involve the application of probability distributions and statistical analysis techniques. The risks associated with such project activities require appropriate use of risk assessment techniques to address the potential benefits or probable negative consequences arising from project applications, business influences and technical issues in dealing with uncertainties. The risk assessment process

presents an evidence-based approach to determine the extent of risk exposures. The risk assessment should be based on relevant data and practical experience.

The risk assessment process involves

- recognising the potential positive and negative effects on the risk identified,
- understanding the sources of risk causes and consequences and the likelihood that the consequences will occur,
- deciding on the significance of the risk if within specified risk criteria.

Following the completion of risk assessment a decision may be made on how to treat risks. The risk treatment involves selecting and agreeing to one or more relevant options for changing the probability of occurrence, the effect of the risks, and implementing the options. Examples include avoiding a risk by not undertaking the activity, accepting a risk with no action, or changing the level of a risk. Decisions may also be made about whether to retain risk or to share it with another party through contract or insurance.

The types of risk assessment techniques [6] applicable to dependability engineering activities are grouped as:

- scenario analysis – examples: root-cause analysis, fault tree analysis, event tree analysis, business impact analysis, cause and effect analysis, cause-consequence analysis;
- functional analysis – examples: FMECA [7], Reliability centred maintenance [8], HAZOP [9];
- statistical methods – examples: Monte-Carlo simulation [10], Markov analysis [11].

The above risk assessment techniques are established standard analysis methods recommended for dependability applications [10]. Detailed descriptions of these risk assessment techniques are included in [6] and [10]. They are not elaborated in this standard.

5.1.3 Dependability methodology applications

There are two main aspects of dependability methodology applications associated with the network life cycle.

a) Network dependability assessment

The network dependability assessment is the application of analysis, testing, verification and evaluation techniques for network development. The assessment techniques are used during the early stages of the network life cycle in concept/definition, design/development, and realization/integration. The assessment objectives are focused on achievement of network dependability performance requirements prior to deployment of the network for operation and service provision. Some of the assessment methods such as FRACAS and risk assessment are the essential analysis and evaluation processes established to facilitate network data information capture to project dependability performance trends in network operation/maintenance, and to support network enhancement/renewal decisions. The dependability assessment methodology applications are described in 5.3.

b) Network dependability assurance

The network dependability assurance is the approaches and processes conducted during the operation/maintenance and enhancement/renewal stages of the network life cycle. The assurance objectives are focused on specific dependability performance issues requiring resolutions during network operation. This is to enhance and sustain network performance and services. The assurance activities collaborate with network performance management, network fault management systems, and the routine network maintenance and support activities by providing specific dependability engineering effort contributions. The dependability assurance methodology applications and technical approaches are described in 5.4.

Table 1 presents the alignment of application methods to major dependability activities relevant to each network life cycle stage.

Table 1 – Summary of network dependability activities and application methods

Network life cycle stages	Network dependability (ND) activities	Typical application methods
Concept/definition	• ND requirements analysis	• Service scenario analysis • Business impact analysis
Design/development	• Network reliability allocation • ND prediction • ND design analysis and evaluation	• Network modelling (RBD, SLB and simulation) • NFMECA • FRACAS • Root-cause analysis • Cause and effect analysis
Realization/integration	• ND features testing • ND test case development • ND service conformance validation	• NFIT • FRACAS • Cause and effect analysis
Operation/maintenance	• ND performance assessment • ND fault management and incident reports • ND maintenance records	• FRACAS • Network health check • Network outage control • Test case management • Reliability centred maintenance • HAZOP
Enhancement/renewal	• Enhanced/renewed service requirements analysis • Enhanced/renewed service dependability assessment	• Service scenario analysis (including legacy service consideration) • Network health check • Network outage control • Test case management • Business impact analysis • Cause and consequences analysis
Retirement	• Network service termination notification to users • Obsolete equipment disposal	• Cause and consequences analysis • Business impact analysis

5.2 Network dependability performance characteristics

The application methods in Table 1 require the identification of relevant network performance characteristics for dependability assessment. These performance characteristics reflect the network performance capability in conformance with the service level agreements for QoS requirements for provision of network services. Analysis of dependability performance characteristics should consider establishing network failure criteria and determining the dependability performance parameters.

a) Establishing network failure criteria

Failure criteria for E2E and full-end network services should be established to provide the units of measurement for the dependability performance parameters. The criteria provide quantitative measures for assessing the performance parameters to determine the status of network service operation and failure conditions. The network failures are categorized to identify probable causes to facilitate root-cause analysis for network dependability improvement. The probability of network failure occurrences and the frequency of failure incidents reported should be taken into consideration.

The following are typical network failures for consideration.

1) Facility-related network failures consist of failures of individual network elements corresponding to the node and link failures of equipment or software causing network interruptions. FRU (field return unit) is a network element, such as a circuit pack or a repairable hardware assembly deployed in network service operation. The FRU is a unit returned from field operation due to failure or other reasons for replacement under network service agreements or network support requirements. The analysis of FRU return rate provides insights to critical field failure problems.
2) Traffic-related network failures consist of failures related to the operation scenarios of network service changes and traffic overload. These failures are caused by network facility and capacity limitations, malfunction of redundant service paths, inadequate backup of network nodes and links, and sudden surges in traffic patterns that create network overload situation.
3) Disaster-related network failures consist of man-made or natural disaster causing network failures. Man-made disasters are the consequence of technological or human hazards such as structural collapse, fire or power outage. Natural disasters are the results of natural hazards such as floods, earthquakes, or volcanic eruptions. All disasters affect human lives and properties causing economic loss and environmental damage.
4) Security-related network failures consist of failures caused by security violation due to insufficient security control to prevent unauthorized intrusions such as hacking, cyber attacks, or sabotage.
5) Scheduled-activity-related network failures consist of failures that have occurred during scheduled network maintenance activities caused by inadequate maintenance procedures or improper implementation of maintenance support process.
6) Human-factor-related network failures consist of failures due to unintentional human errors such as operator errors, misapplication of operating procedures, or intentional damage on deliberate destruction of property.

b) Determining network dependability performance parameters

Table 2 summarizes the important parameters for assessment of network dependability performance characteristics. The relevant dependability performance parameters are identified for full-end network services and E2E network services. These dependability parameters reflect the key dependability performance characteristics and requirements for provision of full-end and E2E network services.

Table 2 – Summary of network dependability parameters

Full-end network services: Dependability performance parameters (service providers' interest)	**E2E network services: Dependability performance parameters (end-users' experience)**
• Full-end network service availability (*% uptime*) • Number of subscribers or users affected due to network service outage • Network downtime (*minutes/year*) • Fault detection time (*minutes*) • Time to restoration (*minutes*) • FRU return rate (*numbers/month*)	• E2E network service availability (*% uptime*) • Service path downtime (*minutes/year*) • Failed service access (*frequency/year*) • Delayed service access (*frequency/year*) • Premature service disconnect (*frequency/year*) • Delay of service media (*minutes/year*)

5.3 Network dependability assessment methodology

5.3.1 Generic dependability analysis and evaluation techniques

Dependability assessment involves both analysis and evaluation and is often conducted on an iterative basis. The generic dependability analysis and evaluation techniques provide a broad range of methods for network dependability applications. Many of these classical reliability techniques are used during the network life cycle for dependability analysis of network elements and service performance operations. Examples such as failure modes, effects and

criticality analysis [7], reliability block diagram analysis [4], Markov analysis [11], and software reliability engineering methods [12], form the basis for network dependability assessment. However, it should be noted that classical reliability techniques have limited scope of applications. Specifically, the existing dependability methods available are often unsuitable for modelling complex network topology and difficult for analysis of multiple network configurations. New methods, more adaptive to the dynamic routing schemes of communication network services, are introduced for network dependability application.

The following application methods noted in Table 1 provide the recommended methodology and processes for network dependability performance assessment and dependability of service evaluation.

5.3.2 Service scenario analysis

a) Description and purpose

Service scenario analysis is an application method for identification of operational profile and analysis of service requirements. The purpose is to determine the network topology and service functions for dependability assessment relevant to provision of planned network services. The application method facilitates the translation of user service needs obtained from various marketing sources into technical requirements in the network dependability requirements analysis process. Business impact analysis is conducted in conjunction with the applicable scenario analysis to assess potential risk exposures and determine appropriate actions for need of recovery plan.

b) Selection criteria and when to use method

- New service requirements, unknown or existing requirements have changed.
- Need to improve existing operational profile to provide competitive service features.
- Need to establish resource requirements to sustain network operation and growth.
- Service scenario analysis is used to plan initial user service needs and determine subsequent service needs when the service requirements have changed or new ones are being identified.

c) Application procedure

- Identify the appropriate network topology to meet service needs. Networks come in different topological forms and describe the active path of service transporting on the network with backup paths and protection mechanisms to facilitate service access and transportation.
- Identify the service functions such as voice, data, and video for provision of network services.
- Determine usage of service functions and their performance requirements.
- Determine usage profile reflecting access frequency, time and duration of communication sessions.
- Determine business impact and the need for appropriate recovery plan.

d) Data requirements

Topology options, alternate service paths, location of protection mechanisms and access points.

e) Interpretation of results

Presentation of essential network service operational profile information, risks and benefits, and data input for network modelling and development of dependability requirements.

5.3.3 Network modelling

a) Description and purpose

Network modelling is an application method to create graphic symbol representations of network nodes and links and interconnections to establish a network configuration. The purpose is to determine suitable network service paths for user service connections. The

application procedure facilitates identification of the relevant network nodes and links and associated protection mechanisms involved in a specific service flow for E2E dependability of service assessment. Network modelling permits selection of alternate service paths for dependability analysis and evaluation to achieve optimum routing. The E2E service network is a communication network for service provision. Annex A describes the SLB method specifically developed for E2E dependability of service application.

For full-end network, the modelling application creates the entire network nodes and links to establish network configuration for dependability performance assessment. The purpose is to determine the overall network availability performance to reflect the network capability and capacity in delivering overall network performance to meet service level agreements in QoS provision. The generic modelling techniques include, but are not limited to RBD, Markov analysis, system simulation and complex network analysis. Full-end network is considered as an extension of the system concept where similar modelling process applies. Annex B shows an example of full-end network assessment.

b) Selection criteria and when to use method

- Need to establish a framework for network analysis and evaluation.
- Need to identify critical network elements for network configuration.
- Need to quantify network availability and establish outage limits.
- Network modelling is used when the network topology and routing schemes have to be established, changed or anticipated to change for service planning purposes.

c) Application procedure

- Create the network nodes and links and interconnections based on the network topology to establish the network configuration.
- Identify the service functions associated with the service paths.
- Select a suitable service path and identify the network nodes and links and associated protection mechanisms involved in the service flow.
- Analyse each service path to determine the E2E service reliability and availability performance for provision of service functions.
- Optimize the network service configuration in delivery of E2E dependability of service by determining the main service path and alternate service paths.
- For full-end network modelling, the assessment of relevant reliability, maintainability, maintenance support performance and recoverability characteristics of the network nodes and links should be identified, examined and evaluated. The availability of the entire network configuration should be analysed to determine total downtime per year for continuous network operation.

d) Data requirements

Dependability characteristics of each selected service path, reliability of nodes and links and associated protection mechanisms, availability of the selected service paths, and service path downtime.

e) Interpretation of results

The application of network modelling forms the basis for development of network dependability requirements. It permits network reliability allocation, network dependability prediction, design analysis and evaluation, and assessment of E2E service for dependability of service**.**

5.3.4 Network failure modes, effects and criticality analysis

a) Description and purpose

NFMECA is an application method adopted from the classical FMEA process for analysis and evaluation of network elements and service functions. The purpose is to identify critical failure modes in the network nodes and links to determine the failure effects on the next higher level service functions. The NFMECA evaluates the criticality of potential failures that might impact network dependability performance and affect user services. Other methods such as Fault Tree Analysis and Petri net should be considered to complement the NFMECA method for more complex network analysis.

b) Selection criteria and when to use method

- Network configuration is established and detailed information on network elements is available.
- Need quantitative and qualitative assessment of causal effects to determine criticality of service impact.
- Need to identify critical network elements for reliability improvement.
- Need to support decision for incorporation of redundancy or fault tolerance design.
- NFMECA is used when critical service impacts are discovered or anticipated.

c) Application procedure

- Use network topology information to identify the network nodes and links for the service paths at each network layer for failure mode analysis.
- Identify the respective failure modes associated with each node (e.g. overload) and link (e.g. interface interruption) from the experience database collected in a network data repository. The failure data reflect the end-users' service experience such as service accessibility, service continuity, and service disengagement.
- Determine the failure effects on the resultant service causing downtimes; such as service path downtime, network downtime, and transmission network downtime.
- Determine the resultant failure criticality and evaluate the impact on the E2E network service.

d) Data requirements

Experienced data captured and collected for network failure modes and effects in the network data repository.

e) Interpretation of results

NFMECA results can be used as inputs for updating network dependability assessment on downtime duration and maintenance effort. The NFMECA results are also used for development of test cases for NFIT where warranted.

5.3.5 Network fault insertion test

a) Description and purpose

NFIT is an application method to verify the effect of network failures by deliberate insertion of faults to test the consequences of the results. The purpose is to verify the effectiveness of redundancy designs, protection mechanisms, and the overall fault management capability of the network.

b) Selection criteria and when to use method

- Criticality of the fault is known and of concern.
- Probable fault location is identified.
- Need to determine the criticality of fault impact to network service operation.
- Need to verify the frequency of fault occurrence.
- NFIT is used when the critical service impacts have been discovered and need verification by means of test cases.

c) Application procedure

- Identify the NFIT object of the planned test case.
- Determine method of fault insertion at a target test layer. Different OSI layers [13] have different fault types (see Clause A.4).
- Execute the test case. Observe all related network elements and service paths during the test. Determine scope and extent of fault impact. Record the test results.

d) Data requirements

Test records and observation.

e) Interpretation of results

Evaluate impact of fault on the network service functions, service recovery time, and fault tolerance capability. Provide information on test case effectiveness, fault coverage, and network fault management efficiency.

5.3.6 Failure reporting, analysis and corrective action system

a) Description and purpose

FRACAS is an application method to capture relevant data on incident reporting and maintenance actions, diagnostic and analysis results for recommending corrective actions. The purpose is to formalize a repository database to capture and retain dependability performance history for network design and service improvement.

b) Selection criteria and when to use method

- Failure information database is established.
- Failure reporting procedure is established.
- Need to capture failure history to establish dependability performance trends.
- Need to support decision for network design and procedural improvement.
- FRACAS is used throughout the network service life to maintain a credible repository database for traceability of recorded network performance history.

c) Application procedure

- Identify the failure information and initiate the incident report for input to FRACAS.
- Categorize the incident reports for action based on established maintenance service criteria such as urgent, routine, or scheduled for implementation during next update.
- Analyse and evaluate criticality of the major failure problems affecting service operation and provide recommended solutions such as design change, parts replacement or configuration control management.
- Implement recommendation for problem resolution.
- Record and monitor FRACAS status for continuous improvement.

FRACAS is usually automated to facilitate data update, follow-up actions and process improvements.

d) Data requirements

Provide failure data classification and database maintenance.

e) Interpretation of results

Establish network dependability performance trends and history of improvement actions.

Annex C shows the evaluation of network dependability performance in field operation. It illustrates an example of typical network failure categories of a public switching network for dependability evaluation.

5.4 Network dependability assurance methodology

5.4.1 Scope of dependability assurance methodology applications

The scope of dependability assurance methodology applications covers the three strategic technical domains identified in 4.5. The application focus is specifically oriented for assurance activities in network operation from a dependability perspective. The network assurance process makes extensive use of the established network management processes to provide practical approaches to support network performance management, network fault management, and QoS. The objective is to enhance and sustain dependability performance in network operation.

The assurance methodologies are the recommended technical approaches based on industry practices to ensure sustainable dependability performance in network operation and timely provision of dependability support needs in network services. The overall network operation responsibility to achieve QoS and customer satisfaction rests with the network operators and

the service providers. Dependability assurance under normal and emergency conditions of network operation is focused primarily on delivery of dependability of service to the network end-users in QoS contribution. The security of service contributing to QoS complements the dependability assurance activities. The dependability performance achieved in network design and service implementation in provision of essential network services could influence the security of network operation.

The network dependability assurance methodologies are grouped in technical application domains to align with the dependability assurance strategies. The assurance methodologies presented herein are typical examples experienced in assurance of network services during network operation such as network health check and network outage control. Network fault management systems are used to support large networks for fault identification, data collection, and performance trend analysis. The following subclauses describe the technical approaches to address the dependability assurance issues.

5.4.2 Assurance of dependability of service

a) Objective

To ensure dependability of network service path for information transfer and delivery of data throughput.

b) Description of methodology applications

1) The network service path is a delivery mechanism for information transfer. The network nodes and links associated with the service path should be incorporated with appropriate protection devices to ensure successful information transfer and redirection to alternate service paths in the event of main service path malfunction. Priority of service path selection should be predetermined. There are several path selection schemes suitable for network designs that incorporate protection devices such as active or standby redundant paths, majority voting, and priority voting techniques. Reliability analysis of the protection device is essential to determine appropriate application. Risk evaluation of the protected network service path is required to assess impact of malfunction and the resulting effects and consequences.

2) The network serviceability reflects the delivery of dependability of service to the end-users. The contributing factors to serviceability include end-user accessibility of service, retainability of service, and disengagement of service relating to the establishment and completion or the start and finish of a communication session. Access delays relate to the inability to establish network connections due to various connectivity reasons. The stability of service retention is influenced by the network capacity and traffic flow conditions during communication. The unsuccessful disengagement of service would result in wastage of available network resources and errors in charging subscribers or users. The effectiveness of network serviceability relies on the dependability of network performance and the reliability, speed and accuracy of disengagement. Network planning should address the serviceability issues from a dependability performance perspective to maximize network resource usage.

5.4.3 Assurance of data integrity

a) Objective

To ensure integrity of data throughput and data security protection.

b) Description of methodology applications

1) Data integrity is dependent on 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. The integrity characteristic of dependability performance is the ability of the network to provide a secured passage for protection of the data contents. Integrity reflects the assurance process for the network service functions to ensure that the data contents are not contaminated, corrupted, or altered in transforming the inputs into outputs.

2) There are numerous methods used for management of secured information and preservation of data integrity. Their application is dependent on the specific

requirements with respect to the information management system, data integrity and the level of security needs, data retrieval capability and recovery speed, the effectiveness of the technology deployed, and the cost of implementation as part of the network assurance process. The data integrity and security protection approaches for implementation are identified in IEC 61907. Examples of data preservation include data backup and duplication, data storage in different locations, and data replication in different formats. Examples of data security protection include authentication, encoding and encryption of data and messages, virus detection and firewall protection to prevent network-based attacks.

5.4.4 Assurance of network performance functions and support process enhancement

a) Objective

To ensure network performance functions and support process enhancement.

b) Description of methodology applications

1) The applicable dependability assurance methodology utilizes the established processes in network management to achieve various dependability performance related tasks associated with network planning, measurements and performance optimization. The dependability activities are involved in identification and resolution of time dependent network performance issues such as latency and time delays for frame delivery and acknowledgement, packet loss, retransmission, and measurement of traffic throughput. The assurance objective is to ensure traffic performance achievement with respect to speed, reliability and capacity of the network design and configuration for maximum resource utilization and network congestion avoidance.

2) The applicable dependability assurance methodology utilizes the established processes in network fault management to detect, isolate, and correct malfunctions in network operation, compensate for environmental changes, and assist in maintenance and diagnostic activities. The assurance objective is to ensure proper diagnosis of network faults, database capture and maintenance of network performance records, and utilization of the fault data source for recommendation of network support service improvement.

3) The applicable dependability assurance methodology utilizes the established processes in network field tracking system, maintenance and logistic support, and relevant performance databases for analysis and evaluation of failure categories to determine network outage downtimes and frequency of network outages. The relevant data are used to establish outage contributions with respect to failure causes and their impact to end-users in network services. The assurance objective is to ensure proper assessment of network performance trends, customer satisfaction and QoS.

5.4.5 Network dependability assurance methods

a) Network health check

The network health check is a method for monitoring and control of the adequacy and efficiency of mitigating on-going field problems in network operation. This is to ensure delivery of dependability of service. Network health check is the primary method for assurance of network dependability performance. The health check process is based on field problems encountered in network operation monitored or checked on a regular basis (e.g. bi-weekly) by means of a series of network simulation studies over a time period. This is to establish a sequence of time lines for investigating problem occurrences in the respective network scenario and operational profile to verify the network performance status for assurance of the network health in operation.

The network scenario is continuously changing with time due to diverse traffic demands, service usage fluctuation, network topology and configuration adaptation, and protection mechanism activation to mitigate network performance malfunctions and rerouting of network paths constrained by capacity limits. The network health check method is used in conjunction with the network fault management system and the FRACAS database information for continuous network operation. The health check process involves the analysis of network scenario and operational profile in dealing with field problems encountered to sustain dependability performance in network operation.

The procedures for network health check are as follows:

1) identify the current network topology and configuration for each scenario analysis;
2) identify the field problem encountered and the time registration in the scenario being monitored;
3) analyse key network elements involved in mitigating the field problem encountered for solution to sustain network operation;
4) determine the network dependability in terms of availability and reliability performance and service support needs of the network operation scenario;
5) establish a network configuration file as input to network simulation, including all relevant time dependent scenario information needed for the simulation;
6) evaluate the simulation results to determine network dependability performance efficiency and adequacy of back-up redundancy and routing schemes for each scenario study;
7) document analysis and evaluation results for various scenario studies to establish a series of network health check profiles to guide network operation for continuous improvement.

It is prudent to verify and validate network performance efficiency and adequacy in delivering network services based on knowledge of operation scenarios and field problems.

b) Network outage control

Network outage control is a method to identify and categorize network field problems by means of incident reports from the network operators and service providers. This is to determine the status of continuous network performance and service impact to ensure customer satisfaction. The objective is to gather network outage statistics and equipment downtime data to verify dependability performance reference against industry performance benchmarks. The relevant information on network outage statistics would facilitate appropriate mitigation action and control of service impact in network operation.

The communications industry practices provide the standard requirements for field problems reporting. The criteria for network element (e.g. equipment) outage measurements are established by industry standards [14, 15]. The network equipment outage information is captured and reported for compliance to service level agreements in network service provision. Network dependability performance is influenced by the effect of equipment malfunction resulting in total or partial service outage. The equipment malfunction would likely cause network performance degradation. It could also compromise the integrity of data during network operation. For network outage control it is essential to record the outage information affecting network services. The outage information data collected through incidents reports is crucial to establish the causal relationships in determining the relevant failure sources causing network service downtimes. Outage downtime is expressed in terms of time duration of the outage occurrence. Additional information is also captured on the source of outage, the frequency of outage occurrence, and the impact to the numbers of subscribers or users being affected. The network outage information enables the network assurance process to justify and recommend corrective or preventive actions for sustained network performance and continuous service improvement.

The network outage control monitors the loss of equipment functionality in the network systems. The outage information presents the outage downtimes duration for service impact and network equipment impact measurements. The objective is to reduce outage downtimes and their associated cost and service impact to enhance revenue generation and customer satisfaction.

The network equipment is categorized to facilitate data collection and assignment of outage measurements. Network equipment categories include for example: switching, signalling, transmission, and common functions.

Network outage measurements consist of the following:

1) service impact measurements – network outage frequency and outage downtime duration affecting the number of subscriber lines in provision of network services due

to partial or total outage from all sources and expressed in minutes/ subscriber line/year;

2) network element (equipment) impact measurements – network outage frequency and outage downtime duration due to equipment malfunction to assess the equipment availability, reliability, and maintenance needs and expressed in minutes/equipment category/year.

The outage data are grouped to facilitate outage statistics compilation.

- Service area of the network affected by
  - total outage, and
  - partial outage.
- Cause of outage due to
  - outage attributable to the equipment manufacturer or the service provider,
  - outage due to procedural error,
  - outage due to software release error, and
  - other causes.

c) Congestion control

The incorporation of congestion control is aimed at sustaining network performance operation to assure continuation of network services. Congestion control involves the controlling of traffic entries into a communication network. The objective is to avoid traffic congestion causing network collapse by means of monitoring and regulating over-subscription of the processing or link capabilities of the intermediate network nodes. The methodology utilizes resource-reducing procedures such as reducing the rate of sending packets.

The key components of a generic congestion-avoidance scheme include implementation of functional control devices for congestion detection, congestion feedback, feedback selector, signal filter, decision function, and increase/decrease algorithms.

To prevent network congestion and collapse the method requires

– establishing overload conditions,

– a mechanism in routers to reorder or drop packets under pre-established overload conditions, and

– end-to-end flow control mechanisms designed into the end points to permit appropriate response to the status of congestion control.

d) Test case management

To manage serious field problems encountered in network operation, it is sometimes necessary to recreate the problem situation with a mirror environment for verification in the laboratory or in captive office by duplicating the specific network system and scenario operation. A test case is generated for management of the field problem resolution. Test cases are enabling mechanisms to facilitate achievement of results as part of the assurance process.

Test cases are developed to simulate actual field operating conditions in which the specific interest areas or potential problems would encounter. A test case is a set of test inputs, execution conditions, and expected results developed for a particular testing objective to verify compliance with a specific requirement. A test case specification is the documentation for specifying inputs, identifying expected test results, and establishing execution conditions for the test.

NFIT is considered as a method for such test cases to deal with field problems.

Annex A
(informative)

Example of E2E network dependability assessment

A.1 Objective

The objective of network dependability assessment of an E2E network is to determine the network service path on dependability of service. The assessment output is the availability performance or the total downtime per year of the E2E connections. The SLB method is introduced to demonstrate the techniques utilized to provide dependability solutions for analysis of network service paths.

A.2 Description of network topology and E2E network service paths

The network service paths are determined from the network topology. The network topology takes into consideration the following:

- service scenarios and requirements for voice, data, video or other network services;
- the criticality of the service provision;
- the relevant nodes and links to establish the E2E main service path;
- the backup service paths in case of main service path failure.

Figure A.1 illustrates a typical example of a network topology, which shows the relevant E2E nodes and links and their relationships in a topological configuration. The symbols for network nodes A, I, K are exchange switches; B, C, D, E are routers; and F, G, H, J are data centres which store the relevant data for user data registration access and authentication to facilitate E2E connections. The network links are connected between the nodes to establish their relationships. The resulting E2E service path is to establish the connection from A to J as initiated by the end-user at A.

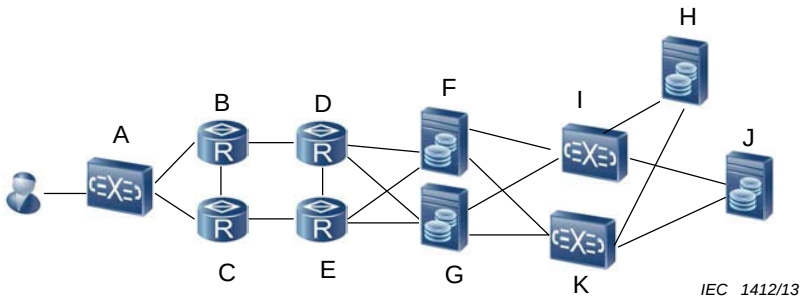


Figure A.1 – A typical example of an E2E network topology

The service scenario can be explained with the following sequence of activities:

- the end-user is accessing A to establish the link to reach J;
- the main service path shown in solid line "——" follows the nodes and links of A-B-D-F-I-H-I-J in order to establish connection;
- when the service flow reaches I, it requires authentication by H to permit continuation of the service flow, representing a loop I-H-I unique to information flows in communications technology;

- when the permission is granted by H, the service flow continues from I to J to complete the E2E network connection. It should be noted that H is a critical node demanding high reliability equipment performance.

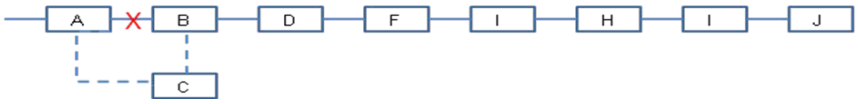
From the set of information provided so far, the backup service paths shown by dotted lines "----" can be established based on the knowledge of the node and link failures shown by "**X**" in the topological configuration. Establishing E2E network service paths needs to deal with legacy issues where existing networks interact with new networks to complete the E2E connection. The arrowhead symbol "—**>**" is only used when the SLBs are too long and is connected to a new line of SLBs to complete the E2E network service path construction.

A.3 Construction of E2E network service paths

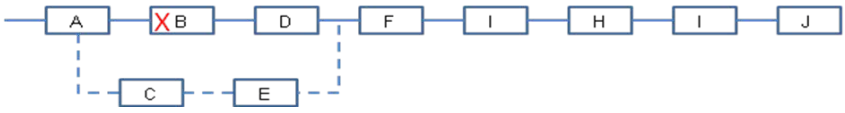
The E2E network service paths, starting with the main service paths and the backup service paths, are constructed with SLB diagrams, as shown in a) to k).

a) Main service path

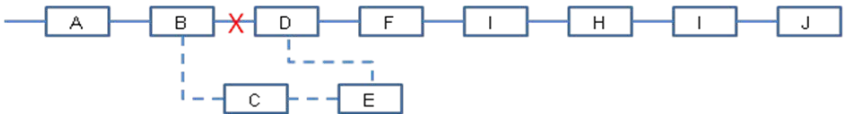
b) Backup service path with failure of link between node A and B



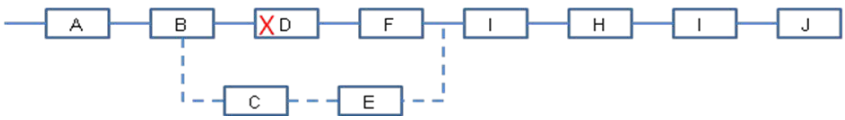
c) Backup service path with failure of node B



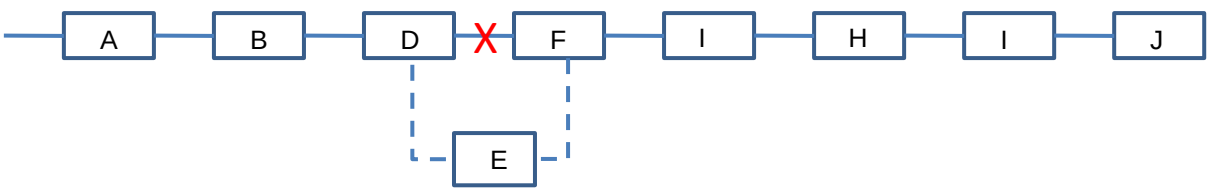
d) Backup service path with failure of link between node B and D



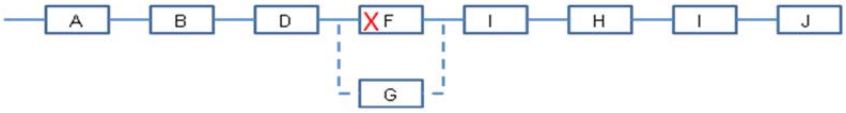
e) Backup service path with failure of node D



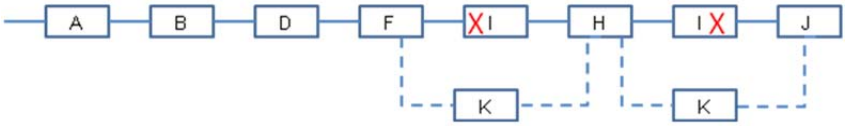
f) Backup service path with failure of link between node D and F



g) Backup service path with failure of node F



h) Backup service path with failure of node I



From this set of SLB diagrams, the availability performance or the total downtime per year of the combined E2E network service paths can be determined by using standard mathematical procedures and experienced data established or estimated for each node and link relevant to the E2E network topology. The success in availability performance of E2E network service operation means that the main service path is available in operation, all backup service paths are also available upon demand, and the switch over of path should be successful as and when required.

Each service path from A to H is a simple serial model of the RBD to determine the availability of path A to H. The availability of the E2E service path is determined by the combined availability of the main path and the availability of the backup paths.

The availability of the E2E service path can be determined from the downtime contribution as follows:

$$A_{\mathrm{E2E}} = 1 - \frac{DT_{\mathrm{E2E}}}{8\,760 \times 60}$$

where

A_{E2E} is the availability of E2E service path;

DT_{E2E} is the downtime of E2E service path, minute/year;

$$DT_{\mathrm{E2E}} = \sum_{i} \left\{ f_{\mathrm{i}} \times \left[r_{\mathrm{i}} \times dt_{\mathrm{i}} + (1 - r_{\mathrm{i}}) \times MTTR_{\mathrm{i}} \right] \right\}$$

f_{i} is the failure frequency of node/link i in main path, times/year;

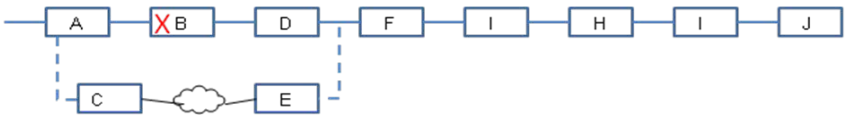
r_{i} is the network failure recovery ratio of node/link i in main path;

dt_{i} is the service downtime of node/link i in the main path failed, but the service is recovered successfully;

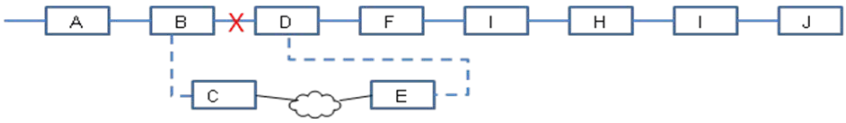
$MTTR_{\mathrm{i}}$ is the mean time to restoration of node/link i in the main path failed, but the service is not recovered.

In network topology, sometimes the topological configuration encounters the routing through an entire interacting network, which already exists in operation. The SLB method can include such interacting network for the E2E network service path modelling. This is constructed by means of representing the interacting network as a “cloud” with the symbol  incorporated in the SLB service path. The “cloud” is treated as a network node in the topological configuration. For example, if the router C needs to go through a transport network to reach router E, the corresponding backup service paths for c), d) and e) can be represented by the corresponding SLB diagrams in i), j) and k).

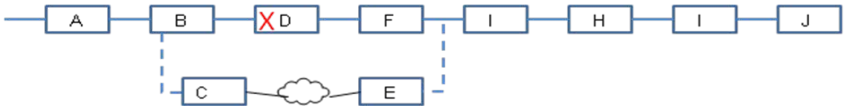
i) Backup service path flow through “cloud” with failure of node B



j) Backup service path flow through “cloud” with failure of link between node B and D



k) Backup service path flow through “cloud” with failure of node D



The SLB method presents the following key application features:

- SLB is developed as a tool specifically for communication network modelling;
- SLB is used to identify and trace critical E2E service paths for further analysis;
- SLB considers the service flow as well as network topology;
- SLB incorporates a loop-back situation to model the network topological configuration unique to information flows in communications technology;
- SLB deals primarily with single point failures; multi-point failures are rare in network paths, but could occur such as overload and disturbance in propagations that would require special consideration on a case by case basis;
- SLB permits further sensitivity studies such as packet delay, jitter, real-time and non-real-time loss and recovery to facilitate planning and selection of network service protection strategies;
- SLB presents a logical flow for simple construction of E2E network service paths;
- SLB facilitates network partition to address relevant E2E network service path construction involved in existing networks interacting with new networks;
- SLB failure database utilizes estimated or experienced data of relavant E2E network service performance to support downtime estimation;
- SLB can be computerized to faciliate iterative analysis of E2E network failures and to evaluate potential network performance impact.

A.4 Analysis of E2E network service paths

The premise for E2E service path analysis is to identify the failure location and the type of failure in the network path under consideration. Typical network failures include:

- equipment failures;
- OAMP performance mishaps;
- facility malfunctions and power failures;
- procedural errors;
- traffic overload;

- accidents and environmental incidents;
- security intrusion and malicious attacks.

The location of network node and link failures can exist in anyone of the network layers as described in the OSI reference model [13]. The following provide examples of some probable network failure symptoms:

- application layer: failure in E-mail file transfer;
- presentation layer: failure in encryption and data conversion;
- session layer: failure to maintain start/stop order in communications;
- transport layer: failure to deliver message;
- network layer: failure to route data;
- data link layer: failure to transmit frames from node to node;
- physical layer: failure of equipment in a network node or cable link.

From these symptoms the responsible network node or link can be traced to identify their responsible failure root causes. The respective failure effects can also be established by network test results or from field experience observations concerning the extent and criticality of the failure impact to the network end-users and the provision of relevant network service functions. These data are most valuable for capturing and storing in a database for on-going and future OAMP performance evaluation.

As an example, a network failure causing message overload and frequent interruptions in an E2E network service is traced to the version compatibility of a software protocol used in the application layer. Upon identification of the failure cause, the protocol is updated to the latest version, hence restoring the E2E network service to its normal operation.

The overall analysis process is known as NFMECA.

The relevant failure information is captured by the FRACAS database as a common repository for failure modes and effects data. The FRACAS database can be effectively used as experienced data for network failure diagnosis of similar failure symptoms to expedite appropriate corrective actions. The FRACAS database is a valuable tool to support network availability performance and network downtime prediction. FRACAS database should be linked to the network fault management system to facilitate common data storage and sharing of information where applicable.

A.5 Evaluation of E2E network service paths

The knowledge gained from the outcome of the NFMECA can be used for decision-making and project risk assessment such as:

a) recommending redesign of the target E2E network service path for improvement of network design for dependability performance;

b) developing test cases for NFIT to verify potential failure effects of the identified failure by initiation of fault insertion tests in the respective E2E network service path. NFMECA data and other relevant information are used to build test cases.

The design realization process of the target E2E network service path in a) is a redesign process which follows a rigorous life cycle process for design/development and realization/integration. The relevant network life cycle stages are described in IEC 61907.

The evaluation of the target E2E network service path in b) is to develop appropriate test cases for NFIT applications. The NFIT is to conduct tests to simulate actual E2E network service path operating conditions by means of fault insertion to explore the test outcome. The objective is to determine the extent of risk exposure in taking the redesign action. NFIT

attempts to verify and confirm the uncertainty of the potential outcome prior to actual implementation action in redesigning the E2E network service path. Depending on the project delivery time schedule and budgetary constraints, the NFIT activities in b) provide additional assurance to the redesign process in a) and present test information to assist in project decision-making. Project tailoring and trade-off would be prudent in the decision process.

A test case is a set of test inputs, execution conditions, and expected results developed for a particular testing object. In this case, the verification of the target E2E network service path redesign is to achieve network performance in delivery of dependability of service. Fault insertion test is a verification technique in which a deliberate fault is introduced into the target E2E network service path to determine the expected test results. The test outcome provides the objective evidence to support the redesign decision.

NFIT also provides a means to assess the efficiency of the test process, the resultant fault coverage, the network service path availability, and the effects on network dependability performance.

As part of the E2E network service paths evaluation process, the following data can be determined:

a) network service downtime
   - sum of service downtime caused by failures of each node of the network;
   - sum of service downtime caused by failures of each link of the network.

b) network service availability

c) failure modes
   - network node: service outage, partial service outage, service intermittent, instantaneous service outage, service performance degradation;
   - network link: link break.

d) network parameter information

Network parameter	*Source*
• network service downtime per year (minutes/year)	calculated result
• number of nodes in network	network topology
• number of links in network	network topology
• frequency of failure on node i	FRACAS statistics
• frequency of failure on link j	business statistics
• service outage duration due to node i (minutes)	NFIT results
• service outage duration due to link (minutes)	NFIT results
• network recovery rate	NFIT results
• mean time to repair of node i	FRACAS statistics
• mean time to repair of link j	operator's statistics

Annex B
(informative)

Example of full-end network dependability assessment

B.1 Objective

The objective of network dependability assessment of a full-end network by the network operator is to determine the entire network dependability performance. The assessment output is the availability performance or the total downtime per year of the entire network. There are many ways to arrive at the answer by using a combination of network modelling techniques and prediction methods, as well as using field performance data relevant to the network failure performance characteristics to establish failure trends over time.

B.2 Description of network topology and full-end network

The network topology is the same configuration used for the E2E network except two end-users at nodes A1 and A2 are connected in communication to illustrate a full-end network. This is presented in Figure B.1.

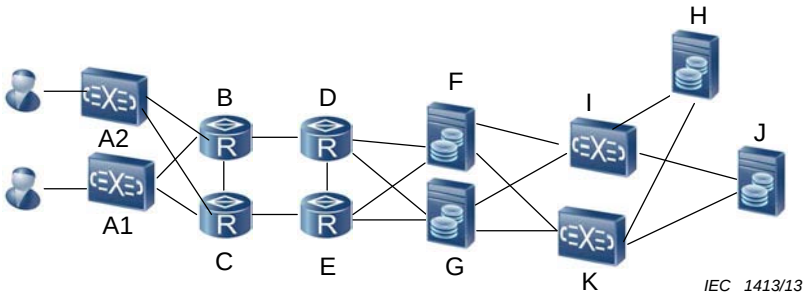


Figure B.1 – A typical example of a full-end network topology

The service scenario can be explained as follows:

- the service provider is interested in determining the availability/reliability of the entire full-end network;
- the assumption is that all the network elements from A to J inclusive have to perform their respective functions at all times on a continuous basis.

B.3 Analysis of full-end network availability model

The availability of the full-end network can be determined by calculating the average downtime contributed by the weighted sum of the E2E network downtimes. The same mathematical symbols are used as in Annex A.

The availability of the full-end network service can be determined as follows:

$$A_N = 1 - \frac{DT_N}{8\,760 \times 60}$$

where

A_N is the availability of full-end network service;

DT_N is the total downtime of full-end network;

$$DT_N = \sum_i DT_{E2Ei} \times P_i$$

DT_{E2Ei} is the downtime of E2E service path i, minute/year;

P_i is the number of users in service path i divided by the users of the whole network.

B.4 Evaluation of the full-end network

The evaluation of a full-end network service is similar to the E2E network service but taking all E2E network service paths into consideration.

NFMECA and NFIT are conducted similar to the E2E evaluation process but with different objectives from a network service provider or operator perspective.

Annex C
(informative)

Evaluation of network dependability performance in field operation

C.1 Objective

The evaluation of network dependability performance in field operation is shown in an example. The objective is to describe a procedure for determining the impact of network outages and outage duration affecting the number of users subscribed to the network services.

This example illustrates the methods used for network analysis and evaluation based on the network performance data collected over a 2-year study period of a nation-wide public switched telephone network operation [16]. Numerical data are presented for illustration purposes to indicate the magnitude of network performance parameters. Percentage values are provided to represent relative network outage contributions and resultant network service impact.

C.2 Data analysis

Network performance statistics indicate a total of 303 network failures causing outages during the two years of network service operation. The 303 network failures affected over one million subscribers or users with cumulative outage duration of 3 196,5 minutes. The service outages are determined by the sum of telephone service outages. They are grouped by the various failure categories. Table C.1 summarizes the network failure data.

Table C.1 – Summary of network failure data of a nation-wide public switched telephone network

Network failure source	Failure category	Number of outages	Number of users affected	Outage duration min
Facility-related	Hardware failure	56	95 690	159,8
	Software failure	44	118 200	119,3
Traffic-related	Functions (overload)	18	276 760	1 123,7
Disaster-related	Acts of nature	32	159 000	828,2
Security-related	Vandalism	3	853 930	456,0
Schedule-related	Maintenance	0	0	0
Human-factor-related	Procedural (human error)	150	265 996	509,5

The service impact is determined by the cumulative downtime measured in user-minutes by category.

User-minutes = *Number of users affected* by the failure category x *Outage duration* of the category in minutes.

Figure C.1 presents the network outage contributions and the resultant network service impact.

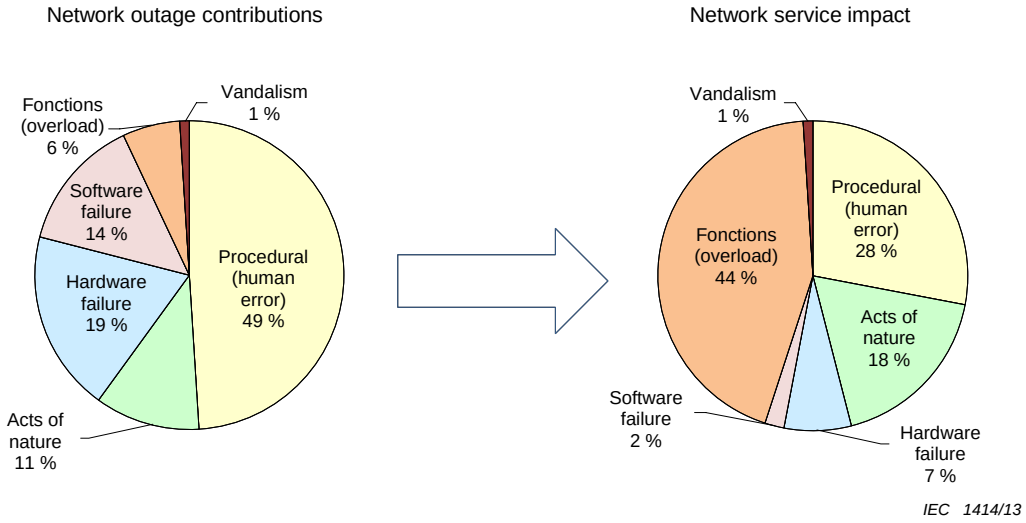


Figure C.1 – Network outage contributions and resultant network service impact

C.3 Network dependability performance evaluation

The availability performance can be determined from the cumulative (3 196,5 min) outage duration from the two years (2 × 365 × 24 × 60 = 1 051 200 min) of continuous network service operation. The average downtime is 1 598 min per year.

Availability of the entire network = (1 051 200 – 3196,5)/1 051 200 = 99,7 %

The network service performance shows a 44 % functions (overload) impact manifested by 6 % of the total network outage contributions. This observation indicates the lack of network performance capacity as a major cause of network outage requiring dependability improvement. The 49 % procedural (human error) outage contribution suggests improvement needs for OAMP procedures.

The network operator is assessing the full-end network dependability performance status with relevant network outage information reported by the cooperation of network service providers. Individual service providers are responsible for their respective network segments for the day-to-day operation of their service contributions. Failure trends and degraded performance for specific network segments would require time-related performance data from the individual service providers for dependability analysis. Determination of fault detection time, time to restoration and FRU return rates would require additional information on the service providers' maintenance records of the network segments.

Bibliography

[1] ITU-T Recommendation I.350:1988, *General aspects of quality of service and network performance in digital networks, including ISDN*

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

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

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

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

[6] IEC/ISO 31010, *Risk management – Risk management techniques*

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

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

[9] IEC 61882, *Hazard and operability studies (HAZOP studies) – Application guide*

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

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

[12] Lyu, M. R. (Ed.): The Handbook of Software Reliability Engineering, IEEE Computer Society Press and McGraw-Hill Book Company, 1996

[13] ISO/IEC 7498-1, *Information technology – Open Systems Interconnection – Part 1: Basic Reference Model: The Basic Model*

[14] TL 9000, *Quality Management System – Requirements Handbook 3.0, March 2001, Quality Excellence for Suppliers of Telecommunications Forum (QuEST Forum*)

[15] TL 9000, *Quality Management System – Measurements Handbook 3.5, March 2003, Quality Excellence for Suppliers of Telecommunications Forum (QuEST Forum*)

[16] KUHN D.R., *Sources of Failure in the Public Switched Telephone Network*, IEEE Computer, Vol.30, No.4 (April 1997), National Institute of Standards and Technology, Gaithersburg, Maryland 20899 USA

———————

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

MÉTHODOLOGIE POUR L'ÉVALUATION ET L'ASSURANCE DE LA SÛRETÉ DE FONCTIONNEMENT D'UN RÉSEAU 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 brevet. La CEI ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

La Norme internationale CEI 62673 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
56/1507/FDIS	56/1514/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 stabilité 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.

IMPORTANT – Le logo *"colour inside"* qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

INTRODUCTION

La sûreté de fonctionnement d'un réseau de communication est fortement influencée par la conception et la mise en œuvre des fonctions de service de réseau qui ont, pour but, d'atteindre les objectifs de satisfaction de l'utilisateur en matière de performance des services.

L'évolution des réseaux, l'accroissement des services et la rénovation fonctionnelle dans le secteur des communications ont longtemps représenté des défis pour les fournisseurs de services de réseau concernant la vaste gamme de services de réseau et les activités liées aux services constatés par les utilisateurs finaux.

Pour assurer la pérennité d'une activité viable dans les services de réseau, il est prudent, dans le domaine des communications, de garantir :

– les fonctions de service de réseau nécessaires,
– la capacité de réseau et les performances adéquates,
– la sécurité de service,
– la qualité de service, ainsi que
– la sûreté de fonctionnement du service.

La présente Norme internationale aborde un des points les plus importants concernant l'évaluation et la sûreté de fonctionnement des services fournis en vue d'assurer la performance des services de réseau. Elle traite également des stratégies d'assurance de la sûreté de fonctionnement des réseaux et des applications de la méthodologie pour améliorer et soutenir le fonctionnement du réseau.

La présente Norme internationale décrit une méthodologie générale pour l'évaluation et l'assurance de la sûreté de fonctionnement des réseaux de communication. Elle spécifie aussi des méthodes d'évaluation et d'assurance qualité des réseaux de communication pour la sûreté de fonctionnement en conformité avec les exigences, par exemple, de la CEI 61907 et des Recommandations de l'UIT-T[1] concernant la sûreté de fonctionnement.

Elle présente une approche pour que l'analyse et l'évaluation de la sûreté de fonctionnement d'un réseau qui garantissent la conception d'un réseau sûr pour une mise en œuvre efficace.

L'objectif de la présente norme est de développer une solution rentable pour obtenir les performances de sûreté de fonctionnement du réseau et permettre de tirer profit du réseau sûr.

---

1 UIT-T : Union Internationale des Télécommunications – Télécommunications.

MÉTHODOLOGIE POUR L'ÉVALUATION ET L'ASSURANCE DE LA SÛRETÉ DE FONCTIONNEMENT D'UN RÉSEAU DE COMMUNICATION

1 Domaine d'application

La présente Norme internationale décrit une méthodologie générale pour l'évaluation et l'assurance de la sûreté de fonctionnement des réseaux de communication du point de vue du cycle de vie d'un réseau. Elle présente les stratégies d'évaluation de la sûreté de fonctionnement d'un réseau ainsi que la méthodologie pour l'analyse de la topologie d'un réseau, l'évaluation de la sûreté de fonctionnement des trajet de services et l'optimisation des configurations de réseau afin d'obtenir les performances de sûreté de fonctionnement du réseau et de sûreté de fonctionnement des services. Elle traite également des stratégies d'assurance de la sûreté de fonctionnement du réseau ainsi que de la méthodologie pour l'application de la vérification de l'état de santé du réseau, du contrôle de la fréquence d'interruption du réseau et de la gestion des tests élémentaires pour améliorer et maintenir les performances de sûreté de fonctionnement des services de réseau.

La présente norme est applicable aux fournisseurs de services de réseaux, aux concepteurs et développeurs de réseaux, ainsi qu'aux spécialistes de la maintenance et aux opérateurs de réseaux pour la garantie des performances de sûreté de fonctionnement des réseaux et l'évaluation de la sûreté de fonctionnement des services.

2 Références normatives

Les documents suivants sont cités en référence de manière normative, en intégralité ou en partie, dans le présent document et sont indispensables pour son application. 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 Electrotechnique International (VEI) – Chapitre 191: Sureté de fonctionnement*

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

CEI 61907, *Ingénierie de la sûreté de fonctionnement des réseaux de communication*

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 et la CEI 61907, 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 et 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 à l'article: Un réseau a ses limites. L'ensemble des nœuds situés au niveau de la frontière d'un réseau s'appellent des terminaux. Dans certaines applications, le terme «nœud» est employé 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 à l'article: 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
sûreté de fonctionnement d'un réseau
aptitude d'un réseau à assurer la fonction requise à l'instant voulu pour répondre à des exigences spécifiques relatives à la communication et au fonctionnement

3.1.3
disponibilité
disponibilité d'un réseau
aptitude d'un réseau à assurer la fonction requise

Note 1 à l'article: La disponibilité dépend des caractéristiques combinées de la fiabilité, de la capacité de restauration et de la maintenabilité du réseau et de l'aptitude de soutien logistique à la maintenance.

Note 2 à l'article: La disponibilité peut être quantifiée en utilisant des mesures appropriées.

3.1.4
fiabilité
fiabilité d'un réseau
aptitude d'un réseau à assurer la fonction requise, sans défaillance, dans un intervalle de temps donné, dans des conditions données

Note 1 à l'article: L'intervalle de temps peut être exprimé dans des unités appropriées au réseau concerné.

Note 2 à l'article: La fiabilité d'un réseau dépend des caractéristiques combinées de performance de fiabilité, de capacité de restauration, de maintenabilité et de logistique de maintenance des éléments qui constituent ce réseau.

Note 3 à l'article: L'expression «dans des conditions données» inclut des aspects qui affectent la fiabilité, tels que: le mode de fonctionnement, les niveaux de contrainte, les conditions d'environnement et la maintenance.

Note 4 à l'article: La fiabilité peut être quantifiée au moyen de mesures de performance appropriées.

3.1.5
maintenabilité
maintenabilité d'un réseau
aptitude d'un réseau à être maintenu ou ramené à un état pour assurer la fonction requise, dans des conditions données d'utilisation et de maintenance

Note 1 à l'article: L'expression «dans des conditions données» inclut des aspects qui affectent la maintenabilité, tels que: l'emplacement de maintenance, l'accessibilité, les procédures de maintenance et les ressources de maintenance.

Note 2 à l'article: La maintenabilité peut être quantifiée en utilisant des mesures de performance appropriées.

3.1.6
logistique de maintenance
logistique de maintenance d'un réseau
fourniture des ressources nécessaires pour maintenir un réseau

Note 1 à l'article: Les ressources comprennent les ressources humaines, les équipements de soutien, les matériaux et les pièces de rechange, les moyens de maintenance, la documentation, les informations et les systèmes informatiques de maintenance.

3.1.7
aptitude de soutien logistique à la maintenance d'un réseau
aptitude de soutien logistique à la maintenance
capacité d'une organisation concernant le soutien de maintenance pour le réseau

Note 1 à l'article: L'aptitude de soutien logistique à la maintenance peut être quantifiée en utilisant des mesures appropriées.

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

Note 1 à l'article: L'aptitude à restaurer peut ou non nécessiter des actions externes.

Note 2 à l'article: La capacité de restauration peut être quantifiée en utilisant des mesures telles que la probabilité de restauration au cours d'une durée spécifiée.

3.1.9
élément
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 à l'article: Un élément de réseau peut nécessiter une intervention humaine pour réaliser ses fonctions de service.

Note 2 à l'article: Les éléments de réseau sont liés par des liaisons de réseau.

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

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

[SOURCE: Recommandation UIT-T I.350 :1988] [1][2]

3.1.12
gestion
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
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 1 à l'article: 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 à l'article: Les services de communication sont les services de réseau auxquels ont souscrit les utilisateurs finaux.

_____

2 Les chiffres entre crochets se réfèrent à la Bibliographie.

Note 2 à l'article: 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 assurer la fonction requise

Note 1 à l'article: La défaillance d'un réseau 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 d'inaptitude d'un réseau à assurer la fonction requise pour une raison interne

Note 1 à l'article: Dans le contexte du fonctionnement d'un réseau, une panne peut être naturelle, due à une cause anormale ou à un dysfonctionnement résultant d'une défaillance d'un élément du réseau, ou induite de l'extérieur, comme par exemple une panne provoquée par injection d'un défaut.

Note 2 à l'article: 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 1 à l'article: 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 à l'article: Un utilisateur peut être l'origine ou le destinataire des informations utilisateur, ou les deux.

Note 2 à l'article: Dans certains cas, l'utilisateur d'un service de télécommunication est également appelé abonné.

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

Note 1 à l'article: Le flux est le taux de réussite d'envoi des messages sur une voie de communication d'un service de réseau.

3.1.21
performance de sûreté de fonctionnement
performance de sûreté de fonctionnement d'un réseau
aptitude du réseau à fournir ou à démontrer que les caractéristiques de sûreté de fonctionnement du réseau satisfont aux objectifs définis pour les services du réseau

Note 1 à l'article: Dans le contexte de la présente norme, la performance de sûreté de fonctionnement d'un réseau fait référence à la fourniture de services d'un réseau avec toutes ses terminaisons.

Note 2 à l'article: Un service de réseau avec toutes ses terminaisons signifie la fourniture d'une connectivité de service établie pour toutes les terminaisons d'émission et de réception d'un réseau de communication.

3.1.22
sûreté de fonctionnement du service
sûreté de fonctionnement du service d'un réseau
aptitude à la fonction de sûreté de fonctionnement requise pour les services de communication des utilisateurs

Note 1 à l'article: Dans le contexte de la présente norme, la sûreté de fonctionnement d'un service fait référence à la fourniture de services d'un réseau de bout en bout (E2E).

Note 2 à l'article: Un service de réseau de bout en bout signifie la fourniture d'une connectivité de service établie entre les terminaisons d'émission et de réception d'un réseau de communication.

3.1.23
sécurité de service
sécurité de service d'un réseau
fait de garantir la sécurité requise pour les services de communication des utilisateurs

3.1.24
trajet de service
trajet de service d'un réseau
trajet de connexion par des liaisons et des nœuds du réseau pour établir les services de communication des utilisateurs

3.1.25
flux
flux d'un réseau
flux d'informations et de données sur le trajet de service

3.1.26
scénario de service
situation opérationnelle dans un réseau de communication pour la fourniture de fonctions de services de réseau et d'applications de services utilisateurs

3.1.27
indisponibilité d'un réseau
état du réseau caractérisé par son inaptitude à remplir sa fonction principale

3.2 Abréviations

Abréviation	Français	Anglais
E2E	De bout en bout	End-to-End
FRACAS	Système de compte-rendu et d'analyse des défaillances et de mise en rendu des défaillances et de mise en œuvre d'actions correctives	Failure Reporting, Analysis, Corrective Action System
FRU	Unité retournée du site	Field Return Unit
HAZOP	Etudes de danger et d'exploitabilité (études HAZOP)	Hazard and operability studies
MTTR	Temps moyen avant restauration du noeud/lien	Mean Time to Restoration of Node/link
ND	Sûreté de fonctionnement d'un réseau	Network Dependability
NFIT	Vérification par insertion de défauts sur le réseau	Network Fault Insertion Test
AMDEC réseau	Analyse des modes de défaillance des réseaux, de leurs effets et de leur criticité	Network Failure Modes, Effects and Criticality Analysis
OAMP	Opérations, administration, maintenance et fourniture de services	Operations, Administration, Maintenance, and Provisioning

Abréviation	Français	Anglais
OSI	Interconnexion de systèmes ouverts	Open System Interconnection
QS	Qualité de service	Quality of Service
BDF	Bloc-diagramme de fiabilité	Reliability Block Diagram
BLS	Bloc logique de service	Service Logic Block

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

4.1 Nécessité de méthodes pour la sûreté de fonctionnement d'un réseau

Un réseau de communication est un système de systèmes qui interagissent avec d'autres réseaux pour atteindre de nombreux objectifs de performance des services. Un réseau de communication est complexe et ses systèmes constitutifs changent et évoluent en permanence. Une méthodologie et des approches techniques appropriées sont nécessaires pour l'évaluation et l'assurance de la sûreté de fonctionnement du réseau.

Du point de vue de l'évaluation de la sûreté de fonctionnement d'un réseau, les techniques classiques d'analyse et d'évaluation de la sûreté de fonctionnement ont un champ d'application limité dans les applications réseau. Les méthodes usuelles d'analyse de la sûreté de fonctionnement sont souvent inadaptées pour la modélisation d'une topologie de réseau complexe et elles sont difficiles à mettre en œuvre pour l'analyse de multiples configurations de réseau et trajets de services de réseau, elles ne fournissent pas les garanties nécessaires quant à la fiabilité des résultats d'évaluation. Des méthodes sélectives – telles que BLS, AMDEC réseau – et une simulation de réseau appropriées pour l'analyse et l'évaluation de la sûreté de fonctionnement d'un réseau peuvent fournir des solutions en réseau adaptées. Ces méthodes constituent à présent les processus essentiels pour assurer la pérennité des services et les performances de sûreté de fonctionnement des réseaux.

Il existe une approche commune permettant d'assurer les performances de sûreté de fonctionnement d'un réseau et de sûreté de fonctionnement d'un service; celle-ci consiste à construire une structure de réseau fiable, à établir des systèmes de trajets effectifs, à assurer une gestion efficace des pannes et un soutien logistique à la maintenance du réseau, et à recueillir des données d'aptitude à la fonction ainsi que des retours d'informations des utilisateurs en vue de l'amélioration et de l'évaluation des services du réseau. Le processus implique l'analyse des fonctions de service du réseau pour une mise en œuvre rentable ainsi que l'évaluation des fonctionnalités de service du réseau avec un apport de valeur ajoutée pour l'amélioration de la sûreté de fonctionnement. Bien que cette approche soit adéquate pour évaluer le cycle de vie des éléments matériels et logiciels du réseau en vue de la détermination des performances de sûreté de fonctionnement, elle n'est toutefois pas adaptée pour le traitement de la connectivité pour établir des services de l'utilisateur au cours du fonctionnement du réseau. En ce qui concerne l'assurance, l'approche classique manque de réactivité par rapport à la dynamique du marché pour les configurations adaptatives des réseaux. Ceci a une incidence sur les objectifs de services du réseau pour assurer les performances de sûreté de fonctionnement du réseau et pour garantir la sûreté de fonctionnement du service dans une activité réseau globale hautement concurrentielle.

De nombreuses méthodes d'analyse de la sûreté de fonctionnement ont été développées au fil des ans, mais seules quelques-unes fournissent une méthodologie appropriée pour une analyse efficace des performances de sûreté des réseaux et de la sûreté de fonctionnement des applications de services. Cette observation est faite en raison de la nature complexe de l'évolution des réseaux, de la topologie innovante pour le développement de fonctions avancées de services de réseaux et des techniques uniques requises pour les applications pratiques des méthodologies d'analyse de la sûreté de fonctionnement. Bien qu'il existe de nombreux facteurs susceptibles d'avoir une influence sur les performances de sûreté de fonctionnement dans le cycle de vie du réseau, l'impact le plus significatif est observé au cours des stades initiaux des processus de concept/définition, conception/développement et réalisation/intégration. De nouveaux ajouts au réseau existant impliqueraient une analyse de

scénario du système existant lors du stade de concept/définition avant de poursuivre et de s'engager dans les stades ultérieurs de conception/développement et de réalisation/intégration. Il convient d'inclure l'étendue des besoins en termes de fonctionnement/maintenance, d'amélioration/rénovation et de retrait, dans l'analyse de scénario du système existant. En vue de l'optimisation du fonctionnement du réseau et de la fourniture de services lucratifs, il convient de surveiller, d'analyser et d'évaluer en permanence les performances de sûreté de fonctionnement du réseau et la sûreté de fonctionnement du service. Les stratégies d'assurance de la sûreté de fonctionnement des réseaux et les applications de la méthodologie constituent des facteurs clés contribuant à améliorer et à poursuivre la fourniture continue de services de réseau du point de vue d'une activité viable.

4.2 Objectifs de la sûreté de fonctionnement du réseau

La capacité d'un réseau à fournir aux utilisateurs des services de communication continus et ininterrompus dépend fortement de ses performances de sûreté de fonctionnement. La sûreté de fonctionnement suppose que la fourniture de fonctions de service en réseau est fiable et capable de réaliser le service souhaité sur demande. Pour obtenir les performances de sûreté de fonctionnement et de sûreté de fonctionnement du service en réseau, il est indispensable d'utiliser des méthodes appropriées pour l'évaluation de la sûreté de fonctionnement du réseau. La présente norme vient à l'appui des exigences d'ingénierie pour la conception des réseaux et la mise en œuvre des processus; elle spécifie également une méthodologie appropriée de sûreté de fonctionnement pour l'analyse et l'évaluation des réseaux de communication. Le cadre technique de la CEI 60300-3-15 traitant des aspects système de la sûreté de fonctionnement et les exigences de la CEI 61907 relatives à l'ingénierie de la sûreté de fonctionnement des réseaux s'appliquent à la présente norme. Les termes relatifs à la qualité de service des communications renvoient à la Recommandation UIT-T G.1000 [2].

Au cours du développement et de la mise en œuvre des réseaux de communication, il existe plusieurs facteurs influents ayant une incidence sur la capacité des opérateurs et fournisseurs de services de réseaux à poursuivre une activité viable. Ces facteurs influents comprennent:

- les fonctions de service du réseau pour satisfaire les besoins des utilisateurs;
- la capacité du réseau à répondre aux demandes de service;
- sécurité de service;
- qualité de service (QS) [3];
- sûreté de fonctionnement du service.

Dans le cadre de l'évaluation et de l'assurance de la sûreté de fonctionnement du réseau, il convient de noter que :

a) les paramètres fonctionnels du réseau, tels que la capacité de transmission et la performance de connectivité, se dégradent avec le temps en raison des défaillances, ce qui a pour effet d'altérer la sûreté de fonctionnement du réseau;

b) la robustesse du réseau, à savoir sa capacité à résister aux atteintes aux performances dues aux intrusions externes et aux interruptions de service, affectent la protection critique de l'infrastructure du réseau.

4.3 Scénarios de services du réseau

Il existe deux scénarios de services du réseau présentant un intérêt pour la sûreté de fonctionnement du réseau.

a) La sûreté de fonctionnement du service des connexions des utilisateurs finaux pour les services de réseau de bout en bout (E2E) (voir l'Article A.2) – l'objectif est de déterminer les performances de sûreté de fonctionnement du réseau concernant les services de réseau de bout en bout (E2E) du point de vue des utilisateurs finaux du réseau. Le service de réseau E2E est un service essentiel pour satisfaire aux besoins des utilisateurs finaux sur la base de la capacité de performance d'un réseau avec toutes ses

terminaisons en fonctionnement. Dans le scénario de services du réseau E2E, la sûreté de fonctionnement du service dépend des systèmes trajets et de la capacité de performance du réseau associés aux trajets de services spécifiques choisis pour les connexions de bout en bout (E2E). La sûreté de fonctionnement du service est constatée par les utilisateurs finaux et elle reflète les demandes des clients ainsi que la satisfaction des utilisateurs.

b) Les performances de sûreté de fonctionnement de l'ensemble du réseau pour des services de réseau avec toutes ses terminaisons (voir l'Article B.2) – l'objectif est de déterminer les performances de sûreté de l'ensemble du réseau, du point de vue de l'opérateur ou du fournisseur de services du réseau. Un réseau avec toutes ses terminaisons peut fonctionner dans un scénario de service selon lequel le fournisseur de service a le contrôle total d'un réseau privé et a la responsabilité de garantir une aptitude à la fonction de sûreté de fonctionnement du réseau adéquate pour les services du réseau. Le réseau avec toutes ses terminaisons peut également fonctionner dans un scénario avec plusieurs fournisseurs de services, chacun contrôlant un segment désigné de l'ensemble du réseau comme dans le cas d'un réseau public commuté. L'opérateur de réseau est responsable de la performance globale du réseau. Les fournisseurs de services individuels sont responsables de leurs contributions à la performance des services du réseau dans le cadre d'accords conclus avec l'opérateur du réseau sur les niveaux de service et de qualité du service (QS).

Les deux scénarios de services de réseau associés aux scénarios avec des services de réseau de bout en bout et de réseau avec toutes ses terminaisons sont interdépendants et complémentaires. Il convient de noter que, si le système n'a pas la capacité d'assurer les performances de sûreté de fonctionnement, les services des utilisateurs ne pourront être ni réalisés ni garantis et que, si l'utilisateur n'est pas satisfait de la sûreté de fonctionnement du service, le fournisseur de service aura des difficultés à répondre aux demandes de services et pourra perdre des abonnés, affectant ainsi la génération de revenus à partir de la fourniture de services de réseau. La collecte des retours d'informations des utilisateurs et l'analyse des données pertinentes de performance du réseau à partir de ces deux scénarios de services de réseau devraient faciliter la planification des ressources et le contrôle de la qualité de service fournie aux abonnés ou aux utilisateurs et assurer la sûreté de fonctionnement de l'ensemble des services du réseau.

Les performances de sûreté de fonctionnement du réseau et la sûreté de fonctionnement du service reflètent les scénarios de services du réseau et les environnements d'exploitation dans l'activité commerciale. Cela passe par une évaluation de la sûreté de fonctionnement pour garantir les performances de sûreté de fonctionnement lors du développement du réseau et par l'assurance de la sûreté de fonctionnement pour maintenir la sûreté de fonctionnement du service pendant le fonctionnement du réseau.

Les stratégies d'évaluation de la sûreté de fonctionnement d'un réseau et l'assurance de la sûreté de fonctionnement sont décrites en 4.4 et 4.5. La méthodologie de la sûreté de fonctionnement et les méthodes utilisées pour les applications réseau sont définies à l'Article 5.

4.4 Stratégies d'évaluation de la sûreté de fonctionnement d'un réseau

L'évaluation de la sûreté de fonctionnement est un processus d'appréciation permettant de déterminer l'état de la performance du réseau concernant la sûreté de fonctionnement des services fournis. Les paragraphes ci-dessous décrivent les stratégies d'évaluation de la sûreté de fonctionnement d'un réseau qui sont pertinentes pour les scénarios de services du réseau.

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

La sûreté de fonctionnement d'un réseau de bout en bout (E2E) est influencée par la topologie du réseau, les systèmes de trajets et le choix des trajets de services pour réaliser les connexions de services des utilisateurs. Pour évaluer la sûreté de fonctionnement d'un réseau E2E, il convient d'analyser les trajets de services de trajets associés aux scénarios de services. Il convient d'évaluer l'ensemble des équipements et

des liaisons de chaque trajet de service pour la sûreté de fonctionnement des services fournis. L'évaluation de la sûreté de fonctionnement d'un réseau E2E couvre divers scénarios de services dans des réseaux publics et privés.

Il convient que la stratégie d'évaluation d'un réseau E2E envisage une approche technique pour l'évaluation de la sûreté de fonctionnement du service. Ceci est dû aux multiples trajets de services qui doivent être analysés en vue de l'optimisation de la sûreté de fonctionnement du service. La nature complexe de la configuration d'un réseau exige une technique et une méthodologie de modélisation uniques fondées sur des schémas de blocs logiques de service (BLS) (voir l'Article A.3) pour faciliter l'évaluation de la sûreté de fonctionnement des services d'un réseau E2E.

b) Stratégie d'évaluation de la sûreté de fonctionnement d'un réseau et de l'ensemble de ses terminaisons

Un réseau et l'ensemble de ses terminaisons fonctionnant dans un scénario de service se compose de plusieurs réseaux en interaction offrant diverses fonctions de services assurés par de nombreux fournisseurs de services. L'assurance des performances de sûreté de fonctionnement d'un réseau est le résultat des efforts collectifs de ces fournisseurs de services dans le cadre d'accords sur les niveaux de service et de qualité du service (QS). La fiabilité des fonctions de service du réseau avec toutes ses terminaisons peut être modélisée par un bloc-diagramme de fiabilité BDF [4] ou par des méthodes similaires. L'évaluation de la sûreté de fonctionnement d'un réseau avec toutes ses terminaisons ne peut être déterminée dans la pratique qu'après la mise en œuvre des services du réseau, par le biais d'une enquête d'aptitude à la fonction sur site et de retours d'informations suite à des enquêtes de satisfaction des clients afin d'obtenir des données pertinentes de performance du réseau. Cela est dû à la nature complexe de l'évolution d'un réseau lorsque de nouvelles fonctions de service sont ajoutées en continu en vue de l'amélioration de la performance et de l'interruption de services du réseau non rentables. Le réseau public à commutation constitue un exemple dans lequel les performances de sûreté de fonctionnement d'un réseau peuvent être évaluées par analyse et détermination de la fréquence signalée des pannes des services utilisateurs, de la durée des pannes et des réclamations des clients concernant l'impact sur les services. Les résultats d'évaluation comprennent le classement des pannes de réseau ainsi que les causes identifiées des défaillances et leur impact sur les services fournis aux abonnés ou aux utilisateurs du réseau.

Un réseau avec toutes ses terminaisons peut être un réseau privé appartenant à un seul opérateur de réseau qui contrôle totalement la fourniture des services du réseau. Un réseau de données sécurisé composé de guichets automatiques pour fournir des services bancaires distribués est un exemple de réseau privé. Pour évaluer les performances de sûreté de fonctionnement du réseau privé avec toutes ses terminaisons, il convient de déterminer tous les éléments du réseau et leurs relations et d'évaluer toutes les caractéristiques pertinentes d'aptitude à la fonction de sûreté de fonctionnement pour établir leur conformité à des critères définis de performances des services de réseau. Les processus techniques utilisés pour l'évaluation de la sûreté de fonctionnement du réseau sont analysés et évalués comme un système avec des conditions aux limites. Pour le développement d'un nouveau réseau, il convient que le processus de cycle de vie du réseau soit suivi et que les activités d'ingénierie de la sûreté de fonctionnement soient menées conformément aux lignes directives recommandées dans la CEI 61907. Pour les projets d'amélioration et de rénovation, il est indispensable de prendre en considération les problèmes hérités des configurations du réseau existant afin d'optimiser la performance du réseau rénové. Il convient que des données statistiques, relatives à la performance du réseau et provenant de l'exploitation sur site, soient recueillies et analysées pour valider l'adéquation de la performance par rapport aux objectifs des services du réseau.

4.5 Stratégies d'assurance de la sûreté de fonctionnement d'un réseau

Les stratégies d'assurance de la sûreté de fonctionnement d'un réseau sont des activités planifiées impliquant des processus systématiques destinés à garantir la sûreté de fonctionnement d'un réseau en termes de performance et de sûreté de fonctionnement des services fournis basés sur l'écoute du client. Les stratégies d'assurance de la sûreté de fonctionnement d'un réseau reflètent les domaines techniques concernés dans des

applications spécifiques du réseau. Elles s'associent à la gestion de la performance du réseau et aux activités de maintenance de routine et de soutien logistique du réseau pour fournir une prestation spécifique d'ingénierie de sûreté du fonctionnement. Les stratégies spécifiques d'assurance de la sûreté de fonctionnement du réseau sont synthétisées du point de vue du fonctionnement du réseau.

a) Sûreté de fonctionnement des services fournis aux utilisateurs finaux

   Il existe deux problèmes stratégiques distincts concernant la sûreté de fonctionnement des services fournis: l'un concerne les contributions du mécanisme de fourniture des fonctions des équipements du réseau ainsi que l'interopérabilité dans le fonctionnement du service; l'autre est lié à la fourniture d'informations sous forme de flux de données en utilisant le mécanisme de fourniture de la configuration du réseau. Les stratégies spécifiques aux applications concernent surtout le mécanisme de fourniture et l'intégrité des données.

b) Garantie d'intégrité des données

   L'intégrité des données est l'élément fondamental pour la génération d'informations crédibles et la transmission de données via les trajets de service du réseau qui représentent le mécanisme de fourniture de la configuration du réseau. La stratégie spécifique aux données concerne surtout les performances de sûreté de fonctionnement du réseau et la capacité d'empêcher la perte d'informations, la corruption de données, l'exposition à des attaques.

c) Amélioration des fonctions de performance d'un réseau et processus de soutien

   Les fonctions de performance et les processus de soutien d'un réseau auront tendance à se dégrader s'ils ne font pas l'objet d'une maintenance adéquate et d'une mise à jour régulière. Une telle situation entraînera une dégradation progressive de la performance du réseau conduisant à des pannes fréquentes du réseau et à une augmentation des durées d'interruption du service, ce qui aura pour effet d'altérer le fonctionnement du réseau et la qualité du service. La stratégie de soutien logistique à la maintenance du réseau pour l'assurance de la sûreté de fonctionnement consiste à favoriser l'amélioration continue en vue d'optimiser les fonctions du réseau et simplifier les procédures concernant les processus de soutien du réseau. Au point de vue technique, l'objectif est d'améliorer les caractéristiques critiques de la sûreté de fonctionnement liées à la performance du réseau, telles que la capacité de restauration, la disponibilité, la fiabilité, la maintenabilité et le soutien logistique à la maintenance. L'amélioration continue du réseau est essentielle pour assurer un fonctionnement viable des services du réseau et pour garantir la satisfaction des utilisateurs finaux. La stratégie d'assurance fournit des mesures correctives et préventives destinées à empêcher la récurrence des problèmes liés au fonctionnement du réseau.

5 Applications de la méthodologie de sûreté de fonctionnement d'un réseau

5.1 Processus du cycle de vie d'un réseau

5.1.1 Applications du processus de cycle de vie

Les applications du processus de cycle de vie d'un réseau impliquent une série d'activités de sûreté de fonctionnement destinées à atteindre les objectifs fixés en matière de performance. Les étapes du cycle de vie d'un réseau comprennent les étapes de concept/définition, de conception/développement, de réalisation/intégration, de fonctionnement/maintenance, d'amélioration/renouvellement, et de retrait. Les méthodes d'application pertinentes pour l'analyse et l'évaluation de la sûreté de fonctionnement d'un réseau sont identifiées. L'objectif est de s'assurer que les exigences de sûreté de fonctionnement du réseau sont satisfaites grâce à l'application judicieuse de méthodes appropriées d'assurance des performances de sûreté de fonctionnement, permettant d'obtenir la sûreté de fonctionnement requise du service.

Les réseaux individuels présentent des différences liées aux conditions aux limites et aux conditions de service. Il convient d'établir le scénario opérationnel d'un réseau applicable à la fourniture de services essentiels de réseau. Il convient de définir des méthodes d'analyse et

d'évaluation pertinentes au cours de la phase d'étude de conception afin d'améliorer les performances de sûreté de fonctionnement. Ce processus contribue à garantir l'obtention de la sûreté de fonctionnement du service du point de vue des services du réseau et de la satisfaction de l'utilisateur. L'approche technique et les flux de processus sont décrits ici dans le but de faciliter les applications de la méthodologie. Il convient de définir des exigences d'entrée et de sortie pertinentes pour l'analyse des services du réseau. Il convient qu'une réponse opportune, en termes de collecte de données, d'analyse et d'interprétation des résultats d'évaluation, et d'appréciation des risques dans le cadre du processus de vérification de la sûreté de fonctionnement, constitue la base sur laquelle il convient de se fonder pour recommander l'amélioration de la sûreté de fonctionnement d'un réseau.

5.1.2 Applications du processus d'appréciation des risques

L'appréciation des risques [5, 6] est le processus global d'identification des risques, d'analyse des risques et d'évaluation des risques. Une appréciation des risques permet de comprendre l'implication des risques ainsi que les causes et les conséquences des risques, lesquelles constituent des données d'entrée utiles pour la prise de décision au cours des étapes du cycle de vie d'un projet de réseau. Les informations obtenues lors d'un processus d'appréciation des risques peuvent contribuer de manière significative aux prises de décisions importantes concernant une activité commerciale ou un projet, y compris lors de l'exécution d'engagements majeurs en termes de ressources. Les informations sont utilisées pour étayer l'analyse de l'impact sur l'activité associée aux risques et aux avantages. Il convient d'effectuer une analyse de l'impact sur l'activité conjointement à l'analyse du scenario de service pour traiter les risques d'investissement et les plans de restauration pour prévenir les pertes ou dommages potentiels des fonctions critiques du réseau.

Les activités d'ingénierie de sûreté de fonctionnement spécifiques à un projet impliquent souvent l'application de lois de probabilités et d'analyses statistiques. Les risques associés à ces activités liées au projet nécessitent l'utilisation appropriée de techniques d'appréciation des risques pour tenir compte des avantages potentiels ou des conséquences négatives probables engendrés par les applications du projet, les influences sur l'activité et les problèmes techniques rencontrés lorsque l'on traite des incertitudes. Le processus d'appréciation des risques présente une approche fondée sur la preuve pour déterminer l'étendue de l'exposition aux risques. Il convient de fonder l'appréciation des risques sur des données pertinentes et sur l'expérience pratique.

Le processus d'appréciation des risques implique :

- la prise en compte des effets positifs et négatifs potentiels sur le risque identifié,
- la compréhension des sources, des causes et des conséquences des risques ainsi que la probabilité pour que les conséquences aient lieu,
- la décision concernant l'importance du risque, s'il se situe dans les limites des critères de risques spécifiés.

Une fois l'appréciation des risques achevée, une décision peut être prise concernant la manière de traiter les risques. Le traitement des risques implique le choix et l'approbation d'une ou de plusieurs options pertinentes pour modifier la probabilité d'occurrence, l'effet des risques et la mise en œuvre des options. Parmi les exemples, il est possible de citer celui qui consiste à éviter un risque en ne comprenant pas l'activité, celui qui consiste à accepter un risque sans engager aucune action, ou celui de modifier le niveau d'un risque. Des décisions peuvent être également prises à propos du maintien du risque ou de son partage avec une autre partie par le biais d'un contrat ou d'une assurance.

Les types de techniques d'appréciation des risques [6] applicables aux activités d'ingénierie de la sûreté de fonctionnement sont regroupés de la manière suivante:

- analyse de scénario – exemples: analyse des causes profondes, analyse par arbre de pannes, analyse par arbre d'événements, analyse de l'impact sur l'activité, analyse des causes et des effets, analyse des causes et des conséquences;

- analyse fonctionnelle – exemples: AMDEC [7], Maintenance basée sur la fiabilité [8], HAZOP [9];
- méthodes statistiques – exemples: simulation de Monte-Carlo [10], analyse de Markov [11].

Les techniques d'appréciation des risques mentionnées ci-dessus sont des méthodes normalisées établies recommandées pour les applications de sûreté de fonctionnement [10]. Des descriptions détaillées de ces techniques d'appréciation des risques sont fournies en [6] et [10]. Elles ne sont pas élaborées dans la présente norme.

5.1.3 Applications de la méthodologie de sûreté de fonctionnement

Les applications de la méthodologie de sûreté de fonctionnement présentent deux aspects principaux associés au cycle de vie d'un réseau.

a) Evaluation de la sûreté de fonctionnement d'un réseau

L'évaluation de la sûreté de fonctionnement d'un réseau est l'application de techniques d'analyse, d'essai, de vérification et d'évaluation pour le développement d'un réseau. Les techniques d'évaluation sont utilisées au cours des étapes initiales du cycle de vie d'un réseau lors des phases de concept/définition, conception/développement et réalisation/intégration. Les objectifs de l'évaluation concernent surtout la satisfaction des exigences relatives des performances de sûreté de fonctionnement d'un réseau avant la mise en place du réseau pour le fonctionnement et la fourniture de services. Certaines des méthodes d'évaluation, telles que le système de compte-rendu et d'analyse des défaillances et de mise en rendu des défaillances et de mise en œuvre d'actions correctives (FRACAS) et l'évaluation des risques, sont les processus essentiels d'analyse et d'appréciation mis en œuvre pour faciliter la collecte d'informations relatives au réseau afin de refléter les tendances de performances de sûreté de fonctionnement dans l'exploitation/maintenance du réseau et de soutenir les décisions concernant l'amélioration/rénovation du réseau. Les applications de la méthodologie d'évaluation de la sûreté de fonctionnement sont décrites en 5.3.

b) Assurance de la sûreté de fonctionnement d'un réseau

L'assurance de la sûreté de fonctionnement d'un réseau correspond aux approches et processus mis en œuvre au cours des étapes d'exploitation/maintenance et d'amélioration/rénovation du cycle de vie d'un réseau. Les objectifs d'assurance se concentrent surtout sur des problèmes spécifiques liés aux performances de sûreté de fonctionnement et devant être résolus au cours de l'exploitation du réseau. Le but est d'améliorer et de soutenir la performance et les services du réseau. Les activités liées à l'assurance sont associées à la gestion de la performance du réseau, aux systèmes de gestion des pannes et aux activités de maintenance de routine et de soutien logistique du réseau pour contribuer de façon spécifique à l'ingénierie de sûreté du fonctionnement. Les applications de la méthodologie d'assurance de la sûreté de fonctionnement et les approches techniques sont décrites en 5.4.

Le Tableau 1 présente l'alignement des méthodes d'application par rapport aux principales activités liées à la sûreté de fonctionnement applicables à chaque étape du cycle de vie du réseau.

Tableau 1 – Récapitulatif des activités liées à la sûreté de fonctionnement et des méthodes d'application

Etapes du cycle de vie d'un réseau	Activités liées à la sûreté de fonctionnement d'un réseau (ND)	Méthodes d'application types
Concept/définition	• Analyse des exigences relatives à la sûreté de fonctionnement d'un réseau (ND)	• Analyse des scénarios de services • Analyse de l'impact sur l'activité commerciale
Conception/développement	• Répartition de la fiabilité d'un réseau • Prévision de la sûreté de fonctionnement (ND) • Analyse et évaluation de la conception de la sûreté de fonctionnement (ND)	• Modélisation du réseau (BDF, BLS et simulation) • NFMECA (AMDEC réseau) • FRACAS • Analyse des causes profondes • Analyse des causes et des effets
Réalisation/intégration	• Essais des fonctionnalités ND • Développement de tests élémentaires ND • Validation de conformité de services ND	• NFIT (Vérification par insertion de défauts sur le réseau) • FRACAS (Système de compte-rendu et d'analyse des défaillances et de mise en rendu des défaillances et de mise en œuvre d'actions correctives) • Analyse des causes et des effets
Exploitation/maintenance	• Evaluation des performances de ND • Gestion des pannes et comptes-rendus d'incidents ND • Dossiers de maintenance ND	• FRACAS (Système de compte-rendu et d'analyse des défaillances et de mise en rendu des défaillances et de mise en œuvre d'actions correctives) • Vérification de l'état général du réseau • Contrôle de la fréquence d'interruption du réseau • Gestion des tests élémentaires • Maintenance basée sur la fiabilité • Etudes HAZOP
Amélioration/rénovation	• Analyse des exigences relatives aux services améliorés/rénovés • Evaluation de la sûreté de fonctionnement des services améliorés/rénovés	• Analyse des scénarios de services (y compris la prise en considération des services du système existant) • Vérification de l'état général du réseau • Contrôle de la fréquence d'interruption du réseau • Gestion des tests élémentaires • Analyse de l'impact sur l'activité commerciale • Analyse des causes et des effets
Retrait	• Notification aux utilisateurs de l'interruption de services du réseau • Mise au rebut des équipements obsolètes	• Analyse des causes et des conséquences • Analyse de l'impact sur l'activité commerciale

5.2 Les performances de sûreté de fonctionnement d'un réseau

Les méthodes d'application mentionnées dans le Tableau 1 nécessitent l'identification de caractéristiques pertinentes de performance d'un réseau en vue de l'évaluation de sûreté de fonctionnement. Ces caractéristiques de performance reflètent la capacité de performance d'un réseau conformément aux exigences des accords sur le niveau de service et de QS pour la fourniture de services de réseau. Il convient que l'analyse des performances de sûreté de fonctionnement considère la définition de critères de défaillance d'un réseau et la détermination des paramètres d'aptitude à la sûreté de fonctionnement.

a) Détermination des critères de défaillance d'un réseau

Il convient de définir des critères de défaillance pour les services de réseau de bout en bout et de réseau avec l'ensemble de ses terminaisons afin de fournir les unités de mesure pour les paramètres d'aptitude à la fonction de sûreté d'un réseau. Les critères fournissent des mesures quantitatives pour l'évaluation des paramètres de performance en vue de déterminer l'état du fonctionnement et les conditions de défaillance des services d'un réseau. Les défaillances d'un réseau sont classées de manière à identifier les causes probables pour faciliter l'analyse des causes profondes en vue d'une amélioration de la sûreté de fonctionnement d'un réseau. Il convient de prendre en considération la probabilité d'occurrence des défaillances d'un réseau et la fréquence des incidents signalés.

Les défaillances suivantes représentent des défaillances types d'un réseau à prendre en considération.

1) Les défaillances d'un réseau liées aux installations comprennent les défaillances d'éléments individuels d'un réseau correspondant aux défaillances de nœuds et de liaisons d'un matériel ou d'un logiciel entraînant des interruptions de réseau. Un FRU (unité renvoyée du site) est un élément de réseau, tel qu'une carte de circuits imprimés ou un matériel réparable mis en place dans le cadre du fonctionnement d'un service de réseau. Le FRU est une unité renvoyée du site en raison d'une défaillance ou pour d'autres raisons en vue de son remplacement au titre d'accords relatifs aux services de réseau ou d'exigences relatives au soutien à la maintenance du réseau. L'analyse du taux de retours d'unités renvoyées du site (FRU) donne un aperçu des problèmes de défaillance critiques sur site.
2) Les défaillances d'un réseau liées au trafic englobent les défaillances correspondant à des scénarios d'exploitation liés aux variations du trafic des services du réseau et à une surcharge du trafic. Ces défaillances sont causées par les limites de l'installation et de la capacité du réseau, par le dysfonctionnement des trajets de service redondants, par la sauvegarde inappropriée des nœuds et des liaisons du réseau et par les pics soudains de trafic qui créent une situation de surcharge du réseau.
3) Les défaillances d'un réseau liées à une catastrophe correspondent à des défaillances du réseau dues à un sinistre d'origine humaine ou naturelle. Les sinistres d'origine humaine sont la conséquence de risques technologiques ou humains tels que les effondrements des structures, les incendies ou les coupures de courant. Les sinistres d'origine naturelle sont le résultat des risques naturels tels que les inondations, les séismes ou les éruptions volcaniques. Tous les sinistres affectent les personnes et les biens et causent des pertes économiques et des dommages environnementaux.
4) Les défaillances d'un réseau liées à la sécurité correspondent à des défaillances causées par la violation de mesures de sécurité en raison d'un contrôle insuffisant de la sécurité pour empêcher les intrusions telles que le piratage, les cyberattaques ou le sabotage.
5) Les défaillances d'un réseau liées à des activités planifiées correspondent à des défaillances qui ont lieu lors d'activités prévues de maintenance du réseau causées par des procédures de maintenance inadaptées ou une mise en œuvre inappropriée du processus de logistique de maintenance.
6) Les défaillances d'un réseau liées à des facteurs humains correspondent à des défaillances dues à des erreurs humaines involontaires telles que les erreurs des opérateurs à la mauvaise application des procédures de service ou à des dommages intentionnels avec destruction délibérée de la propriété.

b) Détermination des paramètres d'aptitude à la fonction de sûreté de fonctionnement d'un réseau

Le Tableau 2 récapitule les paramètres importants pour l'évaluation des caractéristiques d'aptitude à la fonction de sûreté de fonctionnement d'un réseau. Les paramètres pertinents d'aptitude à la fonction de sûreté de fonctionnement sont identifiés pour les services d'un réseau avec toutes ses terminaisons et les services d'un réseau de bout en bout. Ces paramètres de sûreté de fonctionnement reflètent les caractéristiques clés des performances de sûreté de fonctionnement et les exigences relatives à la fourniture de services d'un réseau avec toutes ses terminaisons et d'un réseau de bout en bout.

Tableau 2 – Récapitulatif des paramètres de sûreté de fonctionnement d'un réseau

Services d'un réseau avec toutes ses terminaisons: Paramètres d'aptitude à la fonction de sûreté de fonctionnement (présentant un intérêt pour les fournisseurs de services)	**Services de réseau de bout en bout: Paramètres d'aptitude à la fonction de sûreté de fonctionnement (expérience des utilisateurs finaux)**
• Disponibilité des services d'un réseau avec toutes ses terminaisons (*temps de disponibilité en pourcentage*) • Nombre d'abonnés ou d'utilisateurs concernés par une panne des services d'un réseau • Temps d'interruption du réseau (*minutes/an*) • Temps nécessaire à la détection d'une panne (*minutes*) • Temps de restauration (*minutes*) • Taux de retour d'unités FRU (*nombre/mois*)	• Disponibilité des services d'un réseau de bout en bout (*temps de disponibilité en pourcentage*) • Temps d'interruption des trajets de services (*minutes/an*) • Accès défaillant aux services (*fréquence/an*) • Accès retardé aux services (*fréquence/an*) • Déconnexion prématurée des services (*fréquence/an*) • Retard des supports de services (*minutes/an*)

5.3 Méthodologie d'évaluation de la sûreté de fonctionnement d'un réseau

5.3.1 Techniques d'analyse et d'évaluation génériques de la sûreté de fonctionnement

L'évaluation de la sûreté de fonctionnement implique à la fois l'analyse et l'évaluation et elle est souvent réalisée sur une base itérative. Les techniques d'analyse et d'évaluation génériques de la sûreté de fonctionnement fournissent une vaste gamme de méthodes pour les applications de sûreté de fonctionnement des réseaux. Bon nombre de ces techniques classiques d'évaluation de la fiabilité sont utilisées au cours du cycle de vie d'un réseau pour l'analyse de la sûreté de fonctionnement des éléments d'un réseau et des opérations de performance des services. Des exemples tels que l'analyse des modes de défaillance, de leurs effets et de leur criticité [7], l'analyse par bloc-diagramme de fiabilité [4], l'analyse de Markov [11], et les méthodes d'ingénierie de la fiabilité des logiciels [12], constituent la base de l'évaluation de la sûreté de fonctionnement d'un réseau. Toutefois, il convient de noter que les techniques classiques d'évaluation de fiabilité ont une étendue limitée d'applications. Spécifiquement, les méthodes existantes d'analyse de la sûreté de fonctionnement sont souvent inadéquates pour la modélisation d'une topologie de réseau complexe et sont difficiles à appliquer pour l'analyse de multiples configurations de réseau. De nouvelles méthodes, plus adaptatives aux systèmes de trajets dynamiques des services de réseaux de communication, sont introduites pour l'application de sûreté de fonctionnement.

Les méthodes d'application suivantes, mentionnées au Tableau 1, fournissent la méthodologie et les processus recommandés pour l'évaluation des performances de sûreté de fonctionnement et pour l'appréciation de la sûreté de fonctionnement des services.

5.3.2 Analyse des scénarios de services

a) Description et objet

L'analyse des scénarios de services est une méthode d'application permettant l'identification du profil opérationnel et l'analyse des exigences relatives aux services. Le

but est de déterminer la topologie et les fonctions de service du réseau pour l'évaluation de la sûreté de fonctionnement à propos de la fourniture de services de réseau planifiés. La méthode d'application facilite la traduction des besoins en services de l'utilisateur obtenus par le biais de diverses sources commerciales, en exigences techniques dans le processus d'analyse des exigences relatives à la sûreté de fonctionnement du réseau. L'analyse de l'impact sur l'activité est réalisée conjointement avec l'analyse de scénario applicable pour évaluer les expositions potentielles aux risques et déterminer les actions appropriées pour les besoins du plan de restauration.

b) Critères de sélection et utilisation opportune de la méthode

- Nouvelles exigences pour les services, modification d'exigences non connues ou existantes.
- Nécessité d'améliorer le profil opérationnel existant pour fournir des caractéristiques de services compétitives.
- Nécessité de définir des exigences relatives aux ressources afin de répondre aux besoins d'exploitation et de croissance du réseau.
- Une analyse des scénarios des services est utilisée pour planifier les besoins initiaux en services des utilisateurs et pour déterminer les besoins ultérieurs en services lorsque les exigences relatives aux services ont été modifiées ou que des nouvelles exigences ont été identifiées.

c) Procédures d'application

- Identifier la topologie appropriée du réseau pour satisfaire aux besoins en matière de services. Les réseaux se présentent sous différentes formes topologiques et décrivent le trajet actif de transport de services sur le réseau ainsi que les trajets de secours et les mécanismes de protection pour faciliter l'accès et le transport de services.
- Identifier les fonctions de service telles que les fonctions de voix, de données et de vidéo pour la fourniture des services de réseau.
- Déterminer l'utilisation des fonctions de service et leurs exigences en matière de performance.
- Déterminer le profil d'utilisation reflétant la fréquence, le moment et la durée d'accès aux sessions de communication.
- Déterminer l'impact sur l'activité et le besoin de plan de restauration approprié.

d) Exigences relatives aux données

Options de topologie, autres trajets de services, emplacement des mécanismes de protection des points d'accès.

e) Interprétation des résultats

Présentation des informations essentielles sur le profil opérationnel des services de réseau, les risques et les avantages et la saisie des données pour la modélisation du réseau et le développement d'exigences relatives à la sûreté de fonctionnement.

5.3.3 Modélisation du réseau

a) Description et objet

La modélisation du réseau est une méthode d'application permettant de créer des représentations par des symboles graphiques des nœuds et des liaisons du réseau et des interconnexions pour établir une configuration de réseau. Le but est de déterminer des trajets appropriés de services de réseau pour les connexions de services utilisateurs. La procédure d'application facilite l'identification des nœuds et des liaisons pertinents du réseau ainsi que celle des mécanismes de protection associés impliqués dans un flux de service spécifique pour l'évaluation de la sûreté de fonctionnement des services de réseau de bout en bout. La modélisation d'un réseau permet de sélectionner d'autres trajets de services pour l'analyse et l'évaluation de la sûreté de fonctionnement afin d'obtenir un trajet optimal. Le réseau de services de bout en bout est un réseau de communication destiné à la fourniture de services. L'Annexe A décrit la méthode BLS spécifiquement développée pour l'application de sûreté de fonctionnement des services de bout en bout.

Pour un réseau avec toutes ses terminaisons, l'application de modélisation crée les nœuds et les liaisons de l'ensemble du réseau pour établir la configuration du réseau en vue de l'évaluation des performances de sûreté de fonctionnement. Le but est de déterminer la performance globale de disponibilité du réseau pour refléter l'aptitude et la capacité du réseau à garantir la performance globale du réseau pour satisfaire aux exigences des accords sur le niveau de service et de qualité de service. Les techniques génériques de modélisation comprennent, mais sans toutefois s'y limiter, le BDF, l'analyse de Markov, la simulation de système et l'analyse de réseau complexe. Un réseau avec toutes ses terminaisons est considéré comme une extension du concept du système lorsqu'un processus de modélisation similaire s'applique. L'Annexe B fournit un exemple d'évaluation d'un réseau avec toutes ses terminaisons.

b) Critères de sélection et utilisation opportune de la méthode

- Nécessité de définir un cadre pour l'analyse et l'évaluation du réseau.
- Nécessité d'identifier des éléments critiques du réseau pour la configuration du réseau.
- Nécessité de quantifier la disponibilité du réseau et de fixer des limites d'interruption de services.
- La modélisation de réseau est utilisée lorsque la topologie du réseau et les systèmes de trajets doivent être établis, modifiés ou prévus d'être modifiés à des fins de planification de services.

c) Procédures d'application

- Créer les nœuds, les liens et les interconnexions du réseau en se fondant sur la topologie du réseau pour définir la configuration du réseau.
- Identifier les fonctions de service associées aux trajets de services.
- Choisir un trajet de service approprié et identifier les nœuds et les liens du réseau ainsi que les mécanismes de protection associés impliqués dans le flux de service.
- Analyser chaque trajet de service afin de déterminer la performance en matière de fiabilité et de disponibilité des services de bout en bout pour la fourniture de fonctions de service.
- Optimiser la configuration des services du réseau pour garantir la sûreté de fonctionnement des services de bout en bout en déterminant le trajet de service principal et les trajets de service de secours.
- Pour la modélisation d'un réseau avec toutes ses terminaisons, il convient d'identifier, d'examiner et d'apprécier l'évaluation des caractéristiques pertinentes de fiabilité, de maintenabilité, d'aptitude de soutien logistique à la maintenance et de capacité de restauration des nœuds et des liaisons du réseau. Il convient d'analyser la disponibilité de la configuration de l'ensemble du réseau pour déterminer le temps d'interruption total par an pour un fonctionnement continu du réseau.

d) Exigences relatives aux données

Les caractéristiques de sûreté de fonctionnement de chaque trajet de service sélectionné, la fiabilité des nœuds, des liaisons et des mécanismes de protection associés, la disponibilité des trajets de services et le temps d'interruption des trajets de services.

e) Interprétation des résultats

L'application de la modélisation d'un réseau constitue la base pour le développement des exigences relatives à la sûreté de fonctionnement du réseau. Elle permet la répartition de la fiabilité du réseau, la prévision de la sûreté de fonctionnement du réseau, l'analyse et l'évaluation de la conception ainsi que l'évaluation de la sûreté de fonctionnement des services de bout en bout.

5.3.4 Analyse des modes de défaillance des réseaux, de leurs effets et de leur criticité

a) Description et objet

L'AMDEC réseau est une méthode d'application adoptée à partir du processus AMDE (analyse des modes de défaillance et de leurs effets) classique pour l'analyse et l'évaluation des éléments et des fonctions de service d'un réseau. Le but est d'identifier

les modes de défaillances critiques dans les nœuds et les liaisons d'un réseau en vue de déterminer les effets des défaillances sur les fonctions de service du niveau supérieur suivant. L'AMDEC réseau évalue la criticité des défaillances potentielles susceptibles d'avoir un impact sur les performances de sûreté de fonctionnement et d'affecter les services de l'utilisateur. Il convient d'envisager d'autres méthodes, telles que l'analyse par arbre de pannes et le réseau de Pétri, en complément de la méthode AMDEC réseau pour l'analyse d'un réseau plus complexe.

b) Critères de sélection et utilisation opportune de la méthode

- La configuration du réseau est établie et les informations détaillées sur les éléments de réseau sont disponibles.
- Nécessité d'une évaluation quantitative et qualitative des effets causaux pour déterminer la criticité de l'impact sur le service.
- Nécessité d'identifier des éléments critiques du réseau en vue d'une amélioration de la fiabilité.
- Nécessité d'appuyer les décisions pour l'intégration au réseau d'une conception redondante ou de tolérance aux pannes.
- L'AMDEC réseau est utilisée lorsque des impacts sur des services critiques sont décelés ou prévus.

c) Procédure d'application

- Utiliser les informations concernant la topologie du réseau pour identifier les nœuds et les liens du réseau pour les trajets de services au niveau de chaque couche réseau en vue de l'analyse des modes de défaillance.
- Identifier les modes de défaillance respectifs associés à chaque nœud (par exemple, surcharge) et à chaque liaison (par exemple, interruption d'interface) à partir de la base de données disponible dans un référentiel de données réseau. Les données relatives aux défaillances reflètent les niveaux de satisfaction des utilisateurs du service, tel que l'accessibilité, la continuité du service et la libération du service.
- Déterminer les effets des défaillances sur le service résultant provoquant des temps d'interruption; tels que le temps d'interruption des trajets de services, le temps d'interruption du réseau et le temps d'interruption d'un réseau de transmission.
- Déterminer la criticité résultante de la défaillance et évaluer l'impact sur le service d'un réseau de bout en bout (E2E).

d) Exigences relatives aux données

Les données relatives aux précédentes défaillances du réseau, recueillies pour les modes de défaillances et de leurs effets et enregistrées dans le référentiel des données relatives au réseau.

e) Interprétation des résultats

Les résultats de l'AMDEC réseau peuvent servir de données d'entrée pour la mise à jour de l'évaluation de la sûreté de fonctionnement du réseau en termes de durée des interruptions et de prestation de maintenance. Les résultats de l'AMDEC réseau sont également utilisés pour le développement de tests élémentaires pour la vérification par insertion de défauts sur le réseau (NFIT).

5.3.5 Vérification par insertion de défauts sur le réseau

a) Description et objet

La vérification par insertion de défauts sur le réseau (NFIT) est une méthode d'application destinée à vérifier l'effet des défaillances d'un réseau par insertion volontaire de défauts en vue de vérifier les conséquences des résultats. Le but est de vérifier l'efficacité des conceptions redondantes, des mécanismes de protection et la capacité globale du réseau à gérer les pannes.

b) Critères de sélection et utilisation opportune de la méthode

- Criticité de la panne, connue et préoccupante.
- L'emplacement probable de la panne est identifié.

- Nécessité de déterminer la criticité de l'impact de la panne sur le fonctionnement des services du réseau.
- Nécessité de vérifier la fréquence d'occurrence des pannes.
- Utilisation de la méthode NFIT s'il est avéré que les impacts sur les services critiques ont été décelés et qu'ils nécessitent une vérification par des tests élémentaires.

c) Procédure d'application

- Identifier l'objet de la vérification par insertion de défauts sur le réseau (NFIT) du test élémentaire planifié.
- Déterminer la méthode d'insertion de défaut au niveau d'une couche d'essai cible. Des couches OSI différentes [13] présentent des types de défauts différents (voir l'Article A.4).
- Exécuter le test élémentaire. Observer tous les éléments de réseau et trajets de service concernés pendant l'essai. Déterminer le domaine d'application et l'étendue de l'impact d'un défaut. Enregistrer les résultats d'essai.

d) Exigences relatives aux données

Enregistrements d'essai et observation.

e) Interprétation des résultats

Evaluer 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. Fournir des informations sur l'efficacité des tests élémentaires, le taux de couverture des pannes et l'efficacité de la gestion des pannes du réseau.

5.3.6 Système de compte-rendu et d'analyse des défaillances et de mise en œuvre d'actions correctives

a) Description et objet

Le système de compte-rendu et d'analyse des défaillances et de mise en œuvre d'actions correctives (FRACAS) est une méthode d'application permettant de recueillir des données pertinentes sur le compte-rendu d'incidents et les actions de maintenance, le diagnostic et les résultats d'analyse en vue de recommander des actions correctives. Le but est de formaliser une base de données de référence pour recueillir et archiver l'historique d'aptitude à la fonction de sûreté de fonctionnement en vue de l'amélioration de la conception et des services du réseau.

b) Critères de sélection et utilisation opportune de la méthode

- Une base de données d'information sur les défaillances est constituée.
- Une procédure de compte-rendu de défaillances est établie.
- Nécessité de recueillir des données sur l'historique des défaillances afin de définir les tendances des performances de sûreté de fonctionnement.
- Nécessité d'appuyer les décisions concernant l'amélioration de la conception du réseau et des procédures.
- La méthode FRACAS est utilisée pendant toute la durée vie du réseau afin de disposer d'une base de données de référence crédible en vue de la traçabilité de l'historique enregistré de performance du réseau.

c) Procédure d'application

- Identifier les informations relatives à la défaillance et établir le compte-rendu d'incident en vue de leur intégration dans le système FRACAS.
- Classer les comptes rendus d'incidents en vue d'une action fondée sur des critères définis de services de maintenance, tels que maintenance d'urgence, de routine ou planifiée pour la mise en œuvre lors d'une mise à jour ultérieure.
- Analyser et évaluer la criticité des problèmes liés aux défaillances majeures affectant le fonctionnement des services et fournir des solutions recommandées telles que modification de la conception, remplacement d'équipements ou gestion de contrôle de configuration.

– Mettre en œuvre la recommandation pour la résolution du problème.

– Enregistrer et contrôler l'état du système FRACAS pour l'amélioration continue.

Le système FRACAS est habituellement automatisé pour faciliter la mise à jour des données, les actions de suivi et les améliorations de processus.

d) Exigences relatives aux données

Assurer un classement des données relatives aux défaillances et la maintenance de la base de données.

e) Interprétation des résultats

Déterminer les tendances d'aptitude à la fonction de sûreté de fonctionnement du réseau et établir l'historique des actions d'amélioration.

L'Annexe C traite de l'évaluation des performances de sûreté de fonctionnement des systèmes installés sur site. Elle illustre un exemple de classement des défaillances types d'un réseau public à commutation pour l'évaluation de la sûreté de fonctionnement.

5.4 Méthodologie d'assurance de la sûreté de fonctionnement d'un réseau

5.4.1 Etendue des applications de la méthodologie d'assurance de la sûreté de fonctionnement

L'étendue des applications de la méthodologie d'assurance de la sûreté de fonctionnement couvre les trois domaines techniques stratégiques définis en 4.5. L'application se concentre tout particulièrement sur les activités d'assurance dans l'exploitation d'un réseau du point de vue de la sûreté de fonctionnement. Le processus de vérification de la sûreté de fonctionnement du réseau fait un usage extensif des processus définis de gestion du réseau afin de fournir des approches pratiques pour prendre en charge la gestion de la performance du réseau, la gestion des pannes du réseau ainsi que la qualité des services. Le but est d'améliorer et de soutenir les performances de sûreté de fonctionnement au cours de l'exploitation du réseau.

Les méthodologies d'assurance sont les approches techniques recommandées fondées sur les pratiques dans le domaine pour assurer de manière durable les performances de sûreté de fonctionnement au cours de l'exploitation du réseau et la satisfaction, dans les délais impartis, des besoins en matière de sûreté de fonctionnement des services du réseau. Il est de la responsabilité des opérateurs de réseau et des fournisseurs de services d'assurer la qualité de fonctionnement du réseau et des services ainsi que la satisfaction des besoins des utilisateurs. L'assurance de la sûreté de fonctionnement dans des conditions normales et d'urgence de fonctionnement du réseau a pour objectif principal de garantir la sûreté de fonctionnement du service aux utilisateurs finaux du réseau dans la contribution à la qualité de service. La sécurité de service contribuant à la qualité de service complète les activités d'assurance de la sûreté de fonctionnement. Les performances de sûreté de fonctionnement, obtenue lors de la conception du réseau et la mise en œuvre des services pour la fourniture des services essentiels du réseau, peut avoir une incidence sur la sécurité de fonctionnement du réseau.

Les méthodologies d'assurance de la sûreté de fonctionnement du réseau sont regroupées par domaines d'applications techniques afin qu'elles soient en phase avec les stratégies d'assurance de la sûreté de fonctionnement. Les méthodologies d'assurance présentées ici constituent des exemples types rencontrés dans l'assurance de services de réseau au cours de l'exploitation du réseau, tels que la vérification de l'état général du réseau et le contrôle de la fréquence d'interruption du réseau. Les systèmes de gestion des pannes du réseau sont utilisés pour soutenir les grands réseaux lors de l'identification des pannes, la collecte de données et l'analyse de la tendance des performances de sûreté de fonctionnement. Les paragraphes ci-dessous décrivent les approches techniques pour traiter des questions liées à l'assurance de la sûreté de fonctionnement.

5.4.2 Assurance de la sûreté de fonctionnement du service

a) Objectif

Garantir la sûreté de fonctionnement du trajet d'un service de réseau pour le transfert d'informations et le flux de données.

b) Description des applications de la méthodologie

1) Le trajet de service de réseau est un mécanisme de fourniture pour le transfert d'informations. Il convient d'intégrer les nœuds et les liens du réseau associés au trajet de service avec des dispositifs de protection appropriés pour garantir la réussite du transfert d'informations et le réacheminement vers des trajets de services de secours en cas de dysfonctionnement du trajet principal du service. Il convient de prédéterminer la priorité de la sélection des trajets de services. Il existe plusieurs schémas de sélection des trajets adaptés aux conceptions de réseaux qui intègrent des dispositifs de protection tels que des trajets redondants actifs ou de secours, un vote majoritaire et des techniques de vote prioritaire. L'analyse de la fiabilité du dispositif de protection est indispensable pour déterminer l'application appropriée. L'évaluation des risques liés au trajet protégé de service de réseau est nécessaire pour évaluer l'impact d'un dysfonctionnement ainsi que les effets et les conséquences qui en résultent.

2) L'aptitude à l'emploi du réseau reflète la capacité à délivrer la sûreté de fonctionnement du service aux utilisateurs finaux. Les facteurs contribuant à l'aptitude à l'emploi comprennent l'accessibilité du service à l'utilisateur final, la continuité du service et la libération du service concernant l'établissement et la réalisation ou le début et la fin d'une session de communication. Les délais d'accès se rapportent à l'inaptitude à établir des connexions de réseau pour diverses raisons liées à la connectivité. La stabilité de la continuité du service est influencée par la capacité du réseau et aux conditions de flux de trafic durant la communication. L'échec de la libération du service conduirait à un gaspillage des ressources disponibles du réseau et à l'apparition d'erreurs de facturation pour les abonnés ou les utilisateurs. L'efficacité de l'aptitude au service du réseau repose sur les performances de sûreté de fonctionnement du réseau ainsi qu'à la fiabilité, à la vitesse et à la précision de la libération du réseau. Il convient que la planification du réseau traite des questions d'aptitude au service du point de vue des performances de sûreté de fonctionnement afin d'optimiser l'utilisation des ressources du réseau.

5.4.3 Assurance d'intégrité des données

a) Objectif

Garantir l'intégrité du flux de données ainsi que la protection de la sécurité des données.

b) Description des applications de la méthodologie

1) L'intégrité des données 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. Elle dépend également des mécanismes utilisés pour vérifier la justesse et l'authenticité des entrées et des sorties de données. La caractéristique d'intégrité des performances de sûreté de fonctionnement est l'aptitude du réseau à assurer le passage des données en toute sécurité de manière à protéger le contenu des données. L'intégrité reflète le processus de vérification des fonctions de service du réseau pour s'assurer que le contenu des données n'est pas contaminé, corrompu ou altéré lorsque les entrées sont transformées en sorties.

2) Il existe de nombreuses méthodes utilisées pour la gestion des informations sécurisées et la préservation de l'intégrité des données. Leur application dépend des exigences spécifiques concernant le système de gestion de l'information, l'intégrité des données et le niveau des besoins de sécurité, la capacité de recherche de données et la vitesse de récupération des données, l'efficacité de la technologie déployée et le coût de mise en œuvre en tant que partie du processus de vérification du réseau. Les approches d'intégrité et de protection de sécurité des données dans la mise en œuvre sont définies dans la CEI 61907. Des exemples de conservation des données comprennent la sauvegarde et la duplication des données, le stockage des données dans différents endroits et la réplication des données dans différents formats. Des exemples de protection de sécurité des données 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.

5.4.4 Assurance des fonctions de performance d'un réseau et amélioration des processus de soutien

a) Objectif

Assurer les fonctions de performance d'un réseau et l'amélioration des processus de soutien.

b) Description des applications de la méthodologie

1) La méthodologie applicable pour l'assurance de la sûreté de fonctionnement utilise des processus définis dans la gestion du réseau pour atteindre diverses tâches liées aux performances de sûreté du fonctionnement associées à la planification, aux mesures et à l'optimisation des performances du réseau. Les activités de sûreté de fonctionnement sont impliquées dans l'identification et la résolution de problèmes de performance du réseau de nature temporelle, tels que les temps d'attente et les retards concernant la fourniture et la reconnaissance des trames, la perte de paquets, la retransmission, et le mesurage du flux de trafic. L'objectif de la fonction d'assurance est de vérifier la capacité des trajets de trafic en ce qui concerne la vitesse, la fiabilité et la capacité de la conception et de la configuration du réseau pour une utilisation optimale des ressources et la maîtrise des encombrements.

2) La méthodologie applicable d'assurance de la sûreté de fonctionnement utilise les processus établis dans la gestion des défaillances du réseau pour détecter, isoler et corriger les dysfonctionnements du réseau, compenser les modifications d'environnement et soutenir les activités de maintenance et de diagnostic. La fonction d'assurance a pour but de fournir un diagnostic correct des pannes du réseau, d'enrichir la base de données et de tenir à jour les enregistrements relatifs à la performance du réseau et de se servir de la source des données de pannes pour recommander l'amélioration des services de soutien du réseau.

3) La méthodologie applicable d'assurance de la sûreté de fonctionnement utilise les processus établis dans les programmes de poursuite en champ, la maintenance et le support logistique, ainsi que les bases de données de performance pertinentes pour l'analyse et l'évaluation des classes de défaillances pour déterminer les durées d'interruption du réseau ainsi que la fréquence d'interruption du réseau. Les données pertinentes sont utilisées pour établir les contributions aux interruptions par rapport aux causes des défaillances et leur impact sur les utilisateurs finaux utilisant les services de réseau. L'objectif de l'assurance est de garantir l'évaluation correcte des tendances de performance du réseau, la satisfaction du client et la qualité de service (QS).

5.4.5 Méthodes d'assurance de la sécurité de fonctionnement d'un réseau

a) Vérification de l'état de santé du réseau

La vérification de l'état général du réseau est une méthode pour contrôler et maîtriser l'adéquation et l'efficacité de la résolution de problèmes posés au cours du fonctionnement du réseau. Le but de cette méthode est de garantir la sûreté de fonctionnement des services fournis. La vérification de l'état général du réseau est la principale méthode pour l'assurance de la performance de sûreté de fonctionnement d'un réseau. Le processus de vérification de l'état général du réseau consiste en la vérification et le contrôle réguliers (par exemple, bihebdomadaire) des problèmes rencontrés au cours du fonctionnement du réseau, au moyen d'une série d'études de simulation du réseau sur une période donnée. Le but de ce processus est de définir une séquence de chronogrammes pour l'analyse des problèmes apparaissant dans le scénario et le profil opérationnel respectifs afin de vérifier l'état de performance du réseau en vue de garantir un bon état de fonctionnement du réseau.

Le scénario du réseau varie en permanence avec le temps en raison des diverses demandes de trafic, de l'utilisation fluctuante des services, de la topologie du réseau et de l'adaptation de la configuration, ainsi que de l'activation des mécanismes de protection pour pallier les dysfonctionnements du réseau et des trajets du réseau imposé par des limites de capacité. La méthode de vérification de l'état général du réseau est utilisée

conjointement avec le système de gestion des pannes et la base de données FRACAS pour un fonctionnement continu du réseau. Le processus de vérification de l'état général du réseau implique l'analyse du scénario du réseau et le profil opérationnel pour traiter les problèmes rencontrés sur site pour soutenir les performances de sûreté de fonctionnement au cours du fonctionnement du réseau.

Les procédures de vérification de l'état général du réseau sont les suivantes:

1) identifier la topologie et la configuration actuelles du réseau pour chaque analyse de scénario;
2) identifier les problèmes rencontrés sur site et l'enregistrement des temps dans le scénario faisant l'objet du contrôle;
3) analyser les éléments essentiels du réseau impliqués dans la résolution du problème rencontré sur le site afin de soutenir le fonctionnement du réseau;
4) déterminer la sûreté de fonctionnement du réseau en termes d'aptitude à la fonction de disponibilité, de fiabilité et de besoins de soutien aux services du scénario de fonctionnement du réseau;
5) établir un fichier de configuration du réseau qui fournira des données d'entrée pour la simulation du réseau, y compris toutes les informations pertinentes de nature temporelle se rapportant au scénario et nécessaires pour la simulation;
6) évaluer les résultats de la simulation pour déterminer les performances de sûreté de fonctionnement du réseau en ce qui concerne l'efficacité et l'adéquation des systèmes de redondance des sauvegardes et de trajets pour chaque étude de scénario;
7) analyser les documents et évaluer les résultats des diverses études de scénarios dans le but d'établir une série de profils d'état général du réseau pour soutenir l'amélioration continue du fonctionnement du réseau.

Il est prudent de vérifier et de valider l'efficacité et l'adéquation du réseau quant à son aptitude à fournir des services de réseau en se fondant sur la connaissance des scénarios de fonctionnement et des problèmes rencontrés sur site.

b) Contrôle de la fréquence d'interruption du réseau

Le contrôle de la fréquence d'interruption du réseau est une méthode permettant d'identifier et de classer des problèmes rencontrés sur site, au moyen de comptes rendus d'incidents fournis par les opérateurs de réseaux et les fournisseurs de services. Le but de cette méthode est de garantir la satisfaction du client en déterminant l'état de la performance continue du réseau et son impact sur les services. L'objectif est de recueillir des données statistiques sur les interruptions du réseau et des informations sur les temps d'indisponibilité des équipements afin de vérifier la référence des performances de sûreté de fonctionnement par rapport à des étalons de comparaison reconnus dans le domaine. Le fait de disposer d'informations pertinentes concernant les interruptions du réseau devrait faciliter l'action corrective appropriée et la maîtrise de l'impact sur les services dans le fonctionnement du réseau.

Les pratiques en vigueur dans l'industrie de la communication spécifient les exigences courantes concernant la notification des problèmes rencontrés sur site. Les critères relatifs aux mesures des interruptions des éléments de réseau (par exemple, des équipements) sont établis par des normes industrielles [14, 15]. Les informations concernant l'indisponibilité des équipements du réseau sont recueillies et consignées dans le but de vérifier leur conformité aux exigences sur le niveau de service dans le cadre de la fourniture de services de réseau. Les performances de sûreté de fonctionnement d'un réseau sont influencées par les dysfonctionnements des équipements qui provoquent une interruption totale ou partielle des services. Le dysfonctionnement des équipements est susceptible de provoquer une dégradation des performances du réseau. Il peut également compromettre l'intégrité des données lors du fonctionnement du réseau. Pour le contrôle des interruptions du réseau, il est indispensable d'enregistrer les informations relatives à l'interruption affectant les services de réseau. Les données relatives à l'interruption recueillies par le biais de comptes-rendus d'incidents sont cruciales pour établir les relations causales lors de la détermination des sources de défaillances impliquées provoquant les indisponibilités des services du réseau. Les temps d'indisponibilité sont exprimés en termes de durée d'occurrence de panne. Des informations supplémentaires

sont également collectées sur la source de la panne, la fréquence des pannes et l'impact sur les nombres d'abonnés ou d'utilisateurs affectés. Les informations relatives à la panne du réseau permettent au processus de vérification du réseau de justifier et de recommander des actions correctives ou préventives pour assurer une performance durable du réseau et une amélioration continue des services.

Le système de contrôle des interruptions du réseau surveille la perte de fonctionnalité des équipements dans les systèmes de réseaux. Les informations sur les interruptions indiquent l'impact de la durée des interruptions sur les services ainsi que les mesures d'impact sur les équipements du réseau. L'objectif est de réduire les temps d'interruption ainsi que leurs coûts associés et leur impact sur les services, dans le but d'améliorer la génération de revenus et la satisfaction du client.

Les équipements d'un réseau sont classés afin de faciliter la collecte de données et l'attribution des mesures des interruptions. Les classes d'équipements d'un réseau comprennent, par exemple: les systèmes de commutation, de signalisation, de transmission ainsi que les fonctions communes.

Les mesures des interruptions d'un réseau comprennent:

1) les mesures d'impact sur les services – c'est-à-dire la fréquence des pannes et la durée des interruptions du réseau affectant la fourniture de services de réseau à un certain nombre de lignes d'abonnés en raison d'une interruption partielle ou totale de toutes les sources - ces mesures sont exprimées en minutes/ligne d'abonné/an;
2) les mesures d'impact sur les éléments (équipements) d'un réseau – c'est-à-dire la fréquence des pannes et la durée des interruptions du réseau dues à un dysfonctionnement des équipements - ces mesures ont pour but d'évaluer la disponibilité, la fiabilité et les besoins en maintenance et sont exprimées en minutes/catégorie d'équipement/an.

Les données relatives aux interruptions sont regroupées dans le but de faciliter la compilation des données statistiques sur les interruptions.

- Zone de service du réseau affectée par
  - une interruption totale, et
  - une interruption partielle.
- Cause d'interruption due à
  - une interruption imputable au fabricant des équipements ou au fournisseur de services,
  - une interruption due à une erreur de procédure,
  - une interruption due à une erreur logicielle, et
  - autres causes.

c) Maîtrise des encombrements

L'intégration d'un système de maîtrise des encombrements a pour objectif de soutenir la performance du réseau afin de garantir une fourniture continue des services de réseau. La maîtrise des encombrements implique le contrôle des entrées de trafic dans un réseau de communication. L'objectif est d'éviter un encombrement du trafic à même de provoquer un effondrement du réseau, en contrôlant et en régulant le nombre d'abonnements par rapport aux capacités de traitement ou de liaison des nœuds de réseaux intermédiaires. La méthodologie utilise des procédures de réduction des ressources telles que la réduction du débit d'envoi de paquets.

Les principaux composants d'un système générique de prévention des encombrements comprennent la mise en œuvre de dispositifs de contrôle fonctionnel pour la détection des encombrements et le retour d'informations sur les encombrements, d'un sélecteur de retour d'informations, d'un filtre de signal, d'une fonction de décision et d'algorithmes d'augmentation/réduction.

Pour prévenir la congestion et l'effondrement d'un réseau, la méthode nécessite:

– l'établissement de conditions de surcharge,

- un mécanisme dans les routeurs pour réordonner ou abandonner les paquets dans des conditions de surcharge prédéfinies, et
- des mécanismes de contrôle de flux de bout en bout prévus dans les points de terminaison pour permettre une réponse appropriée au statut de maîtrise d'encombrement.

d) Gestion des tests élémentaires

Pour gérer de sérieux problèmes rencontrés sur site lors du fonctionnement du réseau, il est parfois nécessaire de récréer le contexte du problème dans un environnement miroir en vue d'une vérification au laboratoire ou dans un bureau captif en dupliquant le fonctionnement du système et du scénario de réseau spécifique. Un test élémentaire est généré pour gérer la résolution du problème rencontré sur site. Les tests élémentaires permettent aux mécanismes de faciliter l'obtention de résultats en tant que partie du processus d'assurance.

Les tests élémentaires sont développés dans le but de simuler des conditions de fonctionnement réelles sur site dans lesquelles les zones concernées spécifiques ou les problèmes potentiels sont susceptibles d'être rencontrés. Un test élémentaire est un ensemble de données d'entrée d'essai, de conditions d'exécution et de résultats prévus, développé dans un but précis qui consiste à vérifier la conformité à une exigence spécifique. Une spécification de test élémentaire est la documentation spécifiant les entrées, identifiant les résultats de test attendus et définissant les conditions d'exécution du test.

La vérification par insertion de défauts sur le réseau (NFIT) est considérée comme une méthode appropriée pour que ces tests élémentaires soient utilisés pour traiter les problèmes rencontrés sur site.

Annexe A
(informative)

Exemple d'évaluation de la sûreté de fonctionnement d'un réseau de bout en bout (E2E)

A.1 Objectif

L'objectif de l'évaluation de la sûreté de fonctionnement d'un réseau de bout en bout (E2E) est de déterminer l'influence du trajet de service de réseau sur la sûreté de fonctionnement du service. Le résultat de l'évaluation est la performance de disponibilité ou le temps d'interruption total par an des connexions de bout en bout. La méthode BLS est présentée dans le but de démontrer les techniques utilisées pour fournir des solutions de sûreté de fonctionnement pour l'analyse des trajets de services de réseau.

A.2 Description de la topologie d'un réseau et trajets de services d'un réseau de bout en bout (E2E)

Les trajets de services d'un réseau sont déterminés à partir de la topologie du réseau. La topologie d'un réseau tient compte des éléments suivants:

- les scénarios de services et les exigences pour les services de voix, de données, de vidéo ou autres services de réseau;
- la criticité de la fourniture de services;
- les nœuds et les liens pertinents pour établir le principal trajet d'un service de bout en bout;
- les trajets de secours en cas de défaillance du trajet principal.

La Figure A.1 illustre un exemple type de topologie de réseau qui montre les nœuds et les liens de bout en bout ainsi que leurs relations dans une configuration topologique. Les symboles utilisés pour les nœuds de réseau A, I, K sont des centres de commutation; B, C, D, E sont des routeurs; et F, G, H, J sont des centres de données qui stockent les données pertinentes pour l'accès et l'authentification de l'enregistrement des données de l'utilisateur afin de faciliter les connexions de bout en bout. Les liens du réseau sont connectés entre les nœuds pour établir leurs relations. Le but du trajet de service E2E résultant est d'établir la connexion de A à J, telle qu'initiée par l'utilisateur final en A.

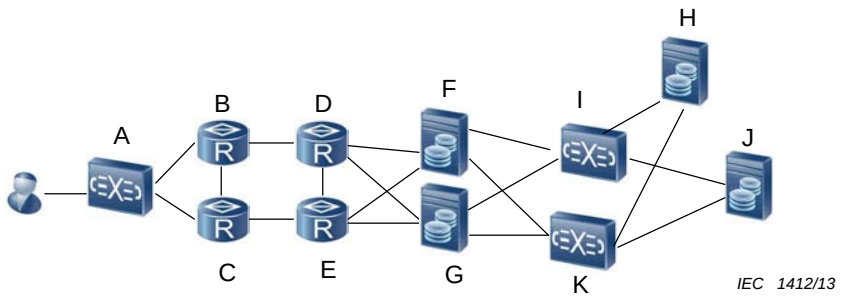


Figure A.1 – Exemple type d'une topologie de réseau de bout en bout (E2E)

Le scénario du service peut être expliqué par la séquence suivante d'activités:

- l'utilisateur final accède à A pour établir la liaison pour atteindre J;

- le principal trajet de service indiqué en trait plein «—» suit les nœuds et les liens de A-B-D-F-I-H-I-J afin d'établir la connexion;
- lorsque le flux de service atteint I, il exige une authentification par H pour permettre la poursuite du flux de service, représentant une boucle I-H-I propre aux flux d'informations en technologie des communications;
- lorsque l'autorisation est accordée par H, le flux de service poursuit son chemin de I à J pour réaliser la connexion de réseau de bout en bout (E2E). Il convient de noter que H est un nœud critique exigeant une performance d'équipements de grande fiabilité.

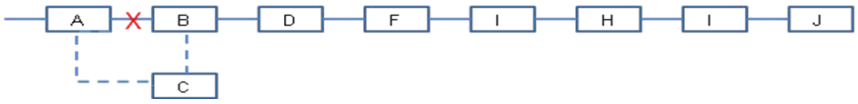
A partir de l'ensemble d'informations fourni jusque là, les trajets de secours indiqués par des pointillés «----» peuvent être établis en se fondant sur la connaissance des défaillances de nœuds et de liens indiquées par un «X» dans la configuration topologique. L'établissement de trajets de services de réseau de bout en bout (E2E) nécessite le traitement des problèmes hérités lorsque des réseaux existants interagissent avec de nouveaux réseaux pour réaliser la connexion de bout en bout (E2E). Le symbole de pointe de flèche «—>» est uniquement utilisé lorsque les BLS sont trop longs et qu'il est connecté à une nouvelle ligne de BLS pour réaliser la construction du trajet de service de réseau de bout en bout (E2E).

A.3 Construction de trajets de services de réseau de bout en bout (E2E)

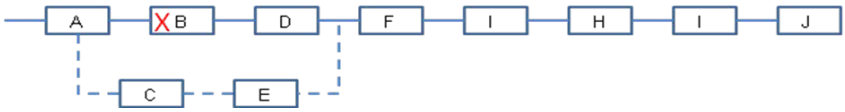
Les trajets de services de réseau de bout en bout (E2E), à commencer par les trajets principaux et les trajets de secours, sont construits à l'aide de schémas BLS, comme indiqué de a) à k).

a) Trajet de service principal

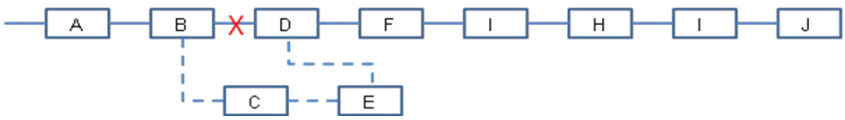
b) Trajet de service de secours avec une défaillance de la liaison entre les nœuds A et B



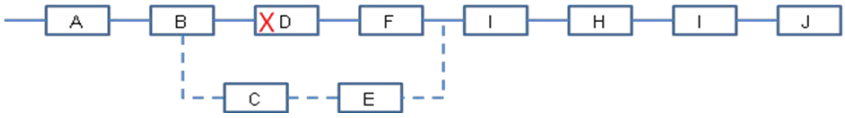
c) Trajet de service de secours avec une défaillance au niveau du nœud B



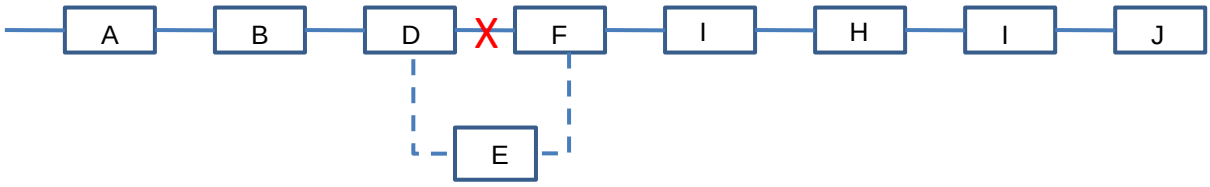
d) Trajet de service de secours avec une défaillance de la liaison entre les nœuds B et D



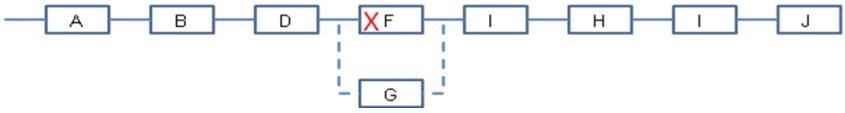
e) Trajet de service de secours avec une défaillance au niveau du nœud D



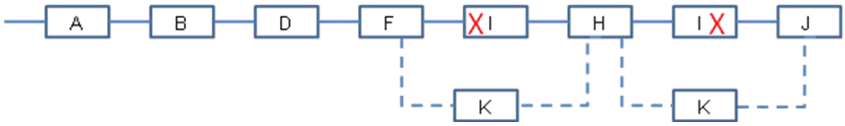
f) Trajet de service de secours avec une défaillance de la liaison entre les nœuds D et F



g) Trajet de service de secours avec une défaillance au niveau du nœud F



h) Trajet de service de secours avec une défaillance au niveau du nœud I



A partir de cet ensemble de schémas BLS, la performance de disponibilité ou le temps d'interruption total par an des trajets de services de réseau E2E combinés peut être déterminé(e) à l'aide de méthodes mathématiques standard et de données de terrain établies ou estimées pour chaque nœud et chaque lien se rapportant à la topologie du réseau de bout en bout (E2E). La réussite de la performance de disponibilité du fonctionnement de services de réseau E2E signifie que le trajet de service principal est disponible pour le fonctionnement, que tous les trajets de services de secours sont également disponibles sur demande et qu'il convient que la commutation entre trajets soit réussie selon la manière requise et au moment voulu.

Chaque trajet de service de A à H est un modèle sériel simple du BDF pour déterminer la disponibilité du trajet de A à H. La disponibilité du trajet de service de bout en bout (E2E) est déterminée par la disponibilité combinée du trajet principal et des trajets de secours.

La disponibilité du trajet de service E2E peut être déterminée à partir des contributions des interruptions comme suit:

$$A_{E2E} = 1 - \frac{DT_{E2E}}{8\,760 \times 60}$$

où

A_{E2E} est la disponibilité du trajet de service E2E;

DT_{E2E} est le temps d'interruption du trajet de service E2E, en minutes/an;

$$DT_{E2E} = \sum_i \left\{ f_i \times \left[r_i \times dt_i + (1 - r_i) \times MTTR_i \right] \right\}$$

f_i est la fréquence de défaillance du nœud/lien i dans le trajet de service principal, en nombre de fois/an;

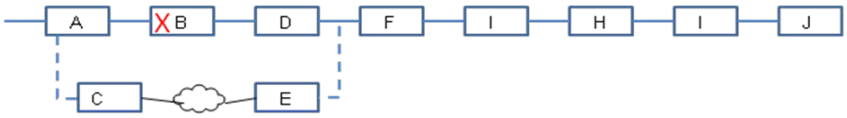
r_i est le taux de restauration, après une défaillance du réseau, du nœud/lien i dans le trajet de service principal;

dt_i interruption de service du nœud/lien i dans le trajet de service principal défaillant, mais le service est restauré avec succès;

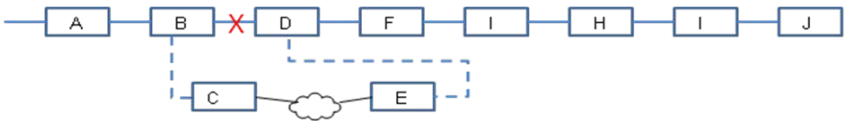
$MTTR_i$ temps moyen avant restauration du nœud/lien i dans le trajet de service principal défaillant, mais le service n'est pas restauré.

En topologie des réseaux, il arrive parfois que la configuration topologique rencontre le trajet d'un réseau complet en interaction, qui existe déjà et en exploitation. La méthode BLS peut inclure un tel réseau en interaction pour la modélisation du trajet de service d'un réseau E2E. La construction est effectuée en représentant le réseau en interaction sous la forme d'un "nuage" avec le symbole incorporé dans le trajet de service du BLS. Le "nuage" est traité comme un nœud de réseau dans la configuration topologique. Par exemple, si le routeur C doit traverser un réseau de transport pour atteindre le routeur E, les trajets de services de secours correspondants pour c), d) et e) peuvent être représentés par les schémas BLS correspondants en i), j) et k).

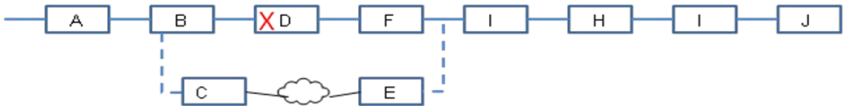
i) Trajet de service de secours à travers un "nuage" avec une défaillance au niveau du nœud B



j) Trajet de service de secours à travers un nuage avec une défaillance de la liaison entre les nœuds B et D



k) Trajet de service de secours à travers un "nuage" avec une défaillance au niveau du nœud D



La méthode BLS présente les principales fonctions d'application suivantes:

- le BLS est développé comme un outil spécifique pour la modélisation des réseaux de communication;
- le BLS est utilisé pour identifier et suivre les trajets de services E2E critiques en vue d'une analyse ultérieure;
- le BLS prend en compte le flux de service ainsi que la topologie du réseau;
- le BLS intègre une situation de bouclage pour modéliser la configuration topologique propre aux flux d'informations en technologie des communications;
- le BLS traite principalement les défaillances ponctuelles; les défaillances multipoints sont rares dans les trajets de réseaux, mais elles peuvent apparaître sous la forme d'une surcharge et d'une perturbation dans les propagations pouvant nécessiter une attention particulière au cas par cas;
- le BLS permet de réaliser d'autres études de sensibilité telles que délai de transfert, gigue, perte en temps réel et perte différée et récupération pour faciliter la planification et le choix des stratégies de protection des services de réseau;
- le BLS présente un flux logique pour une construction simple de trajets de services de réseau E2E;

- le BLS facilite la subdivision du réseau pour permettre la construction de trajets de services de réseau E2E appropriés impliqués dans des réseaux existants en interaction avec de nouveaux réseaux;
- la base de données de défaillances du BLS utilise des données de terrain ou des données estimées relatives à la performance des services de réseau E2E pour estimer les temps d'interruption;
- le BLS peut être informatisé pour faciliter l'analyse itérative des défaillances d'un réseau E2E et pour évaluer leur impact potentiel sur les performances du réseau.

A.4 Analyse des trajets de services de réseau de bout en bout (E2E)

Le principe de l'analyse des trajets de services E2E consiste à identifier le lieu de la défaillance ainsi que le type de défaillance dans le réseau étudié. Les défaillances types d'un réseau comprennent:

- les défaillances d'équipements;
- incidents affectant la performance du système OAMP;
- dysfonctionnement des installations et défaillances de l'alimentation en énergie;
- erreurs de procédures;
- surcharge de trafic;
- accidents et incidents d'ordre environnemental;
- intrusion portant atteinte à la sécurité et attaques malveillantes.

L'emplacement des défaillances des nœuds et des liens du réseau peut se situer dans n'importe quelle couche du réseau comme décrit dans le modèle de référence OSI [13]. Les points ci-dessous fournissent des exemples de quelques symptômes de défaillances probables:

- couche application: échec lors du transfert de fichiers par courrier électronique;
- couche présentation: échec lors du cryptage et de la conversion des données;
- couche session: incapacité à maintenir l'ordre de démarrage/arrêt en communication;
- couche transfert: incapacité de fournir un message;
- couche réseau: incapacité d'acheminer les données;
- couche liaison de données: incapacité de transmette des trames d'un nœud à un autre;
- couche physique: défaillance d'un équipement dans un nœud de réseau ou une liaison par câble.

A partir de ces symptômes, il est possible de tracer le nœud ou la liaison concerné(e) pour identifier les causes profondes de la défaillance. Les effets respectifs des défaillances peuvent être également définis à partir de résultats d'essais du réseau ou à partir d'observations précédentes sur le site à propos de l'étendue et de la criticité de l'impact de la défaillance sur les utilisateurs du réseau et de la fourniture des fonctions pertinentes de services de réseau. Ces données sont les plus utiles à recueillir et à stocker dans une base de données pour l'évaluation en cours et l'évaluation future de la performance OAMP.

A titre d'exemple, une défaillance du réseau entraînant une surcharge de messages et de fréquentes interruptions dans un service de réseau E2E est suivie pour vérifier la compatibilité de la version d'un protocole logiciel utilisé dans la couche application. Une fois la cause de la défaillance identifiée, le protocole est mis à jour par rapport à la version la plus récente, rétablissant ainsi le service de réseau E2E à son état de fonctionnement normal.

Le processus global d'analyse est connu sous le nom d'AMDEC réseau.

Les informations pertinentes sur la défaillance sont recueillies dans la base de données FRACAS en tant que référentiel commun pour les données relatives aux modes de défaillances et à leurs effets. La base de données FRACAS peut être utilisée efficacement comme une source de données précédentes pour le diagnostic de défaillance du réseau présentant des symptômes de défaillance similaires pour engager les actions correctives appropriées. La base de données FRACAS est un outil précieux pour soutenir la performance de disponibilité et la prévision des interruptions du réseau. Il convient que la base de données FRACAS soit reliée au système de gestion des pannes du réseau afin de faciliter le stockage de données et le partage des informations, le cas échéant.

A.5 Evaluation des trajets de services de réseau de bout en bout (E2E)

Les connaissances acquises grâce aux résultats de l'analyse AMDEC réseau peuvent être utilisées pour la prise de décision et l'évaluation des risques liés au projet, comme par exemple:

a) recommander une nouvelle conception du trajet de service de réseau E2E cible en vue d'améliorer la conception du réseau et garantir l'aptitude de la sûreté de fonctionnement;

b) développer des tests élémentaires pour la vérification par insertion de défauts sur le réseau (NFIT) afin de contrôler les effets potentiels de la défaillance identifiée lors de la vérification par insertion de défauts dans le trajet de service de réseau E2E concerné. Les données AMDEC réseau et autres informations pertinentes sont utilisées pour développer des tests élémentaires.

Le processus de réalisation de la conception du trajet de service de réseau E2E cible mentionné en a) est un processus de nouvelle conception qui suit un processus de cycle de vie rigoureux pour les phases de conception/développement et de réalisation/intégration. Les étapes pertinentes du cycle de vie d'un réseau sont décrites dans la CEI 61907.

L'évaluation du trajet de service de réseau E2E cible mentionnée en b) a pour objet de développer des tests élémentaires pour les applications NFIT. La technique NFIT a pour objet de réaliser des essais pour simuler les conditions de fonctionnement des trajets de services de réseau E2E en insérant des défauts pour analyser les résultats d'essai. L'objectif est de déterminer l'étendue de l'exposition aux risques en engageant l'action de nouvelle conception. Le NFIT tente de vérifier et de confirmer l'incertitude du résultat potentiel avant l'action de mise en œuvre réelle d'une nouvelle conception du trajet de service de réseau E2E. Selon le calendrier de réalisation du projet et les contraintes budgétaires, les activités NFIT mentionnées en b) fournissent une assurance pour le processus de nouvelle conception mentionné en a) et présentent des informations d'essai destinées à aider à la prise de décision concernant le projet. Il convient de faire preuve de prudence lors de la prise de décision concernant l'adaptation du projet et la recherche d'un compromis.

Un test élémentaire est un ensemble de données d'entrée d'essai, de conditions d'exécution et de résultats attendus, développé pour un objet d'essai particulier. Dans ce cas, la vérification de la capacité de la nouvelle conception du service de réseau E2E cible est destinée à atteindre le niveau de performance nécessaire pour garantir la sûreté de fonctionnement du service. La vérification par insertion de défauts est une technique de vérification dans laquelle un défaut est introduit volontairement dans le trajet de service de réseau E2E dans le but de déterminer les résultats d'essai prévus. Le résultat d'essai fournit la preuve objective de la nécessité d'appuyer la décision concernant la nouvelle conception.

La vérification NFIT fournit également un moyen pour évaluer l'efficacité du processus de vérification, le taux résultant de couverture des pannes, la disponibilité du trajet de service de réseau et les effets sur les performances de sûreté de fonctionnement du réseau.

Dans le cadre du processus d'évaluation des trajets de services de réseau E2E, les données suivantes peuvent être déterminées:

a) temps d'interruption des services du réseau

- la somme des temps d'interruption des services dus aux défaillances de chaque nœud du réseau;
- la somme des temps d'interruption des services dus aux défaillances de chaque liaison du réseau;

b) disponibilité des services du réseau

c) modes de défaillances

- nœud du réseau: panne du service, panne partielle du service, service intermittent, panne instantanée du service, dégradation de la performance du service;
- liaison du réseau: interruption de la liaison.

d) informations relatives aux paramètres du réseau

Paramètre du réseau	*Source*
• temps d'interruption du service de réseau par an (minutes/an)	résultat calculé
• nombre de nœuds dans le réseau	topologie du réseau
• nombre de liaisons dans le réseau	topologie du réseau
• fréquence de défaillance sur le nœud i	statistiques FRACAS
• fréquence de défaillance sur la liaison j	statistiques d'activité
• durée de panne de service due au nœud i (minutes)	résultats de la vérification NFIT
• durée de panne de service due à la liaison j (minutes)	résultats de la vérification NFIT
• taux de restauration du réseau	résultats de la vérification NFIT
• temps moyen de réparation du nœud i	statistiques FRACAS
• temps moyen de réparation de la liaison j	statistiques de l'opérateur

Annexe B
(informative)

Evaluation de la sûreté de fonctionnement de l'ensemble des terminaisons d'un réseau

B.1 Objectif

L'objectif de l'évaluation de la sûreté de fonctionnement de l'ensemble des terminaisons d'un réseau par l'opérateur est de déterminer les performances de sûreté de fonctionnement de l'ensemble du réseau. Le résultat de l'évaluation est la performance de disponibilité ou le temps d'interruption total par an de l'ensemble du réseau. Il existe de nombreux moyens d'obtenir un tel résultat en utilisant une combinaison de techniques de modélisation et de méthodes de prévision, ainsi que des données d'aptitude à la fonction sur site se rapportant aux caractéristiques de performance en matière de défaillance d'un réseau pour établir les tendances des défaillances dans le temps.

B.2 Description de la topologie d'un réseau et de l'ensemble des terminaisons d'un réseau

La topologie du réseau a la même configuration que celle utilisée pour le réseau de bout en bout (E2E), sauf que deux utilisateurs finaux au niveau des nœuds A1 et A2 sont mis en communication pour illustrer un réseau avec l'ensemble de ses terminaisons. Cette topologie est présentée dans la Figure B.1.

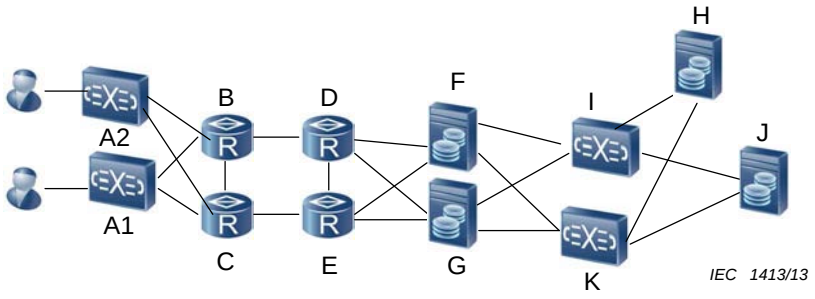


Figure B.1 – Exemple type d'une topologie de réseau avec l'ensemble de ses terminaisons

Le scénario de service peut être expliqué comme suit:

- le fournisseur de services veut déterminer la disponibilité/fiabilité de l'ensemble du réseau avec toutes ses terminaisons;
- l'hypothèse est que tous les éléments du réseau, de A à J inclus, doivent remplir leurs fonctions respectives à chaque instant et de manière continue.

B.3 Analyse du modèle de disponibilité du réseau avec l'ensemble de ses terminaisons

La disponibilité du réseau avec l'ensemble de ses terminaisons peut être déterminée en calculant le temps d'interruption moyen auquel a contribué la somme pondérée des temps d'interruption du réseau de bout en bout (E2E). Les symboles mathématiques sont les mêmes que ceux utilisés en Annexe A.

La disponibilité du service de réseau avec l'ensemble de ses terminaisons peut être déterminée de la manière suivante:

$$A_{\mathrm{N}} = 1 - \frac{DT_{\mathrm{N}}}{8\,760 \times 60}$$

où

A_{N} est la disponibilité du service de réseau avec l'ensemble de ses terminaisons;

DT_{N} est le temps d'interruption total d'un réseau avec toutes ses terminaisons

$$DT_{\mathrm{N}} = \sum\nolimits_i DT_{\mathrm{E2Ei}} \times P_{\mathrm{i}}$$

DT_{E2Ei} est le temps d'interruption du trajet de service E2E i, en minutes/an;

P_{i} est le nombre d'utilisateurs dans le trajet de service i divisé par le nombre d'utilisateurs de l'ensemble du réseau.

B.4 Evaluation du réseau avec l'ensemble de ses terminaisons

L'évaluation d'un service de réseau avec toutes ses terminaisons est similaire à celle du service de réseau de bout en bout (E2E), mais dans ce cas, tous les trajets de service de réseau E2E sont pris en compte.

Les processus AMDEC réseau et NFIT sont réalisés de la même manière que le processus d'évaluation E2E, mais avec des objectifs différents du point de vue du fournisseur de services ou de l'opérateur.

Annexe C
(informative)

Evaluation des performances de sûreté de fonctionnement d'un réseau en exploitation sur site

C.1 Objectif

L'évaluation des performances de sûreté de fonctionnement au cours de l'exploitation sur site est illustrée dans un exemple. Le but est de décrire une procédure pour déterminer l'impact des pannes de réseau et de la durée des pannes affectant le nombre d'utilisateurs abonnés aux services de réseau.

Cet exemple illustre les méthodes utilisées pour l'analyse et l'évaluation d'un réseau en se fondant sur les données de performance du réseau recueillies à l'échelle d'un pays, sur une période d'étude de 2 ans d'un réseau téléphonique public commuté [16]. Les données numériques sont présentées à des fins d'illustration pour indiquer l'ordre de grandeur des paramètres de performance du réseau. Les valeurs en pourcentage sont fournies pour représenter les contributions des pannes de réseau et l'impact qui en résulte sur le service de réseau.

C.2 Analyse de données

Les statistiques de performance du réseau indiquent un nombre total de 303 défaillances du réseau ayant entraîné des pannes au cours des deux années de fonctionnement des services de réseau. Les 303 défaillances du réseau ont affecté plus d'un million d'abonnés ou d'utilisateurs avec une durée cumulée de pannes de 3 196,5 minutes. Les interruptions de services sont déterminées par la somme des pannes des services téléphoniques. Elles sont groupées selon diverses catégories de défaillances. Le Tableau C.1 récapitule les données relatives aux défaillances du réseau.

Tableau C.1 – Récapitulatif des données relatives aux défaillances d'un réseau téléphonique public commuté, à l'échelle d'un pays

Source de défaillance du réseau	Catégorie de défaillance	Nombre de pannes	Nombre d'utilisateurs affectés	Durée de la panne min
Liée à l'installation	Défaillance matérielle Défaillance logicielle	56 44	95 690 118 200	159,8 119,3
Liée au trafic	Fonctions (surcharge)	18	276 760	1 123,7
Liée à un sinistre	Catastrophe naturelle	32	159 000	828,2
Liée à la sécurité	Vandalisme	3	853 930	456,0
Liée à l'ordonnan-cement	Maintenance	0	0	0
Liée à des facteurs humains	Erreur de procédure (erreur humaine)	150	265 996	509,5

L'impact sur le service est déterminé par le temps d'interruption cumulé, mesuré en utilisateur-minutes par catégorie.

Utilisateur-minutes = *Nombre d'utilisateurs affectés* par la catégorie de défaillance x *durée de panne* de la catégorie, en minutes.

La Figure C.1 présente les contributions des pannes de réseau ainsi que l'impact qui en résulte sur les services.

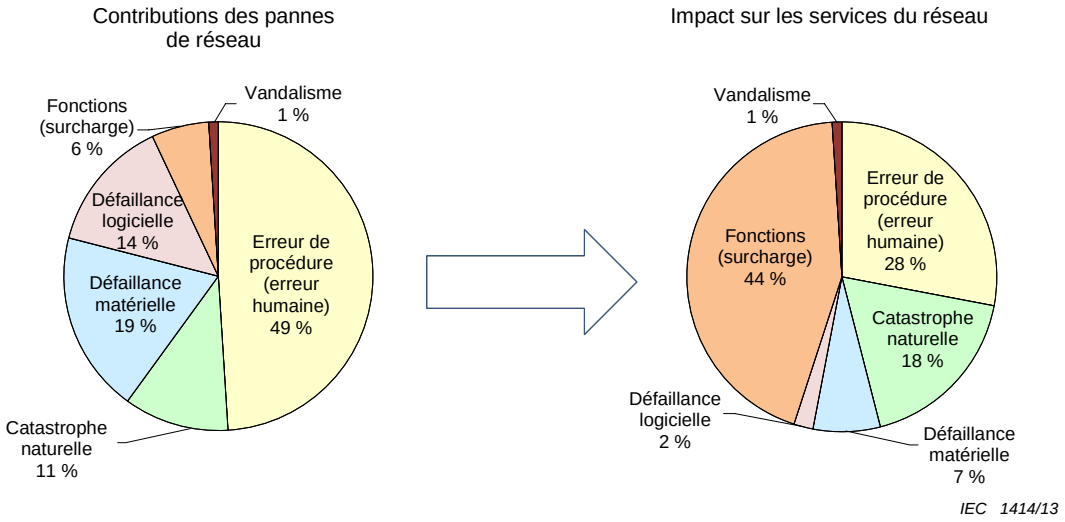


Figure C.1 – Contributions des pannes de réseau et impact résultant sur les services de réseau

C.3 Evaluation des performances de sûreté de fonctionnement du réseau

La performance de disponibilité peut être déterminée à partir de la durée cumulée des pannes (3 196,5 min) qui se sont produites pendant les deux années de fonctionnement continu des services de réseau (2 × 365 × 24 × 60 = 1 051 200 min). Le temps d'interruption moyen est de 1 598 min par an.

Disponibilité de l'ensemble du réseau = (1 051 200 – 3196,5)/1 051 200 = 99,7 %

La performance des services de réseau indique un impact (surcharge) sur 44 % des fonctions se traduisant par 6 % des contributions totales aux pannes du réseau. Cette observation indique que la cause principale des pannes de réseau est due à une performance insuffisante du réseau, nécessitant une amélioration de la sûreté du fonctionnement. Les 49 % de contribution aux pannes liées à des erreurs de procédure (erreur humaine) suggèrent la nécessité d'améliorer les procédures OAMP.

L'opérateur du réseau est en train d'évaluer les performances de sûreté de fonctionnement du réseau avec toutes ses terminaisons, à l'aide des informations pertinentes concernant les pannes du réseau qui lui ont été communiquées par les fournisseurs de services de réseau. Chaque fournisseur de services est responsable de son segment de réseau respectif pour ce qui est du fonctionnement quotidien de ses contributions aux services. Les tendances aux défaillances et la dégradation de la performance pour certains segments de réseau spécifiques devraient nécessiter des données de performance de nature temporelle fournies par les fournisseurs de services individuels en vue de l'analyse de sûreté de fonctionnement. La détermination du temps de détection de panne, du temps nécessaire à la restauration et des taux de retours de FRU (unités retournées du site) devraient nécessiter des informations supplémentaires sur les dossiers de maintenance des segments de réseau des fournisseurs de services.

Bibliographie

[1] Recommandation UIT-T I.350:1988, *Aspects généraux relatifs à la qualité de service et à la performance des réseaux numériques, y compris les RNIS*

[2] Recommandation UIT-T G.1000, *Qualité de service des communications: cadre et définitions*

[3] Recommandation UIT-T E.800, *Définitions de termes relatifs à la qualité de service*

[4] CEI 61078, *Techniques d'analyse pour la sûreté de fonctionnement – Bloc-diagramme de fiabilité et méthodes booléennes*

[5] CEI 62198, *Gestion des risques liés à un projet – Lignes directrices pour l'application*

[6] ISO/CEI 31010, *Gestion des risques – Techniques d'évaluation des risques*

[7] CEI 60812, *Techniques d'analyse de la fiabilité du système – Procédure d'analyse des modes de défaillance et de leurs effets (AMDE)*

[8] CEI 60300-3-11, *Gestion de la sûreté de fonctionnement – Partie 3-11: Guide d'application - Maintenance basée sur la fiabilité*

[9] CEI 61882, *Etudes de danger et d'exploitabilité (études HAZOP) – Guide d'application*

[10] CEI 60300-3-1, *Gestion de la sûreté de fonctionnement – Partie 3-1: Guide d'application – Techniques d'analyse de la sûreté de fonctionnement – Guide méthodologique*

[11] CEI 61165, *Application des techniques de Markov*

[12] Lyu, M. R. (Ed.): The Handbook of Software Reliability Engineering, IEEE Computer Society Press and McGraw-Hill Book Company, 1996

[13] ISO/CEI 7498-1, *Technologies de l'information – Interconnexion de systèmes ouverts (OSI) – Partie 1: Modèle de référence de base: Le modèle de base*

[14] TL 9000, *Quality Management System – Requirements Handbook 3.0, March 2001, Quality Excellence for Suppliers of Telecommunications Forum (QuEST Forum)*

[15] TL 9000, *Quality Management System – Requirements Handbook 3,5, March 2003, Quality Excellence for Suppliers of Telecommunications Forum (QuEST Forum)*

[16] KUHN D.R., *Sources of Failure in the Public Switched Telephone Network*, IEEE Computer, Vol.30, No.4 (April 1997), National Institute of Standards and Technology, Gaithersburg, Maryland 20899 USA

_____

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

3, rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

Tel: + 41 22 919 02 11
Fax: + 41 22 919 03 00
info@iec.ch
www.iec.ch