

BS EN 62673:2013



BSI Standards Publication

# Methodology for communication network dependability assessment and assurance

**bsi.**

...making excellence a habit.™

### **National foreword**

This British Standard is the UK implementation of EN 62673:2013. It is identical to IEC 62673:2013.

The UK participation in its preparation was entrusted to Technical Committee DS/1, Dependability.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2013.  
Published by BSI Standards Limited 2013

ISBN 978 0 580 79004 1  
ICS 03.120.01

**Compliance with a British Standard cannot confer immunity from legal obligations.**

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 September 2013.

### **Amendments/corrigenda issued since publication**

<b>Date</b>	<b>Text affected</b>
-------------	----------------------

---

EUROPEAN STANDARD  
NORME EUROPÉENNE  
EUROPÄISCHE NORM

**EN 62673**

August 2013

ICS 03.120.01

English version

**Methodology for communication network dependability assessment and assurance**  
(IEC 62673:2013)

Méthodologie pour l'évaluation et l'assurance de la sûreté de fonctionnement des réseaux de communication  
(CEI 62673:2013)

Methodik zur Beurteilung und Sicherstellung der Zuverlässigkeit von Kommunikationsnetzen  
(IEC 62673:2013)

This European Standard was approved by CENELEC on 2013-07-23. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

**CENELEC**

European Committee for Electrotechnical Standardization  
Comité Européen de Normalisation Electrotechnique  
Europäisches Komitee für Elektrotechnische Normung

**CEN-CENELEC Management Centre: Avenue Marnix 17, B - 1000 Brussels**

## Foreword

The text of document 56/1507/FDIS, future edition 1 of IEC 62673, prepared by IEC/TC 56 "Dependability" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN 62673:2013.

The following dates are fixed:

- latest date by which the document has to be implemented at national level by publication of an identical national standard or by endorsement (dop) 2014-04-23
- latest date by which the national standards conflicting with the document have to be withdrawn (dow) 2016-07-23

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC [and/or CEN] shall not be held responsible for identifying any or all such patent rights.

## Endorsement notice

The text of the International Standard IEC 62673:2013 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following notes have to be added for the standards indicated:

IEC 61078	NOTE	Harmonised as EN 61078.
IEC 62198	NOTE	Harmonised as EN 62198.
IEC 60812	NOTE	Harmonised as EN 60812.
IEC 60300-3-11	NOTE	Harmonised as EN 60300-3-11.
IEC 60300-3-1	NOTE	Harmonised as EN 60300-3-1.
IEC 61165	NOTE	Harmonised as EN 61165

**Annex ZA**  
(normative)  
**Normative references to international publications  
with their corresponding European publications**

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.

NOTE When an international publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
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	EN 60300-3-15	
IEC 61907		Communication network dependability engineering	EN 61907	

## CONTENTS

INTRODUCTION.....	6
1 Scope.....	7
2 Normative references .....	7
3 Terms, definitions and abbreviations .....	7
3.1 Terms and definitions .....	7
3.2 Abbreviations .....	11
4 Overview of network dependability methodology.....	11
4.1 Need for network dependability methods .....	11
4.2 Network dependability objectives.....	12
4.3 Network service scenarios.....	13
4.4 Network dependability assessment strategies.....	13
4.5 Network dependability assurance strategies .....	14
5 Network dependability methodology applications .....	15
5.1 Network life cycle process .....	15
5.1.1 Life cycle process applications .....	15
5.1.2 Risk assessment process applications.....	15
5.1.3 Dependability methodology applications .....	16
5.2 Network dependability performance characteristics .....	17
5.3 Network dependability assessment methodology.....	18
5.3.1 Generic dependability analysis and evaluation techniques.....	18
5.3.2 Service scenario analysis .....	19
5.3.3 Network modelling .....	19
5.3.4 Network failure modes, effects and criticality analysis .....	20
5.3.5 Network fault insertion test .....	21
5.3.6 Failure reporting, analysis and corrective action system .....	22
5.4 Network dependability assurance methodology .....	22
5.4.1 Scope of dependability assurance methodology applications .....	22
5.4.2 Assurance of dependability of service.....	23
5.4.3 Assurance of data integrity .....	23
5.4.4 Assurance of network performance functions and support process enhancement.....	24
5.4.5 Network dependability assurance methods .....	24
Annex A (informative) Example of E2E network dependability assessment .....	27
Annex B (informative) Example of full-end network dependability assessment .....	33
Annex C (informative) Evaluation of network dependability performance in field operation .....	35
Bibliography.....	37
Figure A.1 – A typical example of an E2E network topology .....	27
Figure B.1 – A typical example of a full-end network topology.....	33
Figure C.1 – Network outage contributions and resultant network service impact .....	36

Table 1 – Summary of network dependability activities and application methods .....	17
Table 2 – Summary of network dependability parameters.....	18
Table C.1 – Summary of network failure data of a nation-wide public switched telephone network .....	35

## 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 <sup>1</sup> 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.

---

<sup>1</sup> 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]<sup>2</sup>

### 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

---

<sup>2</sup> 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	<ul style="list-style-type: none"> <li>• ND requirements analysis</li> </ul>	<ul style="list-style-type: none"> <li>• Service scenario analysis</li> <li>• Business impact analysis</li> </ul>
Design/development	<ul style="list-style-type: none"> <li>• Network reliability allocation</li> <li>• ND prediction</li> <li>• ND design analysis and evaluation</li> </ul>	<ul style="list-style-type: none"> <li>• Network modelling (RBD, SLB and simulation)</li> <li>• NFMECA</li> <li>• FRACAS</li> <li>• Root-cause analysis</li> <li>• Cause and effect analysis</li> </ul>
Realization/integration	<ul style="list-style-type: none"> <li>• ND features testing</li> <li>• ND test case development</li> <li>• ND service conformance validation</li> </ul>	<ul style="list-style-type: none"> <li>• NFIT</li> <li>• FRACAS</li> <li>• Cause and effect analysis</li> </ul>
Operation/maintenance	<ul style="list-style-type: none"> <li>• ND performance assessment</li> <li>• ND fault management and incident reports</li> <li>• ND maintenance records</li> </ul>	<ul style="list-style-type: none"> <li>• FRACAS</li> <li>• Network health check</li> <li>• Network outage control</li> <li>• Test case management</li> <li>• Reliability centred maintenance</li> <li>• HAZOP</li> </ul>
Enhancement/renewal	<ul style="list-style-type: none"> <li>• Enhanced/renewed service requirements analysis</li> <li>• Enhanced/renewed service dependability assessment</li> </ul>	<ul style="list-style-type: none"> <li>• Service scenario analysis (including legacy service consideration)</li> <li>• Network health check</li> <li>• Network outage control</li> <li>• Test case management</li> <li>• Business impact analysis</li> <li>• Cause and consequences analysis</li> </ul>
Retirement	<ul style="list-style-type: none"> <li>• Network service termination notification to users</li> <li>• Obsolete equipment disposal</li> </ul>	<ul style="list-style-type: none"> <li>• Cause and consequences analysis</li> <li>• Business impact analysis</li> </ul>

## 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)
<ul style="list-style-type: none"> <li>• Full-end network service availability (% <i>uptime</i>)</li> <li>• Number of subscribers or users affected due to network service outage</li> <li>• Network downtime (<i>minutes/year</i>)</li> <li>• Fault detection time (<i>minutes</i>)</li> <li>• Time to restoration (<i>minutes</i>)</li> <li>• FRU return rate (<i>numbers/month</i>)</li> </ul>	<ul style="list-style-type: none"> <li>• E2E network service availability (% <i>uptime</i>)</li> <li>• Service path downtime (<i>minutes/year</i>)</li> <li>• Failed service access (<i>frequency/year</i>)</li> <li>• Delayed service access (<i>frequency/year</i>)</li> <li>• Premature service disconnect (<i>frequency/year</i>)</li> <li>• Delay of service media (<i>minutes/year</i>)</li> </ul>

### 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.

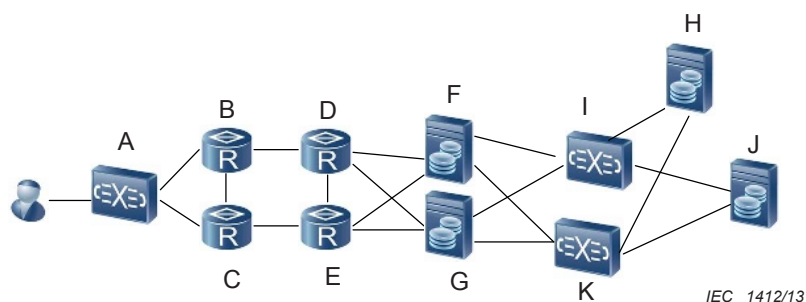


Figure A.1 – A typical example of an E2E network topology

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.

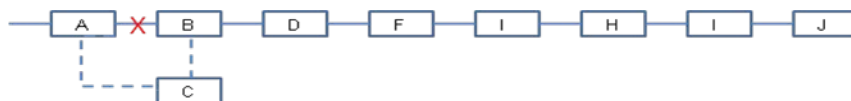
### A.3 Construction of E2E network service paths

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).

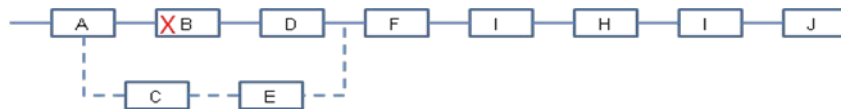
a) Main service path



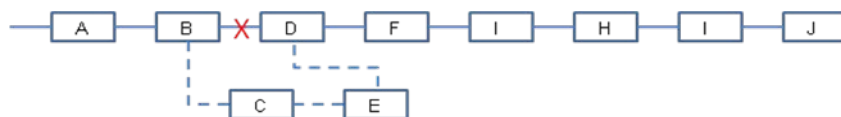
b) Backup service path with failure of link between node A and B



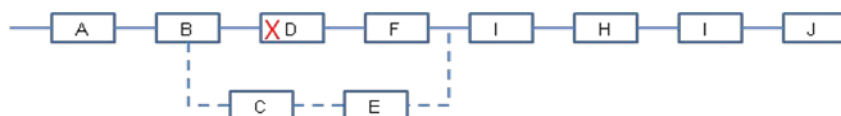
c) Backup service path with failure of node B



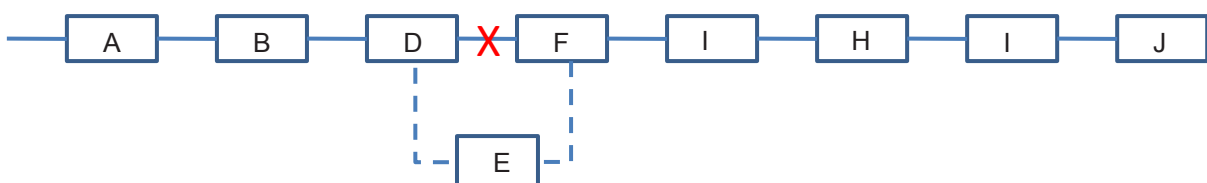
d) Backup service path with failure of link between node B and D



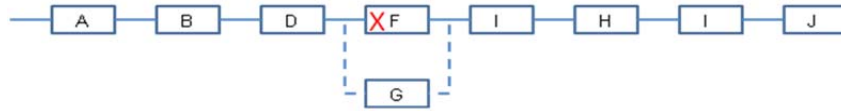
e) Backup service path with failure of node D



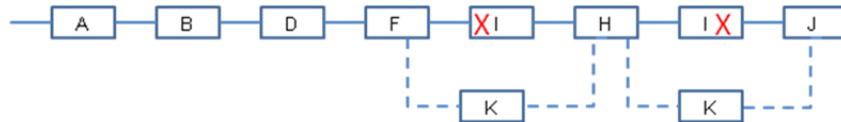
f) Backup service path with failure of link between node D and F



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:

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

where

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

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


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

$f_i$  is the failure frequency of node/link i in main path, times/year;

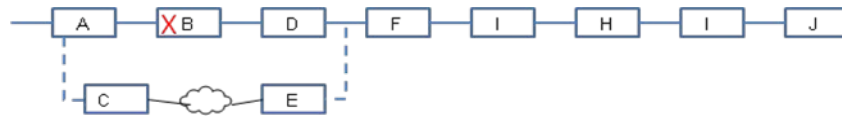
$r_i$  is the network failure recovery ratio of node/link i in main path;

$dt_i$  is the service downtime of node/link i in the main path failed, but the service is recovered successfully;

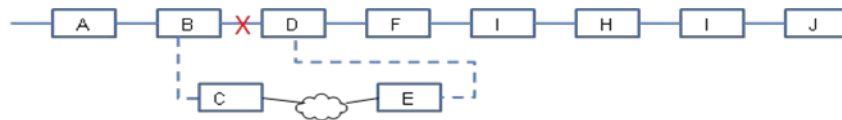
$MTTR_i$  is the mean time to restoration of node/link i in the main path failed, but the service is not recovered.

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).

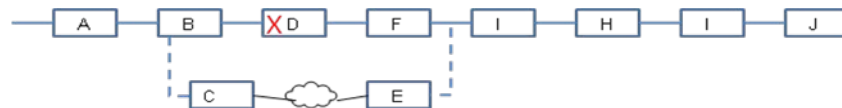
i) Backup service path flow through “cloud” with failure of node B



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 relevant E2E network service performance to support downtime estimation;
- SLB can be computerized to facilitate 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

<i>Network parameter</i>	<i>Source</i>
• 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.

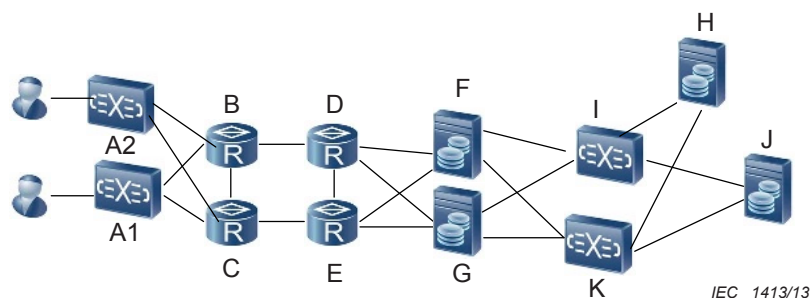


Figure B.1 – A typical example of a full-end network topology

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.

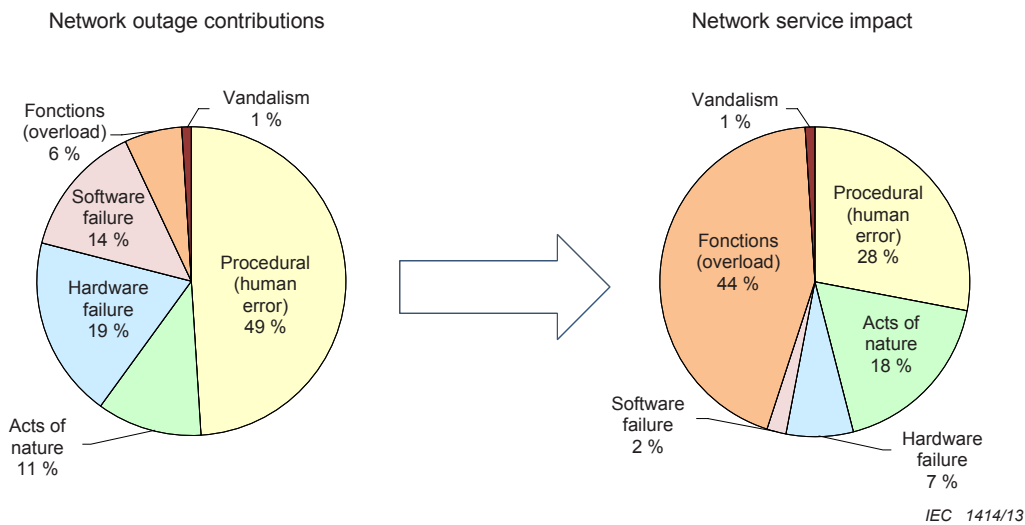
**Table C.1 – Summary of network failure data of a nation-wide public switched telephone network**

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 ( $2 \times 365 \times 24 \times 60 = 1\,051\,200$  min) of continuous network service operation. The average downtime is 1 598 min per year.

$$\text{Availability of the entire network} = (1\,051\,200 - 3196,5)/1\,051\,200 = 99,7 \%$$

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
-







# British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

## About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards-based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

## Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at [bsigroup.com/standards](http://bsigroup.com/standards) or contacting our Customer Services team or Knowledge Centre.

## Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at [bsigroup.com/shop](http://bsigroup.com/shop), where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

## Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to [bsigroup.com/subscriptions](http://bsigroup.com/subscriptions).

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

**PLUS** is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit [bsigroup.com/shop](http://bsigroup.com/shop).

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email [bsmusales@bsigroup.com](mailto:bsmusales@bsigroup.com).

## BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

## Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

## Copyright

All the data, software and documentation set out in all British Standards and other BSI publications are the property of and copyrighted by BSI, or some person or entity that owns copyright in the information used (such as the international standardization bodies) and has formally licensed such information to BSI for commercial publication and use. Except as permitted under the Copyright, Designs and Patents Act 1988 no extract may be reproduced, stored in a retrieval system or transmitted in any form or by any means – electronic, photocopying, recording or otherwise – without prior written permission from BSI. Details and advice can be obtained from the Copyright & Licensing Department.

## Useful Contacts:

### Customer Services

**Tel:** +44 845 086 9001

**Email (orders):** [orders@bsigroup.com](mailto:orders@bsigroup.com)

**Email (enquiries):** [cservices@bsigroup.com](mailto:cservices@bsigroup.com)

### Subscriptions

**Tel:** +44 845 086 9001

**Email:** [subscriptions@bsigroup.com](mailto:subscriptions@bsigroup.com)

### Knowledge Centre

**Tel:** +44 20 8996 7004

**Email:** [knowledgecentre@bsigroup.com](mailto:knowledgecentre@bsigroup.com)

### Copyright & Licensing

**Tel:** +44 20 8996 7070

**Email:** [copyright@bsigroup.com](mailto:copyright@bsigroup.com)



...making excellence a habit.™