
# ATIS-0100524.2004(R2013)

# Terminology for Network Elements in Evolving Communication Networks

**AMERICAN NATIONAL STANDARD FOR TELECOMMUNICATIONS**

As a leading technology and solutions development organization, ATIS brings together the top global ICT companies to advance the industry's most-pressing business priorities. Through ATIS committees and forums, nearly 200 companies address cloud services, device solutions, emergency services, M2M communications, cyber security, ehealth, network evolution, quality of service, billing support, operations, and more. These priorities follow a fast-track development lifecycle – from design and innovation through solutions that include standards, specifications, requirements, business use cases, software toolkits, and interoperability testing.

ATIS is accredited by the American National Standards Institute (ANSI). ATIS is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of oneM2M, a member and major U.S. contributor to the International Telecommunication Union (ITU) Radio and Telecommunications sectors, and a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit < www.atis.org >.

## AMERICAN NATIONAL STANDARD

Approval of an American National Standard requires review by ANSI that the requirements for due process, consensus, and other criteria for approval have been met by the standards developer.

Consensus is established when, in the judgment of the ANSI Board of Standards Review, substantial agreement has been reached by directly and materially affected interests. Substantial agreement means much more than a simple majority, but not necessarily unanimity. Consensus requires that all views and objections be considered, and that a concerted effort be made towards their resolution.

The use of American National Standards is completely voluntary; their existence does not in any respect preclude anyone, whether he has approved the standards or not, from manufacturing, marketing, purchasing, or using products, processes, or procedures not conforming to the standards.

The American National Standards Institute does not develop standards and will in no circumstances give an interpretation of any American National Standard. Moreover, no person shall have the right or authority to issue an interpretation of an American National Standard in the name of the American National Standards Institute. Requests for interpretations should be addressed to the secretariat or sponsor whose name appears on the title page of this standard.

**CAUTION NOTICE:** This American National Standard may be revised or withdrawn at any time. The procedures of the American National Standards Institute require that action be taken periodically to reaffirm, revise, or withdraw this standard. Purchasers of American National Standards may receive current information on all standards by calling or writing the American National Standards Institute.

## Notice of Disclaimer & Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER, NO REPRESENTATION OR WARRANTY IS MADE OFMERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

NOTE - The user's attention is called to the possibility that compliance with this standard may require use of an invention covered by patent rights. By publication of this standard, no position is taken with respect to whether use of an invention covered by patent rights will be required, and if any such use is required no position is taken regarding the validity of this claim or any patent rights in connection therewith. Please refer to [http://www.atis.org/legal/patentinfo.asp] to determine if any statement has been filed by a patent holder indicating a willingness to grant a license either without compensation or on reasonable and non-discriminatory terms and conditions to applicants desiring to obtain a license.

ATIS-0100524.2004(R2013), *Terminology for Network elements in Evolving Communication Networks*

Is an American National Standard developed by the **ATIS Network Performance, Reliability and Quality of Service Committee (PRQC)**.

*Published by*

**Alliance for Telecommunications Industry Solutions**
**1200 G Street, NW, Suite 500**
**Washington, DC 20005**

(R2013)

**ATIS-0100524.2004**

(formerly T1.524-2004)

American National Standard for Telecommunications

# Reliability-related Metrics and Terminology for Network Elements in Evolving Communications Networks

Secretariat

**Alliance for Telecommunications Industry Solutions**

Approved June 23, 2004

**American National Standards Institute, Inc.**

**Abstract**

This standard defines reliability-related metrics, features, and terminology for communication networks to foster industry-wide consistent nomenclature and methodology when specifying and measuring reliability-related attributes.

## FOREWORD

This document is entitled *Reliability-related Metrics and Terminology for Network Elements in Evolving Communications Networks.*

Future control of this document will reside with the Network Performance, Reliability, and Quality of Service Committee (PRQC), formerly T1A1. This control of additions to the specification, such as protocol evolution, new applications, and operational requirements, will permit compatibility among U.S. networks. Such additions will be incorporated in an orderly manner with due consideration to the ITU-T layered model principles, conventions, and functional boundaries.

Suggestions for improvement of this standard will be welcome. These should be sent to the Alliance for Telecommunications Industry Solutions, PRQC Secretariat, 1200 G Street, NW, Suite 500, Washington DC 20005.

This standard was processed and approved for submittal to ANSI by the Technical Subcommittee T1A1 on Performance, Reliability, and Signal Processing. Committee approval of this standard does not necessarily imply that all committee members voted for its approval. At the time it approved this standard, T1A1 had the following members:

R. Wohlert, T1A1 Chair
N. Seitz, T1A1 Vice-Chair
S. Carioti, ATIS Disciplines
S. Barclay, ATIS Secretariat
C. Underkoffler, ATIS Chief Editor
R. Paterson & P. Tarapore, T1A1 Technical Editor

| Organization Represented | Name of Representative |
|---|---|
| Alcatel USA Inc. | Ken Biholar |
| ASTRI | Jacky Chow |
| AT&T | Percy Tarapore<br>Charles A. Dvorak (Alt.) |
| BellSouth Telecommunications | Eric Hauch<br>Archie McCain (Alt.) |
| C.S.I Telecommunications | Michael S. Newman<br>Thomas G. Croda (Alt.) |
| Ericsson Incorporated | Mustafa Kocaturk<br>Sangamesh Vinayagamurthy (Alt.) |
| Intelsat | Mark T. Neibert |
| Lucent Technologies | Stuart O. Goldman |
| National Communications System | An Nguyen<br>Jean Trakinat (Alt.) |
| NTIA | Neal B. Seitz |

| Organization Represented | Name of Representative |
|---|---|
| Nortel Networks | Subhash Patel<br>Oscar Avellaneda (Alt.) |
| Qwest | Bill Wycoff<br>David Clark (Alt.) |
| SBC Communications, Inc. | Randolph Wohlert<br>Pierre Costa (Alt.) |
| Siemens Info & Comm Ntwks, Inc. | Suhas S. Gandhi<br>David E. Francisco (Alt.) |
| Sprint Corporation | Mark L. Jones |
| Telcordia Technologies | Spilios Makris<br>Cliff Halevi (Alt.) |
| Tellabs Operations, Inc. | William A. Walker<br>Kevin Stodola (Alt.) |
| Verizon Communications | John Colombo<br>Wendy Pugh (Alt.) |

Working Group T1A1.2 on Network Survivability Performance, which developed this standard, has the following officers:

O. Avellaneda, T1A1.2 Chair
S. Makris, T1A1.2 Vice-Chair
F. Kaudel, T1A1.2 Chief Editor
R. Paterson & P. Tarapore, T1A1.2 Editors

Over the course of its development, the following individuals participated in the Working Group's discussions and made significant contributions to the standard:

| | | |
|---|---|---|
| O. Avellaneda | F. Kaudel | R. Paterson |
| J. Bennett | P. Kimbrough | P. Tarapore |
| D. Clark | M. Kocaturk | A. Webster |
| C. Dvorak | J. Lankford | R. Wohlert |
| R. Holley | S. Makris | W. Wycoff |
| J. Huang | A. McCain | J. Zebarth |
| A. Nguyen | M. Guha | E. Rojek |

## TABLE OF CONTENTS



## TABLE OF FIGURES

American National Standard for Telecommunications –

# Reliability-related Metrics and Terminology for Network Elements in Evolving Communications Networks

## 1 INTRODUCTION

### 1.1 Scope

This standard defines Functional Element (FE) and Network Element (NE) reliability-related terminology, metrics, and features for evolving communications networks. The term *reliability-related* refers to "reliability, availability, maintainability and survivability." The standard is applicable to any layer 1 to 8 FE and NE.

### 1.2 Purpose

The purpose of this standard is to define a modernized and expanded set of reliability-related terminology, metrics, and feature definitions to facilitate the setting of clear, consistent and complete objectives. The intent is to have a standard that is non-implementation specific. The nomenclature and methodology defined is technology agnostic and not implementation specific.

This standard:

1. *Specifies reliability-related objectives:* Service Providers may use this standard to set reliability-related requirements and Vendors may use this standard as input to product planning and design.
2. *Compare objectives, predictions and actual reliability-related metric values for different Solutions:* This standard may be used to characterize, compare and contrast reliability Solutions in a consistent way.
3. *Facilitates risk management of critical reliability-related feature development:* The design parameters of critical reliability-related features can be reported to the Service Provider by reporting outputs from the development process such as predictions and test results.
4. *Facilitates tracking reliability-related in-service field performance:* Vendors and Service Providers can track actual performance and compare them against objectives to drive corrective and preventive action plans.

### 1.3 Rationale

Many existing reliability-related terminology, metrics, and features have been exhaustively described in several documents (see clause 1.4). Many of the metrics were defined to support traditional voice-based public telephone networks and services where nodal failure mode objectives were set largely independently of how the NE was configured in the network. This standard builds on this body of knowledge by adapting existing definitions to suit network elements as the network is transformed to a converged multi-service packet-based network. Thus, this standard offers the convenience of

consolidating the necessary set of reliability-related metrics and definitions, including expanding the metrics and features to reflect networking-related attributes.

By providing a consistent set of metrics and feature definitions, this standard will enable the comparison of various Solutions. The metrics incorporate both nodal and network reliability-related attributes for a more comprehensive set of reliability-related objectives. Lastly, since the document differentiates between external and internal reliability-related metrics, it provides vendors more flexibility to innovate to meet reliability-related objectives.

## 1.4 Normative References

The following standard contains provisions which, through reference in this text, constitute provisions of this American National Standard. At the time of publication, the edition indicated was valid. All standards are subject to revision, and the parties to agreements based on this American National Standard are encouraged to investigate the possibility of applying the most recent edition of the standard indicated below.

T1.TR.70-2001, *A Reliability/Availability Framework for IP-Based Networks and Services*.[1]

T1.TR.78-2003, *Access Availability of Routers in IP-Based Networks*.[1]

GR-512, *LSSGR-Reliability*.[2]

GR-929, *RQMS-Wireline*.[2]

GR-1110, *BSSGR-ATM*.[2]

GR-63, *NEBS*.[2]

## 1.5 Document Definitions

**1.5.1 Entity:** Refers to any of: Network Service, Solution, Functional Element, Network Element, NE Feature, Hardware module, Software module, hardware component, etc.

**1.5.2 Feature:** A functional capability of a network element.

**1.5.3 Functional Element:** A logical system that fulfills a network function. It can be implemented by one or more network elements

**1.5.4 Network Element:** A physical unit of a Solution that is interconnected (wireline or wireless) to other network elements. Routers, switches, and gateways are examples of network elements.

**1.5.5 Solution:** One or more functional elements that operate together as a system to provide one or more Services to end-users or end devices.

## 1.6 Abbreviations, Acronyms, and Symbols

| | |
|---|---|
| ANSI | American National Standards Institute |
| ATIS | Alliance for Telecommunications Industry Solutions |

[1] This document is available from the Alliance for Telecommunications Industry Solutions (ATIS), 1200 G Street N.W., Suite 500, Washington, DC 20005. <http://www.atis.org>

[2] Telcordia documents are available from Industry Direct Sales, Telcordia, 8 Corporate Place, PYA 3A-184, Piscataway, NJ, 08854-4156, or: < http://telecom-info.telcordia.com >.

| | |
|---|---|
| EMI | Electromagnetic Interference |
| ESD | Electrostatic Discharge |
| FE | Functional Element |
| FRU | Field Replaceable Unit |
| I/O | Input/Ouput |
| NGN | Next Generation Network |
| NE | Network Element |
| OAM&P | Operations, Administration, Maintenance, and Provisioning |
| PSTN | Public Switched Telephone Network |

## 1.7 Key Concepts

- **Anatomy of a Reliability-related measurement or objective.**

  Figure 1 illustrates the key attributes of a reliability-related metric that are required for completeness and unambiguous measurement. (Note the 30 second outage threshold is used for illustrative purposes.)

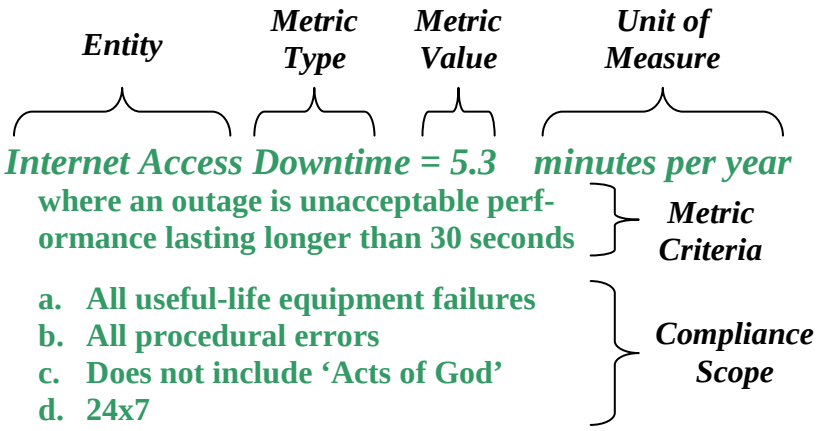


**Figure 1 - Example of Reliability-related Metric**

  The Entity describes what is being measured: a service, a network element, etc. The metric type signifies which reliability-related attribute is being specified, predicted or measured. The metric value is the actual specified, predicted or measured amount[3]. The metric criterion defines the threshold that determines if a failure event contributes to the metric value. Lastly, the compliance conditions define the failure events and time period under which the metric applies. To be complete and unambiguous, all reliability-related metrics must incorporate all these attributes

- **Satisfying customer expectations requires addressing reliability-related aspects across the complete lifecycle of products and solutions, where reliability-related metrics are used to quantify the requirements, design, test results, and field performance.**
  - *Customer expectations* are translated into measurable objectives.

[3] In measured cases, statistical confidence parameters should be defined.

- *System design* is analyzed and modeled to ensure the design is inherently capable of meeting objectives.
- *Detail designs* are analyzed, modeled, and tested to ensure the design implementation meets the objectives.
- *Field tracking* is done and measured values are compared to drive reliability *corrective* and *preventive* action plans. Population sizes and measurement period duration must be considered to determine the statistical significance of departures of measured values from objectives.

- **A NE incorporates capabilities to ensure it is reliable, robust, and maintainable.**

  Good network design starts with reliable, robust, and maintainable network elements. Equipment reliability requires good design practices to ensure low hardware and software failure rates and robustness to environmental, external power, and traffic load extremes. It requires good human factors design to minimize procedural error, and it requires the right security features to prevent service outages or degradation due to denial of service attacks. Equipment maintainability requires packaging strategies and diagnostic features to ensure good fault isolation for minimal repair times and minimal spares inventory costs.

- **NEs incorporate network protection and restoration features that must interwork for successful recovery from network failures.**

  Reliable and maintainable network elements are not sufficient to design networks that provide reliable and available services. Network elements require network protection and restoration features that communicate fault information with each other for successful failure detection, recovery and repair.

- **Functional Element reliability-related performance can be achieved via a number of fault-tolerant design options by using one or more NE's.**

  A functional element (FE) is a logical system that fulfills a network function. It can be implemented by one or more network elements. There are two types of fault-tolerant design strategies: 1. *intra-NE* (internal to a NE), such as redundant control processors; and 2. *inter-NE* (between NE's), such as dual-homed network elements. A reliability-related objective -- such as total system downtime -- when applied to a network element, specifies only intra-NE fault-tolerant design strategy. This design is not always the most optimal in providing reliability. In some network scenarios, redundant network elements without internal redundancy can provide equivalent or higher levels of service reliability. For the next generation network – a multi-service packet-based network – design flexibility is a necessity to satisfy the broad range of service reliability expectations. For this reason, reliability-related objectives should be applied to functional elements as well.

  The following is an example to illustrate the application functional elements to define different fault-tolerant design options. Let us assume that there are two NE types that the network designer can use to implement the functional element: 1. the *FFT NE* (fully fault-tolerant network element), which has a total system downtime of 2 minutes per year; and 2. the *PFT NE* (partially fault-tolerant network element), which has a total system downtime of 10 minutes per year.

As Figure 2 illustrates, *Option A* uses two independent PFT NEs networked together to achieve a total FE downtime of less than 0.001 minutes per year. This option has the benefit of protecting the customer's service from site outages. *Option B* uses one FFT NE to achieve a FE downtime of 2 minutes

per year. And *Option C* employs one PFT NE to achieve a FE downtime of 10 minutes per year. The latter option is applicable where the service is considered non-critical.

NOTE - For successful failure recovery in Option A, the network recovery mechanism requires signaling between the network elements so that they can co-operate in the recovery.

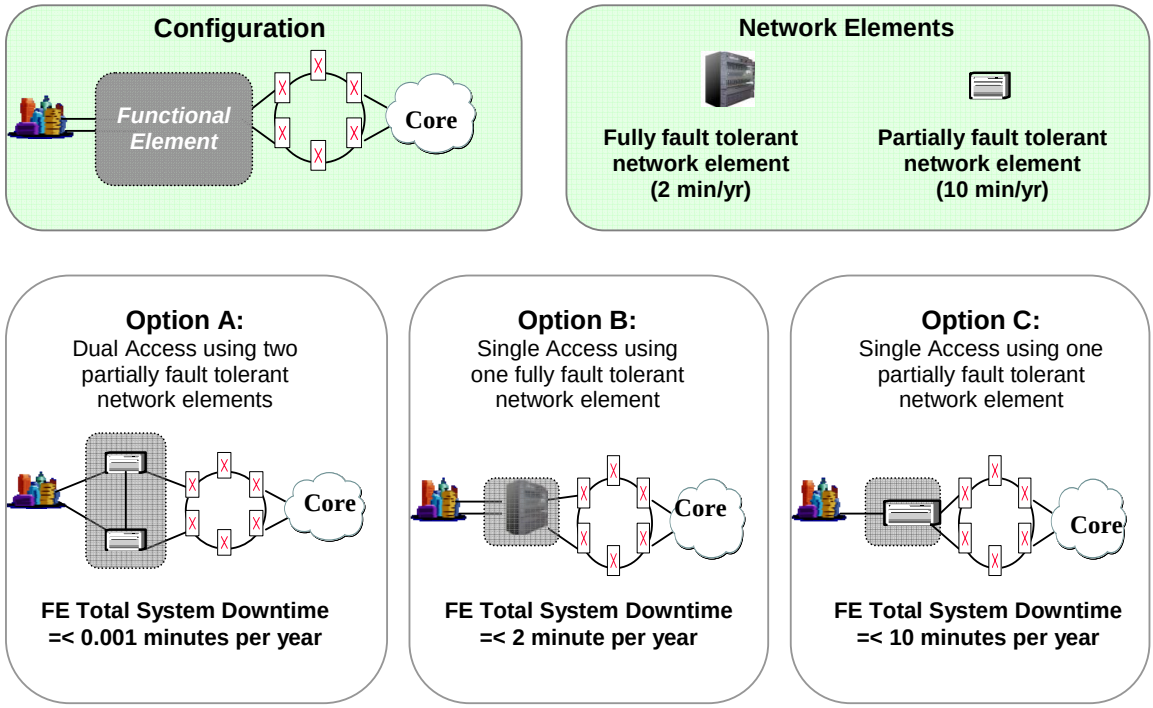


**Figure 2 - Redundancy Options using Functional Elements**

## *1.8 Document Organization*

The standard is organized into four sections: a section on reliability-related terminology definitions followed by three sections aligned to the levels of requirement types (see Figure 3), each dependent on the next underlying level.

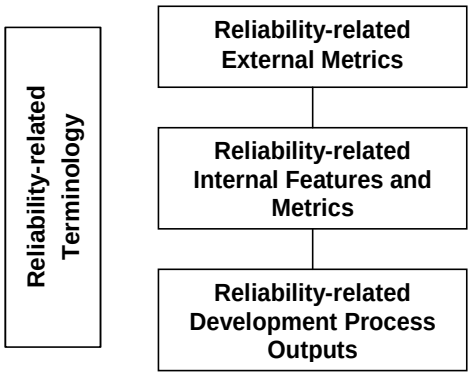


**Figure 3 - Standard Structure**

*The Reliability-related External Metrics* section defines the FE's external reliability-related attributes that are observable, measurable, in-service metrics. They include service downtime, mean-time-to-repair, and maintenance actions. These metrics may be used by Service Providers to specify their reliability-related requirements, to set contractual agreements, or to monitor actual field performance.

*The Reliability-related Internal Features and Metrics* section defines the FE's internal reliability-related capabilities and the metrics that are required to meet the external metrics' objectives. An example is the provision of network element redundancy where a key internal metric is fault coverage that is required to meet a specific value such that the external reliability metric – downtime – is met. Internal metrics may be defined to demonstrate how the solution satisfies the Service Provider's requirements for external metrics.

*The Reliability-related Development Process Outputs* section defines the subset of the Solution Vendor's development process outputs required by the Service Provider to help manage product introduction risk.

*The Reliability-related Terminology* section defines generic terminology to support consistent use of reliability-related language.

# 2 RELIABILITY-RELATED EXTERNAL METRICS

## 2.1 Setting Objectives

The following metrics provide a means for establishing reliability performance objectives. After the establishment of objectives, field performance data may be used to quantify the degree to which specific solutions meet the objectives. And finally, the objectives may be used for field tracking of actual performance to drive corrective and preventive actions.

> NOTE: Reliability-related budgets for Vendor-attributed and Provider-attributed contributions can be set by Service Providers; however, equipment-related budgets such as hardware and software which are implementation-specific should be set by the Solution Vendor.

The document's terminology uses *shall* throughout, though it is the responsibility of the person or persons who set the objectives to decide which metric objectives should be mandatory.

## 2.2 Reliability-related Requirements

1. Predicted and/or field measured values shall be provided for the following reliability-related metrics for the functional element as configured in target network configurations.
2. Reliability-related budgets shall be defined and divided between vendor- and provider-attributed contributions for each of the service-affecting reliability-related metrics.
3. A description of the methodology, measured conditions such as time period and population, and assumptions used to compute or measure the metric values shall be provided.
4. A functional element's single points of equipment failure that require manual repair to restore service shall not impact the service for more than ***n*** simultaneous service-users[4].

[4] The Service Provider should define ***n*** for each service or customer type.

5. External metric objectives for a specified set of failure events including all or some of the following shall be met:
    a. Useful-life software and hardware failures.
    b. Normal OAM&P activities assuming an average upgrade frequency of ***m*** upgrades per NE per unit of time, where ***m*** is based on the Service Provider's upgrade policy.
    c. Procedural errors (some or all of vendor-attributed, service provider-attributed, service customer-attributed).
    d. Cable cuts and facility failures.
    e. Disasters.
    f. Physical and cyber attacks.
    g. Traffic overloads less than ***x*** times the rated load, where ***x*** is a specified factor greater than the functional limit for adequate performance.
    h. For unattended offices assuming a travel time of ***z*** hours, where ***z*** is the average time to select a replacement spare and travel to the site to initiate the repair action.
6. External metric objectives shall be met either for a 24 x 7 operating period, or for a time period that excludes planned maintenance windows.
7. The early life period for hardware reliability shall not last longer than ***l*** months at which time the Field Replaceable Unit (FRU) return rate shall be within specified objectives for statistically significant populations.
8. The external reliability-related metrics are defined as follows:
    - *Customer Service Downtime:* The FE shall ensure that the *service performance*, as experienced by the Service Customer, shall not degrade below a service availability performance threshold or a duration longer than $t_0$ seconds for a long term average of > ***z*** minutes unit of time during a set measurement period, where $t_0$ is the criterion for service outage/unavailability.
    - *Customer Service Failure Frequency:* The FE shall ensure that the *service failure rate*, as experienced by the Service Customer, shall not average greater than '$f_o$' occurrences per unit of time where a service failure results in the end-user or end-device having to re-try to establish service or to re-try a service transaction.
    - *Total FE Outage downtime:* The entire FE bandwidth shall not be completely out of service or degrade below a service availability performance threshold for durations longer than $t_0$ seconds for a long term average of > ***z*** minutes unit of time of a set measurement period, where $t_0$ is the criterion for service outage/unavailability.
    - *Total FE Outage Frequency:* The average frequency of occurrence of the entire FE's bandwidth degrading below a service availability performance threshold for durations longer than $t_0$ seconds shall not exceed '$f_o$' occurrences per unit of time.
    - *Partial FE Outage Downtime:* No more than ***p***% of FE bandwidth shall be out of service or degrade below a service availability performance threshold for a duration longer than $t_0$ seconds for a long term average > ***u*** minutes of a set measurement period, where $t_0$ is the criterion for service outage/unavailability.
    - *Partial FE Outage Frequency:* The average frequency occurrence of ***p***% of FE's bandwidth degrading below a service availability performance threshold for durations longer than $t_0$ seconds shall not exceed '$f_{po}$' occurrences per unit of time.
    - *FE Management Control Downtime:* The FE's management control functionality shall not be unavailable for durations longer than $t_c$ seconds for a long term average > ***w*** minutes per

unit of time of any measurement period, where $t_c$ is the criterion for FE management control outage.

- *Weighted Bandwidth Unavailability:* The ratio of total bandwidth-weighted unavailable seconds of FE ports by total bandwidth-weighted available seconds during a set measurement period (hour, day, month, etc.) shall be less than ***b***%, where unavailability of a port means that the port is out of service or below a service performance threshold for durations longer than $t_0$ seconds.
- *FRU Total Mean-time-to Repair:* FRUs shall be less than ***r*** minutes measured from the time of FRU failure to when a replacement unit has been successfully placed back into service. This metric includes travel and administrative time.
- *FRU Intrinsic Mean-time-to Repair:* FRUs shall average over a specified period less than ***r*** minutes measured from the start of the repair action to when a replacement unit has been successfully placed back into service. This metric excludes travel time, administrative time, and the assumption that spares are available. This metric measures the effectiveness of the NE's diagnostics. Objectives should be set based on type or criticality of the FRU.
- *FE Maintenance Actions:* The frequency of FE maintenance actions per unit of time. This attribute can also be normalized to such metrics as the number of service-users, the number of ports, the amount of bandwidth, etc. The objectives must be set for a defined configuration, size and engineered values.
- *Total FE FRU Return Rate:* The frequency of FRU returns per unit of time. This attribute can also be normalized to such metrics as the number of service-users, the number of ports, the amount of bandwidth, etc. The objectives must be set for a defined configuration, size, and engineered values.
- *Individual FRU Return Rate:* The NE shall package the hardware into FRUs at a size and return rate that minimizes repair and inventory costs without adversely degrading system complexity and cost. The objective average FRU return rate shall be less than ***v***% per year.

# 3 RELIABILITY-RELATED INTERNAL FEATURES AND METRICS

The following is a list of basic reliability-related features and capabilities required to achieve the FE Reliability-related external metrics objectives. They are grouped into the following categories:

- *Hardening:* To prevent the occurrence of a failure event.
- *Fault Tolerance:* A design's capability to prevent or reduce the impact of failure events on service or OAM&P functionality.
- *Fault Management:* To facilitate the containment of a failure and effective repair back to the network system's normal operating state.

## 3.1 Hardening Features

The Solution shall be capable of preventing the following external failure events from causing a functional or equipment failure of the FE as follows:

1. *NE Functional Integrity:* The NE shall not experience a functional failure or equipment failure within the specified limits of the Service Provider's operating environment: climate, operational vibration, earthquake, EMI/ESD, and supplied power.

2. *Traffic Robustness:* Service Customer traffic and control message overloads of $x$ times the specified level shall not cause a service outage.
3. *OAM&P Robustness:* There shall be no impact on established service from non-service-affecting management commands and queries. All potentially service-affecting OAM&P activities shall require command confirmation to minimize accidental service outage.
4. *Human Interface Design Integrity:* The physical design and customer operational documentation shall minimize craft person error.

The Solution Vendor shall provide test or field data for the Solution to demonstrate that the preceding hardening capabilities are met.

### 3.2 Fault Tolerance Features

The Solution Vendor shall provide both the design specification and the test results for the applicable fault-tolerant features used by the Solution to meet the external reliability-related metric objectives. These features mask or mitigate the impact on service due to specified failure events by using internal and/or network fault tolerance features. They are:

- *Network Protection/Restoration:* When configured in a network solution, the NE shall meet the network solution's network protection/restoration features inter-NE signaling specifications for the complete detection-recovery-repair cycle. Recovery of network services should recover in $\leq T_r$ seconds to a predetermined recovery state where the Network Solution is meeting functional and performance requirements. The total recovery time ($T_r$ ) is the sum of the times to detect, to notify for recovery, and to recover to a pre-determined recovery state.

  $T_r = t_d + t_t$ , where:

  $t_d$ = Fault detection time

  $t_t$ = Sum of the time interval for processing and transmitting a fault detection signal AND {the time to recover to the original state in case of a transient failure OR the time to recover to a state where the functional requirements are met}.
- *Hardware Fault Tolerance:* The FE shall automatically detect and recover from $c$ % of the hardware failure rate that impact greater than $x$ % of the customer ports in $\leq t_{rh}$ seconds. The detection time should be $\leq t_{dh}$ seconds.
- *Software Fault Tolerance:* The NE shall automatically detect and recover from $c$ % of the system software failure rate to at least a minimal operating configuration of non-failed hardware and a non-corrupted copy of system software in $\leq t_{rs}$ seconds for a specified reference configuration.
- *External Power Protection:* The NE shall have the capability to automatically recover from external power outages and survive for a duration $> x$ hours without impact on customer service.
- *Internal Power Supply Protection:* The NE shall recover from any single internal power supply or power distribution failure without impact on service.
- *Manual Recovery:* The NE shall have the ability for on-site and remote manual recovery from total outage to at least a minimal operating configuration of non-failed hardware and a non-corrupted copy of system software in less than $x$ minutes for a specified reference configuration.
- *In-service Software Upgrades:* The FE shall be capable of downloading software upgrades without impacting service and installing the software image where the FE's service interruption time shall be less than $x$ seconds for a specified reference configuration.

- *In-service Software Upgrade Resiliency:* The NE shall have the capability to automatically recover from failed software upgrades and patch applications. It shall recover in less than ***x*** seconds for a specified reference configuration.
- *In-service FRU Upgrades:* FRU replacements shall not require the powering down of the NE.
- *Management Control Fault Tolerance:* The NE shall automatically detect and recover from management control hardware failures in less than ***x1*** seconds and shall automatically detect and recover from management control software failures in less than ***x2*** seconds for a specified reference configuration. Recovery shall not impact customer services.
- *Multiple Control Plane Separation:* When the NE supports multiple control planes, failure of one shall not impact the other control plane(s).
- *I/O Port Duplication:* The NE shall provide I/O port protection based on service criticality, that automatically detects and recovers from > ***x*** % port hardware and link failures in ≤ $t_{rl}$ seconds. The detection time should ≤ $t_{dl}$ seconds.

### 3.3 Fault Management Features

The Solution Vendor's NE shall provide the following fault management features which are used to contain, isolate, and record failed equipment (locally and remotely) for effective repair and field tracking.

- *Equipment Fault Recording:* For all equipment failures, the NE shall record module identification (software and hardware), time of the event, and time of return to service.
- *Link Fault Recording:* For all link failures, the NE shall record link identification, time of the event, and time of return to service.
- *Overload Fault Recording:* For all service-affecting traffic overload events, the NE should record ports impacted, level of the overload, time of the event, and time of return to service.
- *Fault Record Storage:* The NE shall be capable of storing all equipment, link, and overload records for '***n***' hours or '***m***' records.
- *Fault Record Communication:* The NE shall be capable of sending the Fault Records to a remote location either automatically or on request.
- *NE Local Diagnostics:* A set of system diagnostics shall be available to meet the intrinsic mean-time-to repair objectives by being able to isolate NE's failures to the FRU for ≥ ***x***% of the NE's equipment hardware failure rates.
- *NE Remote Diagnostics:* A set of remote diagnostics shall be available to meet the total mean-time-to repair objective by isolating faults to the node or link for ≥ ***y***% of the NE's or link's failure rate.
- *System Reset:* NE shall provide capability to have its system level and shelf level control software individually reset locally or remotely through software commands.

The Solution Vendor shall provide reliability-related metric predictions, test results, or field results to demonstrate compliance.

## 4 RELIABILITY PROGRAM RESULTS

The following are the key outputs from the Vendor's reliability program required by Service Providers to help manage the FE reliability, availability, maintainability, and survivability risk across the NE's lifecycle. The Vendor shall be required to produce all of these outputs unless specifically notified to the contrary by a Service Provider.

1. The Vendor shall provide an up-to-date list of non-compliant reliability-related items and a plan for full compliance.
2. The Vendor shall provide to the Service Provider documentation concerning key internal development and support processes and practices including hardware and software design and engineering policies for reliability. This documentation should include descriptions of how the Vendor monitors and controls each of these key internal processes.
3. The Vendor shall provide reliability-related predictions for planning maintenance and sparing inventory programs.
4. The Vendor shall track and report the actual field performance of the external reliability-related metrics and compare with objectives.
5. The Vendor shall do root cause analysis on non-compliant external reliability-related metrics and report effectiveness to the Service Provider of corrective and preventive action plans.

## 5 RELIABILITY-RELATED TERMINOLOGY DEFINITIONS

This section defines basic reliability-related terms:

- *Availability* is the proportion of the operating time in which an entity meets its in-service functional and performance requirements in its intended environment.
- *Failure* is the occurrence of an event in which an entity does not meet its in-service functional and performance requirements or expectations.
- *Failure Frequency* is the rate of occurrence of failure (in time or in number of operations) of an entity to meet its in-service functional and performance requirements in its intended environment.
- *Failure Recovery Coverage* is the fraction of the recoverable failure rate of fault-tolerant equipment that is successfully detected and recovered.
- *Failure Isolation Coverage* is the fraction of the failure rate of an FRU that can be isolated to the failed FRU by the NE's diagnostics.
- *Fault Tolerance* is the ability of a functional entity to mask or mitigate the impact of faults on its specified operation.
- *Maintainability* is the ability of an entity to facilitate its diagnosis and repair.
- *Intrinsic Mean-time-to Repair* is the average time to field repair a failed FRU starting from the initiation of the repair activity to when the replacement FRU is returned to service. This metric excludes travel time, assumes spares are available, and represents the effectiveness of the NE's diagnostics.
- *Total Mean-time-to Repair* is the average time to field-repair a failed FRU starting from the time of the failure to when the replacement FRU is returned to service. This metric includes all travel and administrative time, such as that required to identify and retrieve the required spare.

- *Mean-time-to Restore Service* is the average time to restore service measured from when the service has failed to when it meets its in-service functional and performance requirements or expectations.
- *Network Recovery Cycle* is the steps, initiated by a failure event, that a system of Network Elements executes to detect, recover, and notify for repair, in order to return the network to its original normal operating state. Referring to Figure 4, the successful network recovery from the normal state to the recovered states (initial and optimized) requires that network element involved in the recovery communicate.

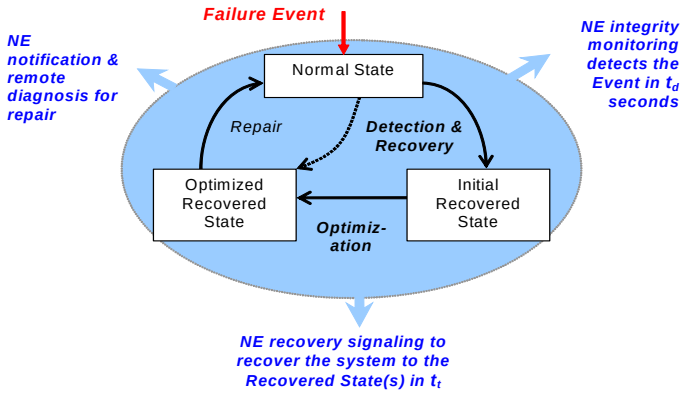


**Figure 4 - Network Recovery Cycle**

- *Reliability* is the probability that an *entity* will complete its intended mission as required over a specified period of time in its intended environment.
- *Reliability-related Prediction* is the computation of reliability-related metrics from design parameters and piece-part failure rate models that have been calibrated from field or life-test data.
- *Reliability-related Estimation* is the computation of reliability-related metrics from development process verification and validation parameter results.
- *Service Performance Threshold* is the level of service performance below which the customer service is considered unacceptable. Performance may be considered with respect to packet delay, packet jitter, packet integrity and other pertinent parameters.
- *Survivability* is the ability of an entity to continue to meet its functional requirements during network events such as cyber-attacks, physical attacks, natural disasters, and traffic overloads.