ATIS STANDARD

ATIS-0100026

A METHODOLOGY FOR DESIGN OF END-TO-END NETWORK RELIABILITY FOR PROACTIVE NETWORK RELIABILITY PLANNING

TECHNICAL REPORT

ATIS is the leading technical planning and standards development organization committed to the rapid development of global, market-driven standards for the information, entertainment and communications industry. More than 200 companies actively formulate standards in ATIS' Committees, covering issues including: IPTV, Cloud Services, Energy Efficiency, IP-Based and Wireless Technologies, Quality of Service, Billing and Operational Support, Emergency Services, Architectural Platforms and Emerging Networks. In addition, numerous Incubators, Focus and Exploratory Groups address evolving industry priorities including Smart Grid, Machine-to-Machine, Networked Car, IP Downloadable Security, Policy Management and Network Optimization.

ATIS is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), 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). ATIS is accredited by the American National Standards Institute (ANSI). For more information, please visit < http://www.atis.org >.

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 OF MERCHANTABILITY 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, WITH RESPECT TO ANY CLAIM, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES ANY AND ALL USE OF OR RELIANCE UPON THIS 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.

ATIS-0100026, *A Methodology for Design of End-to-End Network Reliability for Proactive Network Reliability Planning*

Is an ATIS Standard developed by the **PRQC Quality of Service (QoS) Working Group** under 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

Printed in the United States of America.

ATIS-0100026

Technical Report on

A Methodology for Design of End-to-End Network Reliability for Proactive Reliability Planning

Alliance for Telecommunications Industry Solutions

Approved April, 2010

Abstract

This Technical Report (TR) discusses design for network reliability methodology that supports the delivery of desired service availability. Design for reliability is fundamental to proactive network-reliability and resiliency planning; the TR describes a methodology for approaching this key task. To enable a more informed decision on the appropriate reliability-level for a given network-element (NE) it introduces the Significant Point of Failure (SgPoF) metric. Early computation of the SgPoF in the design process, followed by the implementation of the recommended design will result in Capital Expenditure (CapEx) savings and reduce the cost associated with design changes that occur late in the design for reliability process.

FOREWORD

The Alliance for Telecommunication Industry Solutions (ATIS) serves the public through improved understanding between providers, customers, and manufacturers. The Network Performance, Reliability, and Quality of Service Committee (PRQC) develops and recommends standards, requirements, and technical reports related to the performance, reliability, and associated security aspects of communications networks, as well as the processing of voice, audio, data, image, and video signals, and their multimedia integration. PRQC also develops and recommends positions on, and foster consistency with, standards and related subjects under consideration in other North American and international standards bodies.

The mandatory requirements are designated by the word *shall* and recommendations by the word *should*. Where both a mandatory requirement and a recommendation are specified for the same criterion, the recommendation represents a goal currently identifiable as having distinct compatibility or performance advantages. The word *may* denotes a optional capability that could augment the standard. The standard is fully functional without the incorporation of this optional capability.

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

At the time it approved this document, PRQC, which is responsible for the development of this Technical Report, had the following members:

M. Neibert, PRQC Chair (Telcordia)

P. Tarapre, PRQC Vice Chair (AT&T)

C. Underkoffler, ATIS Chief Editor

H. Pant, Technical Editor (Huawei)

The PRQC Quality of Service (QoS) Working Group, which was responsible for the development of this document, had the following members:

Active Participants:

K. Biholar

J. Colombo

C. Dvorak

M. Fergano

M. Linnell

S. Makris

M. Neibert

A. Nguyen

P. Tarapore

A. Webster

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

Technical Report on

A Methodology for Design of End-to-End Network Reliability for Proactive Network Reliability Planning

1 Scope & Purpose

Service availability has received strong attention in ATIS PRQC in terms of metric definitions as well as measurement methodologies. This Technical Report (TR) addresses the issue of service availability by approaching it from a proactive network planning perspective. Specifically, this TR highlights the planning of necessary network resources such that a desired level of service availability can be engineered. The planning is brought into sharp relief through a step-wise approach to an end-to-end design for network reliability. The methodology leverages the learning from legacy-networks while addressing the challenges faced by the Next-Generation Networks (NGNs). To design network elements at the appropriate level of reliability the Significant Point of Failure (SgPoF) metric is introduced. It measures the impact of network-element (NE) failure on service-subscribers. Calculations are provided to illustrate the concepts introduced.

This proposal supports the ATIS-PRQC issue A0049 “A Methodology for Design of End-to-End Network Reliability for Proactive Reliability Planning” [AT-0049]. The methodology will be of interest to all parties involved in telecommunication (i.e., large enterprises or service-providers that need the communications networks and vendors who supply the networks).

2 Normative References

[AT-PROV]: Provisioning –*ATIS Telecomm Glossary 2007*[1]

[AT-0049]: Issue A0049, “A Methodology for End-to-End Network Reliability for Proactive Reliability Planning,” August 2009.[2]

[AT-100016]: ATIS-0100016, “End-to-end Service Availability: General Definition,” September 2007.[3]

[BL-2005]: Carlos Urrutia-Valdes, Amit Mukhopadhyay, and Mohamed El-Sayed, “Presence and Availability with IMS: Applications Architecture, Traffic Analysis, and Capacity Impacts,” Bell Labs Technical Journal 10(4), 101-107, 2006.

[BL-2008]: H. Pant, C.K. Chu, S.H. Richman, A. Jrad, and G.O’Reilly, “Reliability of Next-Generation Networks With a Focus on IMS Architecture,” Bell Labs Technical Journal 12(4), 109-126, 2008.

[CL-1128]: CableLabs, “VoIP Availability and Reliability Model for the PacketCable Architecture, Cable Television Laboratories,” Tech. Report PKT-TR-VoIPAR-V01-001128, Nov. 28, 2000.

[1] http://www.atis.org/glossary/definition.aspx?id=2474

[2] This reference is a committee contribution. PRQC committee participants can access this document at < http://contributions.atis.org >. Copies of this contribution will be made available to all other interested parties upon request. Such request should be made to the ATIS Document Center Administrator at < doccenter@atis.org >.

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

[TT-512]: Telcordia Technologies, "LATA Switching Systems Generic Requirements (LSSGR): Reliability, Section 12," GR-512, January 1998.[4]

3 DEFINITIONS

The Significant Point of Failure (SgPoF) metric for a network element is a measure of the expected number of subscribers affected by failure of that network element.

Provisioning, as used in this document, is the setting in place and configuring of the hardware and software required to activate a telecommunications service for a customer; in many cases the hardware and software may already be in place and provisioning entails only configuration tasks such as creating (or modifying) a customer record in a database and associating it with the service(s) and service level for which the customer has subscribed. [AT-PROV].

4 ACRONYMS & ABBREVIATIONS

A/S = Active Standby

CapEx = Capital Expenditure

COPT = Capacity Outage Probability Table

CSCF = Call Session Control Function

DT = Downtime

HW = Hardware

IP = Internet Protocol

NE = Network Element

NGN = Next Generation Network

OAM = Operations, Administration and Maintenance

OpEx = Operations Expenditure

PSTN = Public Switched Telephone Network

SgPoF = Significant Point of Failure

SIP = Session Initiation Protocol

SLA = Service Level Agreement

SPoF = Single Point of Failure

SW = Software

TR = Technical Report

5 INTRODUCTION & RATIONALE

The planning and provisioning of telecommunications services is a complex task. It requires a careful balancing of the business and technical aspects. The task involves detailed understanding of sophisticated systems that comprise the various network elements and using this understanding to

[4] 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 >.

design and implement the end-to-end network to support the desired services. Mistakes in the planning and provisioning steps have a direct business impact in terms of Service Level Agreement (SLA) penalties and lost revenue due to the loss of dissatisfied-customers. At the same time business constraints require care to not overspend on CapEx and Operations Expenditure (OpEx).

The planning and provisioning processes have been developed based on experience with legacy networks. At a high-level, the usual process for planning through provisioning is as follows:

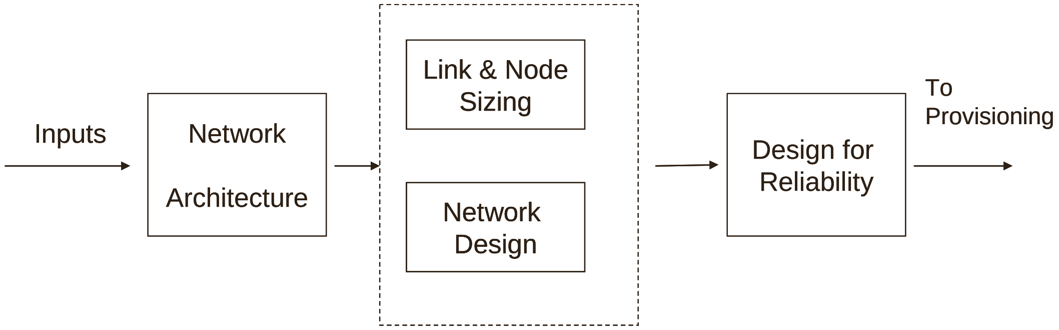

Figure 1 - A High-Level View of the Planning & Provisioning Process

As shown in Figure 1, design for reliability is fundamental to the planning and provisioning of networks for service availability. It is also a task that falls squarely within the purview of reliability engineering. Hence this TR will focus on design for reliability as a key activity for planning and provisioning in the delivery of network service availability.

The design for network reliability in legacy networks incorporates the following essential steps:

- **Data collection**: Reliability data for each NE that is in the network architecture. For each in-scope service, a reference-connection representation of the end-to-end network that supports the particular service.
- **Network reliability modeling and analysis**: Obtain the end-to-end network reliability using the reference-connection and equipment reliability data. (If needed, the same reference connection can be used to calculate other reliability metrics as well.)
- **Comparison of model-derived network availability and other reliability metrics with objectives**: Ensure the designed network meets the reliability objective. In case the objective(s) are not met, the reliability engineer will do a gap-analysis to identify design-areas where improvement can help meet the reliability objectives.
- **Re-Design the network:** The reliability engineer and the designer will together work the changes in the network design to ensure the objectives are met.

With the advent of IP technology, the traditional design for reliability methodologies will be inadequate for NGNs. The distributed nature of the IP network and the multiple services it supports will lead to a very large number of reference connections that are needed in the design for network reliability. As services move to networks based on IP-technology, often the requirements have to be ported over from legacy technologies. This requires using reference-connections and reliability-budgeting to map existing requirements onto the components of the new-technology network. An example of this approach is provided by [CL-1128]. Thus it makes it important for the network-designer to adopt a way of organizing the reference-connections.

Early in the planning and provisioning process the impact of each NE's failure should be assessed when deciding on its reliability design. Making the reliability-related changes late in the design process may entail changes in other design-decisions, (e.g., capacity-sizing). This is especially true for NGNs that will be more complex due to the disaggregated nature of the IP-technology. Secondly, if these design-changes are made without considering the failure impact they could result in CapEx that may not be justified when evaluated for the impact on subscribers. As a simple example, a decision to remove all Single Points of Failure (SPoF) to improve reliability will be expensive and probably unnecessary for many network elements whose failure does not impact a large number of service-subscribers. The impact of NE failure depends on the reliability of the NE and also the traffic (load) that it has to process. An NE that is failed but has no traffic to serve will not impact any subscribers.

In the design for reliability of NGN new failure sources need to be considered. Such failure sources are typically not of concern when designing legacy networks. Examples of such non-traditional failure sources are power and cyber-security attacks. In legacy-network, failures in the telecommunications network are fairly independent of failures in the power infrastructure. The Public Switched Telephone Network (PSTN) wireline phone service is still available when there is a power outage because of power available from backup batteries or diesel-generators. In IP networks, the distributed access media will depend largely on power supplied from commercial sources with many NEs placed in non-Central Office environment without the benefit of backup batteries or diesel-generators. Thus design for reliability methodologies have to put adequate emphasis on power. Lack of security is another new failure-source. With the use of IP technology, cyber-threats are an increasing concern. In legacy Time Division Multiplexing (TDM) networks the SS7 signaling/control network was separate from the transport network. Furthermore, with proprietary hardware and software, it was not possible for the hacker to access and attack these networks. IP technology with widespread use of off-the-shelf hardware and software components has changed this. Planning and provisioning through the design for reliability has to factor in these threats.

6 A DESIGN FOR RELIABILITY METHODOLOGY

To enable proactive network reliability-planning that would address the above mentioned new challenges, the following four-step methodology is proposed. Figure 3 summarizes the concepts. In Section 7, we provide an example of how to calculate the SgPoF metric and use it to improve the design for reliability.

1. Input Collection

The first step consists of collecting input data required at the various steps of the design for network reliability process. The data include the following.

a) NE specific data: Starting with the list of the planned network elements, their component configurations, reliability features, and component failure rates.
b) Traffic Profile: The expected traffic behavior on the planned network. This data is available to network architects as it is used to size the links and nodes.
c) List of the planned applications and services.

d) Reliability requirements for services and networks: The reliability requirements are conveyed as part of their contract. In case these are not explicitly stated, the network-designers can rely on their own experience or derive them from standards using reliability-budgeting.

e) Proposed metrics for reliability measurement: In case these are not specified, the network-designers can rely on experience or obtain them from published standards.

2. Network Architecture (Preliminary Network Design)

This step creates the network architecture (preliminary network design) based on the network elements and the traffic profile.

a) For each in-scope service, identify the call path and the end-to-end reliability requirements. For ease in management of the numerous call paths, they can be collected in a service matrix as shown in Figure 2. To ensure that the correct level of reliability is designed for, objectives should be set for SgPoF and for the end-to-end reliability.

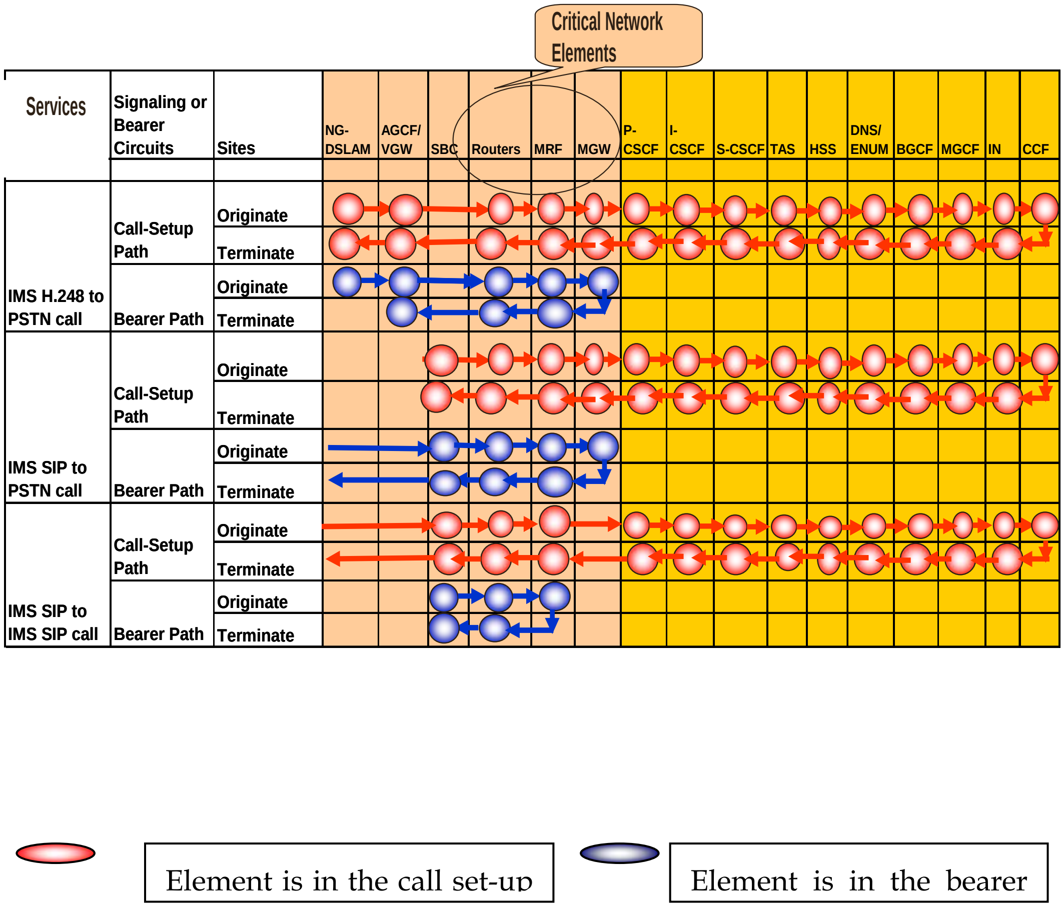

Figure 2 - Example of a Service Matrix for an IMS Network

b) Take a first-cut at improving design such as choice of reliability features and alternative choice of equipment.

3. Model Significant Points of Failure (SgPoF).
   Prioritize network elements by the impact of their failure on service-subscribers. Use of the service matrix will aid the network-designer in limiting this modeling to critical network elements only. Critical network elements are those that appear in the call-paths most frequently (Figure 2).
   a) Measure the significance of an NE's failure by modeling its impact on service. The impact can be measured by the expected number of subscribers affected by the NE's failure. We will refer to this measure as the SgPoF metric.
   b) If the SgPoF metric value for a given NE is too high, (e.g., it does not meet an objective for the NE,) then improve design to mitigate the impact of that NE. Such redesign could be the addition of redundancy or choice of an alternative reliability feature available on that NE.

4. Reliability Validation
   a) Model end-to-end reliability to ensure compliance with end-to-end reliability network and/or service requirements. This reliability model will depend on the metrics under consideration. For service availability metric, standard definition of service availability are provided by ATIS [AT-100016].
   b) Incorporate the effect of non-traditional failure sources in the reliability models. These failure-sources are unique to IP networks, (e.g., power and security).

In a practical design effort, the design is improved iteratively. So as shown in Figure 3, after Step 3 and after Step 4, there are decision points to check if requirements are met. Failure to meet reliability requirements, results in the designer looping-back to improve the design for reliability. Such improvements are achieved through the addition of reliability features, change in choice of NE or re-arranging the links so that particular network-elements handle less traffic.

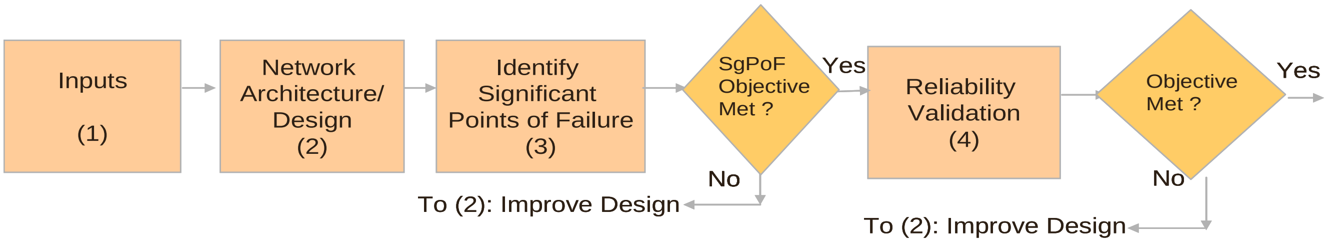

Figure 3 - An End-to-End Design for Reliability Process for NGN

7 EXAMPLE: SIGNIFICANT POINT OF FAILURE (SgPoF) METRIC CALCULATION

We provide an example SgPoF metric calculation for the NE of an IMS network [BL-2008]. The SgPoF for a NE is a measure of the expected number of subscribers affected by failure of the NE being analyzed.
The calculation and its use in improving network design are performed in four (4) steps.

- Step 1: Create the capacity outage probability table (COPT). The COPT shows the NE's remaining capacity to serve traffic after each possible failure mode. It provides the probability of the NE having that capacity.
- Step 2: Create the traffic (or, load) profile for the NE in terms of messages per second.
- Step 3: Convolve the two models to obtain the SgPoF metric.
- Step 4: Use the SgPoF to improve design.

Step 1: Construct the COPT

The following inputs are required.

1. The internal architecture of the NE specifying all the load affecting sub-modules. As an example, a typical CSCF NE of the IMS consists of:
   a) Common core modules such as chassis, power plane and mid plane, power supply, circuit breaker unit and fan tray, alarm card, and Ethernet switch cards,
   b) The operations, administration, and maintenance (OAM) blades, and
   c) The application servers (CSCF instance).
2. The reliability for each of the sub-modules. This is expressed as the hardware and software availability and can be derived from the sub-module's failure-rate data.
3. The rated message-processing capacity of each sub-module. This is expressed in the number of messages processed per second.

The assumed availability data for the common core and application servers are given in Table 1.

Table 1 - Availability for the common core and application servers of the CSCF

	Redundancy	HW Unavailability	SW Unavailability	Total Unavailability	Total DT (min/yr)
Application Server	Duplex	0.0000001	0.00000351	0.0000036101	1.90
Common Core	A/S	0.00000514	0.000000	0.0000051404	2.70
Common Core + OAM Blades		0.00000533	0.00000351	0.0000088416	4.65

Note: A/S- Active Standby, CSCF-Call Session Control Function, DT-Downtime, HW-Hardware
OAM-Operations, Administration, and Maintenance, SW-Software

In our example, the configuration of the CSCF is assumed to be 1 shelf, with 7 CSCF instances.

The availability of the common core elements and of each CSCF instance is combined with the capacity of 3000 messages per second for each CSCF instance to create a COPT for a unit with 1 shelf containing 7 CSCF instances (Table 2).

Table 2 - Capacity Outage Probability Table for 1 unit of 1 shelf with 7 CSCF instances

Mode	Capacity	Probability
0	21000	0.9999658882
1	18000	0.0000252699
2	15000	0.0000000003
3	12000	0.000
4	9000	0.000
5	6000	0.000
6	3000	0.0000
7	0	0.0000088416

The calculation is as follows:

Note that mode k, 0< k < 7, means k out of n (n=7 in this example) CSCF instances have failed but the common core elements are working. The available capacity is then (n-k)*3000 messages per second.

Pr (mode k) = Pr(Available Capacity = 3000*(n-k) messages per second).

= Pr(exactly k out n CSCF instances have failed and common core and OAM blades are available)

Using the independence of the components = [n! / (k!(n-k)!)] *p^{n-k} *q^{k} * Pr(common core and OAM blades are available)

Where n= total number of pairs of CSCF instances
k= number of CSCF instances failed,
p=availability of a CSCF instance = 0.9999963899, and
q=unavailability of the CSCF instance = 0.00000361011.

Thus as an example,

Pr(Mode 1) = Pr(18000 messages per second)

=[7!(1!(7-1)!*$(0.9999963899)^{6}$*0.00000361011)*[0.9999911584]

=0.0000252699

Note that Pr(Mode 7) = Pr(All 7 CSCF instances fail or the common core fails and OAM blades fail)

$$= 1-\sum_{k=1}^{k=6} \Pr(Mode\_k)$$

We also consider the case of 2 shelves each containing 7 CSCF instances because we will need it later in Step 4. For two identical shelves, combining Table 2 with itself will yield the COPT for the case of 2 shelves each containing 7 CSCF instances. The result is shown in Table 3.

Table 3 - Capacity Outage Probability Table for 2 identical units each of 1 shelf with 7 CSCF instances

FailureMode	Capacity	Probability
0	42000	0.99994946
1	39000	5.05385E-05
2	36000	1.18594E-09
3	33000	0
4	30000	0
5	27000	0
6	24000	0
7	21000	0
8	18000	0
9	15000	0
10	12000	0
11	9000	0
12	6000	0
13	3000	0
14	0	0

Step 2: Construct the load profile for the network elements

The load profile for the NE being analyzed should be developed using the actual required load for the time-period considered. The Table 4 shows the Telcordia GR-512 [TT-512] traffic profile that is used in the example.

Table 4 - The Telcordia GR-512 traffic profile (volume and probability)

Percent of Peak	Load Level L(j)	Probability $P_{L(j)}$
1.00	L(0)	0.16666667
0.80	L(1)	0.33333333
0.50	L(2)	0.16666667
0.10	L(3)	0.33333333

Step 3: Convolve the COPT and traffic profile to calculate the SqPoF metric.

Loss of load (LoL) occurs when the traffic exceeds the available capacity. The stochastic behavior of the load and available capacity are captured by the traffic profile and the COPT, respectively. Thus a loss of load analysis is obtained by convolving the two.

Using the following notation,
L(j)=Load level j (see Table 4),
$P_{L(j)}$ = Probability of load level L(j) per traffic profile (see Table 4),
$C_{P(i)}$ = Fraction of peak load capacity corresponding to failure mode i (see Table 5),
P[$C_{P(i)}$]=Probability that fraction of peak load capacity is $C_{P(i)}$,
Peak load = As specified by network designers (as shown in Table 5, the value used in the example is a load of 20,470 messages per second for the CSCF),
n=7 (for our example), and
m=maximum traffic profile level (3, for our example),

the formula for the total expected loss of load is given by:

$$\sum_{i=0}^{n} P[C_{P(i)}] \sum_{j=0}^{m} \max[LoL(j,i),0]$$

where ,

LoL(j,i) = $P_{L(j)}$[L(j) – $C_{P(i)}$]*peak load. The formula follows from the observation that the expected LoL for available capacity $C_{P(i)}$ is:

$$P[C_{P(i)}] \sum_{j=0}^{m} \max[LoL(j,i),0]$$

Table 5- Calculation of SgPoF loss of load for the CSCF with 1 shelf (Peak load = 20,470 messages per second)

Failure Mode	$C_{P(i)}$	$P[C_{P(i)}]$	Expected LoL
0	1.025892	0.99997473	0
1	0.879336	2.52702E-05	0.010402908
2	0.73278	2.73686E-10	3.75041E-07
3	0.586224	1.64673E-15	0
4	0.439668	5.94491E-21	0
5	0.293112	1.28771E-26	0
6	0.146556	1.5496E-32	0
7	0	7.99177E-39	0

Total Expected LoL = 0.010403283 messages per second.

For this example CSCF, Table 5 shows the peak load in messages per second, the available capacity, $C_{P(i)}$, after the occurrence of each failure is expressed as a fraction of the peak load, the corresponding probability is shown in column 3 of Table 5, and the final column gives the expected loss of load. The expected total loss of load due to all failure modes for 1 shelf with 1 CSCF configuration is the sum of the expected loss of load due to each failure mode. Following Table 5, the expected total loss of load due to all failure modes for the configuration of 1 shelf with 7 CSCF instances is 0.010403283 messages per second. Dividing the loss of load by the average number of messages per second per subscriber yields the "expected number of subscribers affected."

Step 4: Use the SgPoF to improve the design

To illustrate the use of this metric we develop the example further.

Taking the simple case of 1 service only, we work out an example where the SgPoF metric is used to make decisions on the reliability design of the CSCF in the network. The service we choose is the presence and availability service. It is viewed as an indispensable feature of the IMS-supported next-generation services to enable generation of additional revenue and reduce churn for the service provider.

All presence-related Session Initiation Protocol (SIP) messages pass through the CSCF. Thus failure of the CSCF will directly impact the subscriber. It has been calculated that during the busy hour, a user of the presence service, will generate the following processing requirements for the CSCF [BL-2005].

Table 6 - Processing Requirements for CSCF due to presence service

	P-CSCF	S-CSCF	CSCF (total)
SIP Messages per subscriber during Busy Hour	24	2.7	26.7

Using the traffic profile from Table 4, the average number of SIP messages per hour for a subscriber

= 26.7(1x1/6 + 0.8x1/3 + 0.5x1/6 + 0.1x1/3) = 14.685 messages per hour per subscriber.

So the number of SIP messages per subscriber per second = 14.685/ (60*60) =0.004079.

From Table 5, the expected Loss of Load = 0.010403283 messages per second.

So, average number of subscribers lost per second by the configuration of 1 shelf with 7 CSCF instances = 0.010403283/0.004079 ~ 3.

This may seem like a small number compared to the total number of subscribers whose SIP messages are being processed by the CSCF. However, as a worst case scenario, the CSCF could be impacting a different set of 3 subscribers every second. This may then build up to over 9,180 (= 60*60*0.010403283/0.004079) subscribers per hour.

Assuming the loss of 3 subscribers per second is not acceptable to the network designer, one option will be to improve the reliability of the CSCF. A common method of improving reliability is to enhance redundancy of the components. For this example the network designer can modify the configuration by adding more CSCF instances to handle the same load (i.e., 20,470 messages per second). We illustrate the effect of adding an extra shelf with 7 CSCF instances in Table 7. The calculation uses the formula explained in Step 3 and utilizes Table 3.

Table 7- Calculation of SgPoF loss of load for the 2 shelves (Peak load = 20,470 messages per second)

Failure Mode	$C_{P(i)}$	$P[C_{P(i)}]$	Expected LoL
0	1.025892	0.99994946	0
1	0.952614	5.05385E-05	0.00817
2	0.879336	1.18594E-09	4.88E-07
3	0.806058	1.71256E-14	0
4	0.73278	1.7002E-19	0
5	0.659502	1.22759E-24	0
6	0.586224	6.64761E-30	0
7	0.512946	2.74271E-35	0
8	0.439668	1.2198E-40	0
9	0.36639	2.08516E-46	0
10	0.293112	3.76385E-52	0
11	0.219834	4.94108E-58	0
12	0.146556	4.45947E-64	0
13	0.073278	2.47681E-70	0
14	0	6.38684E-77	0

Total Expected LoL =0.008170884 messages per second

From Table 7, the expected Loss of Load in the case of 2 shelves with 14 CSCF instances = 0.008171 messages per second.

Average number of subscribers lost per second by the configuration of 2 shelves with 14 CSCF instances = 0.008170884/0.004079 ~ 2.

Thus the average number of subscribers lost per hour by the configuration of 2 shelves with 14 CSCF instances = 7,211 which is about 2,000 less subscribers affected per hour than with the former configuration of 1 shelf with 7 CSCF instances.

It is to be noted that increasing redundancy is one of several options available to the network designers for improving the reliability. The main point is that the SgPoF metric affords a way of comparing the different design-options early in the design process to enable proactive reliability planning.

8 BIBLIOGRAPHY

Work on service-availability is being carried out in different standards bodies. We point out published standards. At the time of publication, the editions indicated were valid. All standards are subject to revision, and interested parties are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below.

- ATIS 0100016, *End-To-End Service Availability: General Definition*.[5]
- ITU-T Recommendation Y.1540, *Internet protocol data communication service – IP packet transfer and availability performance parameters*.[6]
- ATIS-0100020, *Availability from Outages*. [5]
- ITU-T Y.1561, *MPLS Networks*. [6]
- ITU-T Y.1563, *Ethernet Frame Transfer*. [6]

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

[6] This document is available from the International Telecommunications Union. < http://www.itu.int/ITU-T/ >