Network Reliability Council (NRC)

Reliability Issues - Changing Technologies Focus Group

Advanced Intelligent Network Subteam Final Report

February 22, 1996

Ray Bonelli	AT&T Network Systems
Ed Bonkowski	Advantis
Lynda Eckes	Bell Atlantic
Jim Funk	US WEST
Clint Hamilton (Chair)	Bellcore Professional Services
Gabor Luka	NCS
Doris Nagel/Jeff Ragle	Bellcore SCP
Alex Nichols	Nortel
Pete Shelus/George Stanek	AT&T Network Services
Ken Walling	Pacific Bell
Chao-Ming Liu (AIN Subteam Secretary)	Bellcore Professional Services

TABLE OF CONTENTS

1. Executive Summary

The FCC asked the Network Reliability Council (NRC) to address reliability issues that may arise due to an increase of new technologies being deployed in the telecommunications networks, the implementation of advanced new services offered to the public, and the emergence of a proliferation of new service providers. Specifically, the NRC was chartered to study reliability concerns arising out of new technology providing expanded services over new or traditional facilities, which for this study is considered to be Advanced Intelligent Network (AIN) capabilities. The mission of the Reliability Issues - Changing Technologies Focus Group's AIN subteam is to identify major service impacting network reliability, integrity, and interoperability issues related to the architecture, operations, and maintenance of AIN.

The AIN subteam of the Changing Technologies Focus Group has been working for about a year to determine where the potential AIN vulnerabilities are and then recommend improvements. The subteam has concluded that the operation of the Common Channel Signaling (CCS) network has improved as a result of the first NRC effort which concluded in 1993. The network is running well and continuing to improve as carriers gain experience with the technology. However, the networks are now facing the rapid introduction of new AIN technology, AIN services and AIN service providers. Thus, the subteam believes that some areas need to be addressed to maintain the integrity of the networks and the quality of the AIN services. Those areas and recommendations are contained in Section 5.

In addition to recommendations specific to AIN, the subteam also contributed to the development of a New Technology Reliability Template (Appendix F), which can be used as a screening tool for assessing the reliability of any new network technology.

2. Background

2.1 Mission

The National Public Switched Network (PSN) has the deserved reputation of providing its users highly reliable, end-to-end services. The Federal Communications Commission (FCC) and its Network Reliability Council (NRC) want to ensure that this remains the standard mode of operation throughout a dramatic increase in the number of new technologies being deployed, the implementation of advanced new services offered to the public, and the emergence of a proliferation of new service providers. Specifically, the NRC was chartered to study reliability concerns arising out of new technology providing expanded services over new or traditional facilities, which for this study is considered to be Advanced Intelligent Network (AIN) capabilities. The issue statement developed by the Network Reliability Steering Team (NOREST II) committee, which was used as a guide in the subteam's work plan development, is shown as Appendix A.

The mission of the Reliability Issues - Changing Technologies Focus Group's AIN subteam is to identify major service-impacting network reliability, integrity, and interoperability issues related to the architecture, operations, and maintenance of AIN.

> *The prime objective of the AIN subteam is to ensure that there be no FCC reportable outages[*] related to AIN.*

In this report, the subteam identifies reliability issues and opportunities for improvement, and proposes solutions in these areas.

2.2 The Advanced Intelligent Network

The AIN is an evolving, service independent network architecture that provides important new capabilities for the rapid creation of customizable telecommunications services. The subteam looked at the AIN to date, which includes 800 service and some basic AIN services, and emerging AIN services such as Personal Communications Service (PCS) and local number portability. Figure 2.1 illustrates the architecture considered by the AIN subteam.

[*] An FCC reportable outage is an outage in the telephone network that meets the FCC defined outage reporting criteria. These criteria were first introduced in FCC Docket No. 91-273 in 1992 requiring local exchange or inter-exchange common carriers operating either transmission or switching facilities notify the FCC within 90 minutes if they experience service outages potentially affecting 50,000 or more customers and lasting 30 or more minutes. The criteria were later amended in September, 1994; one important change is to require reporting of outages potentially affecting 30,000 or more customers and lasting 30 or more minutes. For detailed information regarding these criteria, please refer to the FCC's Rules and Regulations, Section 63.100.

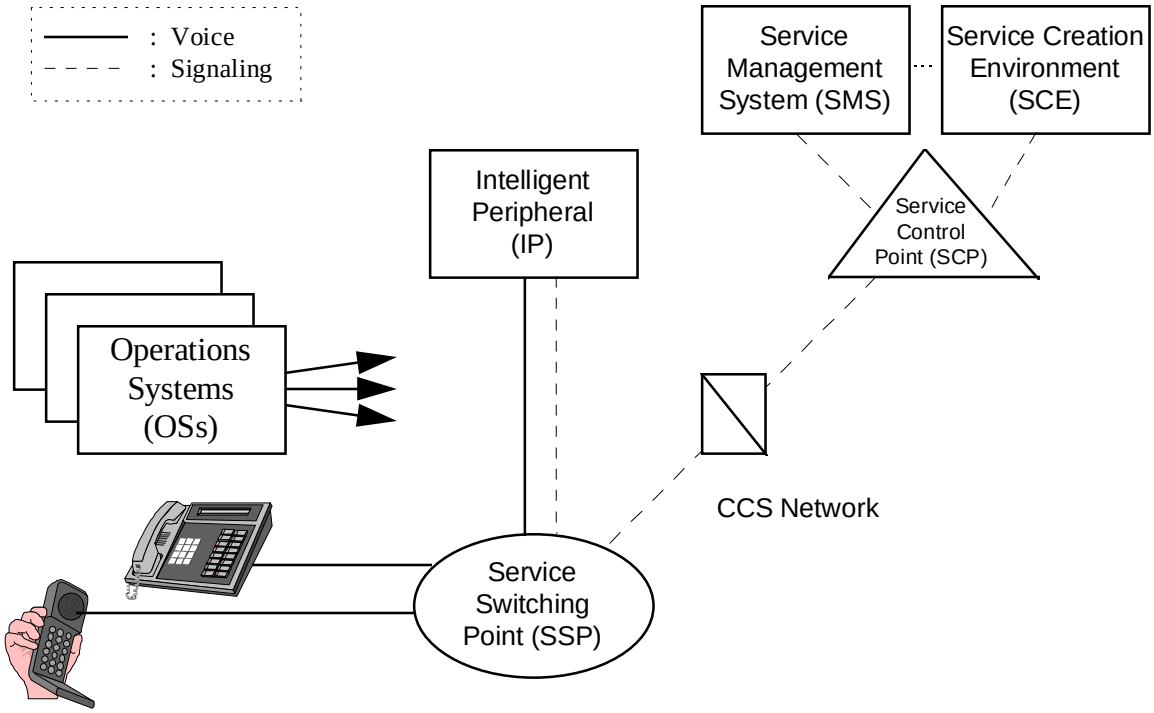


Figure 2.1 AIN Architecture

The major network elements and systems of the AIN are:

- **AIN/SCP** - The Service Control Point (SCP) is a component of an intelligent network that not only stores customer data but also responds to queries from Service Switching Points (SSP).

- **IP** - The Intelligent Peripheral (IP) is a network system in the AIN architecture containing functions that enable flexible information interactions between an end user and the network. The IP provides resources such as customized and concatenated voice announcements, voice recognition, and digit collection. The IP also contains switching fabric to connect users to these resources. It is directly connected to one or more SSPs.

- **AIN/SSP** - The AIN/SSP is a central office switching system with software to recognize a variety of triggers within customer signals and, based on these triggers, to generate queries to SCPs and then use the information received from SCPs to process calls. It communicates with AIN elements and responds to instructions from other AIN elements. It also provides AIN services to users connected to subtending non-AIN exchanges (NAP) (which is not shown in Figure 2.1).

- **SMS** - The Service Management System (SMS), a system outside the network, provides a support interface through which customer data and service logic in SCPs can be added to or managed. The SMS is specifically designed to facilitate the provisioning, maintenance, and administration of service data required by the AIN/SCP.

- **SCE** - To meet the definition of an Advanced Intelligent Network, the network must allow the rapid introduction of new services that are programmable by the service providers and

their customers. The process and environment that allow for this rapid introduction of service is called Service Creation. Service Creation Environment (SCE), a subset of Service Creation, includes all of the physical aspects, including organizational structures and computers.

- **CCS Network** - Issues related solely to the CCS network were not addressed by the AIN subteam because they were previously studied by the NRC's Signaling Network Systems (SNS) Committee.

2.3 Applicability of Results to Services

The AIN subteam recognizes that AIN networks will provide a variety of services and that some service, or features of a service, will not require the same level of service reliability as today's "plain old telephone service." Therefore, the application of the recommendations in this report must be considered in the context of what service(s), service-types, or features will be carried by the service provider's network, and as a result might fail from the customer's view. The subteam has focused on the area of major FCC reportable outages; therefore, service-types would be those where customers could loose their channel of communication and calls will fail (called "dial-tone like services.")

2.4 Recommendation and Best Practice Definition

The term "recommendation" or "Best Practice" as used in this report is as follows: "recommendations are those countermeasures (but not the only countermeasures) that go furthest in eliminating the root cause(s) of outages. None of the recommendations are construed to be mandatory.

Service providers and suppliers are strongly encouraged to study and assess the applicability of all countermeasures for implementation in their company products. It is understood that all countermeasures, including those designated as "highly recommended," may not be applied universally.

3. Team Membership

The AIN subteam was composed of the following representatives of the industry's user, service provider, and equipment supplier segments:

Ray Bonelli - AT&T Network Systems
Ed Bonkowski - Advantis
Lynda Eckes - Bell Atlantic
Jim Funk - US WEST
Clint Hamilton - (Chair) Bellcore Professional Services
Gabor Luka - NCS
Doris Nagel/Jeff Ragle- Bellcore SCP
Alex Nichols - Nortel
Pete Shelus/George Stanek - AT&T Network Services
Ken Walling - Pacific Bell

Chao-Ming Liu - Bellcore Professional Services (AIN subteam Secretary)
Mark Williamson - Bellcore Professional Services (Data Aggregator)

Team members should be recognized for their dedication and contributions to the success of this effort.

4. Study Process and Data Collection and Analysis Activities

Data collection and analysis activities for the AIN subteam were conducted in accordance with its mission; i.e., they were designed to help identify major service impacting issues as well as to identify and propose solutions in these areas.

For more mature technologies, outage data collected over a suitable time period can be effectively used to identify problem areas and to infer solutions to address those problems. Because AIN deployment is in its infancy, the subteam recognized that the existing outage history was likely to be sparse and might not be representative of all potential major reliability concerns that may arise as the technology matures. Therefore, the subteam decided to utilize the following approach utilizing three sources of information to identify the major reliability issues and their potential solutions:

1. *Outage data from AIN/IN networks already in place* - Collect and analyze outage incident reports to determine whether any meaningful trends are emerging that might lead to more serious outages as the technology matures.

2. *Opinions of service provider company experts responsible for the day-to-day operation of these networks* - Survey those responsible for the day-to-day operation of AIN networks to obtain their opinions regarding areas of concern, specific issues that are likely to cause or contribute to significant network outages in the future, and preventative measures that might be taken to achieve the committees' objective of no FCC reportable outages.

3. *Industry experts involved in the development and implementation of AIN networks* - Sponsor presentations from a variety of industry experts representing development and/or operational experience with AIN/IN.

The subteam’s study process is summarized in the following figure:

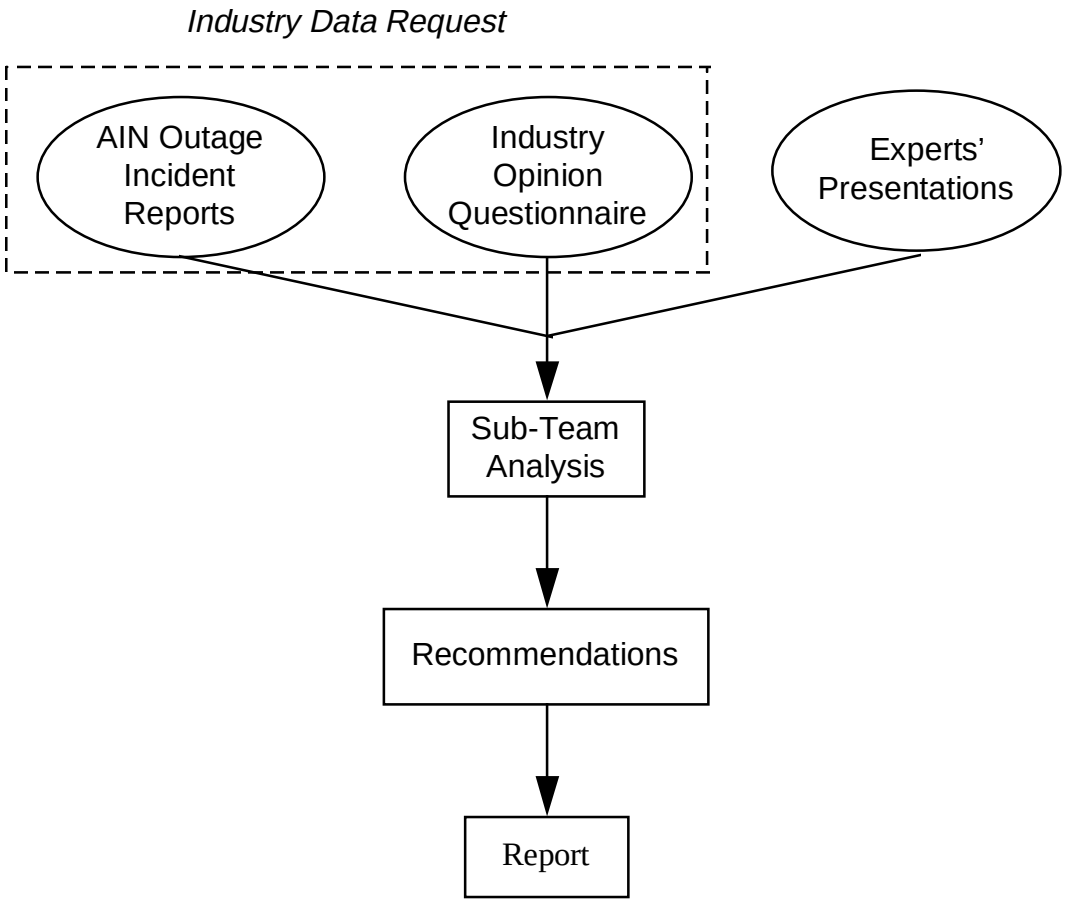


Figure 4.1 AIN Subteam Study Process

The industry data request used by the subteam contained both a request for specific AIN/IN outage incidents and an Opinion Questionnaire.

As in all NRC Focus Teams, Bellcore served as the central point for requesting, collecting, compiling, and aggregating data for all focus area teams. All data provided to Bellcore were protected under a nondisclosure agreement. These data were treated as proprietary information, and specific references to individual service providers or manufacturers were removed during the aggregation process. Each focus area defined its own data needs. The results of the synthesis of this data are included in this report.

4.1 Industry Outage Data

Industry outage data were requested via the *Outage/Failure Information Request Form*, which was mailed to key companies in various segments of the telecommunications industry. The form was adapted from the format of the Service Failure Analysis Report (SFAR) as specified in Bellcore's Special Report entitled "Network Switching Element Outage Performance Monitoring Procedures".[1] These forms requested service providers and manufacturers to document the facts and circumstances involved in outages, duration and effect on service of the outages, the direct and root causes of the outages, and corrective or preventative actions to be taken by involved parties in response to the outages. Respondents were asked to provide one report per event for outages occurring from January, 1994 through the present.

Thirty-eight reports are provided by three Local Exchange Carriers (LEC) and one Interexchange Carrier (IC). The subteam did not perform statistical analyses because the total number of events is small and the results would not represent a general network trend. In general, there are 19 hardware failures, 7 software failures, 8 attributed to unknown causes, and 4 other types of failures. About half (18) of these outages caused only lost calls and did not cause a total system failure. There were no total service failures (loss of mated SCP pair or a single non-mated SCP). Thus, none of the events was FCC-reportable. Interestingly, 6 out of the 8 outages with unknown causes were long outages (greater than 30 minutes).

4.2 Industry Opinion Questionnaire

The opinions of those responsible for the day-to-day operations of AIN networks were requested via the AIN *Deployment and Opinion Questionnaire*. The development and fielding of the questionnaire was a joint effort of Bellcore and the subteam; the subteam provided guidance as to its content, and Bellcore provided expertise in questionnaire construction and distribution and the aggregation of results. The questionnaires were distributed to the same companies as the Outage/Failure Information Request Form. Participation varied by industry segment, as shown in the table below. For example, 10 LECs completed the questionnaire; three sent outage data; one stated that the questionnaire was not applicable to them and thus did not complete the questionnaire; and one did not return the questionnaire.

INDUSTRY SEGMENT	QUESTION-NAIRE COMPLETED	OUTAGE DATA SUPPLIED	NO RESPONSE	NOT APPLICABLE
ICs	4	1	0	2
LECs	10	3	1	1
CELLULAR	2	0	7	8
CABLE	0	0	1	10
MANUFACTURERS	3	0	7	6
SATELLITE	0	0	6	1
MOBILE SATELLITE	0	0	1	2
CAP[†]	0	0	1	0

Table 4.1 Opinion Survey Response

The questionnaire was organized by topical area. These areas were defined by the subteam to provide a logical categorization of potential AIN reliability issues. The areas were as follows:

- Architectural Factors
- Maintenance Tools
- Interoperability
- AIN/IN Software
- Switch Feature Interworking

[†] **CAP - Competitive Access Provider.**

- AIN/IN Service Logic Design
- Service Classes
- Additional Factors

In each topical area, the subteam identified a number of factors which were thought to have the potential of either increasing or decreasing the risk of major network outages. Respondents were asked to rate these factors on a five point scale, indicating their tendency to increase or decrease (as appropriate) risk. When the potential of increasing risk was rated as moderate to very high, the respondent was asked to identify the source(s) of the risk and to suggest potential solutions.

In aggregating the results, responses to the ratings questions were used to identify those factors that are perceived as posing the greatest risk to AIN networks, and those factors that are perceived as most likely to reduce network risk. The follow-up questions were then used to explore the sources of the perceived risk, as well as to identify potential solutions.

The respondents had the following major reliability concerns:

- Simplex SCP
- Growth and retrofit
- SCP reliability
- Congestion control and network management
- Services with officewide triggers
- Service Development/Provisioning Process

A list of all reliability concerns and suggestions for improvement provided by the respondents is included in the Appendix B.

<Recommendation 1>

Service providers and suppliers should review the suggestions in Appendix B (AIN Reliability Concerns from Survey Response) for their applicability to their own networks and systems.

4.3 Experts' Presentations

The experts' presentations cover topics related to AIN reliability. The purpose of the presentations was to update the subteam members with the latest status of AIN development and its impact on network reliability. Through discussion after each presentation, the subteam was able to understand the reliability concerns under each topical area. The following list of the expert presentations were held during the subteam meetings:

Date	Topic	SME
7/11	AIN Architecture	John Brewster (Bellcore)
	AIN - NS/EP‡ Users' Perspective	Rick Sherman (MITRE)
	Bell Atlantic AIN Architecture	Lynda Eckes (Bell Atlantic)
8/15	Issues and Concerns	Jan Ryssemus (Pacific Bell)
	Network Evolution Plan	David Fannin (Pacific Bell)
	Service Development Process	David Fannin (Pacific Bell)
	AIN SCP Capacity	David Fannin (Pacific Bell)
	Testing Process	David Fannin (Pacific Bell)
9/26	Interoperability	Greg Feldkamp (Bellcore)
10/11	AIN SSP Software Design and Testing	Charles Wiebe (BNR)
	Reliability in OSI OS/NE Interactions	Carton Hall (US WEST)

A summary of the expert presentations, attached in Appendix C, provides the reader background and insight into some of the key AIN reliability issues as seen by these experts.

<Recommendation 2>

Service providers and suppliers should review the summary of experts' presentations contained in Appendix C for their applicability to their own networks and systems.

5. Study Results - Key Learnings and Recommendations

Because AIN is new in terms of deployment, the subteam believed that it was not enough to rely only on analyzing outage data collected from the field to formulate our recommendations. Thus, the subteam decided to gather information from three sources:

(1) Industry AIN/IN outage data
(2) Industry opinion questionnaire
(3) Experts' presentations

The outage data from the field, although limited in quantity, indicated field problems. The industry opinion questionnaire responses provided opinions of the people who actually dealt with day-to-day operation of AIN. The experts' presentations provided a forward-looking view of potential reliability concerns and impact of AIN. These recommendations were usually generated from discussions after experts' presentations and from industry opinions. Whenever possible, the subteam tried to confirm or justify the recommendations with the industry outage data so that the recommendations were consistent with the prime objective of the subteam: there should be no FCC reportable outages related to AIN.

‡ **NS/EP - National Security/Emergency Preparedness**, a national telecommunications service that allows authorized government users to initiate a call and communicate with others during national emergency situations, such as disasters.

5.1 Architecture

5.1.1 SCPs and IPs

The most visible concern the survey results show is the lack of redundancy in the AIN architecture, especially in the case of simplex SCPs and simplex IPs (Figures 5.1 and 5.2). Although 60% of the respondents state that their companies deploy SCPs in duplex, some companies deploy SCP in simplex or deploy some key applications in simplex. Most respondents believe that "SCPs in Simplex" has a HIGH to VERY HIGH tendency to increase network reliability risks. This increases the risk of losing key AIN services when one SCP becomes unavailable.

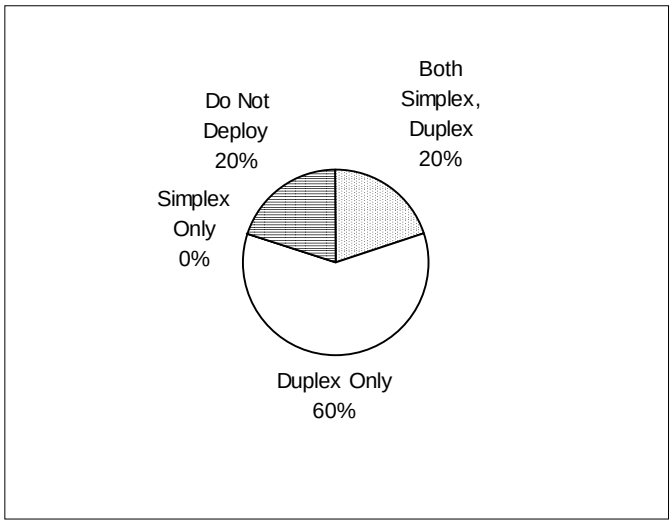


Figure 5.1 SCP Deployment

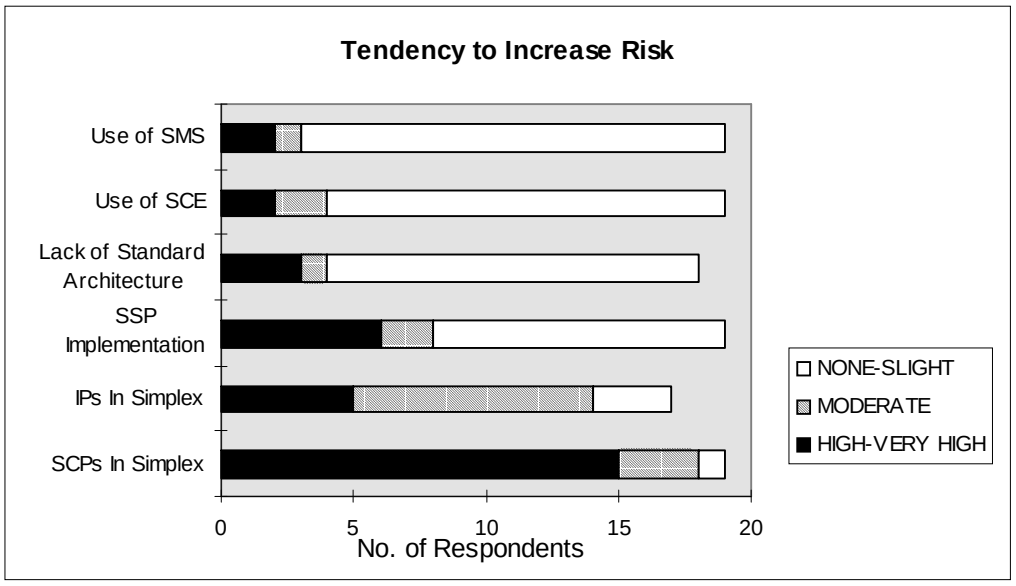


Figure 5.2 Architecture Risk Factors

SCP and IP reliability is also a major concern to the respondents because the SCP/IP availability objectives need to be more clearly defined.

The respondents were concerned about the reliability of their SCPs because the SCP is now a key element in the telephone networks. In terms of reliability requirements, maintenance practices, operations procedures, troubleshooting tools and processes, the SCPs should be treated like key telephone network switches or Signaling Transfer Points (STP). This is very important for the reliability of the PSTN since nontraditional telephony equipment (e.g., information systems such as SCPs and IPs) are being incorporated into the telephone networks. The reliability of new architectural elements should not negatively impact the traditional high reliability of the telephone network. Conformance targets will help keep reliability high.

There is similar concern about simplex deployment of IP products, but at a lower scale. Figures 5.2 and 5.3 show that simplex IP deployment is a concern to the survey respondents. Only 8% of the respondents said that they deploy IPs only in duplex and more than 50% have simplex IPs in the field. However, the root of the concern is the reliability and integrity of the IP products that are going to interconnect with the network. The respondents are concerned that they have been unable to influence the third party IP service providers to maintain the same level of reliability as the regular telephone networks. Service providers would like to ensure that the IPs connected to switches have the same level of reliability as the switches.

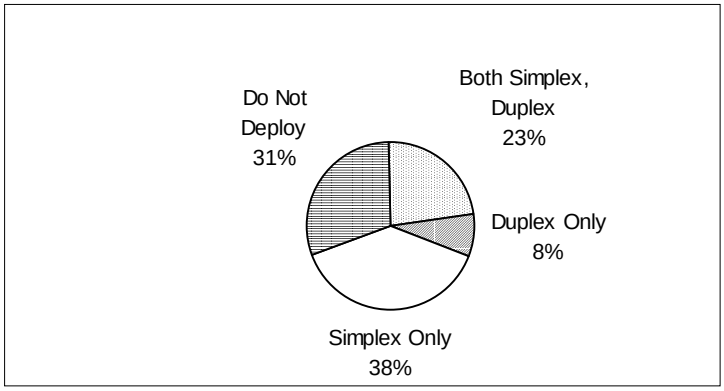


Figure 5.3 IP Deployment

< Recommendation 3>

SCPs should be deployed in duplex by the service providers. Key applications, (such as 800 service), that affect numerous customers should be duplicated in the mated SCPs to reduce network risk.

<Recommendation 4>

SCP/IP reliability objectives should be revisited by the service providers and equipment suppliers to ensure that they are consistent with switch reliability objectives and that the impact of SCP/IP failures is minimized. Reliability objectives, and other interconnection requirements, should be included in the interconnection standards set up by the American National Standards Institute (ANSI) accredited Committee T1 (Section 5.2.5). Service providers should then use these standards to ensure that SCPs/IPs connected to switches have the same level of service reliability as the switches - via equipment reliability, functional redundancy, or duplex deployment.

5.1.2 AIN Architecture Standards

Most survey respondents state that they are planning for evolution toward open networks. Most providers surveyed support a multiple service provider environment, and architecture-related issues (e.g., interoperability and conformance) may be discovered as more services and capabilities are integrated into the network. Although there are AIN guidelines or requirements consisting of Bellcore requirements, there are no industry-wide standards for AIN interconnection across providers. Note that survey responses also viewed *Lack of Standard Architectures* as a minor risk. Interoperation across different architectures will be increasingly important as carriers move toward open architectures.

<Recommendation 5>

Service providers should conduct reliability analyses to ensure that introduction of new architectural elements (e.g., nontraditional components such as information systems) do not negatively impact the high reliability of the network. Redundant functionality of network nodes and physical and logical diversity of links should be implemented where feasible.

< Recommendation 6>

For services requiring high availability/reliability (e.g., 911 service), service providers should direct their effort toward (1) reducing the number of critical elements involved in providing the service, and (2) increasing the level of connectivity available in the network.

<Recommendation 7>

Greater focus is required by Committee T1 on standardization of AIN architectures as architectures evolve toward support of open networks. As a first priority, a set of architecture standards is needed for interconnection among LECs, LEC and IC, LEC and third party vendors, etc.

5.1.3 NS/EP AIN Architecture Review

The National Communications System (NCS) has conducted an AIN network architecture reliability review from the National Security/Emergency Preparedness (NS/EP) users' point of view.[2] A brief overview of this report was presented to the subteam (Appendix C.2). The objectives of this study were to (1) quantitatively compare the architectures in terms of the risk associated with outages of message signaling used in AIN services; (2) quantify the risk contributions for each architecture of different disaster types, different AIN components, and of different types of failures using available field failure data; and (3) suggest and evaluate architectural approaches that can be used to reduce the risk. The NCS report contains many useful recommendations to strengthen AIN service reliability and robustness. Although the main focus was on NS/EP services, the results are applicable to regular AIN services.

<Recommendation 8>

The subteam recommends that service providers review the NCS report and assess the recommendations for application to their networks.

5.2 Operations and Maintenance

5.2.1 Root Cause Analysis Process

The AIN subteam distributed 66 surveys to the industry requesting detail concerning AIN/IN failures. Nineteen surveys were returned and they included data on 38 failures reported by 3 LECs and 1 IC. A few of the reports included the details identifying what happened, why it happened, and what action needed to be taken to prevent recurrence. However, most of the failure reports were one-line reports identifying what happened, with no information on either the root cause of the failure nor any recommendations for prevention. Figure 5.4 is an example of a typical one-line report.

1. Contact Name *S. Far*	2. Contact Telephone *123-4567*	3. Report Number *ABC*	4. CLLI Code *XXXXWWAAA00*
5. Company *X*	6. Hardware Vendor *Y*	7. Software Vendor *Z*	8. Office (Location & State) *CC, SS*
9. Date of Incident *20/2/99*	10. Time of Incident (24hr clock) *23: 5:*	11. Failure Duration *10:38:18*	12. System Cutover Date / /
13. Service Impact (lines) lost/lost calls AIN (Specify)_____ :	Provisioned(check) _____	Affected (check) _____	Average Queries per busy hour _____ Customers _____
14. DESCRIPTION OF SERVICE FAILURE: Describe in detail the incident including a chronological description of events:(Add attachments if necessary.)			
SCP was isolated due to manual init. to recover multiple failed processes.			
15. CAUSES OF FAILURE: Describe the Direct and Root (if appropriate) cause of the outage and state the outage duration resulting from each cause of failure.			
Unknown			
16. Associated Activities:			
17. Restoral Method:			
18. Recommendations for Preventive Actions:			

Figure 5.4 An Example of Outage Report with Insufficient Information

This is a recurring problem and was identified in the 1993 NRC Network Reliability study[3]. A process should to be established to collect failure data and evaluate the root cause of the failure. This failure and root cause data should be shared with equipment manufacturers and other service providers when applicable, based on the NOF guidelines described below. If experience is not shared, preventive measures will not be implemented in a timely manner and the network will be subject to recurring but preventable events.

The AIN subteam recommends that the industry follow the information sharing guidelines developed by the Network Operations Forum (NOF) and referenced in the 1993 NRC Network Reliability study[4]. These guidelines are to enable all service providers and vendors/manufacturers to utilize information uncovered by other service providers and/or vendors/manufacturers through the testing, validation and application of software, hardware, and documentation, procedural issues, and to conform to the following agreed on standards in order to 1) minimize the possibility of major outages and service interruptions that can affect customers' service, 2) maintain and improve the reliability , capacity, and performance of interconnected networks, and 3) meet or exceed the expectations of the subscribers. Such information sharing may also reduce the need for repetitive or redundant testing.

The NOF guidelines state that any information uncovered by any service provider, vendor/manufacturer that reveals the potential for loss of service or compromise in the reliability, capacity, or performance in a single network or interconnected networks should be proactively shared with those parties whose networks and/or products may be affected by the problem. Service providers should inform their vendor/manufacturer of defects or potential defects during testing and daily operation. Service providers should also inform interconnected parties of problems and potential problems that are not attributable to a vendor/manufacturer.

Vendors/manufacturers should make available to a particular customer all trouble report information reported by that customer. When vendors/manufacturers identify problems with their software or hardware that have the potential to cause loss of service or compromise in the reliability, capacity, or performance in a customer(s) network(s), this information should be communicated to the customer within one business day.

<Recommendation 9>

The service providers should establish an AIN data collection process that collects failure specific data, root cause(s) of the failure, and recommendations for prevention. An outage reporting criterion should also be established by each provider so that their employees know what information should be collected/generated and what reporting process should be utilized (i.e., internal company only, industry, or FCC).

<Recommendation 10>

All service providers should follow the information sharing guidelines established by the NOF, Reference Document, Issue 1, April 1993.

5.2.2 Troubleshooting and Fault Isolation Tools

The survey results also indicated a high rate of failures with the cause "unknown" (21% of the reported failures). From a maintenance viewpoint, this indicates that there is a serious deficiency in the tools available for the identification, verification, and isolation of failures in the network. The survey also identified a problem with the ability of the maintenance personnel to detect and identify the cause of failure in the network. These personnel have difficulty identifying the foreign cause(s) of network problems and detecting SCP and SCP-SSP feature interactions. The tools required for these troubleshooting functions are either unavailable or do not provide enough capability. Subject matter experts who were interviewed also identified these problem areas. They also identified a limitation in the training that is available for understanding how these new services work and how the network elements interact. The lack of well-trained technicians and

the limited capability of their troubleshooting tools is an added risk to AIN network reliability. Without the ability to quickly identify and isolate the source of a network fault, an otherwise minor fault could escalate into a long duration network interruption. These limitations and recommendations for their resolution are discussed in depth in Section 5.3.

To date, AIN applications have focused primarily on single service provider, stand-alone applications. Therefore, little effort has been expended to develop automated problem identification and recovery systems. This includes the process and procedure for periodic verification of database and routing translations as well as automated provisioning and network surveillance systems. This lack of automated processes makes the introduction of error more probable and the identification and recovery from the error of longer duration. Thus, the impact of error on the network becomes more onerous. We urge the industry to respond to this deficiency by developing automated AIN support systems as quickly as possible.

<Recommendation 11>

The Committee T1 and other industry forums such as the Network Management Forum (NMF) or Network Operations Forum (NOF) should expand on the work performed by the International Telecommunications Union - Telecommunications Standardization Sector (ITU-T -- formerly, the CCITT) and documented in recommendation M.3010, "Principles for a Telecommunications Management Network (TMN)"[5] with focus on the definition of the industry needs and the development of standards and requirements for network problem isolation and recovery tools, and capability.

5.2.3 AIN Performance Measures

The survey and the experts' presentations (Appendix C.4) also identified a limitation in the ability to measure the performance of the AIN network and AIN applications. Industry standards for AIN application or platform performance monitoring, performance indicators, or measurements do not exist. Until these measures are developed and implemented, customer failure reports will continue to be the primary indicator of failure. A proactive response to a deteriorating network makes a failure imperceptible to customers. A reactive response to network failure can result in serious and long duration network failure.

<Recommendation 12>

The Committee T1 should expand on the work performed by the ITU-T and documented in Recommendation M.3010, and develop industry standards for network health indicators, for Network Element (NE) performance indicators, and for individual AIN application performance monitoring. Verification of these standards should be included in all interoperability, new AIN platform, and AIN application testing.

5.2.4 AIN Reliability Objectives

An attempt has been made by Bellcore to establish platform and application outage frequency and downtime objectives. These objectives, documented in Bellcore Generic Requirements GR-1280-CORE[6], TR-NWT-000284[7], and GR-929-CORE[8] but are too lenient for today's network quality expectations. The downtime performance requirement objective for each AIN service is now 12 hours per system per year. These objectives should be redefined to emulate the end office switch outage and downtime expectations and then be developed and adopted by the industry.

<Recommendation 13>

The working group T1A1.2 should develop reliability standards for AIN platforms and applications that emulate end-office switch outage frequency and downtime expectations. The Bellcore Generic Requirements for AIN platforms and applications (GR-1280-CORE, TR- NWT-000284, and GR-929-CORE) should be used as a starting point and assessed for their applicability to today's network performance expectations.

5.2.5 Growth and Retrofit

Service providers are rapidly signing up more AIN customers. Survey respondents were concerned that with the growth of customer lines and services, processors could not keep up with the traffic load, leading to processor overload and/or network congestion, which would disrupt AIN services and other services. Survey respondents were also concerned about the growth and retrofit process. Most retrofits require long downtime compared with regular telephone switch retrofits, causing reduced system capacity and simplex operations. As discussed in Section 5.1, simplex operation increases the risk of network outage. Some respondents also mentioned the complexity of retrofit procedures and inadequate testing of the retrofit procedures as two reliability concerns. Figure 5.5 illustrates maintenance risk factors.

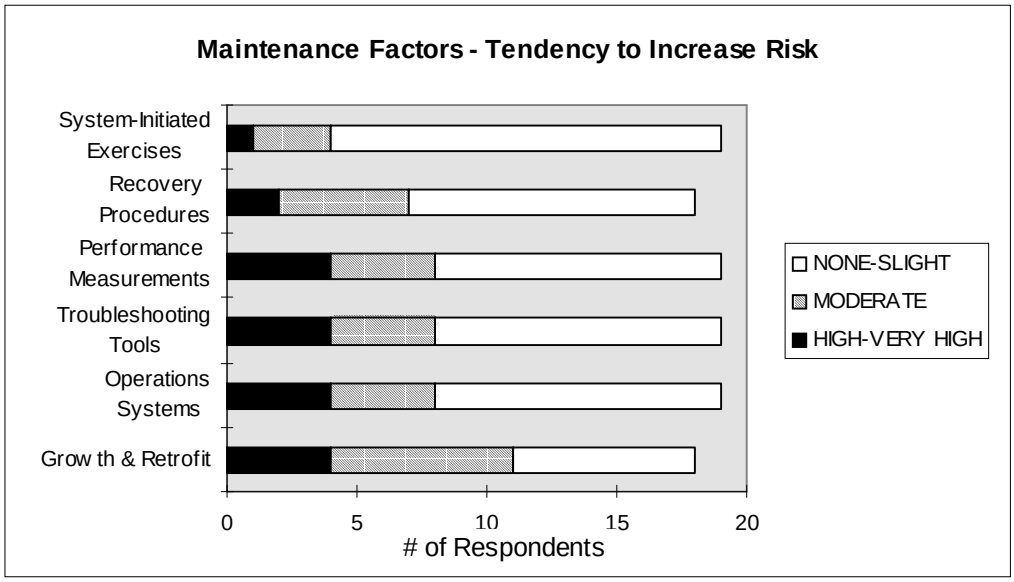


Figure 5.5 Maintenance Risk Factors

In addition, the subteam believes that current AIN downtime objectives are driven by the complexity of retrofit procedures, system capacity, and design. Some applications are installed on simplex platforms that automatically result in service downtime for any major system maintenance or generic software upgrade. Maintenance and administration documentation and procedures are often less than adequate. Generic program software retrofits are complex, requiring long downtime. This leaves the system in a simplex configuration, reduces system capacity, and increases the network's vulnerability.

This risk can be minimized by adherence to a duplex network design (Section 5.1), and improvement, simplification, and automation of retrofit procedures. Improvements in

documentation, robust generic software development processes, and complete verification and interoperability testing will also reduce downtime and service risk.

<Recommendation 14>

The suppliers and service providers should work together to define downtime requirements and to find ways to improve, simplify, and automate the retrofit procedures to reduce the complexity of, and the time required, for retrofits.

5.3 Operations System Interface and Support

The results of the survey showed that current Operations Systems (OS) are not consistent in their interfaces and support functions provided to the various components of the network. Figure 5.6 is a representation of the current state of affairs of Operations, Administration, Maintenance, and Provisioning (OAM&P) OSs across the circuit switch, SS7 and transport services networks. The following conditions exist across all of the existing OSs:

- Interfaces between Network Elements (NE) and OSs are proprietary to the NE vendors.
- Each NE supplies duplicate data to a plurality of OSs across a variety of proprietary vendor controlled interfaces.
- OSs are interconnected and data is cascaded from OS to OS, creating interdependencies between the OSs that can impact the reliability of the reported condition of the NEs.
- Redundant reporting and analysis functions are embedded in each OS. These functions are difficult to enhance or integrate across the entire network and the NE types.
- The OS user's view of data from the NEs is not integrated across the PSN and SS7 networks.
- The OS user's view of data from the NEs is not integrated across the NE vendors.
- Users are required to maintain specialized complex system operation and administrative knowledge for each OS.

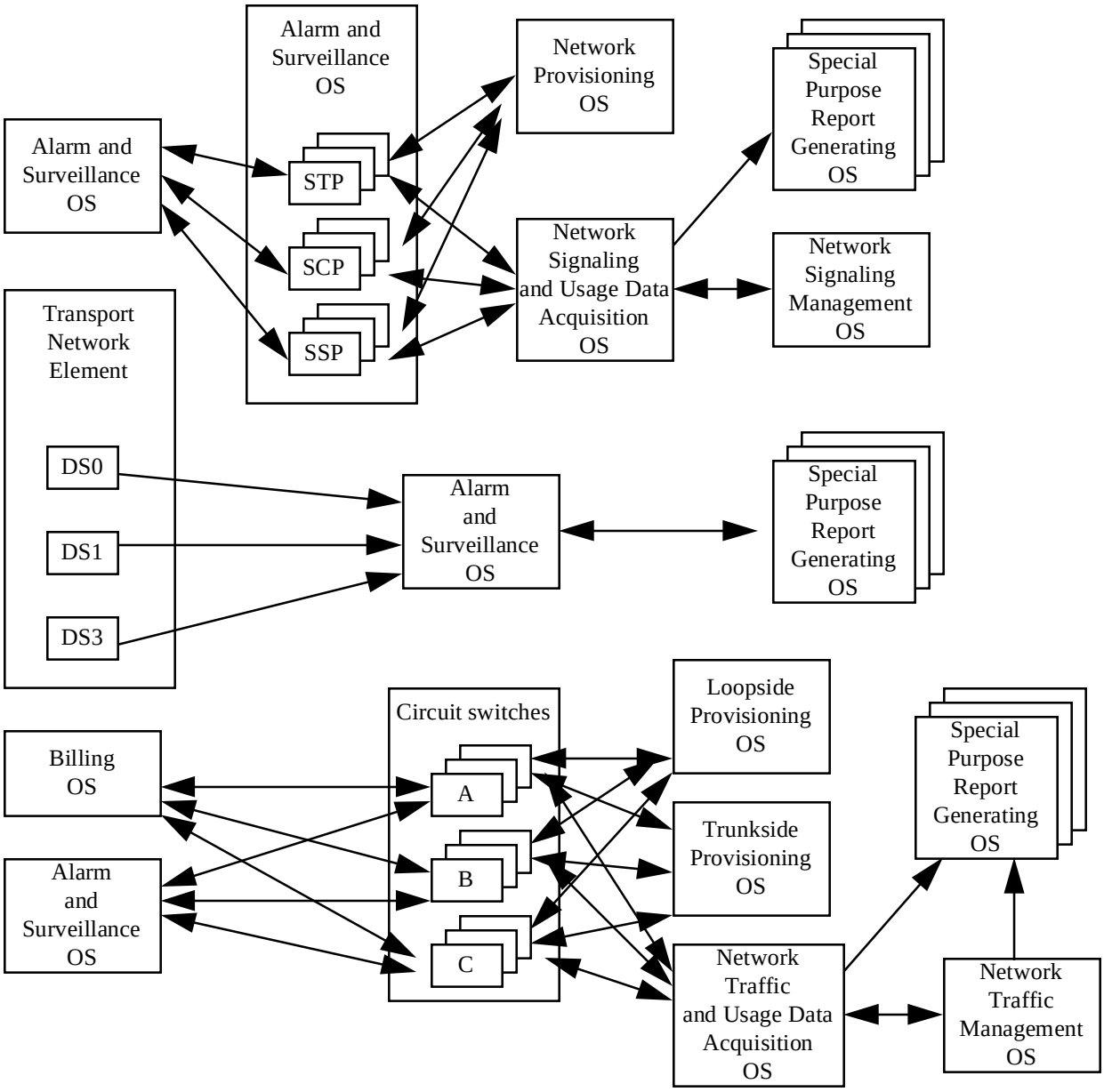


Figure 5.6 Current State of Affairs of OAM&P OSs

As AIN services become more complex with new participants in a multi-vendor/multi-service provider environment, it is becoming more difficult to perform OAM&P functions (e.g., alarm surveillance, network monitoring, data collection, traffic management, and maintenance commands).

In today's complex network, many different and new elements are involved with AIN call completion. Each network element communicates with or is dependent on the entire network for call completion. Yet, the complex web of communication channels to the OSs from each NE causes them to be viewed and operated as isolated entities. The health of the network depends on communicating with and reacting to the entire network in near real time.

The data from each NE is not only redundant in each OS, but, the Network Element central processor requires more processing power to provide identical or similar data to separate systems through multiple OS interfaces.

When personnel have to monitor multiple and different terminals connected to independent OSs on the various components of the network, they become much less effective in identifying multiple notifications of similar events. Personnel will not be able to effectively communicate with a multi-node network. It will become more difficult to understand individual commands and requirements for each node in the network and identify the root cause of an event.

To resolve the problems identified in the survey, an effort should be launched to implement standards for management of telecommunication networks. An international effort, which began in 1985, has been developing standards for management of telecommunications networks. These standards are described in documents produced by the ITU-T. The base document is ITU-T Recommendation M.3010. Appendix D provides an overview showing the general relationship between TMN and a telecommunications network that it manages.

<Recommendation 15>

> The Committee T1, the NMF, and the ITU-T should expand on both existing and emerging network management standards and technologies to allow the TMN standards to be implemented to support development of operations and maintenance tools and to achieve broad deployment of TMN in the telecommunications industry.

The network's health or reliability will be improved with standardized OS implementation. These OSs need to be real-time reactive and responsive to network conditions. By eliminating the number of OS interfaces and user terminals that are now needed to conduct surveillance, maintenance and translations on the many different nodes, and the health and reliability of the network will be improved. The standardization of Management Information Base (MIB) interfaces with OSI and TMN will reduce the number of functional interfaces and add reliability due to the distributed architecture.

The development of the TMN architecture could also require less vendor specific training for personnel to monitor and communicate the correct commands for multi-vendor elements. TMN management functions should be developed to provide the same commands for all of the different vendor network elements for translations, maintenance, surveillance, and data collection.

<Recommendation 16>

> Any service provider that wants to implement TMN must deal with a host of legacy system issues related to existing network elements and OSs. The Committee T1 and the Network Management Forum (NMF) should develop standard mappings, evaluate the economic impact, and develop a practical transition from existing legacy system interfaces to standard TMN interface MIBs.

<Recommendation 17>

> Vendors of TMN components should form working groups with the Committee T1 and the NMF and develop common MIBs and managed objects for use by developers.

Vendors can apply this open system approach by forming information models for industry standard interoperable interfaces.

5.4 Service Creation/Provisioning Process

One key characteristic of AIN is that it is very easy to create new AIN services to meet customer needs. However, the respondents were concerned about the side effect of poor service logic design. This may show up in the new translations, improper provisioning of parameters, or AIN feature interactions. In the case of AIN services with officewide triggers, a single error can create wrong service execution processing and cause a major outage (Figure 5.7). However, the vast majority of AIN triggers are line-based or subscriber-based, not office-wide and should be appropriately considered.

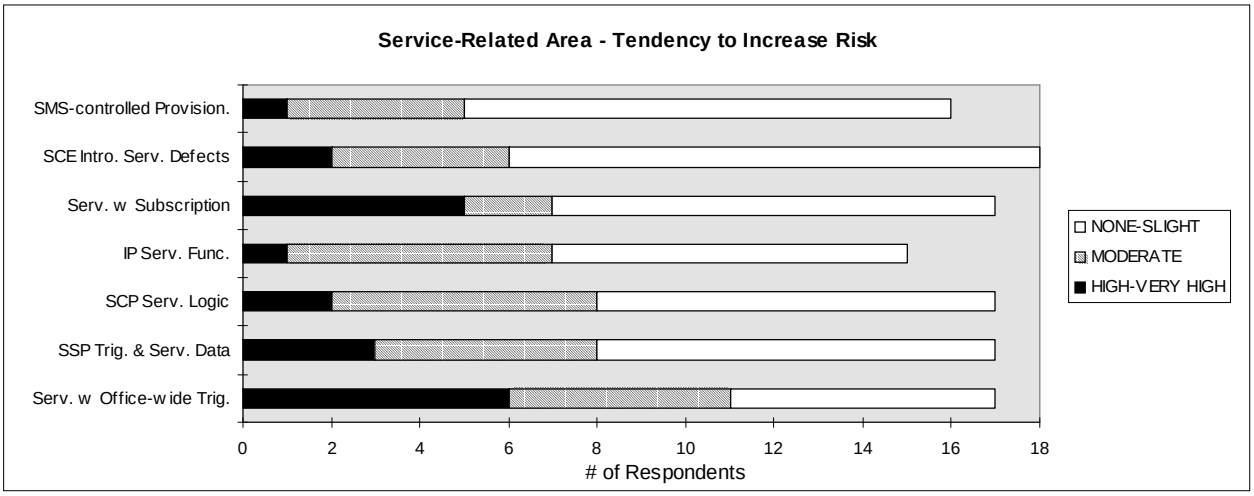


Figure 5.7 Service-Related Risk Factors

The survey respondents also pointed out that the service development/provisioning process that creates these services needs to be examined. Although more than 60% said that they have a process (Figure 5.8), the opinions they shared listed the following problem areas: software errors, service design exceeding node capability limitations, and errors in provisioning of parameters.

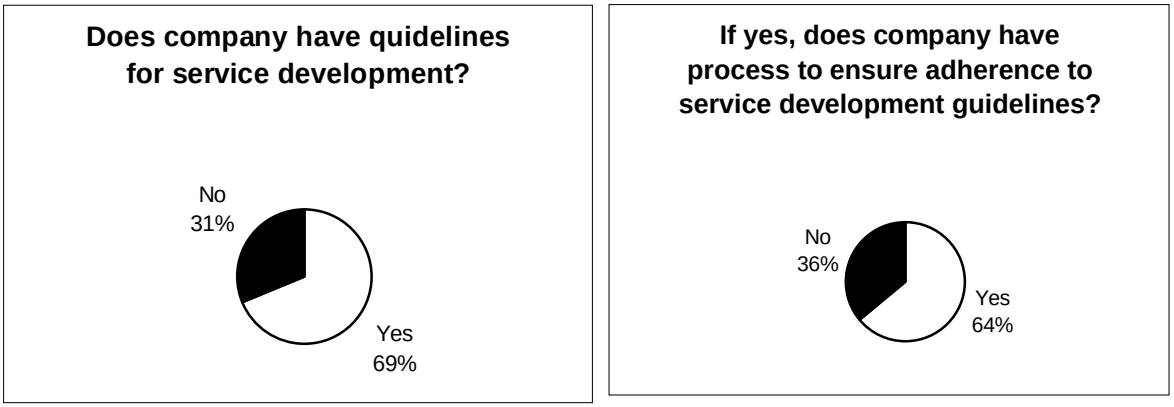


Figure 5.8 Service Development/Provisioning Process

As indicated by the survey response, service creation without the proper network controls, development process, and tools for product verification will result in a poor service design that might increase the risk of a major network reliability problem. A brief overview of a service development process used by one service provider was presented to the subteam (Appendix C.6) as an example. The subteam believes that this example can serve as a “Best Practice” to the industry.

<Recommendation 18>

The service providers should implement a service creation/provisioning process to ensure the quality of the AIN services and maintain the integrity of the network. The following subsection describes an overview of a process that is in use by one service provider. The process has been verified and upgraded based upon their experience. The subteam offers it as a “Best Practice” and urges the industry to replicate its use, upgrade the model from their experience, and share the improvements with the Industry.

5.4.1 A Service Creation/Provisioning Process Example

All service creation efforts should start with the development of a documented Service Development Process and a laboratory containing all equipment and tools required to test the services and their interaction in the switched network. This laboratory should include SSPs, SCPs, IPs, and STPs. The Service Development Process (SDP) should include the rigor of established software development processes, including design and code reviews, system integration and regression testing, and quality gates with specific quality gating criteria. It should also ensure that the development team understands the process and their responsibilities within the development process.

Major network and customer service disruptions can occur if Service Creation design does not consider failure conditions, and customer notification and control during network or service failure. Failure management should be incorporated into product design and tested as part of the software development process. Service providers need to develop customer notification procedures for customer notification and call treatment status during service outages.

The Service Development Model for AIN is similar to any complete and robust software development process. Figure 5.9 provides an overview of the process that is in use by one service provider. The process has been verified and upgraded based on their experience. We offer it as a "Best Practice" and urge the industry to replicate its use, upgrade the model from their experience, and share the improvements with the Industry.

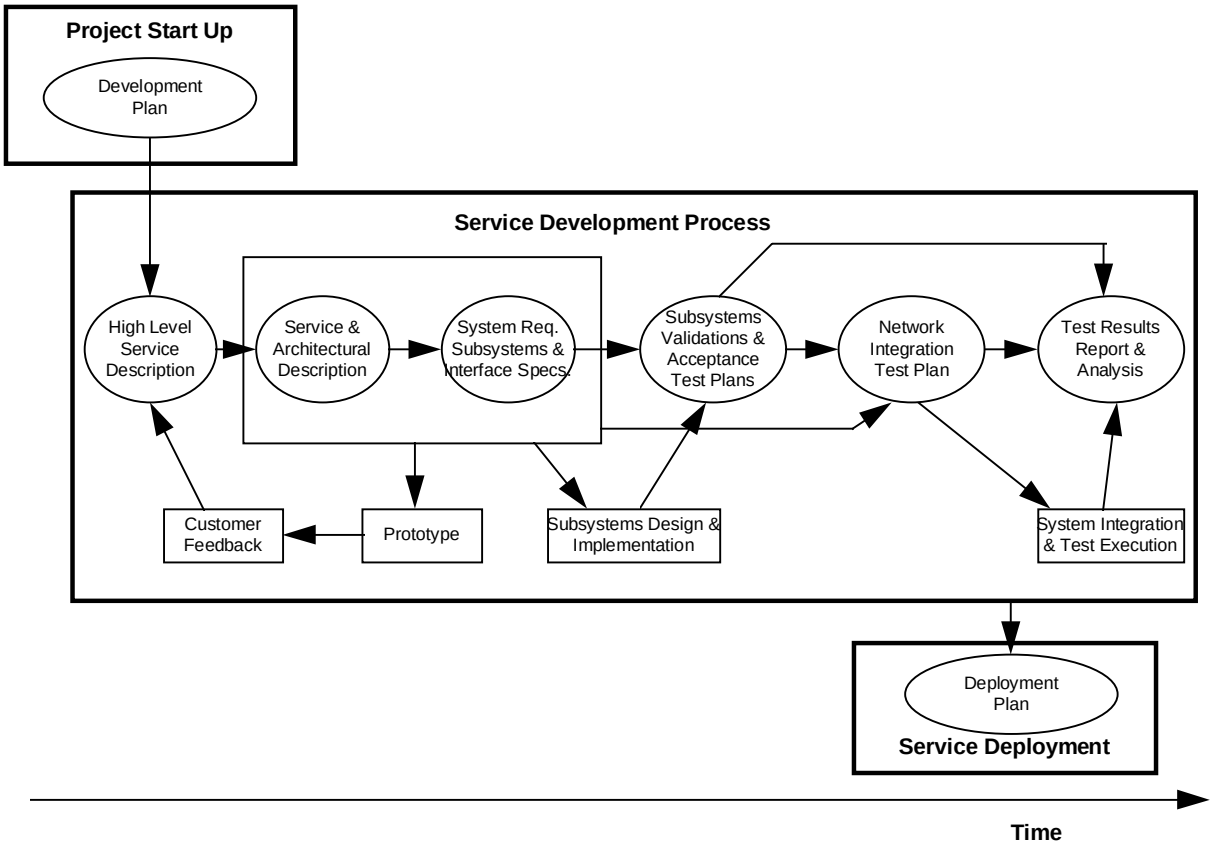


Figure 5.9 Proposed SDP Flow Diagram

The process has three basic parts: the Project Start Up, the Service Development Process, and Service Deployment. These parts are discussed below.

Project Startup

The project startup phase provides for a review and approval of the development plan for the proposed service. This part of the process will verify that the business opportunity and customer's needs have been identified and assessed. It ensures that budget issues and the project team have been identified. It also ensures that the proposed service has been given an appropriate ranking and priority among all competing projects.

Service Development Process

The first step in this phase of the process is the development of a high level Service Description. The development should include customer input and interaction. The description should include a definition of the service, its interactions with other services, service parameters, and billing, provisioning, and maintenance characteristics.

From this description a detailed design specification should be developed. This specification should include a service and architectural description with rigorous grade of service requirements, system requirements, and subsystem and interface specifications. From this specification, a model

should be developed and reviewed with the customer. From this review, the specification should be upgraded and then approved by the customer before proceeding with development.

Next, an evaluation of the service characteristics should be performed. This should include multiple services, varying service characteristics, multiple query/response messages for each call, service-specific peaking for average busy season busy hour (ABSBH), service-specific demand, and varying timing parameters. A forecast for each service should be developed that includes the number of subscribers and their projected usage of the services. The model should then be tested and validated by laboratory testing. Once the model is validated it should again be reviewed with the customer and upgraded as appropriate.

After the customer has approved the model, development of the service should proceed following a documented development process that includes specific deliverables at each stage of the development. The process should include quality gates with specific quality expectations and formal up and down stream stakeholder review and approval required before proceeding to the next development phase. The process should include a requirement for standardized documentation formats and a documentation development process with specific documentation deliverables at each stage of the process. It should also include a process for reporting, documenting, tracking, and resolving all issues or problems encountered. Finally, it should include a clear understanding of the critical development path and an escalation process to be followed when the development is off track.

The development process should also include a subsystems validation and acceptance test plan; a network integration test plan; and a process for documenting, reporting, and analyzing the test results. The test cases and the expected results for three stages of testing should be documented and the results of their execution recorded.

The first stage is laboratory testing, where the functionality of the new service is tested. The service should be tested against the Service Description and the verified model. Integration testing should also be performed to ensure proper interaction with other subsystems and services. Regression testing of other services should be performed to ensure they are still functioning properly.

Next, network integration testing should be performed. This should include testing of the service in an integrated test environment that includes SSPs, ISCPs, IPs, and STPs. End-to-end testing should be performed that includes the billing, provisioning, and maintenance functions and associated support systems. A controlled first application test should then be conducted in the working telephone network. Again, specific documented tests should be performed, any service failures recorded, results evaluated, and appropriate action(s) completed and verified before deployment continues. Finally, a feedback process should be established that collects data on the service after it is operational. This data should be used to verify and upgrade the forecast model.

Service Deployment

Development of a small, multi-functional implementation team will facilitate deployment. This team should be the single point of contact for each organization and should develop and facilitate deployment plans, their execution, status reports, and problem resolution. Team members should

clearly understand their responsibilities, priorities, and the deployment process. This team should be part of the first application testing and service verification. They should also establish, test, and verify a Trouble Reporting process, verify the first application and service verification test results, the interaction with support systems, and service and implementation documentation.

5.5 Interoperability

Though interoperability concerns were not reflected in the survey because interconnecting AIN services across different service providers have not occurred universally (Figure 5.10), the subteam believes that interconnection is not far away and the interoperability problems cannot be ignored. This includes interoperability across various SSP products, and across different SCPs and STPs for the current network. As the number of third parties seeking interconnection of an SCP or an IP starts to increase, the interoperability problems will become more important. For example, feature interactions across different networks may be even harder to detect and prevent. The initial participants seeking interconnections are likely to be carriers who may be experienced in designing SCP based services and are familiar with SS7 type interconnections. However, if open access is provided, it is likely that many carriers will be allowed to interconnect, and this leads to concerns about capacity management, service protection firewalls and confidentiality of data sent between networks.

As the information infrastructure evolves, there will be more interaction between the different service provider networks. To maintain network reliability in this interactive network, network interconnection requirements should be developed. These requirements include processes and procedures for reliable interconnection, interoperability, and operation that must be met before interconnection is allowed. They include requirements for sub-system numbering, and identification of an industry organization responsible for number assignment, tracking, and administration. Finally, they include adherence to security requirements such as Bellcore's GR-1469-CORE[9].

When these requirements are available, effective, and adequate, testing based on these requirements is needed before connecting AIN services across networks. It is assumed that the number of third party interconnection requests will grow as the technology matures. The test process must grow in capacity to accommodate the numerous requests for service (or node) testing.

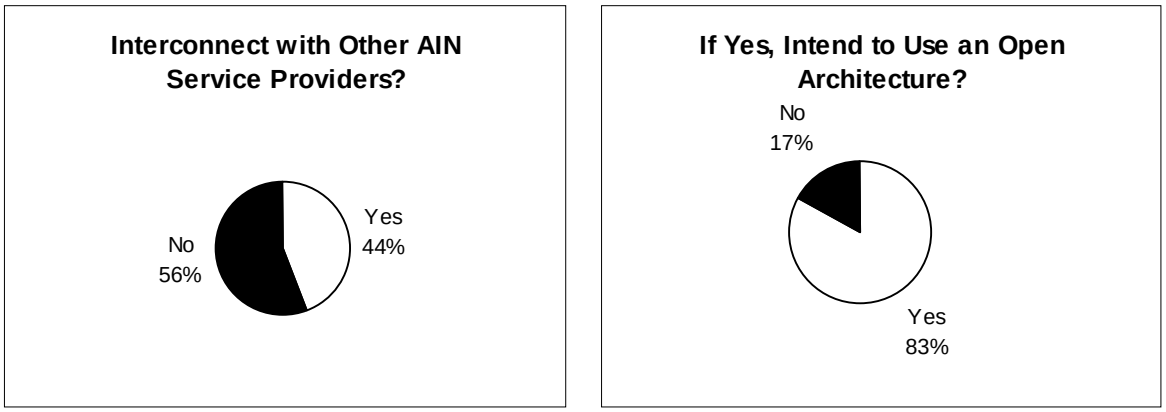


Figure 5.10 Interconnection with Other AIN Service Providers

According to the experts' presentation (Appendix C.9), AIN interoperability testing should include AIN service/application protocol testing, network integrity testing, and overload testing. Service/application protocol analysis includes end-to-end generic service integration tests between SCP and SSPs. An important emphasis is the interaction between AIN services and switch-based features. Network integrity testing focuses on network robustness under failure conditions. Tests were designed to see if the network absorbs failures gracefully. Network overload analysis searches for different ways to protect SCPs.

The Network Interface Specification Template, developed in the Focus Group II - Increased Interconnection report, provides guidance in developing standards and in defining and approving industry interconnection specifications. Readers are referred to that report for more details.

<Recommendation 19>

Service providers should work together or through Committee T1 to develop interconnection standards for AIN service interconnection and AIN network interconnection for the multi-service provider environment.

<Recommendation 20>

Adequate functional testing and pre-service tests need to be performed by the suppliers and by the service providers before cutover. Network node integration testing should be performed by the service providers and the suppliers before integrating any new or upgraded network node or equipment into the network. Network interconnection testing should be performed by the interconnecting networks before interconnection. The interconnection tests should include end-to-end service integration tests, interconnection protocol conformance tests, and overload tests. It may be possible to use the existing Internetwork Interoperability Test Plan (IITP) committee of the NOF to accomplish the internetwork integrity testing. The IITP committee should consider extending the IITP testing activities to include AIN internetwork integrity testing. (See Focus Group II's Technical Paper for recommendations concerning the direction of interoperability testing and IITP.)

5.6 AIN Network Overload Controls and SCP Capacity and Overload

AIN enables a network provider to offer a rich variety of services to its end users. However, this richness contributes to much of the uncertainty that surrounds the issues of SCP capacity and overload. AIN service introduces a variety of variables that can influence the load placed on an AIN SCP. AIN consists of multiple services with unpredictable traffic peaks and penetration rates. Service forecasts for these multiple services must be estimated, aggregated, and fed into a capacity model to determine how to engineer the AIN SCP to handle the predicted load.

Because of the rapid increase in AIN customer lines and traffic, the survey respondents are concerned about the lack of effective congestion control in their networks or the effectiveness of the existing AIN congestion control features. On a broader scale, network management features that allow network operators to effectively detect AIN service/traffic problems and respond to them were part of this concern see (Figure 5.11). Note that some of these features, such as Automatic Call Gapping (ACG), are being developed and/or implemented by the suppliers and

service providers. The respondents want to see quicker implementation to avoid possible network congestion.

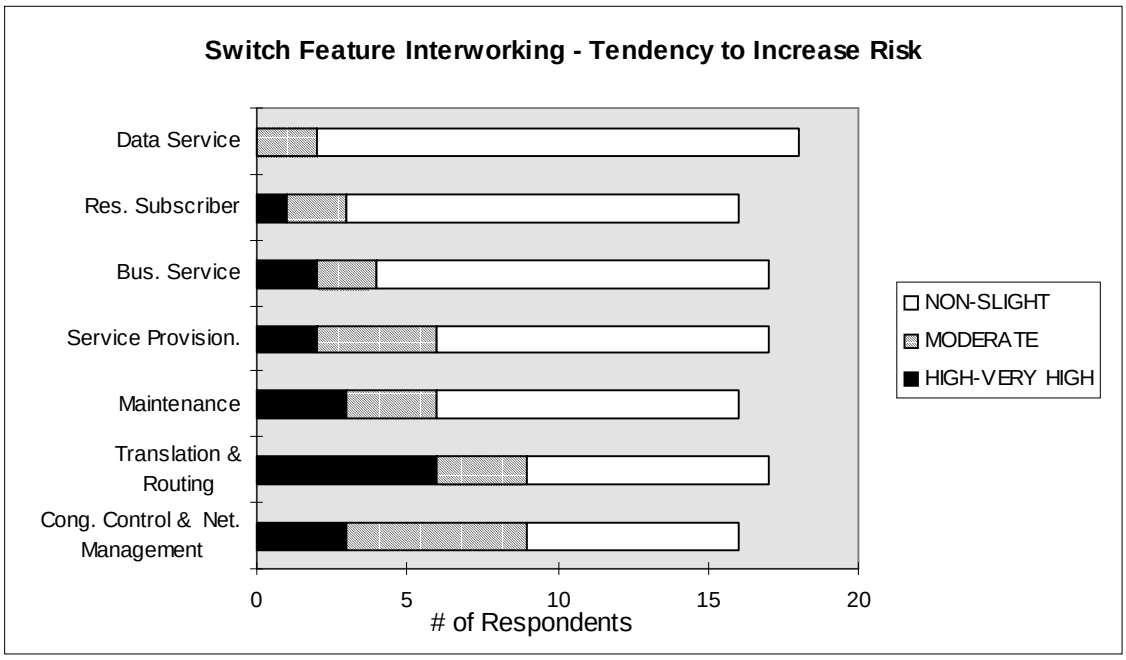


Figure 5.11 Switch Related Risk Factors

The concern for the SCP's capacity and for the effectiveness of the congestion control are closely related. The survey response and the outage data showed that deficiency of congestion control and/or insufficient SCP processing capacity might lead to serious outages. Although congestion in the network can never be totally prevented (e.g., due to mass calling events), the network needs to recover from these congestions gracefully.

Forecasting AIN traffic will be a challenge because of the AIN's open ended, service independent nature. The individual service penetration rates should be understood and aggregated so that the AIN SCP is provisioned with adequate resources to handle the expected blend of services that occur during busy-hour conditions. Poor estimates may cause the AIN SCP to be under-engineered, which can then lead to FCC reportable events.

In the absence of highly accurate estimates of penetration rates and service mixes, it is essential the AIN SCP have overload controls to protect itself when the load presented is greater than the existing resources.

AIN overload control (call gapping) requirements are available but must be fully implemented. Service characteristics are not understood, and Automatic Congestion Control requirements are still not implemented in all subsystems. Overload controls must be implemented for the services, subsystems, and network. To resolve this problem, the NOF committee of ATIS needs to continue the efforts to establish industry alignment on how the Call Gapping and Automatic Congestion Control will be implemented. Equipment manufacturers and service providers should

then implement the requirements, and interoperability testing should be conducted to verify proper implementation in all subsystems.

<Recommendation 21>

The suppliers should provide a model or a checklist that allows the network provider to engineer the variable components of an AIN SCP to satisfy the forecasted demand.

<Recommendation 22>

Network providers should arrange for load testing of their AIN SCPs to verify component utilization under predetermined traffic mixes and load.

<Recommendation 23>

A better automatic congestion control mechanism should to be developed by the SCP suppliers so that the SCP can recover from congestion gracefully without adversely impacting the network. Similarly, the service providers should understand the capacity limitation of the SCPs and follow proper engineering practice (e.g., leaving enough margin for maximum load).

<Recommendation 24>

The NOF should continue its efforts to establish industry alignment on how the Call Gapping and Automatic Congestion Control will be implemented. Equipment manufacturers and service providers should then implement these requirements, and interoperability testing should be performed to verify proper implementation in all subsystems.

5.7 SSP AIN Software

Implementation of SSP software was identified by the subteam as an area of potential risk to cause FCC reportable outages. In particular, robustness of this software was the area of focus.

In the outage reports collected, a total of 38 outages were reported with 18% (7 outages) identified as software failures. A further 21% (8 outages) were identified as having Unknown cause.

Although SSP software was not identified as an area of reliability concern by survey respondents, they did offer opinions on a number of subjects that are relevant with respect to SSP software. One important concern expressed by survey respondents was that vendors should participate in writing specifications and requirement documents.

Different vendors have taken different approaches to their implementation of AIN SSP functionality resulting in development of different subsets of the requirements with varying degrees of interworking with preexisting switch functionality. It was observed that an identical operation was unlikely to be achieved. If driven to achieve a single common view, innovation would be restricted because the lowest common denominator would be the only accepted subset. Instead, there is a need to achieve common behavior for the most heavily used nucleus of functionality while permitting innovative additions around that core and in less heavily used portions.

A major hurdle in achieving common operational behavior is a lack of common understanding among the many people involved in AIN specification, network element implementation and testing, and service design. It is easy to observe differences in the way time honored telephony concepts are understood by various industry participants. Hence, diverse views concerning specifications and requirements in a complex new area such as AIN are inevitable.

One way to reduce the variation caused by different interpretation of requirements is to strive for common standardized terminology. This would need to be supported by a corresponding learning environment. From this it is easy to see the ambiguity-reducing benefits from standardized techniques such as Specification Description Language (SDL[§]) for specification writing. The key to success lies in rapidly achieving widespread education of participants from a single information source.

There is also a need for cross-system tractability. That is, tracking from specification to system implementation to assure compliant implementation. Specification languages that support mechanized code and/or test case generation will enable success in this area.

Prototyping is a way to accelerate the discovery of differences between specification and implementation and between different vendor implementations to the same specification. AIN offers tremendous value to network operators for this reason because service ideas can rapidly be moved to prototype implementations for technical or market trial. In a similar manner, vendors should to offer prototypes in advance of SSP product implementations to allow users and interworking systems an opportunity for early discovery of disconnects.

<Recommendation 25>

A standardized specification language (e.g., SDL) should be adopted in AIN requirements and Committee T1 standards for use in all future AIN specification documents.

5.8 SSP/SCP Testing

SSP and SCP testing was identified by the subteam as an area of potential risk to cause FCC reportable outages. In particular, interworking of AIN functions with switch features was the area of focus.

Survey respondents identify a number of specific concerns with respect to SSP/SCP testing. In general, they said vendors need to improve testing of AIN products. A key area of concern is the interface between SSP and SCP, which needs a more rigorous specification and better testing.

A major factor affecting AIN testing is the open call model[**] with its diverse suite of triggers, messaging, and call control possibilities. Other factors to be considered are the single ended (half-

---

[§] **SDL - Specification Description Language** is a symbolic language that permits unambiguous specification of system behavior. From this or similar forms of representation, it is possible to automate portions of system implementation and test case generation.

[**] **Open Call Model:** AIN as defined in Bellcore's GR-1298 and ITU's CS-1R defines a generic call model as the foundation for all SSP interaction. This call model, divided into an originating and terminating half call, defines a logical flow of control for handling a call. Within that flow, numerous points are defined from which queries can be launched to the SCP. Responses from those queries are used to alter the flow of control within the call model. The call model is defined to be independent of any specific service requirements.

call) model. From the perspective of system testing, messaging links represent a critical point in the system architecture.

The implications of AIN diversity is an infinite number of possible test cases. A complete test is difficult or impossible to achieve.

From a tester's perspective, the challenge is to ensure that the intent of the AIN specification has been met. This must address not only the AIN functionality but also the interworking with existing switch features.

There is benefit to be derived from the solutions suggested for improving SSP software. In particular, as cross-system tractability is addressed by rigorous specification languages, mechanized test case generation can be implemented. In so doing, a strong correlation to the original specification can be ensured in the test plan.

<Recommendation 26>

A standardized interface simulator should be developed for companies that will be conducting testing based on the AIN interconnection interface standards for the purpose of interoperability testing, e.g., a standard SCP simulator would ensure uniform SSP performance over a core suite of test cases.

<Recommendation 27>

A standardized suite of test cases for each network element should be developed and maintained. This could be conducted by Bellcore or the Telecommunications Industry Association (TIA).

5.9 Emerging Challenges - AIN Interconnection

AIN is a network architecture that was designed to provide a means by which the LECs can offer advanced features and services to their end customers independent of local switch feature availability and switch vendor development schedules.

As competition in the local telecommunications market intensifies, and the local network is unbundled, third party service providers want to utilize AIN functionality to create alternative services and offer them via the LEC networks to end customers. This view, however, has created a fundamental concern among all service providers as to whether the addition of third party access to the embedded telecommunications network will require any trade-offs between service functionality and network reliability.

The industry is working on numerous issues regarding AIN interconnections. The following sections discuss some specific activities that must be encouraged.

5.9.1 Mediation and Third Party Service Provider Access

The industry's focus with regard to AIN interconnection has centered around two specific AIN areas: mediation and trigger access. These two areas are the hurdles that must be overcome to continue the evolution of AIN technology into a multi-provider environment.

Mediation

Mediation, or mediated access, has been defined as the set of real time and/or non-real time functions needed to facilitate secure, cost-effective third party access to local and other service provider AIN capabilities that will foster the open evolution of and competition in the local exchange network and other networks.

Mediation functionality can be broadly classified into two categories: 1) network protection, and 2) third party service provider access capabilities in a multi-provider environment. The first category includes screening, authentication, performance monitoring, fault management, and network traffic management. The second category includes routing, recording, billing, provisioning, maintenance, and service/feature interaction resolution.

From an architectural viewpoint, LEC service providers believe that AIN was not designed to readily accommodate third party service provider access and that additional forms of "mediated" functionality are needed to offer third party AIN access.

From a third party service provider's perspective, making AIN functionality available to all service providers in a timely, competitive environment is a prime concern. In addition, they are equally concerned about network reliability, but believe that additional mediation functionality will not be initially needed. This is based on their belief that many functions residing in the network already perform mediation-like functionality.

Note that throughout the evolution of AIN technology the LECs, other network providers and third party service providers need to work together to define and reach an agreement on the type of third party access needed; what mediation functions are needed, if any; the level of mediation; and the placement of mediation functionality in the network. The mediation functions previously identified in this section as network protection must always be addressed.

Trigger Access

Trigger access is the process of identifying calls that need AIN handling. Upon encountering a trigger, the AIN switch, SSP, suspends normal call processing, and launches a query to the SCP. The subsequent SCP reply tells the SSP how to continue processing the call.

Examples of AIN triggers include: off-hook delay, originating - no answer, terminating - busy. Collectively, 24 triggers have been defined through work by Bellcore and the ITU.

Access to AIN triggers implies that the local service provider's switch is equipped with the appropriate trigger detection software, and that the local service provider allows the third party service provider the use of these triggers for call control in support of features and services. The availability of triggers for third party access in a multi-provider environment is another key AIN issue that the industry must address. Without access to local switch triggers, a third party service provider's ability to offer its own AIN services is limited.

Additional issues surrounding third party AIN trigger access include the following:

- who will be responsible for assigning triggers and maintaining ongoing records
- will third party service providers be allowed to provision triggers in the LEC's switch on behalf of their end customers
- what operations support systems will be available to third party service providers in support of maintaining their assigned triggers

Next Steps

The telecommunications industry should work quickly to resolve these AIN issues by providing a balanced solution that addresses third party service needs, and supports the entire telecommunications industry's goal of maintaining network integrity and reliability.

In today's environment, the LEC is the single provider of AIN line-based features to its end customers; no third party access is available; and, therefore, no mediation issues need to be addressed. However, what is available to the end customer is a finite number of AIN service offerings from LEC tariffs.

In the long term, as networks become more complex as a result of an increasing number of triggers offered, message queries initiated, and third party service providers, AIN architecture will need to be redefined to incorporate some set of additional mediation functions. This redefinition effort will probably require input from the LECs, Bellcore, ICs, third party service providers, standards bodies, and the FCC[††]. It will also require continued attention to the network protection forms of mediated access plus the development of new functionality identified as mediation functions related to third party service provider access capabilities in a multi-provider environment.

In this regard, the Information Industry Liaison Committee (IILC), an ATIS forum, is currently addressing mediation and trigger access. The IILC has two open issues related to mediation, and two other AIN issues which deal with third party trigger access (Appendix E). Continued industry participation in forums such as the IILC will be a significant driver toward the successful development of AIN technology in the network. The NRC AIN subteam recommends full industry support and participation of voluntary industry efforts such as the IILC.

The IILC is the first industry group to step forward and start to address some of the issues related to AIN in a multi-provider environment. It is not clear at this point what level of technical expertise, and/or the level of motivation the industry will need to develop a solution that will be acceptable to all parties. If additional industry support such as Committee T1 standards on AIN is needed, the NRC AIN subteam would clearly support such activity.

[††] In 1993, the FCC proposed that local exchange telephone companies having annual revenues from regulated telecommunications operations of $100 million or more permit mediated access to their AINs by third parties. Intelligent Networks, FCC Docket No. 91-346, released August 31, 1993.

Evolutionary Considerations for Third Party Access

Today, there seem to be major technical issues in evolving to an environment where multiple providers are able to offer end customer services using the LEC's AIN platforms. Time, technology, and Industry resources are among the factors involved in resolving these issues.

Upon consideration of the AIN evolutionary timeline, the subteam agreed in principle that the Industry should work to resolve outstanding technical issues in such a manner as to minimize any delay in facilitating third-party AIN access. However, the subteam could not reach consensus on a recommended solution. None of the potential methods of facilitating third-party AIN access were extensively or exhaustively considered by the subteam. The agreement in principle reached by the subteam should guide further discussion by Industry participants on AIN interconnection arrangements.

Summary

All issues associated with AIN multiple service provider architectures are centered around the interfaces between providers. Any interface that is created must not adversely impact the integrity, reliability, security, and privacy of the network or services provided in the network.

Aside from some of the issues identified and the need for them to be addressed by the industry, the promise and power of AIN technology and software is significant. Ultimately, the potential exists to deliver to consumers the choice of multiple AIN services offered by multiple AIN service providers.

<Recommendation 28>

As a result of an increasing number of triggers offered, message queries initiated, and third party service providers interconnecting to the network, the networks will become more complex. Major technical issues exist in interconnecting multiple AIN network, and will need to be resolved. The increased scope of complexity that may surround these will require an increased awareness of network reliability. Business issues need to be resolved as well. The NRC's Focus Group II on *Increased Network Interconnection* has created a template of interconnection issues that should be addressed before two networks interconnect. Focus Group III on *Reliability Issues - Changing Technologies* has also created a *New Technology Template* to be used before introducing new technologies into the network. AIN network providers and third party service providers wishing to interconnect should be encouraged to work through the issues in these templates. The completeness of addressing the template issues should be the yardstick for measuring the progress of open AIN network interconnection.

<Recommendation 29>

The industry needs to resolve the uncertainty over what mediation functionality is needed to ensure network reliability while allowing third party service providers the freedom they need to competitively offer their AIN services. It is recommended that the industry continue to work through the IILC and other industry forum such as T1S1 and T1M1 to address AIN issues related to multiple third party service provider access.

5.9.2 Industry-Wide AIN Applications

5.9.2.1 Local Number Portability (LNP)

Network capabilities for the provision of LNP are being explored by the industry in national and state arenas. Number portability is defined as a network capability provides end users the ability to retain their geographic telephone numbers when they change their service provider, their location, or their service (e.g., a change of local service providers, a change of service from POTS to Integrated Services Digital Network [ISDN]).

There is agreement within the industry that with the implementation of LNP, the use of telephone numbers to provide customer identification and network address should no longer be supported. Rather, customer numbers must be separated, and made distinct, from network addresses. Portability can then be provided by the mapping of a given customer number to a unique network address that identifies the switch that serves the customer and to which the call must be routed. The mapping of customer numbers to network addresses will be provided in external network databases and obtained during call processing with appropriate database queries and responses.

LNP will be introduced regionally by specifying certain NPA-NXXs in which numbers can be ported. Accordingly, potentially portable numbers and the need to launch database queries to obtain necessary routing information will be based on the recognition of specific NPA-NXXs. Further, the triggers within network switches that will be used to initiate these queries are likely to be provided through an AIN platform. It should be recognized that if a currently available AIN trigger were used for LNP, it could potentially interfere with other existing features. It has, therefore, been suggested through the work of the Industry Numbering Committee (INC) that a new AIN based LNP trigger be developed to accommodate number portability without the concern of feature interaction.

<Recommendation 30>

LNP designs should ensure that emergency services (e.g., 911 services) are fully supported through pre-service testing.

<Recommendation 31>

Proposed LNP architecture designs should reduce the potential impact of increased signaling traffic on the CCS network.

<Recommendation 32>

Local service providers should ensure that network robustness is maintained during local number portability database unavailability.

<Recommendation 33>

All service providers should ensure service reliability in a multi-provider, local number portability environment. IILC and other industry forum efforts related to service provider interactions in a multi-provider environment, and INC efforts related to local number portability will be needed as essential supportive input to help ensure service reliability in this area.

5.9.2.2 Personal Communications Services (PCS)

PCS provides the capabilities for a subscriber to initiate and/or receive calls at any terminal, fixed or mobile, across multiple service provider networks irrespective of geographic location, based on some combination of a personal number or a terminal number, and a service profile. The nongeographic “500” NPA has been allocated specifically for PCS numbering. The “533” NPA will be used when all of the “500” NPA numbers have been assigned. Additional NPAs (i.e., 544, 566, 577, 588, 599) have been reserved for growth within this service application. The NXX code, as part of the current 500-NXX-XXXX North American Numbering Plan (NANP) format, has been assigned to identify the PCS service provider.

From a nongeographic services numbering perspective, PCS number portability, as identified in the Industry Numbering Committee Report (INC 95-0512-010), will be based on AIN capabilities. PCS number portability is defined as a network capability that provides end users an ability to retain their nongeographic telephone numbers when they change their PCS service provider.

The network elements in this proposed PCS architecture include call originating switches that have SSP capability to recognize the dialed PCS “500” NPA, and to launch database queries to the SCP to obtain routing information from a regional/local PCS numbering database. The regional/local PCS numbering databases will be periodically updated from a nationwide service management PCS administrative database. The information received from the numbering database will either be a carrier identification code (CIC), a geographic based number, or an SS7 point code of a PCS service provider's home location register (HLR). Receipt of an SS7 point code will require the SCP to launch a query to the HLR to obtain routing information. The HLR contains the geographic routing address for the PCS subscriber's current location.

In addition, network access arrangements for nongeographic services, such as PCS, are being addressed at a workshop under the Industry Carriers' Compatibility Forum (ICCF). This workshop is developing a document that will identify, evaluate, and recommend possible technical interconnection and routing arrangements, using some AIN solutions, associated with call setup for services that use nongeographic codes.

6. Summary of Recommendations

Industry Opinion Questionnaire (Section 4.2)

> **<Recommendation 1>**
> Service providers and suppliers should review the suggestions in Appendix B (AIN Reliability Concerns from Survey Response) for their applicability to their own networks and systems.

Experts Presentations (Section 4.3)

> **<Recommendation 2>**
> Service providers and suppliers should review the summary of experts’ presentations contained in Appendix C for their applicability to their own networks and systems.

SCPs and IPs (Section 5.1.1)

< Recommendation 3>
SCPs should be deployed in duplex by the service providers. Key applications,(such as 800 service), that affect numerous customers, should be duplicated in the mated SCPs to reduce network risk.

<Recommendation 4>
SCP/IP reliability objectives should be reviewed by the service providers and equipment suppliers to ensure that they are consistent with switch reliability objectives and that the impact of SCP/IP failures are minimized. Reliability objectives, and other interconnection requirements, should be included in the interconnection standards set up by the American National Standards Institute (ANSI) accredited Committee T1 (Section 5.2.5). Service providers should then use these standards to ensure that SCP/IPs connected to switches have the same level of service reliability as the switches - via equipment reliability, functional redundancy, or duplex deployment.

AIN Architecture Standards (Section 5.1.2)

<Recommendation 5>
Service providers should conduct reliability analysis to ensure that introduction of new architectural elements (e.g., nontraditional components such as information systems) do not negatively impact the high reliability of the network. Redundant functionality of network nodes and physical and logical diversity of links should be implemented where feasible.

< Recommendation 6>
For services requiring high availability/reliability (e.g., 911 service), service should direct their effort toward (1) reducing the number of critical elements involved in providing the service, and (2) increasing the level of connectivity available in the network.

<Recommendation 7>
Greater focus is required by Committee T1 on standardization of AIN architectures as architectures evolve toward support of open networks. As a first priority, a set of architecture standards is needed for interconnection among LECs, LEC and IC, LEC and third party vendors, etc.

NS/EP AIN Architecture Review (Section 5.1.3)

<Recommendation 8>
The subteam recommends that service providers review the NCS report and assess the recommendations for application to their networks.

Root Cause Analysis Process (Section 5.2.1)

<Recommendation 9>
The service providers should establish an AIN data collection process that collects failure specific data, root cause(s) of the failure, and recommendations for prevention. An outage

reporting criterion should also be established by each provider so that their employees know what information should be collected/generated and what reporting process should be used (i.e., internal company only, industry, or FCC).

<Recommendation 10>
All service providers should follow the information sharing guidelines established by the NOF, Reference Document, Issue 1, April 1993.

Troubleshooting and Fault Isolation Tools (Section 5.2.2)

<Recommendation 11>
The Committee T1 and other industry forums such as the Network Management Forum (NMF) or Network Operations Forum (NOR) should expand on the work performed by the International Telecommunications Union - Telecommunications Standardization Sector (ITU-T -- formerly the CCITT), and documented in recommendation M.3010 "Principles for a Telecommunications Management Network (TMN)," with focus on the definition of the industry needs and the development of standards and requirements for network problem isolation and recovery tools, and capability.

AIN Performance Measures (Section 5.2.3)

<Recommendation 12>
The Committee T1 should expand on the work performed by the ITU-T and documented in Recommendation M.3010, and develop industry standards for network health indicators, for Network Element performance indicators, and for individual AIN application performance monitoring. Verification of these standards should be included in all interoperability, new AIN platform, and AIN application testing.

AIN Reliability Objectives (Section 5.2.4)

<Recommendation 13>
The working group T1A1.2 should develop reliability standards for AIN platforms and applications that emulate end-office switch outage frequency and downtime expectations. The Bellcore Generic Requirements for AIN platforms and applications (GR-1280-CORE, TR- NWT-000284, and GR-929-CORE) should be used as a starting point and assessed for applicability to current network performance expectations.

Growth and Retrofit (Section 5.2.5)

<Recommendation 14>
The suppliers and service providers should work together to define downtime requirements and to find ways to improve, simplify and automate the retrofit procedures to reduce the complexity of, and the time required for retrofits.

Operations System Interface and Support (Section 5.3)

<Recommendation 15>
The Committee T1, the NMF and the ITU-T should expand on both existing and emerging network management standards and technologies to allow the TMN standards to be implemented to support development of operations and maintenance tools and to achieve broad deployment of TMN in the telecommunications industry.

<Recommendation 16>
Any service provider that wants to implement TMN must deal with a host of legacy system issues related to existing network elements and OSs. The Committee T1 and the Network Management Forum (NMF) should develop standard mappings, evaluate the economic impact, and develop a practical transition from existing legacy system interfaces to standard TMN interface MIBs.

<Recommendation 17>
Vendors of TMN components should form working groups with the Committee T1 and the NMF and develop common MIBs and managed objects for use by developers. Vendors can apply this open system approach by forming information models for industry standard interoperable interfaces.

Service Creation/Provisioning Process (Section 5.4)

<Recommendation 18>
The service providers should implement a service creation/provisioning process to ensure the quality of the AIN services and maintain the integrity of the network. The following subsection describes an overview of a process in use by one service provider. The process has been verified and upgraded based on its experience. The subteam offers it as a "Best Practice" and urges the industry to replicate its use, upgrade the model from their experience, and share the improvements with the Industry.

Interoperability (Section 5.5)

<Recommendation 19>
Service providers should work together or work through Committee T1 to develop interconnection standards for AIN service interconnection and AIN network interconnection for the multi-service provider environment.

<Recommendation 20>
Adequate functional testing and pre-service tests need to be performed by the suppliers and by the service providers before cutover. Network node integration testing should be performed by the service providers and the suppliers before integrating any new or upgraded network node or equipment into the network. Network interconnection testing should be performed by the interconnecting networks before interconnection. The interconnection tests should include end-to-end service integration tests, interconnection protocol conformance tests, overload tests, etc. It may be possible to use the existing Internetwork Interoperability Test Plan (IITP) committee of the NOF to accomplish the internetwork integrity testing. The IITP committee should consider extending the IITP testing activities to include AIN internetwork integrity testing. (See Focus Group II's

Technical Paper for recommendations concerning the direction of interoperability testing and IITP)

AIN Network Overload Controls and SCP Capacity and Overload (Section 5.6)

<Recommendation 21>
The suppliers should provide a model or a checklist that allows the network provider to engineer the variable components of an AIN SCP to satisfy the forecasted demand.

<Recommendation 22>
Network providers should arrange for load testing of their AIN SCPs to verify component utilization under predetermined traffic mixes and load.

<Recommendation 23>
A better automatic congestion control mechanism needs to be developed by the SCP suppliers so that the SCP can recover from congestion gracefully without adversely affecting the network. Similarly, the service providers need to understand the capacity limitation of the SCPs and follow proper engineering practice (e.g., leaving enough margin for maximum load).

<Recommendation 24>
The NOF needs to continue the efforts to establish industry alignment on how the Call Gapping and Automatic Congestion Control are going to be implemented. Equipment manufacturers and service providers should then implement the requirements, and interoperability testing should be then performed to verify proper implementation in all subsystems.

SSP AIN Software (Section 5.7)

<Recommendation 25>
A standardized specification language (e.g., SDL) should be adopted in AIN requirements and Committee T1 standards for use in all future AIN specification documents.

SSP/SCP Testing (Section 5.8)

<Recommendation 26>
A standardized interface simulator should be developed for companies that will be conducting testing based on the AIN interconnection interface standards for the purpose of interoperability testing, e.g., a standard SCP simulator would ensure uniform SSP performance over a core suite of test cases.

<Recommendation 27>
A standardized suite of test cases for each network element should be developed and maintained. This could be done by Bellcore or the Telecommunications Industry Association (TIA).

Mediation and Third Party Service Provider Access (Section 5.9.1)

<Recommendation 28>

As a result of an increasing number of triggers offered, message queries initiated, and third party service providers interconnecting to the network, the networks will become more complex. Major technical issues exist in interconnecting multiple AIN networks exist, and will need to be resolved. The increased scope of complexity that may surround these will require an increased awareness of network reliability. Business issues need to be resolved as well. The NRC's Focus Group II on *Increased Network Interconnection* has created a template of interconnection issues that should be addressed before two networks interconnect. Focus Group III on *Reliability Issues - Changing Technologies* has also created a *New Technology Template* to be used before introducing new technologies into the network. AIN network providers and third party service providers wishing to interconnect should be encouraged to work through the issues in these templates. The completeness of addressing the template issues should be the yardstick for measuring the progress toward open AIN network interconnection.

<Recommendation 29>

The industry needs to resolve the uncertainty over what mediation functionality is needed to ensure network reliability while allowing third party service providers the freedom they need to competitively offer their AIN services. It is recommended that the industry continue to work through the IILC and other industry forums such as T1S1 and T1M1 to address AIN issues related to multiple third party service provider access.

Local Number Portability (LNP) (Section 5.9.2.1)

<Recommendation 30>

LNP designs need to ensure that emergency services (e.g., 911 services) are fully supported through pre-service testing.

<Recommendation 31>

Proposed LNP architecture designs need to reduce the potential impact of increased signaling traffic on the CCS network.

<Recommendation 32>

Local service providers need to ensure that network robustness is maintained during local number portability database unavailability.

<Recommendation 33>

Local service providers need to ensure service reliability in a multi-provider, local number portability environment. IILC and other industry forum efforts related to service provider interactions in a multi-provider environment, and INC efforts related to local number portability will be needed as essential supportive input to help ensure service reliability in this area.

7. Path Forward

Data collected by the ATIS Network Reliability Steering Committee (NRSC) indicates that the reliability of the Common Channel Signaling Network has improved in both the areas of frequency and impact. Data collected by this subteam indicates that some AIN outages have occurred but none have been severe enough to have met the threshold for reporting to the FCC and, therefore, inclusion in the NRSC analyses. With the rapid implementation of AIN technology and services the industry is challenged to meet this subteam's objective that " *there should be no FCC reportable outages related to AIN*. "The data and recommendations contained in this report are only a starting point toward achieving that objective. Service providers and systems manufacturers must also analyze the data in this report, assess the recommendations in the context of their own networks and products, and be the final judges for what is needed to ensure a high level of AIN reliability. The analyses conducted by the NRSC will, in the end, be the monitor to see if the objective will be met.

8. Acknowledgments

The AIN subteam would like to extend their sincere appreciation to the Industry Single Points of contact and the individuals working with them who actually gathered the data and filled out the survey forms for the time and effort dedicated to this project, and to the Subject Matter Experts (see list in Section 4.3) for their insightful presentations at the subteam meetings. The subteam's recommendations are based largely on the invaluable data supplied by the NRC participating companies and the technical presentations by the Subject Matter Experts.

The subteam would also like to extend their appreciation to the Bellcore data aggregator, specifically Mark Williamson, for his effort in designing the questionnaire form, collecting responses and analyzing the data received.

9. References

[1] SR-TSY-000963, *Network Switching Element Outage Performance Monitoring Procedures)*, Bellcore, Issue 1, April, 1989.

[2] *AIN NS/EP Reliability Risk Analysis*, National Communications System (NCS), September 1994.

[3] *Network Reliability: A Report to the Nation*, June 1993, Section C, Page 10, Paragraph 5.1.3.2

[4] *Network Reliability: A Report to the Nation*, June 1993, Section B, Page 32, Paragraph 6.1.2 and Section B, Appendix 6.

[5] ITU-T, Recommendation M.3010, *Principles for a Telecommunications Management Network.*

[6] GR-1280-CORE, *Advanced Intelligent Network (AIN) Service Control Point (SCP) Generic Requirements*, Bellcore.

[7] TR-NWT-000284, *Reliability and Quality Switching Systems Generic Requirements (RQSSGR)*, Bellcore.

[8] GR-929-CORE, *Reliability and Quality Measurements for Telecommunications Systems*, Bellcore.

[9] GR-1469-CORE, *Network Security Generic Requirement*, Bellcore.

10. Appendices

Appendix-A Network Reliability Council Issue Statement

Issue Title: Reliability Concerns Arising Out of Changing Technologies **Author:** Gary Handler
Bellcore

Problem Statement/Issue to be Addressed

The national Public Switched Network (PSN) which is truly a network of networks, has the deserved reputation of providing its users highly reliable, survivable and secure end-to-end services. The FCC and its Network Reliability Council (NRC) want to ensure that this remains the standard mode of operation in spite of a dramatic increase in the number of new technologies being deployed, the implementation of advanced new services offered to the public, and the emergence of a proliferation of new service providers. In specific, the NRC will study a) the reliability aspects of the provision of key services over new network facilities, (i.e., broadband hybrid fiber/coaxial cable distribution, SONET and ATM, wireless, and satellite), and b) reliability concerns arising out of new technology providing expanded services over new or traditional facilities, i.e., Advanced Intelligent Network (AIN) capabilities. The emphasis of this FocusTeam should be on new technology that will be implemented in the public network within the next three years.

Areas of Concern and Problem Quantification

The following are the main areas of concern:

A. Reliability Aspects of Provision of Key Services Over New Network Facilities

1. *Broadband Networks* - One concern about new network technologies is how the reliability of services such as plain old telephone service provided over new broadband networks will compare with that of the same service provided over existing wireline technology. These new systems should be modeled and analyzed for potential reliability risks and possible reliability improvement techniques. Implementation "Best Practices" should be developed and a plan for their dissemination and implementation should be derived. Two specific areas should be addressed:
   - *Hybrid Fiber/Coaxial Cable Distribution Systems* - This technology is expected to be providing telephone service shortly. The reliability issues with this technology need to be defined and addressed.
   - *SONET Facilities and ATM Technology* - SONET transport and ATM technology are rapidly progressing and will be providing new broadband services as well as existing narrowband services over common facilities. The reliability issues with these technologies need to be defined and addressed.
2. *Wireless Network (Cellular and PCS)* - Another example of a concern about new technologies is the role and reliability of cellular facilities in connection with line-based networks. This issue was discussed by the NRC at its September 30, 1992 meeting and in the document *Network Reliability: A Report to the Nation.* The reliability of the telecommunications services provided over a combination of new technologies has to be reviewed. Customers who rely on cellular technology need service providers to have

and follow established "best practices." These do not now exist. Best practices for Personal Communications Services (PCS) and Networks should also be considered in this study.

3. *Satellite Networks* - Another area of reliability concern is the provision of telephone services over new satellite technology networks such as low earth orbiting satellites. The reliability issues with this technology should also be defined and addressed.

B. Reliability Concerns Arising Out of New Technology Providing Expanded Services over New or Traditional Facilities, i.e., Advanced Intelligent Network (AIN) Capabilities - Concerns have also been raised regarding the interoperability and reliability of multiple advanced intelligent services with their inherently independently developed software management and control. As John Clendenin stated at the July 6, 1994 NRC meeting "this is not the kind of problem that could be solved (once) and laid aside". However, to provide a near term objective from which a model or process might be developed, it is suggested that the team focus on the interoperability and reliability concerns in the development of Advanced Intelligent Network Services.

Description of Proposed Work

The team working this issue should consider the following total quality process to identify reliability concerns arising out of changing technologies, quantify network vulnerabilities, identify the major reliability issues and propose problem solutions.

1. Identify the new technologies being introduced into the network.

2. Collect appropriate data from all available industry sources to determine and/or confirm areas/technologies of greatest criticality and risk, and those with the greatest potential for network reliability improvement potential. (Work with the ATIS Network Reliability Steering Committee (NRSC) and its Network Reliability Performance Committee to coordinate data collection activities).

3. Collect data from the industry concerning the reliability of new technologies if already deployed. (Work with the ATIS Network Reliability Steering Committee (NRSC) and its Network Reliability Performance Committee to coordinate data collection activities)

4. Perform sufficient analysis of the data to determine the root cause(s) of the problem(s).

5. From the root cause analysis determine an appropriate action plan to reduce/eliminate the possibility or severity of failures in high risk areas. Also consider ways that recovery procedures may be implemented more quickly or efficiently.

6. Determine industry "best practices" for dealing with the root cause analysis findings and share this information with industry participants as soon as possible. Deployment should consider cost/benefit tradeoffs of "best practices."

7. Develop a timeline and metrics to measure the effectiveness of the team's recommendations.

8. Consider the following tactics/ideas offered by the Steering Team as potential means to supplement the total quality process and address the findings of the root cause analysis. These represent ideas from the Steering Team that we want to share.

   A. New Technology Reliability Template - Design a generic template that serves as a reliability screen for assessing the reliability of new network technologies. This could be used as a process for the rapid and reliable evolution of the telecommunications networks.

   B. Provision of Key Services Over New Network Facilities

   1. *Broadband Networks (Hybrid Fiber/Coaxial Cable Distribution* and *SONET Facilities & ATM Technology*), *Wireless Networks (Cellular & PCS),* and *Satellite Networks.*

      - For each technology, determine the scope of the reliability study. Develop a bounded definition of the reliability problem; for example, the provision of basic telecommunications over a new broadband hybrid fiber/coaxial cable distribution network.
      - Construct an order of magnitude (major failure modes and vulnerabilities) reliability model of a reference system for each technology.
      - Collect available reliability data (e.g. current coaxial cable systems network outage & failure data, current cellular network outage and failure data, current SONET network outage and failure data and ATM switch reliability), concerns and "best practices" associated with each technology.
      - Analyze data to quantify reliability and determine the most significant problem areas, and the areas with the greatest risks.
      - Determine applicability of current "best practices" to the new technology and identify any additional "best practices" that describe quality as part of the introduction of new technologies (i.e., "best practices" applicable to hybrid fiber/coaxial cable networks, cellular networks, and SONET networks).
      - Recommend implementation strategies for "best practices" and on-going process information for insuring continued quality.

   2. Advanced Intelligent Network (AIN) Capabilities

      - Determine the reliability issues associated with AIN services (e.g., management of many different versions of software).
      - Identify efforts taken to date to address AIN reliability issues and to ensure AIN service reliability. Identify existing "best practices."
      - Identify potential reliability "holes" or problem areas and recommend solutions.
      - Identify the role that the IITP process might play as part of an implementation strategy for interoperability control and as a reliability qualification process for new AIN platforms, services and software. (Coordinate potential overlapping interconnection issues with the Network Interconnection Focus Team)

Existing Work Efforts

There are several work efforts that have addressed or are addressing some of these issues. The Fiber Cable Focus Team recommendations in the *Network Reliability: A Report to the Nation***,** *the Telecommunication Industry Benchmark Committee (TIBC) Report*, Draft Congressional Bills S2101 and HR4394 on one-call legislation, and the ATIS/NRSC Annual Report provide significant data from which to begin to address the Provision of Key Services Over New Network Facilities issue. The ATIS Working Group on Network Survivability Performance, T1A1.2 and the News Release, DA-1343, requesting comments on Joint Petition for Rulemaking on Cable Television Wiring, RM No. 8380, November 15, 1993 provide background on the cellular and coax cable concerns. The Switching Systems (focus on software) Focus Team Recommendations in the *Network Reliability: A Report to the Nation* as well as ATIS/NOF/IITP charter and test plans give good background material for addressing the services and software concerns.

Recommended Team Leader
Ken Young - Bellcore

Recommended Team Participants

Ray Bonelli - AT&T Network Systems
Ed Bonkowski - Advantis
Lynda Eckes - Bell Atlantic
Jim Funk - U S WEST
Clint Hamilton - Bellcore Professional Services (Chair)
Gabor Luka - NCS
Doris Nagel/Jeff Ragle- Bellcore SCP
Alex Nichols - Nortel
Pete Shelus/George Stanek - AT&T Network Services
Ken Walling - Pacific Bell

Chao-Ming Liu - Bellcore Professional Services (AIN subteam Secretary)
Mark Williamson - Bellcore Professional Services (Data Aggregator)

Appendix-B AIN Reliability Concerns From Survey Response

#	Concerns	Reliability Risks	Suggestions
1	Simplex SCPs	Could result in total system outage for some services.	Mated SCPs with each able to handle combined load.
2	Simplex IPs	Single processor outage will cause system outage.	Fault-tolerant software, functional redundancy.
3	Mediated Access	Fraud, overload, hacker	Limits and checks, regulated and frequent audits.
4	Lack of US/T1 Standard Architecture	Different interpretation/implementation of architecture and services, interaction between different suppliers and providers.	Agreement among major suppliers, common platform for service providers.
5	Direct Access to SCP/IP Data	Data corruption, security	Security checks
6	Growth and Retrofit	At high annual growth, processor overload results in service disruption. Most retrofits require long downtime - reduced system capacity, simplex operation, ... Complexity of procedures, testing inadequate.	Temporary soak interval before integration, good technician and procedures, better testing during development, vendor verification/testing of procedures.
7	Adequacy of Current Manual and Automatic Recovery Procedures	Length of time to recover, manual processes prone to human error.	Streamline and improve functionality; automate processes.
8	Performance Measurement	Cannot predict platform overload quickly enough.	Need better way to measure service load; need AIN "service" view of performance.
9	Troubleshooting	Cannot identify foreign cause of network problem; unable to detect SCP and SCP-SSP feature interaction; tools not available, do not provide enough capability.	Develop functionality; need tool enhancements and evaluation; training.
10	Adequacy of Currently Available OS Interfaces/support	Lack of developed interfaces to nonvendor OS, lack of OS for total network surveillance and monitoring, lack of robustness, poor human factor design.	Develop interfaces; need effective network surveillance tool; robust, redundant design for OS; artificial intelligence to correlate distributed systems.
11	Vendor Implementation of Requirements	Vendor interpretations, inadequate testing.	Involve vendors in writing requirements; improve and validate testing.

12	Supplier SSP Implementation Differences	Unexpected SSP discrepancies may overload SCP; trigger table, call model variations; no standard/defined interfaces.	Better SSP/SCP interface definition; standard implementation; better testing; common call model.
13	SSP	IP connection to single E/O; software protocol errors, vendor code errors can impact call routing at trunk level, causing application failures, large scale customer impact.	Duplex IPs served off 2 E/Os; better testing of software before release; better error detection, troubleshooting, recovery mechanism.
14	SCP	Simplex deployment, insufficient operative testing, application failure, new application software releases, congestion.	More testing during development, better testing with real world environment, duplex deployment, network traffic planning, ACG.
15	IP	Insufficient operative testing, simplex deployment.	More testing during development, duplex deployment.
16	Congestion Control and Network Management Features	Not implemented, traffic blockage, node overload, congestion.	Need to be better developed; ACG; all vendors up to speed on requirements and implementation.
17	Translation and Routing Features	Call blocking due to improper screening, incorrect routing, traffic blocking, network overload, improper translation and routing potential for propagation to adjacent nodes and/or networks.	Periodic re-evaluation of translations, quality development methodology, complete requirements, multiple testing phases.
18	Services based on Office-wide Triggers	New translations; failures can affect large # of customers; improper provisioning of parameter; simple error can create wrong service execution processing.	Strict control, early prototyping and testing; restrict access; Use SMS/SCE with modeling capabilities; testing, validation.
19	Service Provisioning	Software errors, capability limitation.	SMS/network management coordination, training.
20	Mediated Access	No control of what others are doing.	Strict control.

Appendix-C Summary of Experts' Presentations

C.1 Overview of Advanced Intelligent Network Architecture

John Brewster of Bellcore provided a briefing for the AIN Subteam on the Advanced Intelligent Network. His topics included the historical background of AIN, the AIN architecture, AIN evolution, and network reliability considerations.

C.2 Advanced Intelligent Networks - An NS/EP User Perspective

Rick Sherman of MITRE presented a summary of an AIN architecture analysis for the NCS from an NS/EP use perspective. He mentioned that, to achieve higher reliability and survivability, efforts needed to be directed toward 1) reducing the number of critical elements involved in providing the AIN service, 2) reducing the level of connectivity available in the architecture, 3) decentralizing services, and 4) providing a high level of functional redundancy. He also said that the engineering of specific AIN architectures that support NS/EP services must include strong emphasis on reliability, availability, and recovery from failures.

C.3 Bell Atlantic AIN Architecture

Lynda Eckes of Bell Atlantic gave a brief presentation of Bell Atlantic's AIN architecture. She also shared the following list of requirements for the AIN architecture design:

- grade of service equality
- survivable/reliable
- service offering/creation
- operations control
- mated pair AIN/SCPs
- dual power feed from commercial power

C.4 AIN Operation Issues and Concerns

Jan Ryssemus of Pacific Bell discussed AIN issues and concerns from the network operations point of view.

He mentioned that most of the AIN equipment is fairly reliable. However, there are some operations issues that may cause reliability problems. The first on this list is the lack of consistency or standard of service design. This creates a problem for the network operations people. The problem will be even bigger when carriers interconnect their AIN services. Issues related to this include (1) inconsistent translation implementation, (2) incomplete service documentation, and (3) training - how the service works.

He also mentioned a critical challenge in training. Indications of AIN failures exist in many places of the network, which makes troubleshooting not so straightforward. Thus, there is a need to use protocol analyzers in troubleshooting AIN service problems. However, not enough people are trained to use protocol analyzers. Moreover, it is too costly to train all the people in maintenance

centers, switching control centers, etc., to use protocol analyzers. The support systems in use typically lag two years in terms of meeting our current needs. These factors need to be taken into account when designing AIN services.

A fundamental change that AIN brings, Mr. Ryssemus said, is the inclusion of information systems in telephone networks. An example of this is the AIN/SCP. These information systems or databases did not use the same standard, reliability requirements, redundancy philosophy, and maintenance philosophy as the telephone network in the past. We need to make sure that reliability of the network is not negatively affected by the inclusion of these systems.

C.5 AIN Network Evolution Plan

David Fannin of Pacific Bell shared the status of AIN deployment in Pacific Bell. He mentioned that there were two major AIN technology lifecycles, namely, infrastructure and service development. He also mentioned that Pacific Bell has successfully completed the Phase 1 deployment of the AIN platform. Planned AIN capabilities in 1996 include IPs and SMS.

C.6 AIN Service Development Process

Dave Fannin continued discussion about the AIN service development process. He said that was a real key to AIN reliability. He also said that we can decrease the cycle time and increase the quality of the services by properly documenting the service development process. The development process looks like traditional software design process. Factors that worked in Pacific Bell's experience include (1) small multifunctional teams, (2) single point of contacts, (3) good project planning and execution, (4) testing, and (5) service design before deployment. In the end, he made the
following recommendations: (1) continue with small multi-functional teams, (2) greater customer involvement, (3) tighter communication with field site, (4) formal design review and stakeholder sign-off, (5) well-defined problem escalation procedures, and (6) standardized document formats.

C.7 AIN-SCP Capacity Analysis and Management

Dave Fannin discussed how AIN-SCP capacity analysis and management are accomplished in Pacific Bell. He briefly reviewed (1) forecast and modeling, (2) platform validation testing, and (3) in-service data collection and analysis. Future work in this area includes (1) accurate forecasting for services, (2) multiple service capacity testing - multiple services working together in a platform, and (3) overload control.

C.8 AIN Testing Process

Dave Fannin briefly described the AIN testing process in Pacific Bell, including infrastructure testing and service testing (network integration).

C.9 Interoperability

Greg Feldkamp of Bellcore described AIN interoperability testing work in Bellcore, which includes AIN service/application protocol testing, network integrity testing, and overload testing.

Service/application protocol analysis includes end-to-end generic service integration tests between SCP and SSPs. An important emphasis is the interaction between AIN services and switch-based features. Network integrity testing focuses on network robustness under failure conditions. Tests were designed to see if the network could absorb failures gracefully. Network overload analysis looks for different ways to protect SCPs. Greg concluded his presentations by identifying the following
current challenges and *emerging internetwork challenges:*

Current Challenges

- Many uncatalogued interactions between AIN triggers and switch-based features
- Need for SSP-specific AIN service logic due to varying implementations
- Integration of Automatic Code Gap (ACG) capabilities among SCPs and SSPs
- Capacity planning and engineering in face of highly flexible service design and utilization
- Use of non-SS7 networking mechanisms for Intelligent Peripheral-SCP communication

Emerging InterNetwork Challenges

- Third-party service provider access to local a exchange carrier's AIN
- Local number portability
- LEC-provided access services for PCS

C.10 AIN SSP Software Design and Testing

Charles Wiebe of BNR described the challenges of AIN software development. He pointed out that a major difficulty in AIN SSP software design is the confusion of terminology. A term can mean different things even within one customer company. He also noted that because of different interpretations of the terminology used in the requirements, it is difficult for software designers to determine what the customers want. In conclusion, he suggested the following possible solutions:

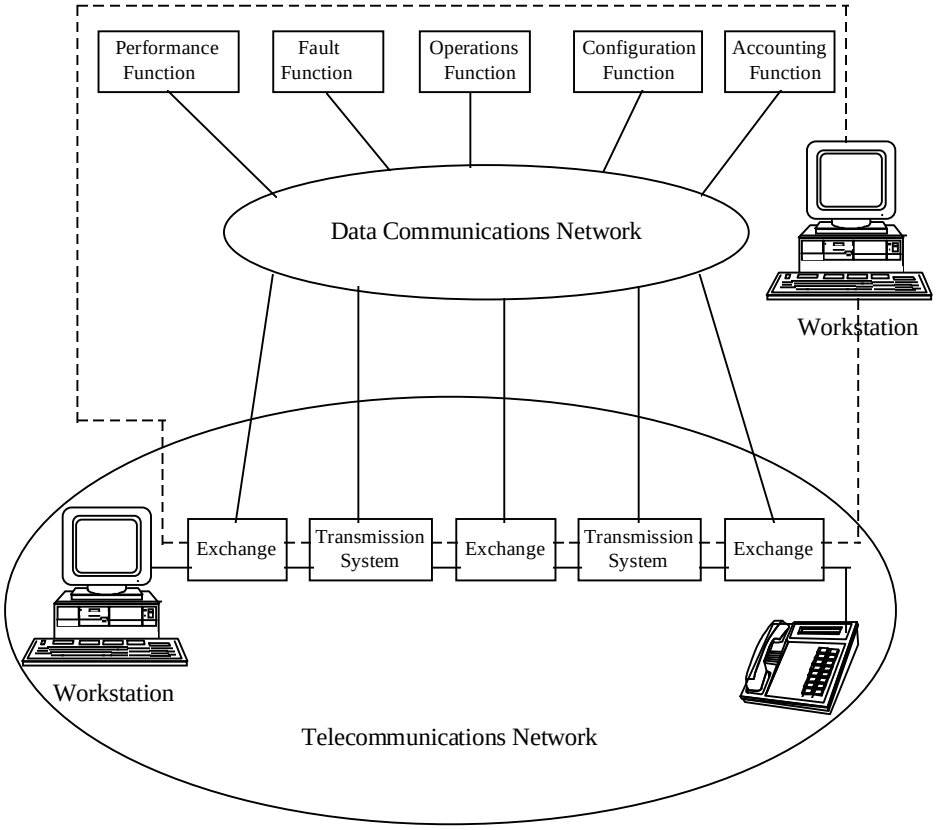
- Common and standardized terminology
- Upgraded learning practices so that people understand the terminology
- Better methodology in writing software design specification, (e.g., using SDL)
- Emphasizing tractability across software system design
- Prototyping

C.11 Reliability in OSI OS/NE Interactions

Carl Hall of US WEST discussed his involvement in an effort to develop standard interfaces for OS in network nodes using the OSI model (Attachment B). He explained that the support systems for SS7 and transport networks did not currently have interfaces between them today. Building a common interface so that all the support systems of the network nodes could interface with one another would enable interconnection and centralized surveillance and maintenance and thus allow cost reduction. It would also allow the service providers to have more control over the data collected by the OS. The availability of centralized knowledge of the various network nodes would also help in event correlation and trouble resolution.

Appendix-D Telecommunication Management Network Overview

Telecommunication Management Network (TMN) is an extension of the Open Systems Interconnection (OSI) standardization process of the ITU-T. Figure D-1 shows the general relationship between a TMN and a telecommunications network which it manages. A TMN is conceptually a separate network that interfaces a telecommunications network at several different points to send/receive information to/from it and to control its operations.



Note: The TMN boundary may extend to and manage customer/user service and equipment.

Figure D-1 Relationship of TMN to Telecommunications Networks.

These standards are intended to result in interoperability of management software. Software modules within a TMN from different vendors should be able to interoperate through standardized interfaces. Standardized TMN interfaces are also intended to allow the exchange of management information between the TMNs of different service providers and between a service provider and a customer.

When fully realized, TMN interoperability will result in integrated network management both within a single service provider and across multiple service providers. The goal is that every

management system within a service provider should be part of an interconnected management hierarchy, able to access the management capabilities of other systems, and allow its own capabilities to be utilized through standardized interfaces.

Recommendations concerning OSS interfaces to NEs that will add to the health of the network and reliability of call completion in the PSN, SS7, and AIN networks address the following areas:

- Standards
- OSS Architecture

1. Standards

Interface standards or requirements need to be implemented to meet the needs of service providers to ensure service and network reliability as follows:

- Implement TMN standardized protocols and data models that are Open Systems Interconnection (OSI) Common Management Information Protocol (CMIP) compliant with standardized Management Information Bases (MIB) for NE data communication interfaces and security to:
  - eliminate proprietary, vertically segregated data streams.
  - achieve an integrated view of the network.

- Implement a standardized OSS architecture that is TMN compliant to:
  - eliminate redundant and interdependent management functions.
  - achieve an integrated network management environment.
  - synchronize event times for not only TMN data collection and control, but for the Network Elements in the managed network.
  - provide standardized authorization and authentication security MIBs.

- Take advantage of opportunities to replace current (legacy) vertical systems, as they reach end-of-life, with standards-based-architecture compliant OSS's.

The development and implementation of standards, requirements, and guidelines for OSS architecture and NE interfaces are directly related to AIN and network reliability.

The OSS development and deployment usually lag one to two years behind AIN service deployment. Therefore, the standards work for OSS architecture and interfaces need to move into implementation immediately.

2. OSS Architecture

Service Providers should take advantage of opportunities to replace current vertical systems, as they reach end-of-life, with standards-based-architecture compliant OSS's. A standard TMN platform will improve network reliability by having a single platform to control and synchronize the network data. Troubleshooting of network and OSS outages will become more efficient with a single platform approach.

The management functions running the platform can be developed to react to different network management issues more quickly than human interaction to manage overload, congestion, and rerouting of traffic. These management functions need to react to all network elements or a single node.

There is a need to measure the health and performance of the AIN network. The most logical place for this is in the OSS management functions developed for performance measuring and monitoring of the health of AIN services.

The TMN (M.3000 series) documents from ITU-T provide a concept for a management network infrastructure that facilitates interoperability and integration. However, many items necessary for practical interoperability are not covered.

Appendix-E IILC Issue Identification Forms

ISSUE TITLE: AIN/IN Trigger Usage In a MultiProvider Environment (from Issue 026 Logical T/O1)	**ISSUE**	**049**
	DATE SUBMITTED	**2/16/95**
	LATEST REVISION	**6/28/95**
	CURRENT AS OF	**6/28/95**
	RESOLUTION DATE	
	IAG REVIEW DATE	
	IILC ADOPTION DATE	

1. ISSUE STATEMENT:

ESPs and other Non LECs want to control certain aspects of switch feature functionality to provide end user services, this may indicate a need for access to switch trigger queries. (The query would be the result of detection of a specified trigger at a designated point in call processing.)

2. SUGGESTED RESOLUTION OR OUTPUT(S):

- Document the generally accepted definitions of triggers available on most AIN/IN platforms as defined in recognized industry documentation.
- Identify and document the needs of the various industry providers for triggers (carriers, ESPs, etc.).
- Identify the technically feasible scenarios for trigger usage in a general AIN/IN platform in a multiple provider environment.
- Compare and analyze industry needs, vendor availability, and pertinent LEC plans to determine expected timeframes for availability of desired triggers.
- Identify and work to resolve (within the scope of the IILC) any technical and operational issues.
- Propose guidelines on multiprovider use of triggers, for presentation to and review by appropriate industry bodies.

3. OTHER IMPACTS

There are impacts on technical requirements for such trigger usage in a multiprovider environment. For instance, how many providers can use the same trigger on the same subscriber line (on different calls and on the same call)? Is the number of providers per trigger affected by the class of service? Can the number of providers and/or the sole designated provider be changed by the time of day or other criteria?

Issue resolution may affect T1 standards activity.

4. ISSUE CO-CHAMPIONS:

Name:	Anthony Toubassi	Name:	Don Davis
Company:	MCI	Company:	BellSouth
Address:	2400 Glenville Rd. Richardson, TX 75081	Address:	675 Peachtree St. 38L64 SBC Atlanta GA 30376
	Phone: 214 918-5167 Fax: 214 918-6038		Phone: 404 420-8057 Fax: 404 885-9920

IILC ISSUE IDENTIFICATION FORM

ISSUE TITLE: AIN/IN Trigger Provisioning in a Multi-Vendor Environment (Resulting from Issue 026 Logical T/O 2)

ISSUE **050P**
DATE SUBMITTED **2/16/95**
LATEST REVISION **6/28/95**
CURRENT AS OF **6/28/95**
RESOLUTION DATE
IAG REVIEW DATE
IILC ADOPTION DATE

1. ISSUE STATEMENT:

Some ESPs and other Non-LECs believe that in order to provide some Intelligent Network services to their customers they must be able to provision triggers (including data input to and administration of operations systems) on behalf of their customers.

2. SUGGESTED RESOLUTION OR OUTPUT(S):

- Develop a common definition of trigger provisioning.
- Identify the management support systems needed for trigger provisioning.
- Determine Non-LEC access methods to LECs' trigger provisioning mechanisms.
- Identify potential protocols to access trigger provisioning mechanisms.
- Identify and work to resolve (within the scope of the IILC) any technical and operational issues.

3. OTHER IMPACTS

Concerns related to reciprocal access to and provisioning of Non-LEC triggers may need to be addressed.

4. ISSUE CO-CHAMPIONS

Name: Don Davis
Company BellSouth
Address 675 Peachtree St.
38L64 SBC
Atlanta GA 30376

Phone: (404) 420-8057
Fax: (404) 885-9920

IILC ISSUE IDENTIFICATION FORM

ISSUE TITLE: Definition and Criteria for Placement of Logical Interconnection Mediation Functions (From Issue 026, Logical M1)	**ISSUE** **052** **DATE SUBMITTED** **2/15/95** **LATEST REVISION** **6/15/95** **CURRENT AS OF** **6/28/95** **RESOLUTION DATE** **IAG REVIEW DATE** **IILC ADOPTION DATE**

1. ISSUE STATEMENT:

Some parties have recognized the need for mediation in an environment of logical interconnection with intelligent network capabilities or platforms, by multiple providers. An industry view is needed of what constitutes mediation and what are the appropriate criteria for determining where and/or how it should be accomplished.

2. SUGGESTED RESOLUTION OR OUTPUT(S):

- Identify and document typical functions that are candidates for inclusion in mediation
- Identify and document criteria for determining the placement of those functions

3. OTHER IMPACTS

Related proceedings at state and federal levels (e.g., CC 91-346) acknowledge the need to define mediation and determine the feasibility to develop and implement it. Output from this issue may be valuable input to such efforts. This Issue further enables the industry participants to shape the definition and determine the criteria for design and development of mediation platforms, operational support systems and procedures.

4. Targeted Resolution Date

May 1996 (presentation to IILC for Initial Closure)

5. ISSUE CO-CHAMPIONS:

	NON-LEC		LEC
Name:	George Stanek	Name:	Christine Maglott
Company:	AT&T	Company	Ameritech
Address:	900 Route 202/206N Rm 5A260A Bedminster NJ 07921	Address:	2000 W. Ameritech Dr. Rm 2C23D Hoffman Estates IL 60196
Phone:	(908) 234-7411	Phone:	(708) 248-4441
Fax:	(908) 234-3628	Fax:	(708) 248-3198

IILC ISSUE IDENTIFICATION FORM

ISSUE TITLE: Guidelines for Mediation Among Multiple Service and Network Providers (From Issue 026, Logical M2 and M3)

ISSUE	**053**
DATE SUBMITTED	**2/15/95**
LATEST REVISION	**5/31/95**
CURRENT AS OF	**6/7/95**
RESOLUTION DATE	
IAG REVIEW DATE	
IILC ADOPTION DATE	

1. ISSUE STATEMENT:

Various service and network providers want access to the logical unbundled functions of each other's networks. Any mediation function needs to provide to any requesting service or network provider required throughput, flexibility and management of the functions while maintaining the integrity and robustness of each network.

2. SUGGESTED RESOLUTION OR OUTPUT(S):

- Identify the characteristics of delivery, control and management, e.g., real time versus non-real time) needed to support mediation in a multiple provider environment.
- Identify the throughput, flexibility and control criteria that might be associated with each mediation function (from M1/052P).
- To ensure the ability to deliver services and management of mediation functions:
  Determine procedures
  Identify technical requirements
- Define suggested guidelines for coordinating mediated interactions among multiple providers.

3. OTHER IMPACTS

Output from Issue 052P, Definition and Criteria for Placement of Logical Interconnection Mediation Functions, may affect the work associated with this issue. Resolution of this issue may aid various network providers in determining the viability and suitability of deploying mediation functions, and any effect on existing network operations.

4. Targeted Resolution Date

5. ISSUE CO-CHAMPIONS:

Name:	George Stanek	Name:	Christine Maglott
Company:	AT&T	Company	Ameritech
Address:	900 Route 202/206N Rm 5A260A Bedminster NJ 07921	Address:	2000 W. Ameritech Dr. Rm 2C23D Hoffman Estates IL 60196
Phone:	(908) 234-7411	Phone:	(708) 248-4441
Fax:	(908) 234-3628	Fax:	(708) 248-3198

Appendix F - New Technology Reliability Template

The New Technology Reliability Template is a generic template that can serve as a reliability screen for assessing the reliability of new network technologies. It would be used primarily by a service provider but also is useful to a supplier of the particular technology to understand the important reliability criteria from the service provider's perspective. A person or organization in the service provider company who has primary responsibility for network reliability, planning for integration of a new technology, or having overall technical responsibility for a network would be potential users. These potential user's have the need to assure that all of the issues in the template have been adequately considered/addressed before the technology is integrated into the network. This template could be used as part of the service provider's process for the rapid and reliable evolution of their telecommunications networks.

New Technology Reliability Template

Criteria	Comments
1.0 Architecture	
Technology complies with industry/company standard architecture	
Specific architecture and its reliability features	
Architecture is robust enough to prevent FCC reportable outage	
Worst case percentage of key services restorable with this technology	
New operations support systems identified and meet architectural guidelines	
All changes to existing (legacy) systems have been identified	
Disaster recovery requirements identified and addressed	
Official network interfaces consistent with networking architectural plans and guidelines	
Industry “best practices” exist and have been considered	
List industry “best practices” to be followed	
Architecture is robust enough to meet customer reliability requirements	
Mechanism exists to evaluate end-to-end customer reliability for key services	
Customers have such a mechanism	
If so, what is observed reliability?	

New Technology Reliability Template

2.0 Technology Reliability	**Comments**
Technology reliability criteria defined	
Supplier documentation of reliability reviewed and meets criteria	
Operations support systems reliability criteria defined and met	
Is provision of key services using this technology as reliability of current technology?	
For each major failure mode of the technology providing key services, list:	
Describe the failure mode	
What is the failure mode impact in terms of equivalent blocked calls?	
What is the estimated duration of the failure mode?	
What is the estimated frequency of the failure mode?	
What actions(s) are required to recover from the failure mode?	
3.0 Installation	
Standard equipment configurations developed	
Installation methods and procedures developed	
Acceptance procedures documented	

New Technology Reliability Template

4.0 Service Provisioning	**Comments**
Service order documents have sufficient detail for field personnel and network element administration	
Service provisioning methods and procedures developed	
Feature interaction testing plan developed	
5.0 Monitoring	
Availability objectives exist	
Technology has self-diagnostic and auditing capabilities	
Technology can be remotely monitored and is consistent with existing monitoring system architecture	
Technology has full alarming capabilities	
Monitoring methods and procedures developed	
Required changes to monitoring systems completed	
Network element and OSS tested to ensure surveillance integrity	

New Technology Reliability Template

6.0 Maintenance/Repair	**Comments**
Technology operation consistent with current maintenance process flow and supporting systems	
Routine maintenance methods, procedures and time frames developed	
Software maintenance plans exist	
Non-intrusive software change/maintenance capabilities exist	
Appropriate test tools/equipment selected and available	
Remote testing and inventory capability exists	
OSS provides technology work force management reports	
Troubleshooting procedures exist including fault visibility, trouble verification and isolation, recovery/repair	
Is operator action or conformation required to recover from failures?	
Post-mortem analysis methods exist	
Process exists to feedback findings and recommendations to improve future reliability	

New Technology Reliability Template

7.0 Interoperability	**Comments**
Does this technology interoperate with other networks in provision of key services?	
How does the technology achieve reliable operation when interconnecting?	
How is reliable operation monitored and controlled?	
8.0 Training	
Required training courses available in time frames consistent with deployment schedule	
List required training	
9.0 Reliability Monitoring	
Process to collect outage data exists	
Process to do root cause analysis on outage data exists	
Process to develop best practices to improve new technology reliability exists	