SIGNALING NETWORK SYSTEMS COMMITTEE TECHNICAL PAPER

John W. Seazholtz
Bell Atlantic
1310 North Court House Road - 11th Floor
Arlington, Virginia 22201
(703) 974-3652

1.0 Executive Summary

Major services outages relating to Common Channel Signaling (CCS) networks occurred between June 10 and July 2, 1991. Bellcore, at the requests of its clients, investigated these outages and documented their findings in a Special Report available to the industry. The industry came together and cooperatively investigated the outages, determined the root cause and implemented corrective actions. The industry did not stop there. Numerous activities have taken place and are continuing. For example, the outages have placed more focus on potential improvements to the Signaling System 7 (SS7) protocol, especially with regard to its performance during severe congestion and its ability to recover. These activities are discussed later in the paper, in addition to the Federal Communications Commission's (FCC) leadership role in this matter.

The FCC established the Network Reliability Council (NRC) to address not only Signaling Network Systems (SNS), but other areas of potential vulnerability. The SNS Committee analyzed the outage data received from the industry and recommends steps in this paper to improve network reliability. In addition, a status of the steps taken since the outages of 1991 is briefly discussed. The data received from both the industry and the FCC reportable incidents produced a very positive finding -- no major mated pair STP (Signaling Transfer Point) failure events occurred in 1992. This indicates a successful industry focus on congestion control procedures.

The SNS Committee has been working for nearly a year to determine where the CCS Network vulnerabilities are and then recommend improvements. The team has concluded that the operation of the network has improved as a result of CCS. The network is running well and continuing to improve as carriers gain experience with this relatively new technology. This Technical Paper addresses steps to make it even better.

The major conclusions and recommendations are:

- Individual companies, including competitors, have recognized the utility of sharing "Best Practices" among each other. The teamwork demonstrated through the entire NRC effort clearly reflects that Telecommunications companies are working together to enhance network reliability.

- Some network element suppliers do varying amounts of software fault insertion testing. The SNS Committee recommends that this type of testing should be performed as a standard part of an SP (Signaling Point)/STP supplier's development process. Hardware failures should be tested and/or simulated to stress SS7 fault recovery software.

- SP/STP procedural errors can be mitigated by carriers enhancing their escalation procedures, retrofit procedures (e.g., pre-testing procedures in the laboratory, developing the quickest recovery actions from errors, etc.) and overall training program.

- SCP (Service Control Point)

B

owner/operators should ensure proper Uninterruptable Power Supply (UPS) functionality through periodic maintenance and testing.

- Signaling link diversity is generally followed, however, over time diversity may be lost due to normal churn. A compendium of "Best Practices" on Maintaining Link Diversity is presented in Section 6.

- The industry data request highlighted the need for a better Root Cause Analysis Process and improved Information Sharing.

- Signaling network enhancements (software or hardware) or alternative architectures should be considered, based on individual service providers cost versus benefit analysis.

- The work is not over - The SNS Committee recommends that the Exchange Carriers Standards Association (ECSA), through its' various sponsored committees and forums, as the appropriate industry organization to address future general network survivability issues and architectural proposals.

More specific recommendations are discussed later in the Technical Paper. These recommendations and suggested "Best Practices" are based on industry-wide data which, when taken as a whole, should result in continued good performance of the CCS network. As individual items, however, they should not be taken out of the center of the whole document.

The SNS Committee further recommends the FCC's outage data collection (i.e., 30,000 or more customers affected for more than 30 minutes) be used as a high level metric, supported by an analytical process, as an indicator of network reliability performance. The SNS Data Analysis Team utilized the FCC reported outages as one source of data with several recommendations being made as a result.

2.0 Background

2.1 Common Channel Signaling (CCS)

Common Channel Signaling (CCS) transmits the signaling information used to set up telephone calls. The CCS network, which is built on an international standard, consists of high speed data links and data switches called Signal Transfer Points (STPs). A central office switch (SP/SSP) is connected to the STPs, which route signaling information. The protocol used for network control signaling is Signaling System 7 (SS7) - see figure 2-1.

CCS Network Architecture

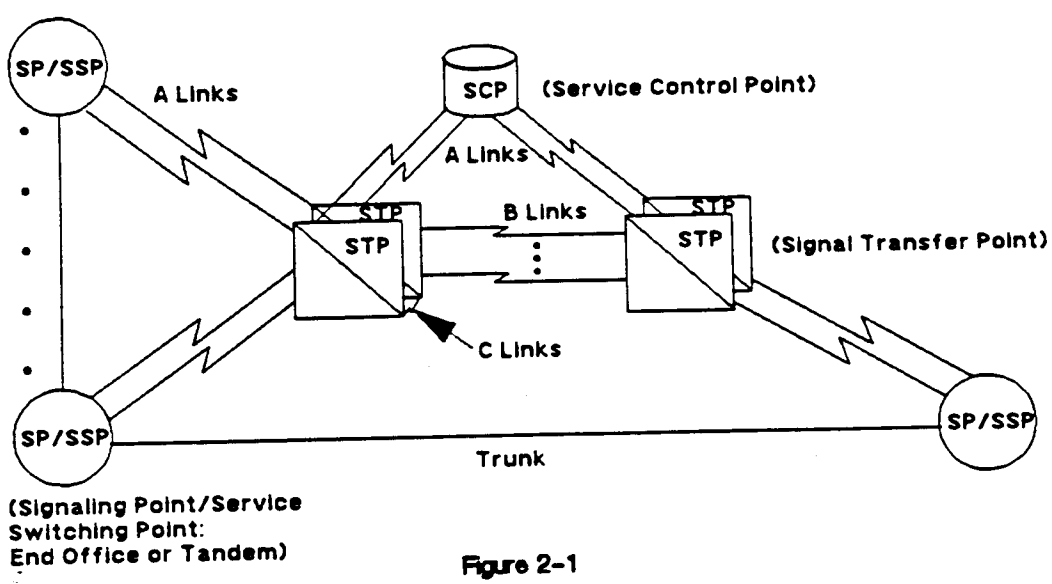


Figure 2-1

B

CCS is being deployed by local and interexchange carriers in the United States and around the world because it allows telephone networks to operate more efficiently. Previously, expensive, maintenance intensive signaling equipment was used on each trunk. The central office switch processors sent signaling information over the trunks themselves. CCS establishes a high speed data network over which the switching systems can communicate with each other directly to speed call setup times (with CCS, most calls set up in less than 1 second, compared to 3-5 seconds or longer before CCS implementation).

STPs are deployed in mated pairs. If one STP fails, the other takes over and service is not affected. STPs are placed in different locations with diverse data links. Each STP is engineered to only 40% capacity so that the STPs can share the load evenly and one can take the full load of its mate having a failure with 20% spare capacity.

The SS7 Protocol, designed by leading international experts, and standardized worldwide, embodies provisions for network recovery in the event of a component failure through redundancy, automatic re-routing and reconfiguration.

2.2 Network Reliability Council

The Network Reliability Council (NRC) was established by the Federal Communications Commission (FCC) to bring together leaders of the telecommunication industry and telecommunications experts from academic and consumer organizations to explore and recommend measures that would enhance network reliability. The NRC, which convened for the first time on February 27, 1992 is composed of Executive Officers of most of the major U.S. telephone companies, principal equipment suppliers, long-distance companies, consumer, corporate and Federal users' representatives and State regulatory agencies.

The NRC was chartered by the FCC in late 1991 in the aftermath of serious telephone network disruptions that affected roughly nine million subscribers on both the East and West Coasts. Following these outages, as well as others experienced by several interexchange carriers, the FCC instituted significant new investigatory and reporting measures, convened a meeting of international telecommunications regulators which met in Geneva, Switzerland, in October 1991, to review industry standards development procedures, and held a special all - U.S. industry meeting in September 1991 to stress the need for sound action. The Geneva meeting prompted new procedures for sharing of service-related information. Following the FCC's September meeting, the Internetwork Interoperability Test Plan (IITP) Ad Hoc Committee was established by the ECSA's Network Operations Forum (NOF). This committee has developed interoperability internetwork test scripts and successfully interconnected multiple carrier and supplier laboratories to cooperatively execute those test scripts. The SNS Committee recommends that this activity should be continued on an ongoing basis. This recommendations is discussed later in this paper.

The NRC quickly began their work by establishing a Steering Committee under the direction of Ross Ireland (Pacific Bell). The Network Reliability Steering Team (NO REST) reviewed the areas of potential vulnerability. The areas identified were Signaling Network Systems, Digital Cross-Connect Systems, Fiber Cable Cuts, Fire Prevention, E911, Power, and Switching. A NO REST "Champion" was assigned to each area. An issue statement was drafted for each area which contained: 1) Problem statement and issues to be addressed, 2) Areas of concern and problem quantification, 3) Description of proposed work and 4) Existing work efforts.

2.3 Signaling Network Systems Committee

The Signaling Network Systems (SNS) Committee's chairman is John Seazholtz (Bell Atlantic) and the NO REST champion is Gary Handler (Bellcore). Mr. Handler's issue statement (See Appendix 1 for Issue Statement) provided the SNS Committee with an excellent starting point. The team revisited the original statement on several occasions to assess progress. This proved to be a valuable tool that provided the group with a common understanding of the issues and allowed

B

the committee to begin working quickly. In addition to the issue statement, the SNS Committee developed the following charter at the first meeting:

- Vision: The Signaling Network Systems Committee will develop recommendations for improving the availability, reliability and survivability of the CCS network and the ability to react to CCS network events in order to minimize their impact.

- Process: The committee will be a catalyst for improving the quality performance of the CCS network. This team will utilize existing industry forums where possible and track its own recommendations to closure.

- Priorities:

1) Collect and analyze CCS outage data to determine:

- Root causes
- Greatest risks
- Recovery methods used

2) Based on the previous analysis, determine how to improve:

- Network Node Reliability
- The robustness of the CCS network architecture
- CCS network operations

3) Develop quantitative methods and parameters to measure the scope and impact of CCS network outages

2.4 Organization of Technical Paper

Section 1:	Overview and key messages
Section 2:	Background information on Common Channel Signaling, the Network Reliability Council and the Signaling Network Systems Committee
Section 3	SNS Committee members and the major focus teams established
Section 4	Data sources used by the SNS Data Analysis Team and the process used to collect outage information
Section 5	Results and recommendations of the outage data analysis
Section 6	Status of the steps taken by the industry as a result of the outages of 1991 and SNS Committee's key learnings and recommended best practices
Section 7	Metrics used to measure the effectiveness of the recommended solutions
Section 8	Public forums available, and the agreements reached, to continue supporting network reliability
Section 9	Conclusion including a summary of all recommendations
Section 10	Acknowledgements
Section 11	References
Section 12	Appendix

All recommendations and "Best Practices" are "*italicized*" throughout the paper and restated in Section 9.

3.0 Team Members

The SNS Committee Members are:

Team Leader: John Seazholtz (Bell Atlantic)
Champion: Gary Handler (Bellcore)

AT&T - NS	Al Loots
AT&T - NSD	Bob Hirsch
Bell Atlantic	Harold Daugherty
Bellcore	Rich Baseil
	Clint Hamilton
Bellcore (SCP)	Kelly Gaylord

B

BellSouth	Charlene Echols
Chairman, Committee T1	Arthur Reilly
DSC	John Bischoff
	Peter Jackson
Ericsson	Angel Ruiz
GTE	Dave Fiasco
MCI	Jack Walters
NCS	Ken Boheim
	Gene Phillip
NOF	Rick Harrison
NTI - BNR	Bob Kenedi
	Peter Budihardjo
Pacific Telesis	Dick Bostdorff
U S WEST	Mike Carlson

The SNS Committee met about once a month beginning June 30, 1992. The team established several sub-committees to provide more detailed analysis of several issues. The results of their work is presented later in this paper. The major sub-committees and their members are:

Data Analysis Team

Clint Hamilton (Bellcore)
Harold Daugherty (Bell Atlantic)
Al Loots (AT&T - NS)
Peter Budihardjo (NTI - BNR)
Larry Graham representing John Bischoff (DSC)
Kelly Gaylord (Bellcore - SCP)
Luis Reto representing Jack Walters (MCI)
Mark Enzmann representing Charlene Echols (BellSouth)
Dana Shillingburg (Bell Atlantic)
Eric Tollar (Bellcore)
Chao-Ming Liu (Bellcore)

Best Practices - Maintaining Diversity

Mike Carlson (U S WEST)
Charlene Echols (BellSouth)
Harold Daugherty (Bell Atlantic)

CCS Failure Root Cause Analysis Process

Rich Baseil (Bellcore)
Bob Hirsch (AT&T - NSD)
Charlene Echols (BellSouth)
Peter Jackson (DSC)
Jack Walters (MCI)

4.0 SNS Team Data Collection Process

In order to quantify signaling network vulnerabilities, identify major reliability issues and propose problem solutions, the SNS team adopted the Total Quality Process (TQP) outlined in the NRC SNS issue statement. This section describes the data collection process the SNS team used as part of the TQP. During this process, the team compiled and analyzed three separate signaling network reliability databases to develop its recommendations 1) an immediately available Bellcore database, 2) an SNS Industry collected database and 3) an FCC Docket 91-273 signaling related outage database. Each of these databases is described in the sections below.

4.1 Immediately Available Data

To start the team's analysis, and to help set its direction, the team began by searching for immediately available signaling network systems reliability data to analyze. The following list summarizes the potential sources of data that were immediately available to the team:

- CCITT International Reports
- Network Operations Forum (NOF) SS7 Workshop Reports
- Government Accounting Office (GAO) Requested Outage Reports
- Federal Communications Commission (FCC) Docket 87-313 Service Quality Reports
- FCC Docket 91-273 Major Outage Reports
- Bellcore Service Failure Analysis Report (SFAR) Database

In reviewing these sources, the team determined that the Bellcore database was the only one at the time containing a complete (a large number of reports) and comprehensive set (relatively detailed

B

reports) of reliability information specific to signaling network systems. The team also recognized that some of the other sources were just beginning to collect data. It was agreed that later in the team's data analysis process other reports related to signaling network systems, in particular FCC Docket 91-273 Major Outage Reports, should be analyzed.

The team, therefore, requested Bellcore to provide an analysis based on the data it had been collecting from its Bell Operating Company clients during 1991 and 1992. The detailed technical results of this analysis are contained in Section 5.

However, the team did recognize that some shortcomings existed with the Bellcore database from a total industry perspective. These include:

- not all Local Exchange Companies (LECs) had contributed to the database,
- there was no Service Control Point (SCP) data included,
- no Interexchange Carriers (IXCs) had contributed to the database,
- there was a need to supplement the carrier outage cause results with the supplier's perspective which had not always been included.

To conduct a thorough analysis, addressing the root causes of all signaling outages from a total industry perspective, the team determined that it must collect additional industry signaling network reliability data.

4.2 Industry Data

The team developed an industry data request to supplement the existing data and address the shortcomings identified above. First, to assure complete coverage of data sources, the data request was directed to the following two segments of the industry:

- Carriers - including LECs, Independents, IXCs and other service providers. It was felt that the carriers would have the best perspective on descriptions of events, triggering events, recovery actions and root causes of outages related to network architectures, implementations and operations.
- Suppliers - manufactures of signaling network systems equipment including STPs, SCPs, SP/SSPs. It was felt that the equipment suppliers would have the best perspective on the root causes of equipment related outages, including hardware and software problems.

To help assure consistency across companies in reporting the committee developed the following criteria as guidelines for answering the data request:

- Types of Outages/Failures to be Reported

  - Signaling Point (SP)/Service Switching Point (SSP) CCS Outages: Total loss of call processing capabilities due to CCS-unique failure modes of a CCS-equipped end office/access tandem.

  - CCS Node Isolations: CCS network nodes (SP/SSP, STP, SCP) isolation from the CCS network caused by facility failure (e.g., cable cut, digital cross-connect failure, etc.) or combination of node and link failures.

  - STP Total System Failures: Total loss of CCS message processing capabilities of an STP; Note that routine maintenance events (scheduled events) of STPs need not be reported unless they were service affecting.

  - Service Control Point (SCP) Total System Failures: Total loss of CCS message-inquiry capabilities of an SCP.

  - Network Outages: Any combination of node and link outage/failure events that result in loss of service(s) to customers in a number of SP/SSPs, e.g., mated pair STP failure, mated pair SCP failure, loss of Line

B

Information Database (LIDB) or 800 Service application in an SCP.

- Length of Outage Failure - Outages/failures lasting two minutes or more (the Bellcore current reporting/investigation threshold).

- Reporting Time Period - Outages/failures occurring from January 1, 1991 to September 30, 1992, if data is available.

- Data Collection Vehicle - The team identified the Bellcore Service Failure Analysis Report (SFAR)[1] Form as an Industry "Best Practice" which could be used as the data collection vehicle. A few modifications were made resulting in the form shown in Appendix 2 which was used for data collection from the carriers. For suppliers, a format was developed with more emphasis on root cause identification and recommendation and plans for correction and preventive actions (See Appendix 3). If similar information was available from any data provider, but in a different format, those reports were accepted as long as the content was the same.

The data collection questionnaires were then assembled including, vehicle, instructions for completion and a network element population request form (See Appendix 4). The population data would be used for statistical normalization of reliability metrics such as system downtime. The request was made using the Network Reliability Steering Team (NO REST), Industry Single Points of Data Collection (SPOCs) process with independent Bellcore data aggregation. The data collection requests were then distributed to NRC participating LECs, IXCs and suppliers of STPs, SP/SSPs and SCPs using the NO REST process. The data analyses which were conducted and the corresponding results are contained in Section 5.

4.3 FCC Major Outage Reports

In addition to the Industry request, the team also collected and analyzed the FCC Docket 91-273 major outage reports related to signaling network systems that occurred during the time period April 6, 1992 to December 31, 1992. Results of the analyses performed are also contained in Section 5.

5.0 Signaling Network Systems Data Analysis Results

This section presents the data analysis results on CCS network reliability performance. Analyses were conducted independently on each of the following three signaling network reliability databases described in the previous section:

1. Immediately Available Bellcore Data

2. SNS Industry Collected Data

3. FCC Docket 91-273 Signaling Related Outage Events

Analysis of each database has produced separate recommendations which are contained in the applicable sections.

5.1 Analysis of Immediately Available Bellcore Data

This section presents the data analysis results on CCS network reliability performance based on CCS network failure information collected by Bellcore from November 1, 1990 to June 30, 1992. This data was obtained from Service Failure Analysis Reports (SFARs) and other similar outage reports, provided to Bellcore by a number of Bellcore's Bell Operating Company clients.

Data analyses contained in the following sections will use Pareto Charts[2] as the primary data analysis technique. Pareto charts show the relative contributors to a reliability parameter of interest. For example, one might show the causes of STP downtime. The charts use a bar to reflect both the value of the contribution shown on the left axis, and the percent contribution, shown on the right axis. A series of connected dots above each bar is also shown which represents the cumulative value and percentage for all contributions.

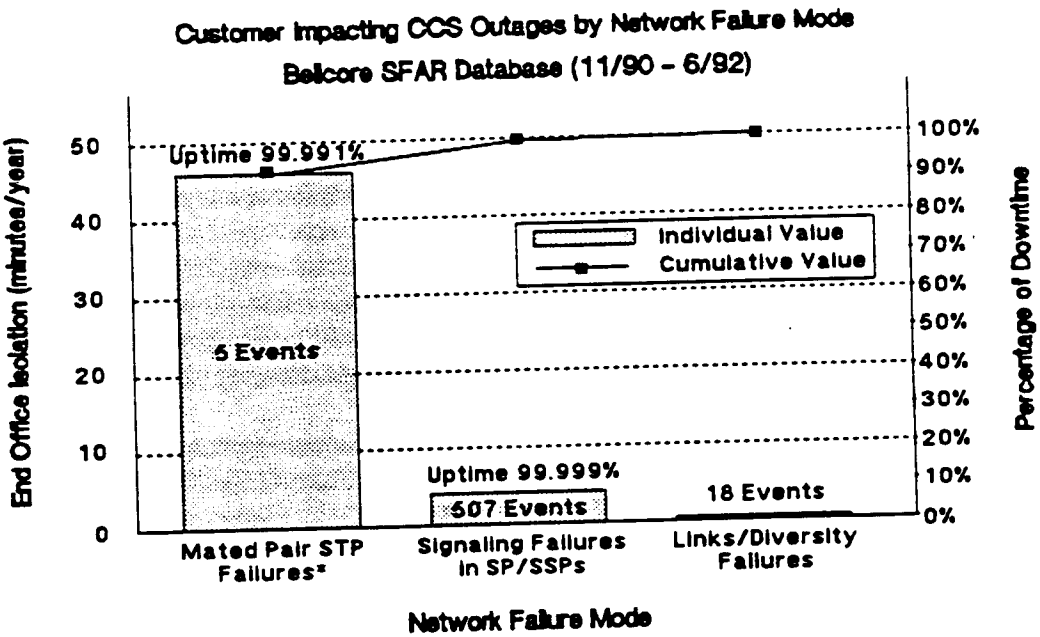
B

5.1.1 Network Failure Modes of CCS Service Affecting Outages

This analysis was first conducted to determine the failure modes in the CCS network (STPs, links, etc.) which contribute most to customer service disruptions. Service affecting CCS network failures generally result in the inability of switching systems (SPs/SSPs) to process customer calls which require access to the signaling network. This is typically called a CCS end office isolation. The analysis uses the downtime metric *end office-minutes/year* as a measure of CCS end office isolation. Three CCS network failure modes were observed in the data to cause end office isolations. These included;

1. mated pair STP failures,
2. end office switch (SP/SSP) CCS unique failures, and
3. link/diversity related failures.

Figure 5-1 shows the distribution of customer impacting CCS outages for these three failure modes using the end office-minutes/year of downtime metric. It indicates that over this time period, the mated pair STP failure was the largest contributor to CCS end office isolation. Note that most of this downtime is related to the mated pair STP failures of the June-July 1991, major CCS network failure events[3]. The above result indicates a need to review STP reliability performance and the causes of STP failures. In addition, the signaling failures in SP/SSP and links/diversity failures are also significant contributors. They are analyzed as part of the industry data analysis in Section 5.2 where their contributions are not askew.



* Due to the 1991 major CCS network outages [1]

Figure 5-1

B

5.1.2 STP Reliability and Outage Causes

Although mated pair STP failures have been observed, failures of single STPs typically do not affect service because of the independent nature of most failures and the deployment of STPs in mated pair configurations. Therefore, to get a complete picture of STP reliability, and the root causes of failures, single STP downtime is a useful metric here. Figure 5-2 shows the reported single STP downtime compared to the 3 minute per year Bellcore objective.[4] This data includes contributions from reported single STP failures as well as the STP failures which were associated with the mated pair failures. It shows that during the data collection period, the average STP annual downtime (approximately 43 minutes/year) is significantly higher than the objective. Even when the mated pair failures are removed, STPs are not meeting the downtime objective.

In analyzing the causes of total STP failures we found that they are distributed among six different types of failure modes. The distribution of the downtime in each category is shown in Figure 5-3. This figure indicates that software-related failures were the single largest contributor, by far, to all of the STP downtime.

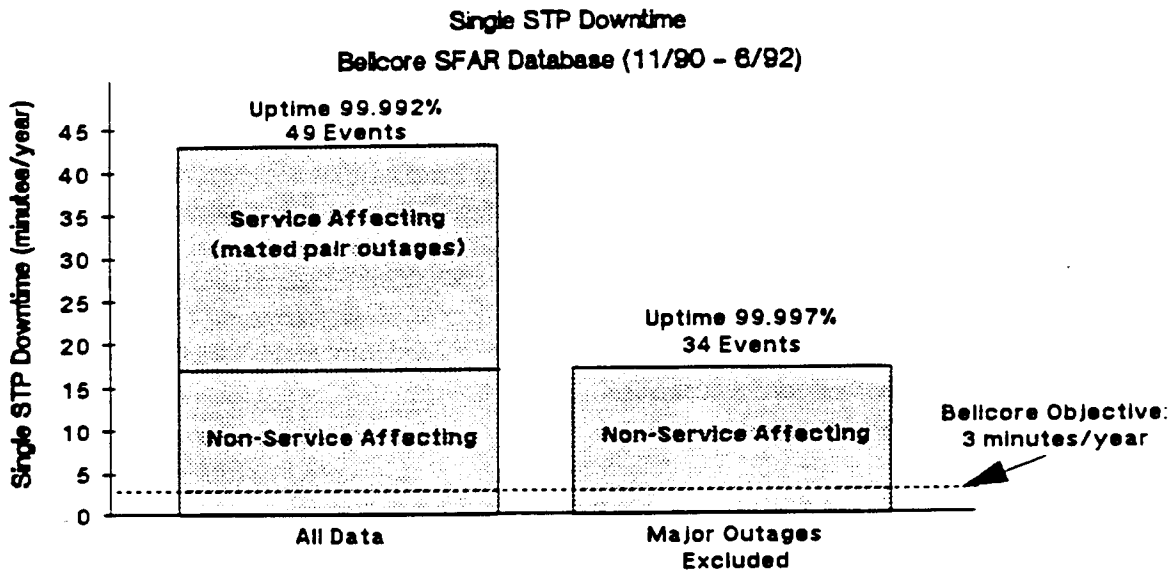


Figure 5-2

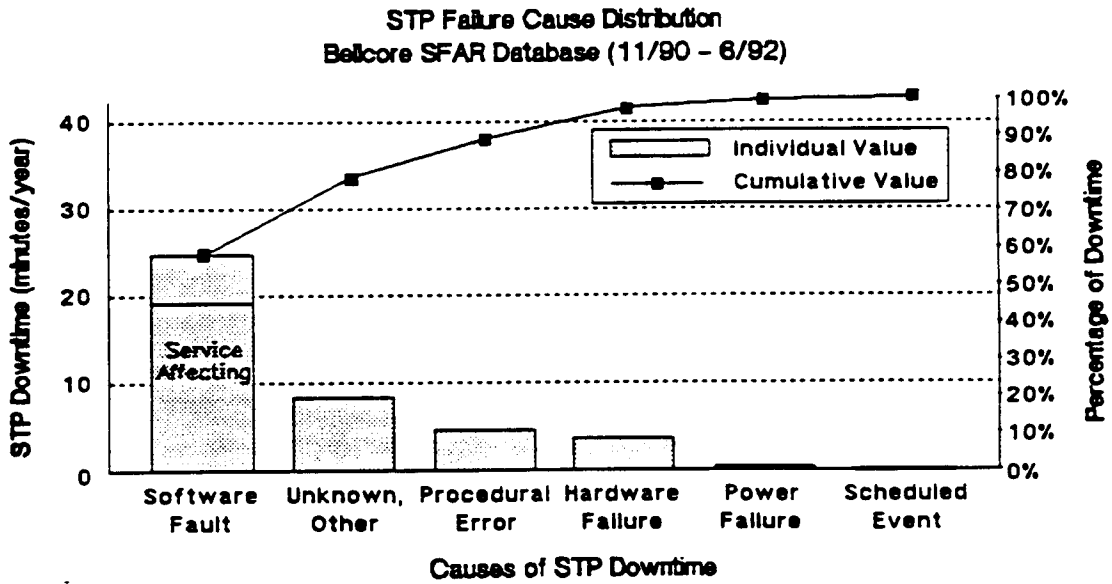


Figure 5-3

B

Looking into the specific incidents that contributed to the software related downtime we find in Figure 5-4, that over 75% of all the software downtime was related to problems with congestion control. Again, most of this downtime is related to the mated pair STP failures during the June-July, 1991, major CCS failure events. The remaining downtime was spread across a number of other cause categories with no obvious major contributor.

5.1.3 Recommendations

The 1991 major CCS network outages related to congestion control are the dominant root cause of observed CCS network service affecting downtime in this database. As a result of these events, a number of recommendations were made and many industry reliability improvement activities initiated. The industry has taken many specific actions to address problems directly related to congestion control. Work has also occurred on developing protocol improvements, network architecture enhancements and improved operations procedures, including better information sharing. Detailed discussion on the accomplishments and status of this industry work is presented in Section 6.

5.2 Analysis of Industry Data

5.2.1 SNS Data Team & Analysis Process

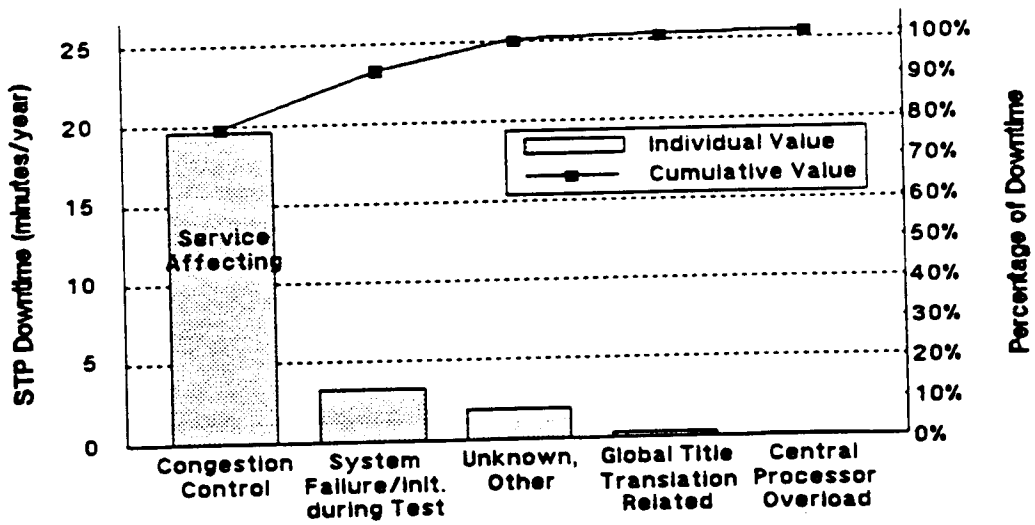
The response to the SNS team's industry data request was an excellent example of industry cooperation to report signaling network reliability problems. A total of over 20 industry respondents, carriers and suppliers, provided their available data in response to the request. To analyze this industry data an SNS Data Analysis Team was formed.

In Section 5.1 a summary of CCS network reliability findings was provided based on Bellcore data available prior to the industry data request. As such, the Data Team's analysis in the following sections concentrate primarily on presenting industry analysis findings which were not apparent in the Bellcore analysis. In general, the emphasis of the Data Team's results concern the reliability of the CCS network during 1992. This is because:

- The 1992 data in the industry database was of higher quality than 1991 in terms of completeness of descriptions, causes, etc,

STP Failures due to Software Fault Subcategories

Bellcore SFAR Database (11/90 - 6/92)



Software Causes of STP Total System Failures

Figure 5-4

B

- As a result of the first bullet, the team felt it was most important to concentrate on the most recent reliability performance of the signaling network, and

- It was recognized that some under-reporting existed in the 1991 industry data. An improving trend in availability of data was observed in 1992.

The following are the results of the Data Team's analysis.

5.2.2 Network Failure Modes of CCS Service Affecting Outages

As was done in Section 5.1.1, Figure 5-5 shows the customer impacting CCS outages by network failure mode for 1992. The data indicates an average end office isolation downtime of approximately 6.9 minutes/year because of CCS unique outages. Unlike 1991, in which the major CCS network outages were a result of mated pair STP failures, in 1992 the only sources of CCS unique service affecting outages were:

1. signaling failures in end office SP/SSPs, and

2. links/diversity related failures.

The data received from both the industry and the FCC reportable incidents produced a very positive finding -- no major mated pair STP failure events occurred in 1992. This indicates a successful industry focus on congestion control procedures.

The SP/SSPs events accounted for 5.7 minutes/year (83% of the total isolation downtime), and the link events accounted for the remaining 1.2 minutes/year (17% of the total isolation downtime). If the mated pair STP failures of 1991 are removed from consideration in that year, there is not a significant difference in the breakdown of CCS unique service affecting outages between 1991 and 1992. The above downtimes can be compared to the 3 minutes/year loss of CCS capability in a switch and the 2 minutes/year network access downtime objective, respectively.

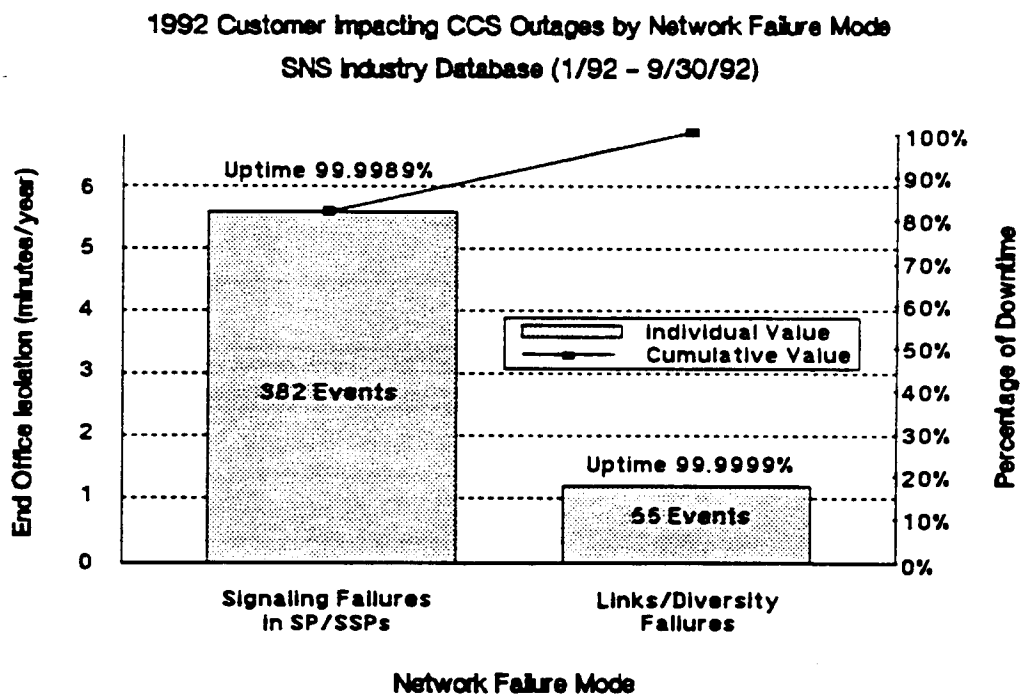


Figure 5-5

B

5.2.3 Link Related Failure Analysis and Causes

Link related failures accounted for 1.2 minutes/year of the 1992 end office isolation or about 17% of the total end office isolation downtime. This downtime value is well within the expected network access segment downtime objective of 2 minutes/year. [5][6][7]

Because of the nature of the information provided in the industry data, determination of the failing component had to be made by interpreting the descriptive text of the various outage reports. Figure 5-6 provides the breakdown of the link related end office downtime by the various link components which causes the service disruption.

The major component, indicated on the chart as just links, accounted for almost 40% of the downtime. These failures were not diversity related. They appear to be independent failures on each of the two A-links. The failures were related to a variety of different causes including link hardware failures, remote facility failures, procedural errors, scheduled events and unknown causes.

However, almost 30% of the downtime was a result of a single failure resulting in isolation of the SP/SSP because of an A-link diversity violation. In addition, a few percent of the incidents indicated that Digital Cross-Connect Systems (DCSs) and timing systems were the cause. These, in all likelihood, are also diversity violations. Furthermore, the bar labeled Facilities corresponds to an additional 28% of all link downtime in which the descriptive text was insufficient to determine the circumstances or what particular component(s) actually failed. Most likely, a substantial portion of these incidents are also related to diversity violations. In the worst case, about 60% of the link related downtime could be diversity related.

5.2.3.1 Link Recommendations

It is clear from the data that lack of link diversity is the primary, identifiable contributor to link related CCS network service disruptions. The data also clearly indicates that all components of links such as facilities, DCSs, timing systems, etc. must be considered when designing and maintaining diversity to assure link failure mode independence. This service affecting failure mode is an addressable

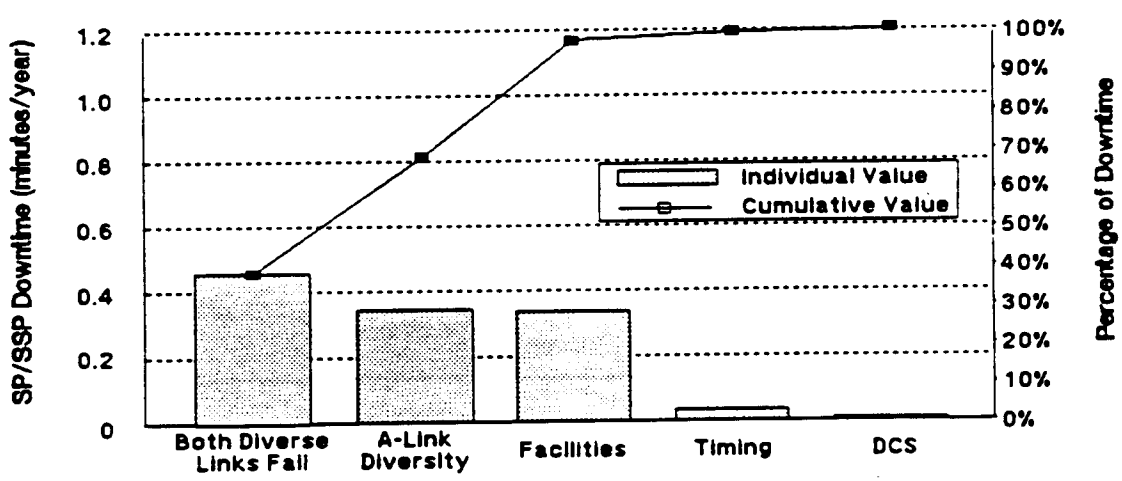


Figure 5-6

B

problem, one which need not be there. Section 6 contains the SNS team's more specific recommendations on diversity, including its compilation of industry "Best Practices".

5.2.4 SP/SSP Outage Analysis

As indicated, about 80% of the end office isolation downtime in 1992, 5.7 minutes/year, was the result of CCS unique SP/SSP outages. These are failures in switching systems, typically signaling peripherals and signaling related software, which result in the inability of the switch to access the CCS network. The switch, however, continued to process other call types such as intra-switch calls.

5.2.4.1 SP/SSP Downtime and Trend

Figure 5-7 shows the downtime associated with SP/SSP outages for each of the seven quarters contained in the industry data. A 6 month rolling average is also shown and is used to smooth the fluctuations. Other than the results for the first quarter of 1991, there is a significant increasing trend in the downtime associated with SP/SSPs. The main effect associated with this increase in downtime is a general increase in the event reporting rate for SP/SSPs throughout the period of this study. There is no evidence that the increase is a result of an increased frequency of any particular cause of the outage, nor is there any evidence that any particular event type is increasing in duration.

While the data is insufficient to determine the actual cause of this increase, it is suspected that this is simply an improved reporting phenomenon. Increased awareness on the part of the participating companies, and an increased capability to comply with the data request could certainly account for the increase. The 3Q92 rolling average downtime value of 6.2 minutes/year is in excess of the 3 minutes/year Bellcore LSSGR objective for loss of CCS capability in a switch.[8]

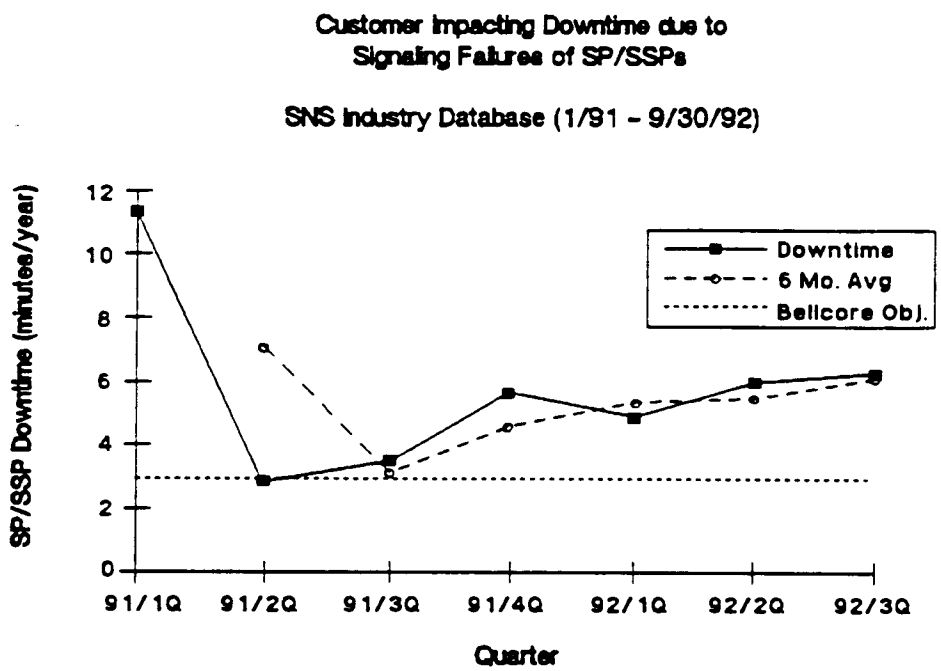


Figure 5-7

B

5.2.4.2 SP/SSP Causes of Downtime

Figure 5-8 provides the SP/SSP downtime broken down by the causes of the outages. Of the 5.7 minutes/year downtime associated with SP/SSPs, a total of 2.24 minutes/year (39% of the total downtime) was caused by procedural errors, with by far the largest component being Telco procedural errors (1.71 minutes/year, or 30% of all downtime). The next largest cause of downtime was software faults, which contributed 1.63 minutes/year downtime (29% of the total downtime). Of the remaining causes, none accounted for more than 9% of the total downtime. The relative frequency and duration of events by cause has not changed during the study period. The results indicated that further analysis of the underlying causes associated with procedural errors and software faults was warranted.

5.2.4.3 Analysis of Procedural Errors

On further investigation of the data on SP/SSP failures which listed procedural errors as the cause, a major identifiable root cause of the procedural errors was the misidentification of the "unit" which required repair in those instances in which there was a redundant active unit to the failed component. In these cases, the maintenance person would start work on the redundant active unit, resulting in the SP/SSP outage. These outages, which varied from misidentification of link interfaces and link processors to misidentification of frames or power supplies, accounted for 15% of all procedural errors, or a total of 0.33 minutes/year of SP/SSP downtime. No other single root cause accounted for any significant amount of the procedural errors.

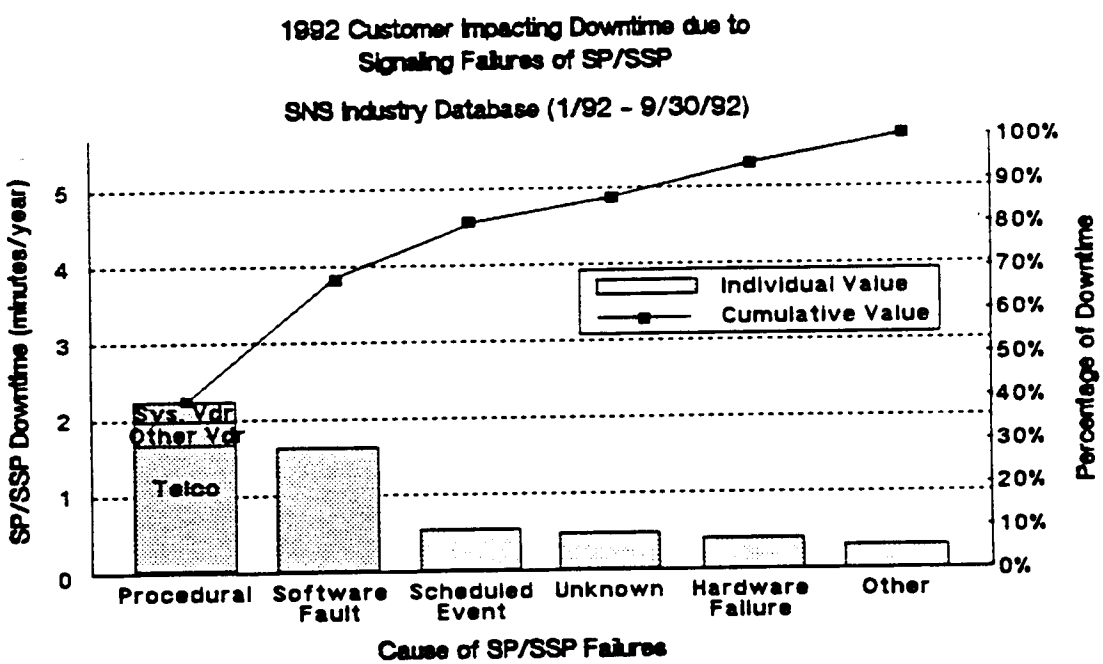


Figure 5-8

B

Figure 5-9 provides a pie chart which indicates the contribution of identification errors to procedural errors.

For the procedural errors, another area of investigation was the time of day the work activity was being performed, and if the work was scheduled maintenance or was a response to a failure event. Figure 5-10 provides a pie chart of the procedural error downtimes broken down by work activity.

Based on the descriptive text provided in the outage data, it was determined that 70% of the downtime associated with procedural errors occurred during scheduled maintenance activities. Of the remaining 30% of the downtime, 16% was identified as a response to some outage, while the remaining 14% could not be determined based upon the data provided.

Furthermore, of the 70% of downtime associated with procedural errors on scheduled activities, 23% occurred during the business hours (where we have defined the business hours to be from 6 a.m. to 6 p.m., Monday through Friday). About 1/3 of this downtime is coming from events that start off-hours but "spillover" into the business day.

As such procedural errors occurring during scheduled activities during business hours account for 0.52 minutes/year of the SP/SSP downtime. While certain scheduled activity during business hours is necessary, these results indicated that a large proportion of business downtime may be avoided by a closer examination of the scheduling of CCS related switch work activities.

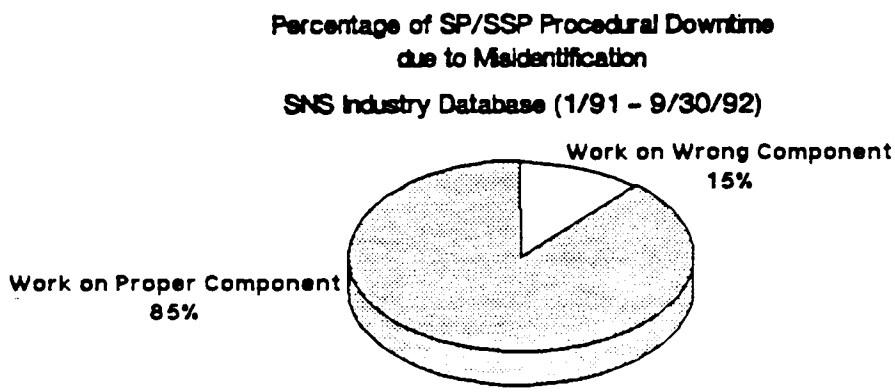


Figure 5-9

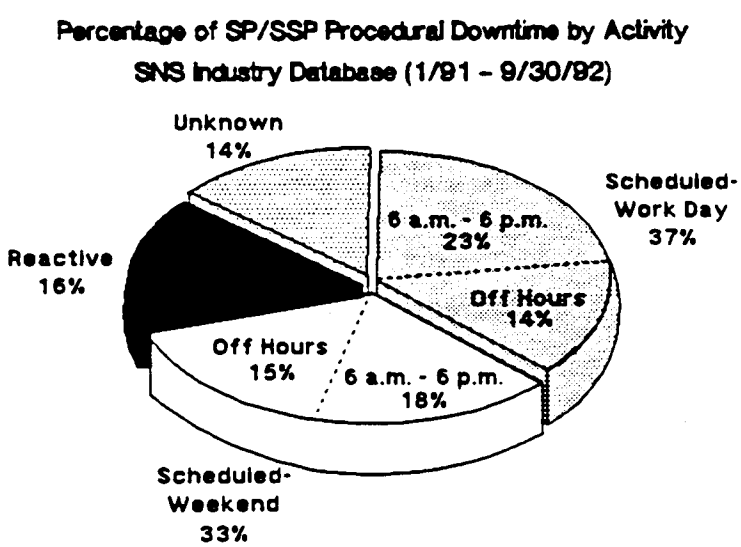


Figure 5-10

B

5.2.4.4 Analysis of Software Caused Outages

In the further investigation of the SP/SSP downtime contribution associated with software faults, the descriptive text of the data for all software outages were examined. The software outages were then classified based on the general software task that was being performed which resulted in the outage. Figure 5-11 provides a breakdown of the SP/SSP software fault downtime by these tasks. Because of the nature of the descriptive fields in the data, it was not possible to classify outages accounting for 0.84 minutes/year downtime (49% of the total SP/SSP downtime associated with software faults). Of the remaining 0.87 minutes/year downtime, 0.58 minutes/year of the faults occurred during recovery actions as a result of some hardware failure. In these events, the software failed to recover correctly from an initial hardware failure trigger. Of the remaining root causes, no other single root cause accounted for more than 4% of the total SP/SSP downtime associated with software faults. It appears that an increased emphasis is required on software performance of recovery tasks from hardware outages.

Further corroborating evidence of the vulnerability of SP/SSPs to software faults during recovery tasks is provided in Section 5.2.5, in which the FCC reportable events are analyzed. Although the number of outages associated with software faults are not large in the FCC reportable events, the level of detail available in the information allowed a more accurate root cause analysis than was possible with this data.

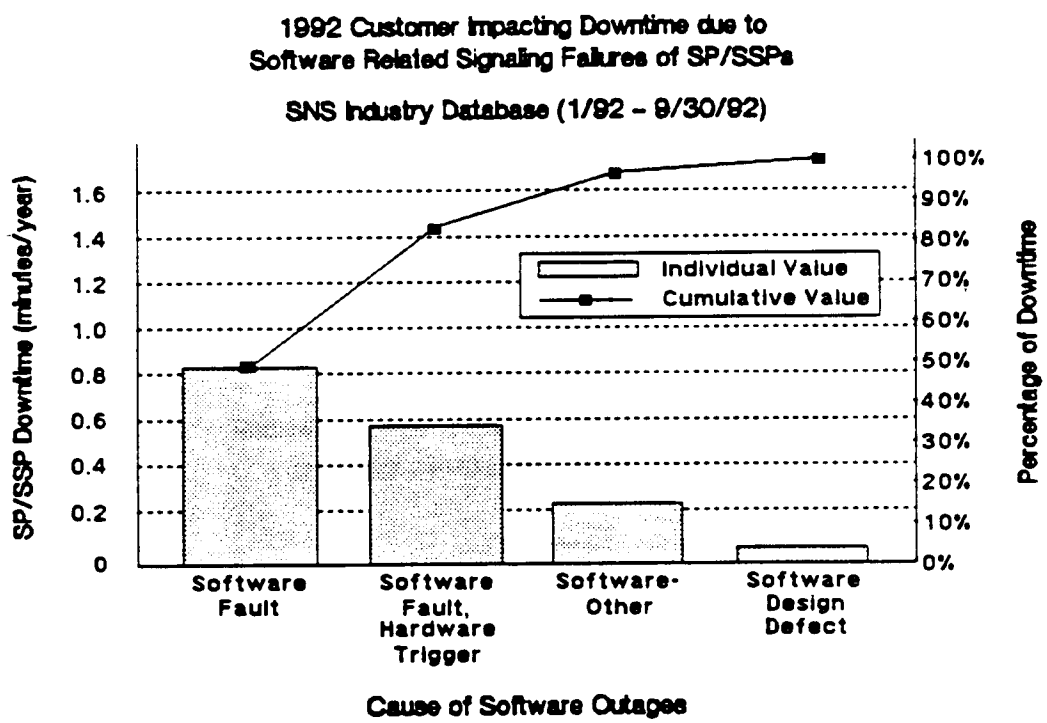


Figure 5-11

B

5.2.4.5 SP/SSP Recommendations

The following are the team's recommendations:

Procedural Errors:

- *Inadvertent Maintenance of Redundant Active Units - To minimize human errors related to misidentification of active CCS units as failed units requiring repair, network service providers should conduct an "Awareness Training Program" for all maintenance persons who work on SP/SSP CCS equipment including the importance of end to end communications when maintenance is being performed. The training must emphasize the functionality, identification of active and alternate/redundant units and the network impact of failure of redundant equipment in link processors, link interfaces, link peripheral power suppliers, and other link related components.*

  In addition, architectural or design alternatives are possible and should be evaluated, initially, for large end offices (e.g., 30,000 lines or more), which will make links more robust to these types of errors during link maintenance (see T1S1.3 Architecture Evaluations). Some additional alternatives currently in use in the industry and presented here as "Best Practices" are:

  - Two or more links per link set. With this design three or more simultaneous failures/errors must occur at the same time to cause a service interruption.

  - While not specifically switch related, the use of dedicated DS1 facilities for links to reduce the frequency of procedural activity on links.

  - Use of quad A-links, i.e., four diverse A-links to an SP

- *Scheduled Work Activities: While certain scheduled activity during business hours is necessary, these results indicate that a large proportion of CCS impacting business hour downtime may be avoided by carrier company scheduling of SP/SSP CCS related work activities during off hours. At a minimum, high risk, potentially service affecting maintenance and growth procedures should be scheduled during weekend and off-hours. Scheduling should also take into account the fact that if the procedure fails, and a significantly longer than expected outage occurs, it should not run into the business day. It is recommended that the methods, procedures and scheduling of these work activities be reviewed by a 2nd tier maintenance organization such as an Electronic Systems Assistance Center (ESAC). The SNS Committee further recommends that activities that may affect other network service providers must be coordinated, which includes both intra- and inter-carrier networks (See NOF Reference Document Section III, Installation and Maintenance - SS7 [sub-section 1.6, 2B, 2C, 3J]).*

Software:

- *CCS Related Recovery Software: It appears that increased emphasis is required by SP/SSP Manufacturers on improving the software which performs recovery tasks for CCS related functions that have been initiated by hardware failures. This result is consistent with the findings of the Switching Focus Team. The following specific recommendations are made which are consistent with those of the Switching Focus Team.*

  1. Software and hardware fault insertion testing (including simulating network faults such as massive link failures) should be performed as a standard part of a supplier's development process. Hardware failures and data errors should be tested and/or simulated to stress SS7 fault recovery software.

B

2. Fault recovery actions that result in a loss of SS7 signaling functionality need to be reviewed periodically by SP/SSP manufacturers to assure that the least SS7 signaling impacting strategies are being used for classes of failures implicated during root cause analyses. For example, if a set of failure conditions resulted in a system initialization, that condition should be reviewed to determine if a system initialization of that level is appropriate.

3. Initialization durations should be optimized to minimize service impact. Given that a particular failure needs an initialization to recover, manufacturers can minimize the service impact by optimizing the design and execution of the initialization. Again, data from root cause analyses should be used to determine areas for investigation.

5.2.5 STP Failure Analysis

As previously mentioned, no service affecting outages associated with STPs were reported in the industry data for 1992 which is a very positive finding. However, because of the crucial nature of STPs to the signaling network, the Data Team analyzed the single STP failures that were reported.

5.2.5.1 STP Downtime and Trend

Figure 5-12 provides the single STP downtimes observed for the industry data. The 43 minutes/year downtime obtained from the Bellcore SFAR Database, discussed previously in Section 5.1.2, is shown as a single triangle in the Figure as a reference. In 1992, the downtime for each of the quarters is provided as well as a 6 month rolling average. The average single STP downtime for 1992 is 25.5 minutes/year which is a significant improvement over that observed in the Bellcore data. However, this is still well in excess of the 3 minutes/year Bellcore downtime objective.[9]

In addition, after excluding the 1991 mated pair STP outages from the Bellcore data, the STP failure data was examined for any trends during the study period. There was no evidence of any overall trend, when looking at the failure rate, duration, or downtime.

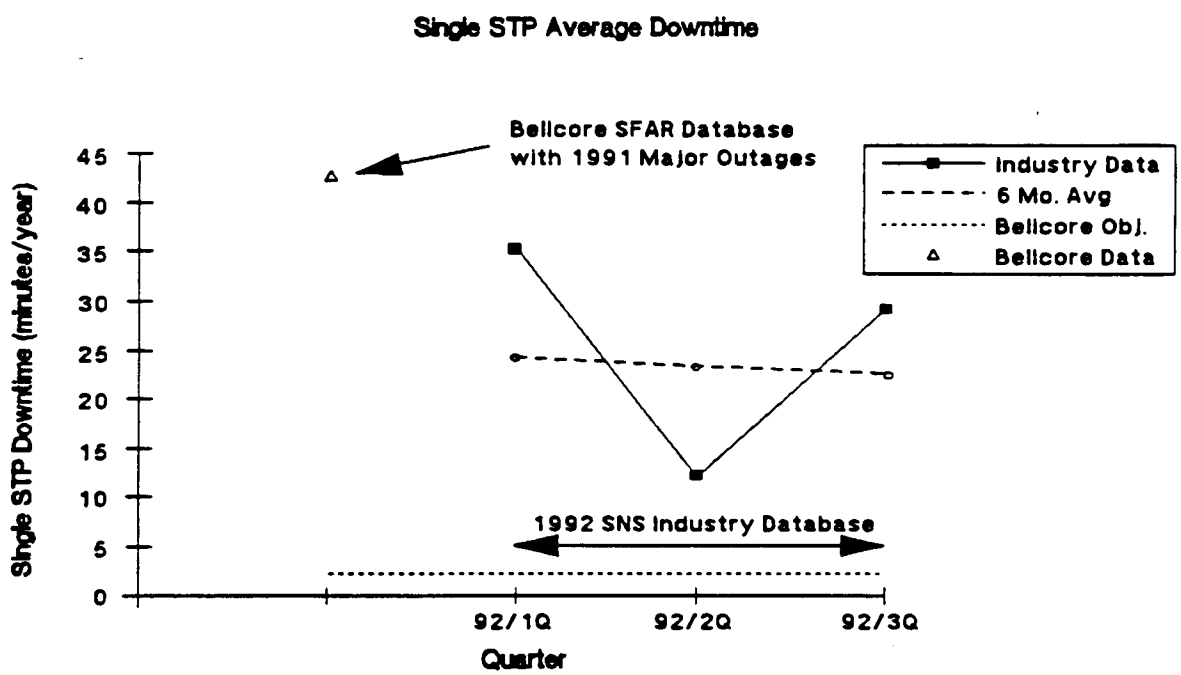


Figure 5-12

B

5.2.5.2 STP Failure Causes

Figure 5-13 provides the single STP downtime for 1992, broken down by failure cause. For single STPs 12.6 minutes/year of downtime is associated with software faults (48% of the total STP downtime). Of the 12.6 minutes/year, it was determined from the descriptive text that at least 3.8 minutes/year of the STP downtime is again associated with software faults uncovered during recovery actions from hardware failures. This finding is similar to the one observed in the SP/SSP analysis.

Procedural errors accounted for another 7.2 minutes/year of STP downtime (29% of the total STP downtime). No other single cause accounted for more than 7% of the total STP downtime. Unfortunately, the descriptive text in the data did not allow further root cause analysis of the industry data.

5.2.5.3 Procedural Errors and STP Growth

Upon examination of the STP failures separated by cause, there is a significant increase by quarter in the downtime associated with the procedural error related events. This increase is due entirely to a corresponding significant increase in the failure durations associated with procedural errors. There is no evidence of any increase in the rate of occurrence of procedural errors. It is suspected that this increase in duration of procedural errors may be related to the rapid growth of STPs and links in the network. It is further suspected that such growth required some carriers to use maintenance forces with lower levels of CCS expertise to handle the maintenance for a part of the existing embedded base of STPs. It is expected that as the growth of STPs stabilizes, the failure duration of procedural errors will eventually decrease as training increases and expertise grows.

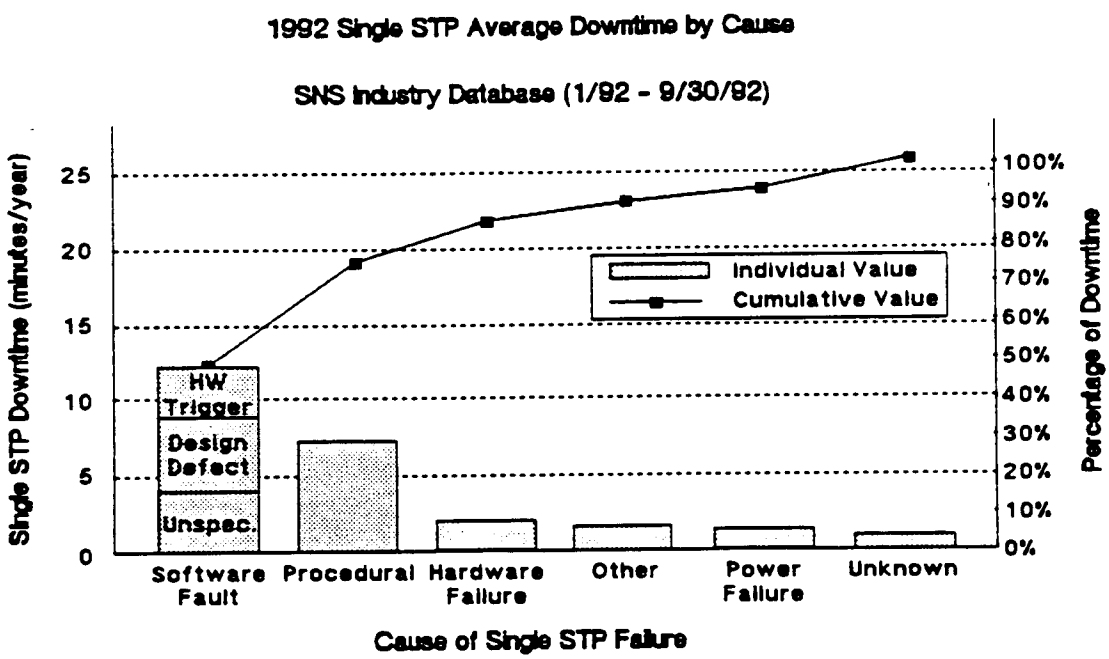


Figure 5-13

B

Figure 5-14 provides the average STP downtime due to procedural errors and the number of STPs deployed by quarter in the study.

5.2.5.4 STP Recommendations

The following are the team's recommendations in this area:

Recovery Software

- *A significant amount of STP downtime is associated with software faults uncovered during recovery actions from hardware failures. This is a similar finding related to recovery software for signaling functions as that observed in the SP/SSP analysis. It appears that increased emphasis is required by STP manufacturers on improving the software which performs recovery tasks that have been initiated by hardware failures. The specific recommendations made for SP/SSPs are repeated here for STPs.*

  1. Software and hardware fault insertion testing (including simulating network faults such as massive link failures) should be performed as a standard part of a supplier's development process. Hardware failures and data errors should be tested and/or simulated to stress SS7 fault recovery software.

  2. Fault recovery actions that result in a loss of SS7 signaling functionality need to be reviewed periodically by SP/SSP manufacturers to assure that the least SS7 signaling impacting strategies are being used for classes of failures implicated during root cause analyses. For example, if a set of failure conditions resulted in a system initialization, that condition should be reviewed to determine if a system initialization of that level is appropriate.

  3. Initialization durations should be optimized to minimize service impact. Given that a particular failure needs an initialization to recover, manufacturers can minimize the service impact by optimizing the design and execution of the initialization. Again, data from root cause analyses should be used to determine areas for investigation.

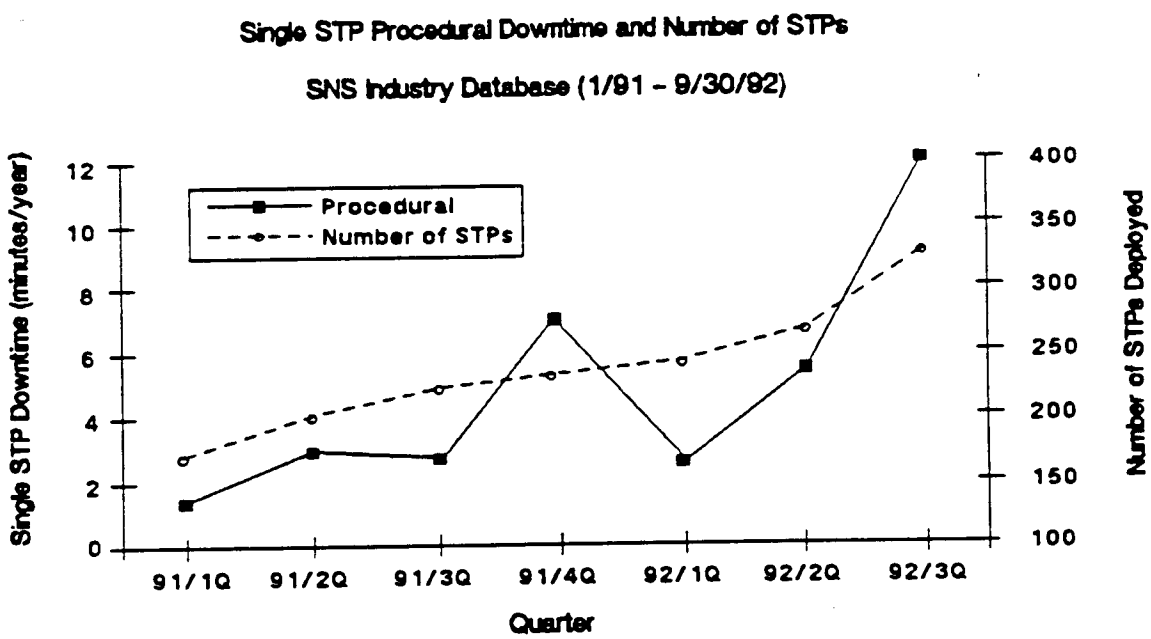


Figure 5-14

B

Procedural Downtime & STP Growth

- *A significant increase in the failure durations associated with procedural errors has been observed with no evidence of any increase in the rate of occurrence of procedural errors. This increase is correlated with the recent rapid growth of STPs and links in the network. It is recommended that network service providers consider the following actions to quickly train maintenance forces with insufficient levels of CCS expertise that must handle STP maintenance.*

  1. Determine the current levels of training for all maintenance personnel that will perform STP maintenance functions (See NOF Internetwork Interoperability).

  2. Each network service provider should establish a minimum set of courses and experience that are required before maintenance can work on STPs ("Best Practice" - See Appendix 5 for U S WEST training program developed for SCC Field Technicians and Control & Analysis Responsible for STPs).

  3. Establish an aggressive training program to be completed within 6 months.

  4. As a "Best Practice" for training, CCS/SS7 courses, curriculums are available from each STP supplier [10][11][12][13] and Bellcore Technical Education Center.[14]

5.2.6 SCP Failure Analysis

SCPs are becoming an increasingly important network system because of their role in providing network elements information regarding the handling of Intelligent Network (IN) calls. With the growing reliance on these systems it is important to identify any SCP reliability problems.

To assure IN service reliability, SCPs are typically deployed in a mated pair configuration. The analysis of industry data on SCPs indicated that no mated pair SCP failures occurred. The team's analysis, therefore, concentrates on single SCP failures, failures which were not service affecting.

In the analysis, single SCP total system failures and single SCP networking capability (a function performed by the MTP) failures are combined in one category because their effect on the network is similar. Figure 5-15 shows the average downtime trend across the data collection period. The overall average downtime is higher than the Bellcore objective of 3 minutes per year for a single SCP loss of MTP functionality,[15] however, the data indicates that the average single SCP MTP/total system downtime is decreasing.

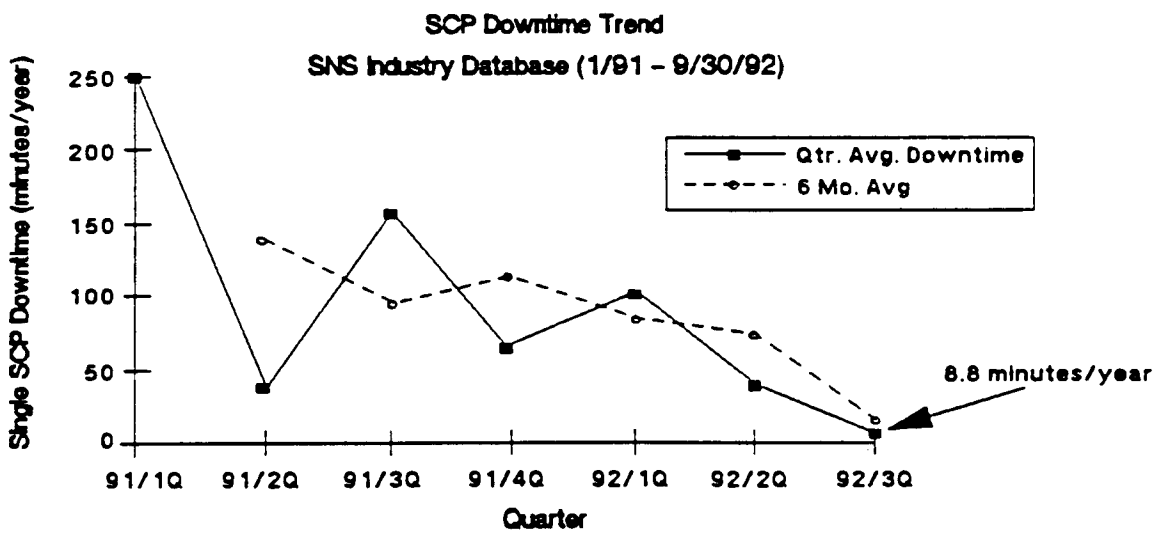
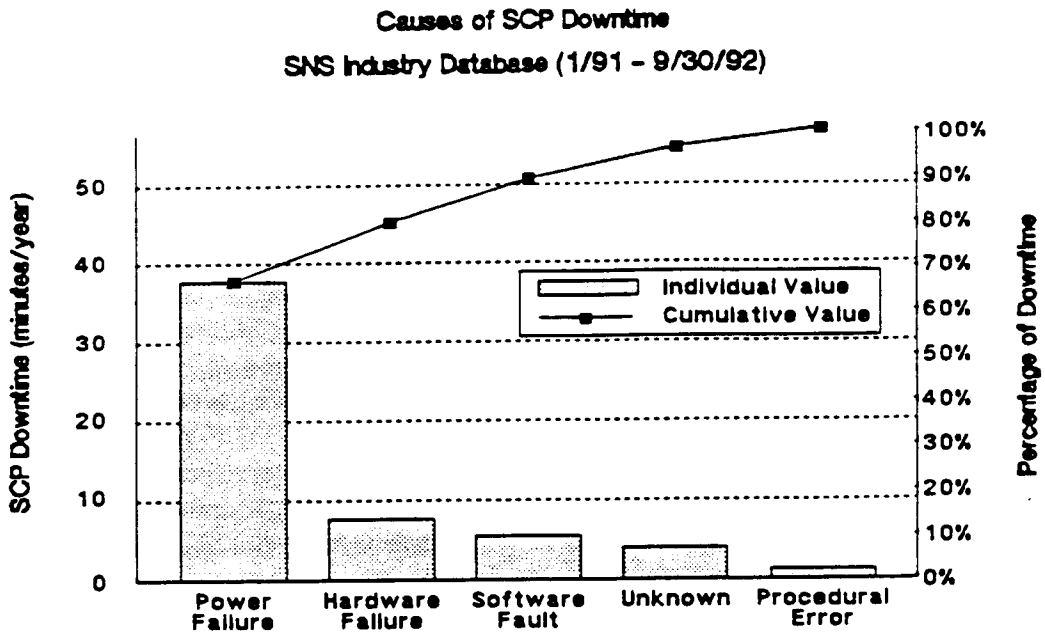


Figure 5-15

B

5.2.6.1 Causes of Failures

The cause distribution of the SCP failures in Figure 5-16 shows that almost 70% of all downtime was caused by power-related failures. Actually, the decreasing trend shown in Figure 5-15 was contributed to mainly by the decrease in downtime in power-related failures, as shown in Figure 5-17. Although the downtime was decreasing, the failure rate remains higher than that observed in STPs and SPs.



Causes of SCP Total System/MTP Failures

Figure 5-16

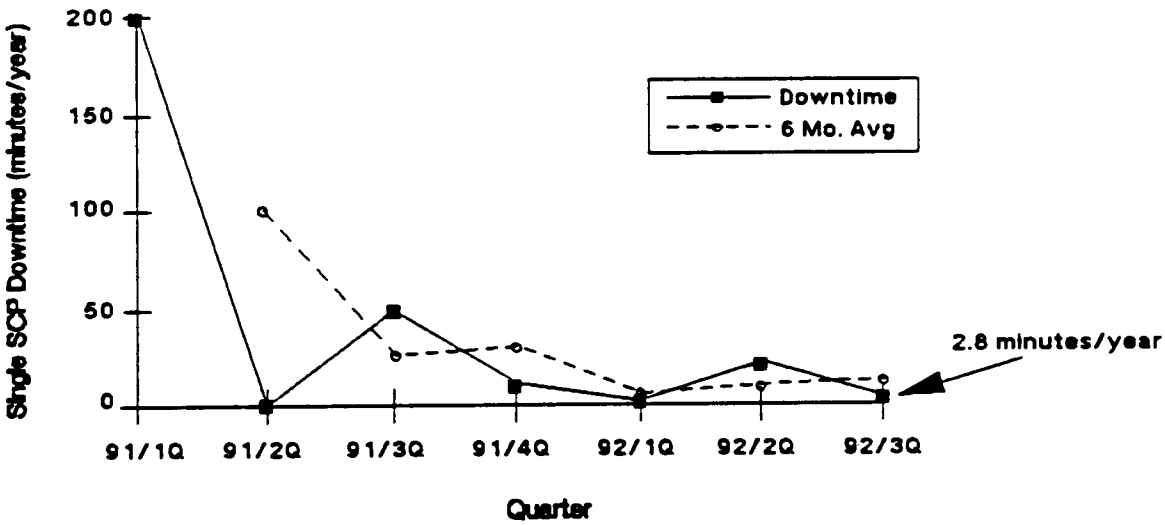


Figure 5-17

B

Based on analysis of the SCP failures categorized as power failures, the findings are:

- The majority of the failure events of long duration are results of external interruptions of power, where the UPS (Uninterruptable Power Supply) for the site did not function properly and the power supply to the SCP failed.

- The other failure events (smaller in number and in duration) are results of internal interruptions of power, where human error caused the UPS to not function properly.

- Outage events due to power failures occurred in SCPs in both computer center and central office environments.

5.2.6.2 SCP Power Recommendations

Based on the above findings, the following recommendation and Best Practice is made:

- *SCP owner and operators should have planned evaluations of the UPS for each SCP site. They should also schedule periodic maintenance and testing of UPSs to ensure functionality when needed.*

  The industry group, "Power Systems Focus Group", has completed a detailed analysis in the area of power failures and has documented their findings and recommendations. They are in line with this analysis and should prove effective in minimizing downtime due to power failures in the future.

- *"Best Practice" - Several carriers on the SNS Team recommended that SCPs be placed in a "central office (CO) environment." The carriers indicated that the existing CO design criteria (including power, fire, etc., that exist in documents such as Network Equipment Building Systems (NEBS)[16]), CO operations procedures and availability of maintenance personnel would generally enhance reliability performance of these systems. NOTE: This is not suggesting that SCPs should be taken out of "computer conditioned space", but ideally placed in concert with a "CO environment".*

5.2.6.3 Other Causes

Based on the analysis of the SCP failures categorized as everything other than power failures, the findings are:

- The majority of the other failures were classified as hardware related failures.

- Over 75% of the failures reported occurred on SCPs that are no longer in service. These sites have been replaced by new SCPs comprised of newer technology (hardware). Based on the data provided, it is not possible to determine if the same problems will occur and result in outages on the new SCPs. The reliability indicators on the new hardware indicate a lower probability of failures.

  There is no data available on the new SCPs since they were placed in service after the period reported in this analysis.

- The remaining outages do not provide enough data to determine any trend or specific are of concern.

5.2.6.4 SCP Summary

The majority of SCP failures reported and those with long duration are classified as power failures. The data indicated that more emphasis needs to be placed on ensuring adequate and functioning backup power sources and controllers (UPSs). The majority of the sites reporting failures due to other causes have been replaced with newer technology subsequent to the reporting period.

5.2.7 FCC Docket 91-273 Signaling Related Outage Events

5.2.7.1 Summary of Data

B

A total of 128 FCC reportable outage events occurred from April 6, 1992 through December 31, 1992. Of these, 30 (or 23%) were SS7-related. These 30 FCC reportable SS7-related events are categorized as follows:

- 6 were due to combined A-link set failures. Four (two-thirds) of the combined A-link set failures resulted from single failures on non-diverse link sets. Two events (one-third) were due to two independent, concurrent, hardware failures
- 24 were due to end office failures.

The 24 SS7-related end office failures can be broken down as follows:

- 14 had software design as a (partial) root cause
- 12 had procedural errors as a (partial) root cause (5 had software design and procedural as root causes, and 1 had procedural and unknown as a root cause)
- the remaining 4 were hardware failure, lack of power diversity, loss of timing during transfer of timing source and unknown.

Of the 14 software design-related failures, 12 had faults with the recovery procedures such that the software was not robust enough to detect and/or recover from specific failures (9 out of 12) or a software error prevented recovery (3 out of 12). The remaining 2 software-design related failures allowed maintenance personnel to perform actions detrimental to the network without providing sufficient warnings (e.g., maintenance personnel accidentally busied out both linksets, isolating an office or allowed an inconsistency in entry of translation data which prevented calls from being routed on that trunk group).

Examples of a lack of fault tolerance in the software design for recovery procedures included;

- no detecting of (and hence no recovery from) data corruption (2 events)
- no attempt to reload data from an alternate backup storage device
- inability to recover a redundant control unit that was out of service for routine testing when the primary control unit failed (3 events)
- failure to reinitialize nodes during a recovery from an initialization or hardware failure (3 events)
- software error which prevented failed links from recovering (3 events from the same error)

The 12 procedural-related failures resulted from a wide variety of errors which include:

- lack of an available patch (2 events)
- incorrect data on a tape or in translations (3 events)
- incorrect facility assignment on work form
- incorrectly marked fuse panel
- installation of an incorrect circuit pack in a standby processor
- error in an instruction manual provided by the vendor

5.2.7.1.1 Recommendations

The following recommendations are based on the 30 FCC-reportable SS7-related outages described above and in part on comparing these results with those of the switching sub-teams, who looked at a wider range of failure events (including, but not limited to the FCC-reportable events).

A-Link Diversity;

- *It is apparent that the diversity of A-links needs to be ensured, since the above data had twice as many events where an office was isolated (and caused an FCC reportable*

event) due to a single link-affecting failure than from two failures on the independent hardware associated with each link. Section 6 contains recommendations and best practices for maintaining link diversity.

SP/SSP Recovery Software:

- *It is also clear from the above data that the switching system software fault tolerance needs to be enhanced to aid in the recovery process. Since the number of events in the above data is small, it is difficult to pinpoint the specific areas/problems for which software fault tolerance needs to be increased. The "Switching System Focus Group (specifically the Software Subteam)" also identified the need for enhanced software design to increase the fault tolerance of switching software to problems such as data corruption (see Section 4.1.2 of their report). Thus, we would like to reiterate the following specific recommendations made by the switching system software sub-team:*

  - Suppliers should enhance design and code inspections to increase software fault tolerance (See Section 4.1.2 of the Switching System Software Report).

  - Suppliers should perform software fault insertion testing, with faults inserted in data and in programs (See Section 4.1.5 of the Switching System Software Report).

Procedural Errors:

- *Finally, the data above indicates a need for improvement related to reducing the number of procedural errors. The Switching System Focus Group (Procedures Subteam) identified four main sub-problems in their study, of which two were also identified as sub-problems in the FCC reports; failure to follow the correct hardware maintenance procedures (including mislabeling and removing the wrong unit from service) and data entry errors (See analysis section of Switching System Telco procedures subteam report). For these subcauses, the procedures subteam recommends (and thus, the SNS Data Team) manufacturers place an added focus on human factors design to reduce these types of failures. Additionally, as mentioned earlier, network service providers should conduct an "Awareness Training Program" for all maintenance personnel who work on SP/SSP CCS equipment.*

5.2.8 Recommendations to Prevent Long Duration Events

The data team also conducted in-depth analyses of long duration failure events to determine root causes of these events. The purpose of this effort is to make recommendations to improve the failure recovery process and limit the duration of failure events. The following major recommendations were made based on the analyses:

- *SP/SSP rehome activities appear to carry a high risk factor in that they can result in long outages when performed incorrectly. A similar situation exists for hardware and software expansion. It is recommended network service providers carefully review all rehome procedures and undertake meticulous pre-planning before execution. Communication to all inter-connected networks will be essential for success in the future. It is also important to make sure that rehome procedures are carefully followed.*

- *In some cases detection and manual intervention to assist recovery was slow. This suggests that network operators should be adequately trained in (1) detection of conditions requiring intervention, (2) escalation procedures and (3) manual recovery techniques.*

- *Lack of troubleshooting experience and proper training in this area usually prolongs the trouble detection and isolation process. It is recommended that network operators be*

B

adequately trained in the trouble detection and isolation process.

- *Failures related to a lack of link diversity can cause long outages depending on the ability to either correct the problem or switch to other transmission facilities. The ability to maintain link diversity is also important and is discussed in more detail in Section 6.*

- *The data shows that outages caused by procedural errors that occurred during maintenance activities of power equipment were associated with long recovery times. There is no single solution to this problem because the data did not indicate a single root cause. However, better training in power equipment maintenance activities and emphasis on the importance of CCS network equipment should be considered by network service providers.*

5.2.9 Additional Observations

5.2.9.1 Quality of Root Cause Analyses

As with most field collected data, there were a number of problems in the industry data. Of primary concern was the inability of some companies to obtain root cause analysis information on the outages they experienced. This was primarily due to the fact they just did not collect this type of data. In addition, when companies did provide data, a variety of requested fields were often left blank. Specifically, the lack of information in the descriptive field in the reports made any effort to perform further root cause analysis impossible. This indicated to the team that most members of the industry could improve their outage data collection and root cause analysis processes for signaling related outages.

5.2.9.2 Outage Information Sharing

The team's questionnaires request outage reports from both carriers and suppliers. As such, the number of reports from both carrier and supplier about the same outage was expected to be high. However, only 17% of the outages were reported by both the carrier and suppliers. The rate varied greatly based upon the component being reported on. For the single STP outages, 57% of all outages were reported by both the carrier and the supplier. For SP/SSP outages, 8% of all outages were reported by both the carrier and the supplier. For single SCP outages, none of the outages were reported by both the carrier and the supplier.

Figure 5-18 shows the percentage of outage reports submitted by their source. This certainly indicates that the industry could do a much better job of sharing information, especially between carriers and their suppliers of signaling systems.

Percentage of Reports by Source

SNS Industry Database (1/91 - 9/30/92)

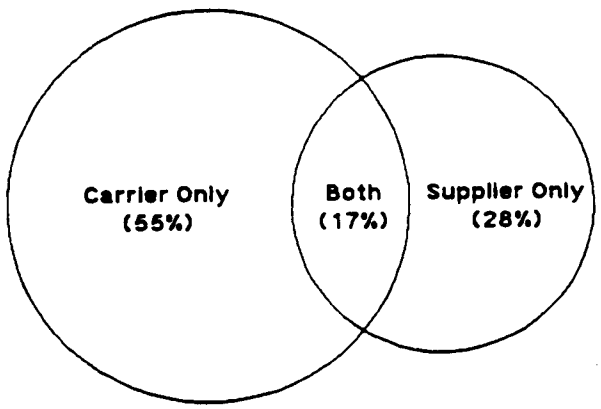


Figure 5-18

B

5.2.9.3 Recommendations

The team has the following recommendations in these areas:

- *Failure Data Collection and Root Cause Analysis - The team recommends that carriers and suppliers improve their own failure data collection and analysis procedures for better root cause analysis. Carriers and suppliers should form partnerships to jointly perform these analyses. Section 6 of this report defines a "Root Cause Analysis Process" that the team developed along with references to a number of industry "Best Practices."*

- *Signaling Information Sharing - The team recommends that the industry improve its information sharing between all industry segments, specifically between carriers and their suppliers of signaling systems. Section 6 of this report provides the status of recent industry efforts in the Network Operations Forum (NOF) to improve signaling outage information sharing.*

6.0 Key Learnings, Recommended Best Practices and status of response to 1991 CCS Network Outages

This section contains countermeasures resulting from the SNS Committee's deliberations over the past 12 months. These are divided into three categories - 1) Key learnings, 2) Recommended best practices and 3) Status of the industry's efforts resulting from the CCS Network outages of 1991.

The definition of "Best Practices" as used in the network reliability focus area Technical Papers is as follows: "Best Practices" are those countermeasures (but not the only countermeasures) which go furthest in eliminating the root cause(s) of outages. None of the practices are construed to be mandatory; however, a very small number of countermeasures that are deemed by the Focus Team, and concurred by the Network Reliability Steering Team (NO REST), to be especially effective countermeasures will be designated as "recommended".

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

6.1 Key Learnings

6.1.1 Need for better Root Cause Analysis

In analyzing industry outage/failure data, the CCS Failure Root Cause Analysis Process Subteam observed the following:

- The quality and quantity of outage reports varied significantly across the industry and over time. Relevant or needed data was not always readily available. Thoroughness and completeness of outage analysis have shown improvement of late, however.

- In many cases, both the descriptions of failure events and the recommendations for improvement lacked sufficient depth to identify the root cause(s) of the outage or to provide sufficiently detailed corrective measures to prevent recurrence of failures of this type.

- Attempts to involve other companies in root cause analysis were not always evident.

The team therefore recommends that:

> *Carriers and suppliers should improve their own failure data collection and analysis procedures for better root cause analysis. Carriers and suppliers should form partnerships to jointly perform this analysis.*

To achieve this goal, the team developed the following "root cause analysis process" and identified some industry examples of best practices. The ultimate goal of this effort is to eliminate the occurrence of future failures or at least to minimize

B

their impact.

6.1.1.1 Recommended Generic Process

The process entails collecting and analyzing failure data, determining the failure's root cause(s), recommending corrective actions, following up on these recommendations using measurable success criteria, and documenting findings. This process is recommended to the industry for its use in postmortem analysis and appraisal of the events surrounding any signaling system failure whose severity warrants the generation of a formal report.

Figure 6-1 depicts this recommended process:

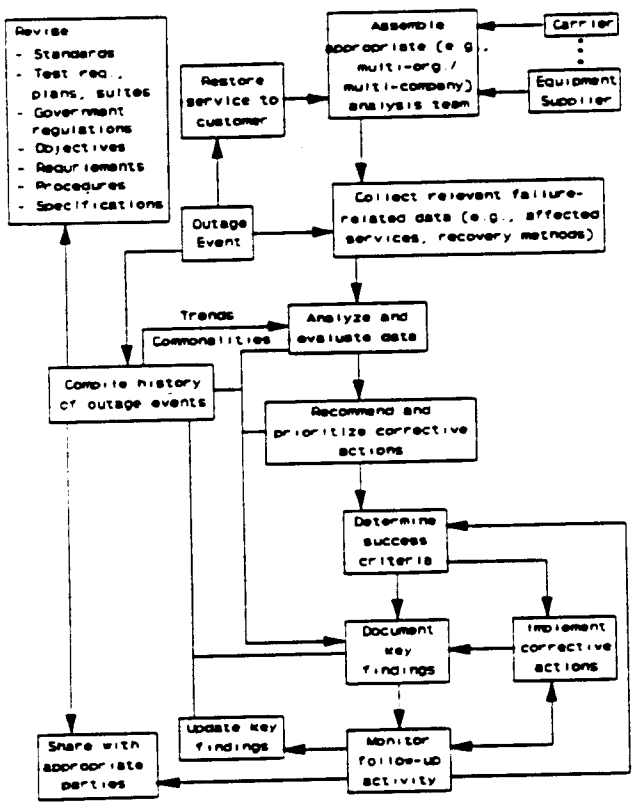


Figure 6-1

It is further recommended that this process be integrated, to the extent possible, with corresponding processes for other types of network failures (e.g., switching, hardware).

Implementation of any failure root cause analysis process must be preceded by the establishment of criteria that define which service interruption or degradation events or abnormal network conditions merit investigation, analysis, and a formal report. These criteria would be expressed in terms of the impact of the outage on service. Within the framework of these criteria, levels of severity could be defined each of which might trigger different or nested subsets of the following process. Some criteria in use today are discussed in the Section 6.1.1.2.

With the above discussion providing useful guidelines, we will leave it to individual service providers in conjunction with their suppliers to establish their own criteria. These would have to be at least as strict as those in FCC Docket 91-273 to assure adherence to the latter. Tighter criteria might be justified to maintain strict control and surveillance over network performance. Indeed, identification and analysis of incidents which result in relatively minor customer impact (e.g., fewer than 30,000 affected customers) could provide an early warning of the possibility of a more serious event.

Upon occurrence of a failure, the first order of business must be to identify the source of the outage and correct the fault. The appropriate and necessary resources would be devoted to this task until the problem has been resolved. This identification and analysis of and corrective response to a specific incident is sometimes referred to as the "reactive" portion of the root cause analysis process because these steps constitute a reaction to a stimulus (e.g., the outage). The reactive root cause analysis provides input to the "proactive" root cause analysis described below.

Upon repair of the failed system and restoration of the affected services, the "proactive" portion of root cause analysis would commence. This process is "proactive" because it offers system and procedural improvements and is conducted to prevent future outages or in anticipation of their eventual occurrence, to limit their impact. This

B

proactive portion of root cause analysis or simply root cause analysis henceforth is the focus of this section. The root cause analysis process is defined as a sequence of steps to be conducted following a failure event. These steps are:

1. Assemble a team appropriate to conduct the analysis. This team might be multi-organizational or, according to the circumstances of the outage, even multi-company consisting of representatives of the carrier and system suppliers. A "Best Practice" identified by the team was Bellcore's Outage Performance Monitoring Procedures[17], which contains a list of potential carrier personnel to be included on this team (This is discussed later in Section 6.1.1.2). In particular, the carrier should notify the supplier of any product (e.g., equipment, software, etc.) when that product experiences an outage and request its participation in this team effort. This team-forming step might be expedited by establishing a standing core team and adding experts as needed on a per failure event basis.

2. Collect relevant failure-related information:

- description of facts and circumstances involved in the outage (e.g., date and time of occurrence, affected geographic area, history of failures of this type, safeguards in effect to prevent such a failure)

- list of affected network elements (e.g., node, equipment, switch, STP, SCP, DCS, software release, facility, carrier, cable, power supply, or other)

- list of affected network services (e.g., intra-/inter-LATA/switch, basic/primary rate, 911)

- cause of failure as well as any related incident triggers (e.g., a hardware malfunction that leads to a software failure would be such a trigger) if known, otherwise best estimate or guess

- planned or unplanned event

- recovery methods employed to restore service

- duration and impact on service of the outage (e.g., estimated numbers of blocked/lost calls and customers affected)

- maintenance and traffic data related to the failure (e.g., Were failures or planned downtime, for administrative or maintenance activities, for example, on another system causing traffic overload on the system whose failure is being investigated?)

- steps taken to prevent recurrence of an outage of this type

This information is also needed to facilitate subsequent analysis.

3. Analyze and evaluate this data in a consistent fashion

- Determine the most likely cause(s) of the outage. Multiple causes may be responsible. Care should be taken to distinguish between actual root causes and incident triggers. For example, a malfunction in subsystem A should not be identified as the root cause of a resulting subsequent failure in subsystem B if B should have been designed to be fault-tolerant to failures in A by, for example, automatically reverting to an alternate mode of operation after an A-subsystem failure. In this example, the failure in subsystem A would be the incident trigger and the improper response of B to A's failure would be the cause of B's failure.

- Classify outage by cause(s) into one of a set of pre-defined categories or into a different category defined by network administrators during analysis of the outage (As an example, a list of possible outage cause categories for switching element failures is contained in Bellcore's Outage Performance

B

Monitoring Procedures - See Section 6.1.1.2 below). This allows the root cause of the failure to be diagnosed and corrected.

- Compile statistics of failure events. Main cause categories and trends could then be identified for a corrective action focus. This should also be useful in analyzing subsequent failures.

4. Recommend and prioritize corrective actions to be taken to reduce the:

- number,
- frequency,
- duration, and
- severity

of any future outage events to minimize their impact on customer service. The impact of an outage on operations and network capacity is also important and must therefore also be controlled. These are really interim goals. The ultimate goal is to eliminate the occurrence of these events.

These recommended actions might be procedural (e.g., more timely installation of a new software generic, schedule future maintenance activities during low traffic volume time periods), preventative (e.g., provisioning of additional protection switching, installation of power surge grounders, increasing deployment diversity, limiting software patches and hardware upgrades which require restarts, conducting fault insertion tests to evaluate system's fault tolerance, i.e., its ability to prevent a failure from spreading to other parts of the system, focus on software development and pre-deployment testing for failures caused by faulty software), or educational (e.g., additional training), for example. Test configurations and scripts might also be recommended to gauge the value of other recommendations by conducting these tests before and after implementation of these other recommendations.

5. Determine success criteria to evaluate:

- system's performance improvement after implementation of recommended corrective actions and/or

- the effectiveness of recommended corrective actions (e.g., the outcome of the aforementioned tests might be used here)

6. Document the key findings. This documentation should include:

- the data collected in step 2 above

- cause and failure category of the outage

  Disruption of signaling capability of sufficient magnitude to necessitate a formal report might be caused by an exchange or network element (e.g., switch) isolation, CCS network congestion or synchronization failure, a severed SS7 link set, or a signaling software malfunction, for example. Additionally, a combination of a failed STP and failed SS7 A links could render an STP mated pair inaccessible.

- trend analysis graphs or charts to highlight problem areas

  These displays might depict, for example, the number of failures:

  a. affecting different types of network elements (NEs) or components/subsystems thereof

  b. occurring by time of day

  c. per root cause category

  d. with an associated incident trigger

  e. normalized or scaled by number of deployed network elements, pieces of equipment, or software releases of that type,

  This failure profile should be helpful in

identifying failure trends. The Software Design Team of the NRC's Switching Committee used this idea effectively to identify the leading cause of software design outages as data corruption[18].

- recommendations to:

  a. prevent recurrence of this type of outage

  b. reduce the impact of future occurrences

  c. develop any necessary requirements and standards for suppliers to include appropriate mechanisms in their network products to:

  - correct the fault that led to the failure

  - identify and report the source of an outage of this type

  - collect failure data

  Supplier procedures might include in-plant testing to assure that changes made to one subsystem do not adversely affect another and that operational status and failure mode identification and recovery mechanisms are updated to reflect subsystem modifications. Depending on the extent of the modification, some preconditioning tests such as accelerated aging, operational mode cycling, and environmental stresses (e.g., thermal extremes, vibration) might be repeated. Many more possible ideas for supplier efforts to improve product reliability are contained in[19], but that document focuses on hardware.

  Documentation should be available within a specified timeframe to be agreed upon by involved providers and suppliers. This timeframe needs to be consistent with the 90-minute and 30-day initial and final service disruption report guidelines provided in reference 1.

7. Monitor follow-up activity to ensure that:

- recommendations are being implemented (details on how to implement this recommended process are at the discretion of the individual company) and achieving desired results

- no un-anticipated negative effects result from implementation of these recommendations

- appropriate portions of the analyzed data, findings, and recommendations are being shared with entitled and interested parties such as:

  a. the FCC and other agencies requiring incident reports

  b. suppliers of the failed network element

  c. other customers of the supplier such as LECs and IXCs.

  d. other industry members through the Exchange Carriers Standards Association (ECSA); e.g., suppliers

  This information sharing would be partly accomplished via the documentation step described above. Improving the failure analysis and response process and results is just one reason this information sharing is important. Demonstrating that best attempts to maintain a reliable network are being made is another.

6.1.1.2 Industry Best Practices

For each best practice discussed in this section, the highlights are briefly described, including, where available, outage/failure definitions, root cause analysis procedures following an outage, and the contents of an outage report.

Bellcore SR - Outage Performance Monitoring (OPM) Procedures (Reference 17)

Upon occurrence of a reportable failure, the OPM procedures commence with the formation of

B

a Service Failure Analysis Committee or SFAC. Recommended SFAC membership includes carrier operations, administration, and maintenance personnel as well as vendor technical support. This Committee is responsible for conducting and documenting an analysis which would determine:

1. facts and circumstances of the outage
2. duration and effect on service of the outage
3. cause and outage classification of the outage (see below)
4. corrective and preventative actions and recommendations

A standard report format for documenting this information, the Service Failure Analysis Report or SFAR, is also described.

Additionally, a 3-tiered classification of outages is described. These are loss of service to a single line or trunk, partial system failure, and total system failure each for a minimum duration of 30 seconds. A commonly-used definition of reportable outages, those that exceed 2 minutes in duration, is also discussed. Calculation of outage performance metrics is also described. Failure cause classifications (e.g., procedural, design, environmental) are also described in detail.

FCC Docket 91-273

The FCC's Report and Order provides specific outage level threshold reporting criteria and defines useful elements of a final failure report. The published thresholds must be complied with for FCC reporting purposes. Basically, these criteria require that an analysis be conducted and a report generated and submitted whenever at least 50,000 customers are potentially affected by an outage enduring at least 30 contiguous minutes, whether planned or not, without full restoration of normal call processing. Additionally, failures of duplexed equipment (e.g., SS7 link sets, mated STPs, SCPs) meeting the 50,000 line/30 minute threshold must also be reported. Subsequent to the release of the FCC Docket, the NRC has recommended that the reporting requirements be tightened to include failures affecting 30,000 customers or any of certain specially designated capabilities (e.g., 911 services). The 30,000 customer threshold has now become the accepted industry standard pending formal adoption by the FCC. See FCC Docket 91-273 and Reference 20 for more detail including a definition of "outage" and methods to calculate the number of customers potentially affected.

The FCC Docket defines useful elements of a final failure report including:

1. date and time of the incident
2. affected geographic area
3. number of customers affected
4. type of equipment affected
5. types of services affected
6. duration of the incident
7. cause of the failure
8. method(s) used to restore service
9. measures taken to prevent recurrence of this type of failure.

6.1.2 Outage Information Sharing

Listed below is a summary of Network Operations Forum (NOF) Information Exchange Issue (See Appendix 6 for Information Exchange Document). The SNS Committee requested Al Loots, who is part of the NOF working group, to keep our team appraised of the status of this issue. The issue was completed and the SNS Committee endorses this process. Listed below is a summary of the information sharing process which is based upon and largely extracted from the final document (NOF Reference Document Section VII).

The purpose of information sharing is to enable all service providers and vendor/manufacturers to utilize information uncovered by other service

providers and/or vendor/manufacturers through the testing, validation and application of software, hardware, and documentation; procedural issues; and conformance to agreed upon 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 our "customers". Such information sharing may also serve to reduce the need for repetitive or redundant testing.

The basic premises is that Telecommunications Service Providers and Vendors/Manufacturers have an obligation to their collective Customers to cooperatively provide assurance for the integrity of the public switched telephone network.

Information associated with testing and/or problem/failure scenarios of the network can and will provide invaluable assistance when shared with other Service Providers and/or Vendors/Manufacturers. The sharing and use of this information may: 1) Minimize and/or prevent failures, 2) Minimize and/or prevent degradation of the network, 3) Minimize and/or prevent reoccurrence of the same problem in another network and 4) Assist in problem resolution.

Criteria for Sharing Information: Information uncovered by any Service Provider or Vendor/Manufacturer which 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 impacted by the problem.

The scope includes the exchange of information between: 1) A Vendor/Manufacturer and its Customer(s), 2) A Vendor/Manufacturer and its Customer and the Customer's interconnected Service Providers, 3) Vendors/Manufacturers, 4) Access Service Providers and 5) Access Service Providers and Access Service Customers.

The following list is intended to represent a complete list of sources of information for sharing. The identified sources include:

- Service Provider Stand alone Testing environment
- Compatibility testing between Service providers
- Service Provider daily operations
- Service Provider outage reports and analysis
- Service Provider and/or Vendor/ Manufacturer documentation
- Vendor/Manufacturer development testing
- Vendor/Manufacturer trouble information reports and analysis
- Vendor/Manufacturer trouble resolution reports
- Observed ambiguities or differences in requirements interpretations.

6.1.2.1 Service Provider's Responsibilities

Service providers should inform their Vendor/Manufacturer of defects and potential defects discovered during testing and daily operation. This information is critical to the Vendor/Manufacturer's root cause analysis and information sharing processes. Service providers should not share Vendor/Manufacturer defects or potential defects with other service providers but instead allow the Vendor/Manufacturer to share the information with their customers.

Service providers should inform interconnected parties of problems and potential problems not attributable to a Vendor/Manufacturer. Examples of this would be translation configurations and procedural issues.

Vendors/Manufacturers should make available to a particular Customer all trouble report information reported by that Customer.

6.1.2.2 Vendor/Manufacturer's Responsibilities

When Vendors/Manufacturers identify problems with their software or hardware that has the potential to cause loss of service or compromise in the reliability, capacity, or performance in the network(s) of a Customer(s), such information should be communicated to its customers within 1

B

business day.

If the situation allows, the Vendor/Manufacturer should also inform its Customers of the long-term or short-term solution to the problem at the time of informing them of the potential problem. In the event that the Vendor/Manufacturer has not developed a solution at the time of notification, the Vendor/Manufacturer should inform its Customers of the action plan to avoid/correct the situation.

Two modes of communication are recommended: 1) Proactive notification and 2) Vendor/Manufacturer Electronic Message System. The mode of communication used is determined by the potential severity of the problem.

6.2 Recommended Best Practices

6.2.1 Compendium of Best Practices on Maintaining Diversity

The initial outage data analyzed by the group revealed that A-Link downtime performance was meeting the downtime objective established by ANSI. As a result the group focused their industry outage data request to SPs, STPs and SCPs. Signaling links meeting the downtime objective is encouraging, however, the team felt the industry should continue to improve on these results. Several carriers pointed out that CCS signaling link circuits may be initially designed and installed with complete diversity, over time diversity may be lost due to normal churn. As a result a sub-team was formed to compile a compendium of Best Practices on how to maintain diversity. Listed below are the "Best Practices"/Documents that network service providers should consider to assist with maintaining diversity:

6.2.1.1 TA-TSV-000905, "Common Channel Signaling (CCS) Network Interface Specification", Issue 3, December 1992

This document specifies two architecture configurations used for interconnection of CCS networks. In particular,

- Section 6.2 discusses diverse physical level facility routing for combined link sets and gives diversity provisioning and maintenance guidelines. It also lists representative physical level equipment that should be taken into account when provisioning or maintaining CCS link diversity

- Section 7.2 gives CCS link diversity guidelines for STP-to-STP and STP-to-CCSSO interface architectures to meet CCITT, ANSI Committee T1 (see Chapter T1.111.6 of ANSI T1S1 Standards), and Bellcore (TR-NWT-000246) performance requirements for the CCS networks. Also, to maintain link set diversity, Section 7.2.1 states that operations procedures should specify the following:

  - Link set diversity should be routinely confirmed
  - Whenever maintenance or circuit order activity occurs on a link, or a failed link is restored, diversity of the combined link set should be confirmed.

6.2.1.2 Network Operations Forum (NOF) Reference Document Section III SS7 Link & Trunk, Issue 3, April 1993

This document gives recommended criteria for Interconnecting Link diversity. It also describes:

- what should be taken into account during the provisioning process to achieve Physical Link diversity, and

- what should be addressed by operational procedures in order to maintain link diversity.

6.2.1.3 S. E. Makris, "Digital Cross-Connect Systems and CCS Network Survivability," IEEE International Communications Conference (ICC'93), May 23-26, 1993 Geneva, Switzerland.

This paper provides a systems engineering study of the survivability impact of using Digital Cross-

B

Connect Systems (DCSs) in various CCS network architectures. Specifically, it (1) gives a brief overview of the DCS functionality, (2) examines major factors (e.g., number and location of deployed DCSs, type and percentage of link sets traversing a DCS, etc.) in deriving CCS network alternative architectures using DCSs, (3) provides examples of network configurations and engineering guidelines for survivable deployment of DCSs in the CCS network, and (4) states areas for future work.

6.2.1.4 Trunk Integrated Records Keeping System (TIRKS)

Diversity Field Identifier (FID): Release 15.5 provides the capability to identify a circuit as diverse. When a circuit containing this identification is processed, the order will fall out of the flow through process for manual assistance.

Facility and Equipment Hierarchy Report (FEHR) allows comparison of up to three circuits. This report compiles facility assignments "up" the hierarchy. It also compiles equipment assignments by looking at the equipment posted to each level of the facility hierarchy. This is the only TIRKS output which provides all of the TIRKS inventoried facility and equipment associated with a given circuit. The intersection summary portion of this report provides the common facilities and equipment (lack of diversity). TIRKS does not automatically provide notification to the user when CCS link diversity is violated. The user must manually review the report.

The SNS Committee recommends that Bellcore evaluate the following enhancements to TIRKS:

- *FEHR today can only look at in-effect and pending add circuits. Enhance this report so that it can also look at rearranges*
- *Enhance flow-through to accept PDAC as an optional FID (Use of system specific PDACs will specify diverse routes). Allow the system specific PDACs to process on FEHR so the planner can "test" the routing prior to the assignments being posted in inventory.*
- *Develop a report so that when a planner is considering a facility removal at any level, a list of diverse circuits can be obtained. Additionally generate a report so that when a planner is considering an equipment bay removal a list of diverse circuits can be obtained.*

6.2.1.5 CCS Signaling Link Element Diversity (Checklist)

BellSouth compiled the following practical diversity guidelines based on application of Bellcore recommendations (Bellcore has supplemented BellSouth's original list somewhat). See Appendix 7 for BellSouth's Checklist.

- Power and Fusing: No components of a paired CCS link transmission path should share a common fuse or load
- Cabling: There should be diverse cable routes between individual CCS link paths within the central office
- Distributing Frames/Mounting Blocks: Termination of diverse CCS links must be on separate Main Distributing Frames (MDF), or if not possible, separate mounting blocks on the same MDF
- Office Repeater Bays, DSX Bays, Patch Bays: Not all of a given type of CCS link from the same network element (A, B, C or D) should traverse a single bay of these types
- DCS: Not all of a given type of CCS link from the same network element should transverse a single DCS
- D4/D5 Bays (and associated channel bank equipment): The channel bank equipment associated with each CCS link should be located in separate bays.
- Fiber Optic Terminals and Multiplexers: Paired CCS links should not transit a common fiber terminal or common

multiplex equipment

- Test Access Equipment: Not all of a particular CCS link type from the same network element should traverse a single test access unit

- Analog/Digital Radio: Not all of a given type of CCS link from the same network element should traverse the same analog or digital radio

6.2.1.6 Diversity Requirements for CCS7 Network Interconnect

AT&T has prepared a recommendation for the minimum requirements for SS7 Link Diversity for Access Services. The information is based upon, and largely extracted from the Network Operations Forum (NOF) - Installation & Maintenance Responsibilities - SS7 Link and Trunk Installation & Maintenance - Access Services (See 6.2.1.2).

The document (See Appendix 8) contains specific criteria for connection of Local Exchange Carriers (LEC) to Interexchange Carriers (IXC) networks regarding diversity. This document is similar to BellSouth's diversity checklist but provides a more detailed discussion of the individual components that require diversity.

6.2.1.7 Stickers on SS7 equipment

BellSouth has implemented an additional safeguard to protect equipment used for their CCSN. They have placed brightly colored stickers on SS7 equipment for easy identification. This alerts maintenance workers to the importance of this equipment. The wording on the sticker is:

– WARNING –
CONTAINS SS7 SERVICE
CALL SCC BEFORE INTERRUPTING
(TELEPHONE NUMBER)

6.2.1.8 U S WEST Restructuring Plan

The CCS7 Program Management & Operations (CCS7 PM&O) group was established in May, 1992 to integrate key functions and processes critical for the successful operation of the CCS/SS7 network. The goal of this group is to maintain a high level of expertise for CCS/SS7 in one focused and specialized area.

The key strategies that resulted in the formation of the CCS7 PM&O were:

- Network Signaling Management Center - A change in structure and expansion of the responsibility for the existing Signaling Network Control Center (SNCC) was required to maintain critical expertise and increase responsiveness to the CCS/SS7 network. In addition to the monitoring and maintenance responsibilities of the CCS/SS7 network, 800 DB administration, and "message" network management functions are included in the new CCS/SS7 center, the Network Signaling Management Center (NSMC). The NSMC will allow improved responsiveness on day to day service and increase control of disaster conditions.

- CCS7 Regional Engineering Group - To ensure diversity requirements and consistent design and engineering for the major network components (STP, SCP, Links) a regional CCS/SS7 engineering group responsible for design engineering of the major network components was established.

- Network Integrity Lab - a new function, Network Integrity Management will be formed through the establishment of a Network Integrity Lab. This will provide the ability to identify vulnerabilities in the CCS/SS7 network, prevent network failures, perform expanded testing capabilities and new service trials off of the live CCS/SS7 network.

- Systems Engineering - To assure adequate Operational Support Systems (OSS) tools for

B

the NSMC, a systems engineering group will be established to evaluate current OSS tools, update existing OSS tools, and design OSS tools that are unavailable from any other sources.

- CCS7 Project Management - Because of the amount of CCS/SS7 activity anticipated in the 1993-1994 time frame, and the need for high accountability and responsibility, CCS/SS7 specific project management will report into the CCS7 PM&O. CCS7 Project Management is required to coordinate and oversee several regional wide projects. These projects include 800 number portability (mandated by FCC Docket 86-10), continuing CCS/SS7 deployment and CLASS service deployment.

- CCS7 Product and Process Support - In order to maintain high expertise, accountability, and responsibility, CCS/SS7 operational staff support will report into the CCS7 PM&O. CCS7 Product and Process Support develops the methods and evaluates processes required for the NSMC to maintain the CCS/SS7 network.

- Disaster Recovery - A comprehensive network Disaster Recovery Plan is essential. This group will be responsible not only for developing plans, but for training the field on disaster recovery and collecting information on outages.

- Link Provisioning - The entire link provisioning process will be reevaluated to create a new process that will be managed and controlled within the CCS7 PM&O group.

The CCS7 PM&O functions as a single reporting entity as depicted here, ensuring that all critical CCS/SS7 operational and support functions are in concert with each other.

The organization chart is shown in Figure 6-2:

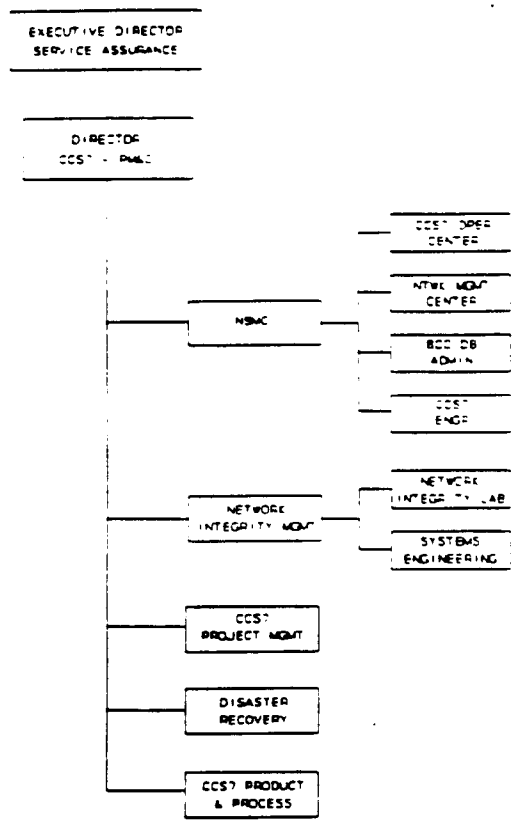


Figure 6-2

The CCS/SS7 network can not be successfully maintained and supported in the same way that we have been supporting the existing voice network. Problems in the CCS/SS7 network can quickly escalate and impact large areas of the voice network.

U S WEST is moving from a more reactive operations approach, to one where network vulnerabilities can be identified and resolved before they result in network failures. By pursuing an integrated operations approach, this will be achieved.

6.2.1.9 Example of a Planning and Provisioning Process for CCS Link Diversity (There are several opportunities within these steps to check for diversity in the planning and provisioning process)

a. Determine routes to be used

B

Elements in decision making process include the following:

- Availability of physical facility (cable or fiber in the ground)
- Plans for aggregating CCS links in DCS, etc. for test access and facility utilization
- Whether existing systems are available or new systems must be provisioned

b. Plan system using the desired routes, if necessary. (Facility & Equipment Planning System, [FEPS])

c. Pass planning information to TIRKS to provision systems, if required or to mark existing systems for CCS links

d. Provision (TIRKS) systems as required to support CCS link provisioning

e. Provision link circuits, using Circuit Provisioning Center (CPC) Message and Procedures (M&Ps) which are designed to ensure diversity of the DS0s (links), based on the above planning.

f. Install and test CCS links.

6.2.2 Crisis Management Exercises

The SNS Committee recommends that network service providers, as a "Best Practice", develop crisis management exercises to become better prepared in the event a disaster strikes. This was demonstrated most recently by flooding in Chicago, IL and Fairfax, SC, earthquakes in California and hurricanes in Louisiana, Florida and Hawaii. The telecommunications industry had held up remarkably well in each case.

The flooding in Fairfax, South Carolina on October 9, 1992 disrupted services from Sprint. A report was given at the December 15, 1992 Network Reliability Council Meeting. Sprint's reaction to the disaster was exemplary. They attribute this to "PRACTICE".

Listed below is a high level overview of Bell Atlantic's crisis management exercise. Central office and CCSN disasters are simulated with the following objectives:

- Practice Disaster Recovery Strategy Development
- Learn from mistakes
- Update call out lists
- Update response procedures and tasks
- Verify vendor and support contacts
- For everyone involved in the Disaster Recovery Plan to become more familiar with their role
- To give the various team leaders an opportunity to practice their role.

NOTES:

- NOT A TEST - Not intended to test anyone's knowledge of their discipline
- The Process is Important - Not the actual decisions reached.
- Want the field teams and the team leaders to make mistakes - so they do not make the same ones in a real disaster
- A very important part of any disaster exercise is simply giving people the time to think through what they would do, what they would need - in an actual situation
- As a reminder, please be sure to tell everyone you call that this is a disaster simulation. Staff has advised the BOCC Group, Security, and the Building Guard in order to avoid any confusion.

6.2.3 Prevention of Mated STP Outages

NYNEX has developed a plan which describes actions to be taken in a STP building and other locations deemed essential when the STP's mate goes out of service. All work activity is suspended in the mated STP building and other essential sites until the original STP is restored to service. The procedures are designed to prevent mated STP pair

B

outages (See Appendix 9 for NYNEX Condition Red Procedures).

There are two conditions where this plan would be utilized. They are:

- Condition Red is described as a network condition in which a single STP has failed and the appropriate SCC organization has notified the proper work entities to have certain work suspended immediately.

- Condition Green is when the previously failed STP has completely recovered and is in the stable state; and the appropriate SCC organization has notified the proper work entities to allow previously suspended work to commence.

General responsibilities for each organization involved are discussed. Additionally, detailed requirements for a wide range of work items are provided. The requirements include toll, translations, engineering, power, frame, outside plant and buildings. NYNEX is also utilizing stickers/tags to mark CCS equipment. These are similar to those utilized by BellSouth and discussed earlier (see section 6.2.1.7).

6.2.4 Emergency Response Plan

The NOF Reference Document Section VI entitled Network Management Guidelines and Contact Directory includes; guidelines for network restoration planning; various contact directories to aid internetwork and inter-company notification for various types of network events and a recommendation for an emergency communications system for both voice and data to be used to in the event normal communications channels are not available to effect notification and restoration.

The following text from the NOF Reference Document Section VI, serves as an introduction to an appendix to that document entitled Emergency SS7 Restoration. The guidelines and recommendations in this document should be considered in the formulation of any emergency response plan. This appendix is provided as an appendix to this technical paper (See Appendix 10 for NOF Emergency Network Restoration Plans):

- "The SS7 protocols designed to manage the network may not be sufficient in some failure scenarios. The potential for propagating a trouble in an integrated network increases the need for some manual network management capabilities. It should be noted that Manual controls applied to the SS7 network represent a serious undertaking and must be implemented only under extreme failure conditions. In these circumstances the interconnecting carrier should be informed in accordance with the SS7 Network Failures procedures in Section 6 of the Network Management document.

- The specific actions to be taken will be dependent upon the particular network failure, the network traffic management strategy and the manual control capabilities available by the vendor network element.

- The following options may be available to restore and manage network or node stability in the event of a catastrophic SS7 outage. Internetwork preplanning is strongly advised since these options may not be all inclusive and could be interrelated. Appendix A, entitled Emergency SS7 Restoration Operations Planning Considerations, is recommended to be used as a guide for preparing such pre-plans:

  - Deactivation of specific links to a SS7 network node.

  - Deactivation of all links in internetwork gateway link sets.

  - Use of STP Gateway screening to block additional incoming traffic from the remote SS7 network.

  - Activation of protective controls to CANCEL traffic destined for the node and route it to the announcement. (CANT, CANF, CODE, BusyTrk)

B

- Activation of expansive controls to REROUTE traffic to nodes/trunk groups that do not normally carry that traffic. (REROUTE, SKIP, DRE, PRE).

- The network Management Centers should monitor the traffic performance of the offices affected to assure quality controls are being implemented.

- Before any public switched traffic is allowed to proceed, every effort should be made to ensure the SS7 network is up and stable. It is recommended that the first traffic to flow should be the POTS traffic since other services, such as 800 Service, etc. require a POTS network.

- Re-introduction of POTS traffic on to the SS7 network should be assessed in the same manner that network managers currently use today. (i.e., Type of office and time of day). See Appendix A for additional preplanning considerations."

Activation of any emergency response plan will require intercompany communications channels and contact numbers. The NOF Reference Document Section VI. contains contact lists and recommendations for emergency communications.

The contact lists contained in the NOF document are as follows:

- Network Management Contacts
- Catastrophic SS7 Network/Failure Restoration Contact Directory
- Media Stimulated Calling Event Contact Directory
- Mutual Aid and Restoration Contact Directory.

These lists are frequently updated and should be utilized for notification and restoration of CCS Network Outages as appropriate.

The emergency communications section of the NOF document proposes an ECS for use by industry in the event that the Public Switched Telephone network (PSTN) is not available. One existing network that meets the criteria of an ECS is BEAMS the Bellcore/Bellcore Client Company Emergency and Alerting Management System. A number of carriers are connected to BEAMS and many others, including vendors, have expressed an interest in interconnecting to BEAMS.

The NOF has also recommended that all interconnecting networks (ICNs) and manufacturers interconnect via Public Packet Switched Network (PPSN) non PSN Access, as part of a Closed User Group, for the exchange of data on a day to day basis and as an adjunct to the Emergency Communications System (ECS).

6.3 1991 CCS Network Outages - Status of on-going efforts

This section is intended to document the major efforts that are still in progress as a result of the 1991 outages. It is not intended to be all inclusive.

6.3.1 SS7 Network Architecture Evaluations and Protocol Enhancements

Though the CCS networks have been operating reliably for several years, recent outages and accelerated interconnection of networks have led to several proposals for alternate CCS network architectures to further increase network robustness. The SNS Committee requested that SS7 experts in ECSA sponsored Committee T1 (T1S1.3) assess alternative architectures for CCS networks which have been proposed in several industry forums. Committee T1 is the U.S. Telecommunications Network Standards Developer. T1 is accredited by the American National Standards Institute (ANSI) and sponsored by the Exchange Carriers Standards Association (ECSA).

T1S1.3 provided the CCS network architecture evaluations and described the SS7 protocol enhancements that have been recently identified and agreed on. In addition, a brief analysis of recent CCS network outage data were provided and a description of T1S1.3 agreements made to enhance the SS7 protocol and increase the robustness of

CCS networks. These results as outlined below were reported to and accepted by the SNS Committee in contribution T1S1.3/92-11212R1.

Studies of outage data collected over a two year period indicate that the type of failure that has the most severe impact on CCS networks is the failure of STP pairs, even though the probability of an STP pair failure is small. The impact is severe because many end offices are isolated from the CCS networks if a pair becomes unavailable. However, most of the reported SS7 failures are associated with individual end offices.

Three alternative CCS network architectures were analyzed - architectures for interconnecting networks, architectures for A-Link Concentrators (ALC), and logical STP pair architectures.

- The basic or reference CCS network interconnection architecture is a mated pair of STPs from one network interconnected with a mated pair of STPs of the other network (see Figure 2-1, page 2). Additional interconnecting link sets and STP pairs can be added to each network to incrementally increase the survivability of the interconnection. An analysis of the cost versus benefit of the potential additions to the reference architecture must be performed by each network provider to determine the combination of backup components needed to increase reliability.

- Since ALCs perform the SS7 protocol Message Transfer Part (MTP) functions of an STP, it is recommended that an ALC be deployed as an STP in a reference-type architecture. Of the ALC interconnect architectures examined, an analysis has shown that the mated pair reference architecture has the lowest unavailability, least network management impact and message loss during failures, and least likelihood of end office isolations.

- The logical pair architecture, where each STP is pairwise mated with every other STP in the network, is shown to have no significantly greater availability than the reference architecture. In addition, the multiple interconnections needed add to routing and operational complexity; and it is more difficult to provide supplier diversity and manual recovery from failure. As a result, the overall reliability of this architecture could be less than the reference architecture, and therefore it is not recommended.

Although the SS7 protocol is relatively stable, recent CCS network experiences have stimulated protocol enhancements for improved CCS network robustness. The enhancements T1S1.3 has made to the SS7 protocols have been largely to the MTP and have dealt with prevention and recovery from link and network congestion, recovery from node failures, improved tests in the protocol for link functionality, and improved procedures for automatic testing of routes and transmitting network management messages. Work on the protocols to increase network reliability continues and includes the areas of network testing, traffic management procedures, and increasing signaling link capacity. However, there were some concerns about the need for providing some additional guidance to facilitate uniform industry deployment of the protocol enhancement already recommended.

As a result, the SNS Committee established a subgroup of SNS volunteers to prioritize the protocol enhancements described in the report from T1S1.3 into two or three levels. Bellcore volunteered to chair and host the prioritization meeting.

Since the SS7 protocol enhancements were designed to increase CCS network robustness, the prioritizing was based mainly on the relative measure of improved network integrity to be achieved by the enhancements and the greatest perceived network need. The enhancements were placed into two categories, where category 1 reflected the highest integrity benefits. Thus, category 1 enhancements would have the greatest impact on minimizing the effects of CCS network failure scenarios; minimize impact on the remaining or interconnecting networks; and maximize the CCS network (and telephone network) stability. Category 2 enhancements reflect lesser impact in that these enhancements do not apply to severe network failure scenarios and may be more localized in their network impact. In addition to help categorize these enhancements, the following

B

additional considerations were used:

- Indication that a specific failure scenario has occurred, and
- That need for internetwork compatibility has been identified.

Although two priorities were used, all the enhancements in each category should be considered as important and dealt with in a degree of urgency. Although the outcome of the SNS-initiated subgroup is a recommended priority list to the industry, the final priority and deployment by a carrier can be influenced by factors other than those considered by the subgroup.

Of the seventeen protocol enhancements completed and described in the report to the SNS (See Appendix 11 for Contribution T1S1.3/93-02113), nine were placed in category 1 and eight in category 2. The items within each category are not prioritized or ranked further.

The SNS committee expresses their sincerest appreciation to Stan Wainberg (Bellcore) for his Technical Contributions and leadership in the SS7 Protocol Enhancement Prioritization effort, and the SNS Committee representatives for a truly outstanding effort.

6.3.2 General Network Survivability Issues (T1A1.2)

T1A1.2 has developed a draft Technical Report to address growing concerns from the telecommunication community about the survivability of telecommunications networks. The report is needed to provide a common understanding and common assessment techniques for network survivability. It provides a basis for designing and operating telecommunications networks to meet users' expectations regarding network survivability. The intended audience of this report includes providers, users and regulators of telecommunications networks and services, as well as telecommunications equipment suppliers. The draft report which is progressing through the T1 approval process also provides a foundation for continuing industry activities in this area.

Terminology to characterize network survivability is provided. In particular, network survivability is defined to be: 1) the ability of a network to maintain or restore an acceptable level of performance during network failure conditions by applying various restoration techniques, and 2) the mitigation or prevention of service outages from potential network failures by applying preventative techniques. Network survivability includes other industry terms, such as "network integrity" and "network reliability," and is related to "network availability."

A framework for measuring service outages is developed. The parameters for this framework are the availability of services affected by the network failure, the duration of the outage, and the extent of the failure (e.g., geographical area, population, network). Categories of service outage are outlined. The categories depend on type of user, network and service. Types of users include carriers, residential customers, government agencies, educational and medical institutions, as well as business and financial customers.

A four-layer framework is described for classification of network survivability techniques in telecommunication networks. These layers are physical, system, logical and service. In addition to providing a common basis for describing and comparing techniques, the framework identifies layer(s) responsible for reacting to the various types of failures and their interaction.

Techniques available to network providers to enhance the survivability of their telecommunications networks at each layer are described. Two basic approaches to compare survivability techniques and evaluate network survivability performance are given. The first approach (Given Occurrence of Failure or GOF) uses a conditional approach and defines survivability measures for a network assuming that given failures have occurred. The second approach (Random Occurrence of Failure or ROF) uses probability of network failure and, possibly, rates of repair and/or restoration, to calculate various measures of network unavailability or loss.

Suggestions are given for the general industry. Key suggestions are outlined here:

- measure service outages with the framework described herein,
- use the terminology defined herein for describing network survivability, including network reliability and network integrity,
- use the layered network survivability framework described herein for clarifying failure survivability analyses, objectives and methods,
- plan survivability jointly (e.g., interexchange carrier and exchange carrier interworking),
- use the performance measures defined herein to compare survivability techniques and to evaluate network survivability performance, and

Recommendations are also given for future standards work. Key recommendations are outlined here:

- better qualification of service outage categories,
- validation of traffic characteristics
- analysis of user expectations of network survivability performance, planning, engineering and operations guidelines for network survivability performance, and
- standardization of network survivability performance measures.

Through Art Reilly (Chairman, Committee T1), the SNS Committee has been tracking the progress on this work that is expected to provide valuable information on Network Survivability to the industry. Final approval of this Technical Report by Committee T1 is expected in mid-1993. Work is already underway on the areas identified for future work.

6.3.3 Internetwork Interoperability Test Plan

On September 12, 1991 the FCC hosted an inter-industry meeting on Network Reliability. Bellcore was asked to develop a proposal for CCS internetwork testing. In January 1992 the Exchange Carriers Standards Association sponsored Network Operations Forum chartered the Internetwork Interoperability Test Plan (IITP) Ad Hoc Committee. The proposal was implemented based on the industry's recommendations. The objectives were to provide a unique environment to enable SS7 service providers and suppliers to stress off-line networks as an additional means of assessing internetwork product reliability and interoperability in a multi- supplier, multi-carrier laboratory environment and facilitate identification and sharing of CCS network vulnerabilities with the industry. The first tests ("Phase 0") focused on stressing the networks to reflect potential live network failure conditions. These tests were accomplished by cooperatively interconnecting six carrier and supplier labs, using Bellcore's CCS Hub as a central connection and data collection point, to form a network of a LEC to IXC to LEC.

Phase 0 testing completed on September 4, 1992 and results were released December 1, 1992 (See Appendix 12 for Phase 0 Final Report). The highlights of this effort include:

- An intensive 4 week testing schedule to put the network through numerous tests stretching the limits of network integrity. This resulted in only two unexpected events with the potential to affect service. These events have been addressed by affected suppliers and carriers.
- A new level of cooperation was set between suppliers and carriers. Suppliers and carriers worked cooperatively to collect and analyze data and report on results.
- Reinforced confidence in the robustness of the network through recovery, no matter how stressful, from the test scripts
- Information sharing has migrated to a two

B

step process (1) real time notification of the event and (2) analysis/fix/corrective action

Phase 1 testing was completed on November 20, 1992 and the results are to be released by mid-year. The IITP continues to create test scenarios for testing in 1993. Three test windows have been identified for multi-carrier and multi-supplier internetwork testing: mid-May to Mid-June, August and October. Some Phase 0/1 tests will be repeated in a new configuration and Phases 2, 3 and 4 will also include several new tests now being developed. The information sharing process used in 1992 will be used again in 1993.

7.0 Metrics to measure effectiveness of solutions

7.1 Network Reliability Performance Monitoring

The SNS Committee recommends the Exchange Carriers Standards Association (ECSA) utilize the FCC's outage data collection (i.e., 30,000 or more customers affected for more than 30 minutes) as a high level metric, supported by an analytical process, as an indicator of network reliability performance. The SNS Data Analysis Team utilized the FCC reported outages as one source of data with several recommendations being made as a result.

This would assure the FCC, Members of Congress and other concerned parties that the Network Reliability gains made through the efforts of the NRC, NO REST and the Focus Teams are working, a process was established. A high level metric, supported by an analytical process, will provide a satisfactory indicator of network reliability performance. The FCC outage data would be utilized as the data source to formulate the metric. The form and substance of the analysis will be based on and aggregated along the lines of the seven focus areas such as the SNS Committee (See Appendix 13 for SNS Industry Network Reliability Initiatives Matrix). The SNS Data Analysis Team utilized, as reported earlier, the FCC reportable outages relating to signaling networks as one sources of data. These reports provided useful information and allowed for root cause analysis.

Reporting would be developed to reflect matters such as Technology disciplines, IXC versus LEC and overall trending. Data would be normalized and reported quarterly and annually.

This monitoring process mirrors the Process recommended earlier in Section 6.1.1 when the SNS Committee determined a need for Better Root Cause Analysis.

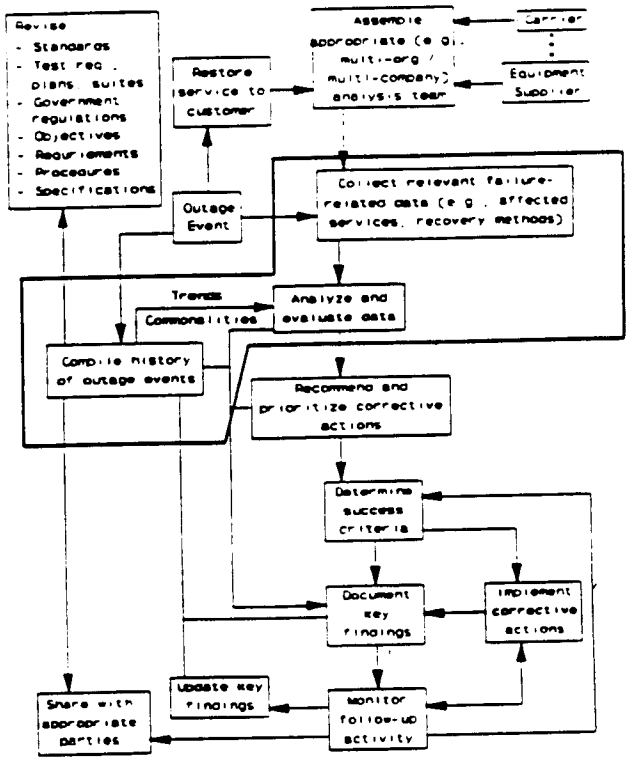


Figure 7-1

The outlined area in Figure 7-1 would be performed, at the national level, by the ECSA. That is, ECSA would:

- Collect relevant failure-related data
- Analyze and evaluate data
- Compile a history of outage events looking

B

for trends or commonalities and if indicated:

- Refer the matter to the appropriate forum for resolution.

7.2 Measure Scope, Duration & Impact of an Outage

The NOF and T1A1.2 are focusing on a UDE (Unavailability, Duration and Extent) based metric. The NOF has tabled its issue, #162, deferring this work to T1A1. T1A1.2 has identified this as a future activity (see section 6.3.2). The NOF will maintain an active liaison on this issue.

8.0 Path Forward

8.1 Network Architecture Evaluation - T1S1.3

The SNS Committee requested T1S1.3 to assess existing CCS network reference architectures and proposed alternatives. The architectures have been proposed in several industry forums. Additionally, a summary of T1S1.3's recommendations to enhance the SS7 protocol was requested (This was previously described in Section 6.3.1).

In an extremely short period of time this group presented the SNS Committee with an outstanding document. The SNS Committee believes this will serve as an invaluable tool and will be extremely beneficial to the industry as an implementation guide. The SNS Committee requested a supplement to the report to further maximize the benefit. This supplement contains additional detail on the impact on annual downtime for some of architectures evaluated.

The SNS Committee recommends future architectural proposals be reviewed by the appropriate Committee T1 working group, currently the T1S1.3 working group. T1S1.3 by virtue of its openness, due process and mission is well-positioned to accept this recommendation and continue the outstanding work it performed at the SNS' request. Special appreciation is extended to the leadership in T1S1.3 provided by Brian Foster (GTE-TeleOps) and Mike McGrew (AT&T) along with Andy Jacob (Bellcore, Editor T1S1.3 Report to SNS).

8.2 General Network Survivability Issues - T1A1.2

As mentioned earlier, the SNS Committee has been tracking the progress, through Art Reilly (Chairman, Committee T1) of T1A1.2's Technical Report on Network Survivability. Future work has been proposed and is already underway.

T1A1.2 focused its work to quickly provide general information on Network Survivability for the industry to support the work by the SNS Committee. The SNS appreciates these efforts especially the leadership provided to the T1A1.2 efforts by its editor Fred Kaudel (Northern Telecom, Inc.) and under the chairmanship of Ali Zolfaghari (Pacific Bell).

The SNS Committee recommends that future general network survivability issues be reviewed by the appropriate Committee T1 working group, currently T1A1.2. T1A1.2's future activities, referenced in Section 6.3.2, clearly reflect their commitment to network survivability.

8.3 Internetwork Interoperability Test Plan

The viability of this cooperative type of test development and execution has been proven through the efforts of the NOF IITP Committee. The IITP testing has also provided additional assurance on the completeness and implementation of industry generated Standards.

The IITP will continue to develop tests to be run three times in 1993. These tests will use industry-selected configurations of available carriers and supplier laboratories. In addition, it is expected that the publicly-available tests scripts developed by the IITP committee will be updated by individual companies, (to be reflective of their test configuration) and will continue to be used by them. These tests will continue to be run on an ongoing basis as new hardware and software are deployed and implemented

An Assessment has been prepared by Bellcore

(See Appendix 14 for IITP Assessment) that details areas of IITP success; areas where the industry has implemented improvements since the IITP's inception, and additional areas for consideration intended to further improve the response time and cost-effectiveness of this industry-wide testing. *Specific recommendations of the Bellcore Assessment that are supported by the SNS focus team are:*

- *Increased commitment of personnel and resources across the industry for IITP testing. While many companies have contributed to IITP activities, a limited number of companies have committed large quantities of resources to date in order to assure the IITP's success. This unfair burden has complicated and delayed the scheduling and execution of the tests.*

- *The IITP should continue development of test scripts to test the network under additional potential failure modes already identified by IITP and others resulting from outage analysis or other sources.*

- *The IITP should enhance the network integrity tests already developed to be more reflective of varied network conditions (e.g., traffic load) and revised Standards/requirements.*

- *The industry should establish a backbone network of dedicated transport facilities to accommodate post-mortem testing on demand without the lengthy start-up time involved in reestablishing a test network.*

In addition, the SNS focus team recommends:

- *The industry needs to identify a focal point for testing efforts. The efforts assumed by one company (Bellcore) in 1992, include providing an interconnection hub, editing test scripts, facilitating reporting, and providing administrative support. These responsibilities need to be assigned to assure long-term success.*

- *High-level support and direction are needed from all segments of the industry for continued IITP success. If an overseer committee is established to coordinate and provide direction to network integrity initiatives, it should include the NOF's IITP activity as one of those initiatives.*

- *The SNS recommends that the IITP testing be aligned with equipment suppliers schedules of new software releases. This would allow IITP testing to be scheduled immediately before field release, thereby assuring internetwork integrity testing as a part of products' development cycle.*

9.0 Conclusion

The SNS Committee began with an issue statement, supplied by Gary Handler, on June 30, 1992. The Committee developed a Vision and Mission statement and began brainstorming on how to improve network reliability in the signaling network. Massive amounts of outage data were reviewed from a variety of sources. Throughout the process we struggled with "this should not happen" because of the redundance and robustness of the CCS network and the SS7 protocol. Once the team overcame this and began listing "why outages/events did happen" we were able to make the recommendations in this Technical Paper. As stated earlier, the operation of the network has improved as a result of Common Channel Signaling. The network is running well and continuing to improve as carriers gain experience. The SNS Committee presented a number of recommendations addressing how to make the network even better.

A summary of the SNS Committee's recommendations and "Best Practices" presented in this paper are as follows:

SP/SSP Recommendations

Procedural Errors:

- *Inadvertent Maintenance of Redundant Active Units - To minimize human errors related to misidentification of active CCS units as failed units requiring repair, network service providers should conduct an "Awareness Training Program" for all maintenance persons who work on SP/SSP*

CCS equipment including the importance of end to end communications when maintenance is being performed. The training must emphasize the functionality, identification of active and alternate/redundant units and the network impact of failure of redundant equipment in link processors, link interfaces, link peripheral power suppliers, and other link related components.

In addition, architectural or design alternatives are possible and should be evaluated, initially, for large end offices (e.g., 30,000 lines or more), which will make links more robust to these types of errors during link maintenance (see T1S1.3 Architecture Evaluations). Some additional alternatives currently in use in the industry and presented here as "Best Practices" are:

- Two or more links per link set. With this design three or more simultaneous failures/errors must occur at the same time to cause a service interruption.

- While not specifically switch related, the use of dedicated DS1 facilities for links to reduce the frequency of procedural activity on links.

- Use of quad A-links, i.e., four diverse A-links to an SP

- *Scheduled Work Activities: While certain scheduled activity during business hours is necessary, these results indicate that a large proportion of CCS impacting business hour downtime may be avoided by carrier company scheduling of SP/SSP CCS related work activities during off hours. At a minimum, high risk, potentially service affecting maintenance and growth procedures should be scheduled during weekend and off-hours. Scheduling should also take into account the fact that if the procedure fails, and a significantly longer than expected outage occurs, it should not run into the business day. It is recommended that the methods, procedures and scheduling of these work activities be reviewed by a 2nd tier maintenance organization such as an Electronic Systems Assistance Center (ESAC). The SNS Committee further recommends that activities that may affect other network service providers must be coordinated, which includes both intra- and inter-carrier networks (See NOF Reference Document Section III, Installation and Maintenance - SS7 [sub-section 1.6, 2B, 2C, 3J]).*

Software:

- *CCS Related Recovery Software: It appears that increased emphasis is required by SP/SSP Manufacturers on improving the software which performs recovery tasks for CCS related functions that have been initiated by hardware failures. This result is consistent with the findings of the Switching Focus Team. The following specific recommendations are made which are consistent with those of the Switching Focus Team.*

  1. Software and hardware fault insertion testing (including simulating network faults such as massive link failures) should be performed as a standard part of a supplier's development process. Hardware failures and data errors should be tested and/or simulated to stress SS7 fault recovery software.

  2. Fault recovery actions that result in a loss of SS7 signaling functionality need to be reviewed periodically by SP/SSP manufacturers to assure that the least SS7 signaling impacting strategies are being used for classes of failures implicated during root cause analyses. For example, if a set of failure conditions resulted in a system initialization, that condition should be reviewed to determine if a system initialization of that level is appropriate.

  3. Initialization durations should be

optimized to minimize service impact. Given that a particular failure needs an initialization to recover, manufacturers can minimize the service impact by optimizing the design and execution of the initialization. Again, data from root cause analyses should be used to determine areas for investigation.

STP Recommendations

Recovery Software

- *A significant amount of STP downtime is associated with software faults uncovered during recovery actions from hardware failures. This is a similar finding related to recovery software for signaling functions as that observed in the SP/SSP analysis. It appears that increased emphasis is required by STP manufacturers on improving the software which performs recovery tasks that have been initiated by hardware failures. The specific recommendations made for SP/SSPs are repeated here for STPs.*

  1. Software and hardware fault insertion testing (including simulating network faults such as massive link failures) should be performed as a standard part of a supplier's development process. Hardware failures and data errors should be tested and/or simulated to stress SS7 fault recovery software.

  2. Fault recovery actions that result in a loss of SS7 signaling functionality need to be reviewed periodically by SP/SSP manufacturers to assure that the least SS7 signaling impacting strategies are being used for classes of failures implicated during root cause analyses. For example, if a set of failure conditions resulted in a system initialization, that condition should be reviewed to determine if a system initialization of that level is appropriate.

  3. Initialization durations should be optimized to minimize service impact. Given that a particular failure needs an initialization to recover, manufacturers can minimize the service impact by optimizing the design and execution of the initialization. Again, data from root cause analyses should be used to determine areas for investigation.

Procedural Downtime & STP Growth

- *A significant increase in the failure durations associated with procedural errors has been observed with no evidence of any increase in the rate of occurrence of procedural errors. This increase is correlated with the recent rapid growth of STPs and links in the network. It is recommended that network service providers consider the following actions to quickly train maintenance forces with insufficient levels of CCS expertise that must handle STP maintenance.*

  1. Determine the current levels of training for all maintenance personnel that will perform STP maintenance functions (See NOF Internetwork Interoperability).

  2. Each network service provider should establish a minimum set of courses and experience that are required before maintenance can work on STPs ("Best Practice" - See Appendix 5 for U S WEST training program developed for SCC Field Technicians and Control & Analysis Responsible for STP).

  3. Establish an aggressive training program to be completed within 6 months.

  4. As a "Best Practice" for training, CCS/SS7 courses, curriculums are available from each STP supplier [10][11][12][13] and Bellcore Technical Education Center.[14]

SCP Recommendations

Power

- *SCP owner and operators should have planned evaluations of the UPS for each SCP site. They should also schedule periodic maintenance and testing of UPSs to ensure functionality when needed.*

- *"Best Practice" - Several carriers on the SNS Team recommended that SCPs be placed in a "Central Office (CO) environment." The carriers indicated that the existing CO design criteria (including power, fire, etc., that exist in documents such as Network Equipment Building Systems (NEBS)[16]), CO operations procedures and availability of maintenance personnel would generally enhance reliability performance of these systems. NOTE: This is not suggesting that SCPs should be taken out of "computer conditioned space", but ideally placed in concert with a "CO environment".*

Recommendations based on (but not limited to) FCC reportable outages - SS7 related

A-Link Diversity;

- *It is apparent that the diversity of A-links needs to be ensured, since the above data had twice as many events where an office was isolated (and caused an FCC reportable event) due to a single link-affecting failure than from two failures on the independent hardware associated with each link. Section 6 contains recommendations and best practices for maintaining link diversity.*

SP/SSP Recovery Software:

- *It is also clear from the above data that the switching system software fault tolerance needs to be enhanced to aid in the recovery process. Since the number of events in the above data is small, it is difficult to pinpoint the specific areas/problems for which software fault tolerance needs to be increased. The "Switching System Focus Group (specifically the Software Subteam)" also identified the need for enhanced software design to increase the fault tolerance of switching software to problems such as data corruption (see Section 4.1.2 of their report). Thus, we would like to reiterate the following specific recommendations made by the switching system software sub-team:*

  - Suppliers should enhance design and code inspections to increase software fault tolerance (See Section 4.1.2 of the Switching System Software Report).

  - Suppliers should perform software fault insertion testing, with faults inserted in data and in programs (See Section 4.1.5 of the Switching System Software Report).

Procedural Errors:

- *Finally, the data above indicates a need for improvement related to reducing the number of procedural errors. The Switching System Focus Group (Procedures Subteam) identified four main sub-problems in their study, of which two were also identified as sub-problems in the FCC reports; failure to follow the correct hardware maintenance procedures (including mislabeling and removing the wrong unit from service) and data entry errors (See analysis section of Switching System Telco procedures subteam report). For these subcauses, the procedures subteam recommends (and thus, the SNS Data Team) manufacturers place an added focus on human factors design to eliminate these types of failures.*

Recommendations to Prevent Long Duration Events

- *SP/SSP rehome activities appear to carry a high risk factor in that they can result in long outages when performed incorrectly. A similar situation exists for hardware and software expansion. It is recommended network service providers carefully review*

all rehome procedures and undertake meticulous pre-planning before execution. Communication to all inter-connected networks will be essential for success in the future. It is also important to make sure that rehome procedures are carefully followed.

- *In some cases detection and manual intervention to assist recovery was slow. This suggests that network operators should be adequately trained in (1) detection of conditions requiring intervention, (2) escalation procedures and (3) manual recovery techniques.*

- *Lack of troubleshooting experience and proper training in this area usually prolongs the trouble detection and isolation process. It is recommended that network operators be adequately trained in the trouble detection and isolation process.*

- *Failures related to a lack of link diversity can cause long outages depending on the ability to either correct the problem or switch to other transmission facilities. The ability to maintain link diversity is also important and is discussed in more detail in Section 6.*

- *The data shows that outages caused by procedural errors that occurred during maintenance activities of power equipment were associated with long recovery times. There is no single solution to this problem because the data did not indicate a single root cause. However, better training in power equipment maintenance activities and emphasis on the importance of CCS network equipment should be considered by network service providers.*

Additional Recommendations based on Industry Data Analysis

- *Failure Data Collection and Root Cause Analysis - The team recommends that carriers and suppliers improve their own failure data collection and analysis procedures for better root cause analysis. Carriers and suppliers should form partnerships to jointly perform these analyses. Section 6 of this report defines a "Root Cause Analysis Process" that the team developed along with references to a number of industry "Best Practices."*

- *Signaling Information Sharing - The team recommends that the industry improve its information sharing between all industry segments, specifically between carriers and their suppliers of signaling systems. Section 6 of this report provides the status of recent industry efforts in the NOF to improve signaling outage information sharing.*

Trunk Integrated Records Keeping System (TIRKS) Recommendations

Facility and Equipment Hierarchy Report (FEHR) allows comparison of up to three circuits. This report compiles facility assignments "up" the hierarchy. It also compiles equipment assignments by looking at the equipment posted to each level of the facility hierarchy. This is the only TIRKS output which provides all of the TIRKS inventoried facility and equipment associated with a given circuit. The intersection summary portion of this report provides the common facilities and equipment (lack of diversity). TIRKS does not automatically provide notification to the user when CCS link diversity is violated. The user must manually review the report.

The SNS Committee recommends that Bellcore evaluate the following enhancements to TIRKS:

- *Facility and Equipment Hierarchy Report (FEHR) today can only look at in-effect and pending add circuits. Enhance this report so that it can also look at rearranges*

- *Enhance flow-through to accept PDAC as an optional FID (Use of system specific PDACs will specify diverse routes). Allow the*

B

system specific PDACs to process on FEHR so the planner can "test" the routing prior to the assignments being posted in inventory.

- *Develop a report so that when a planner is considering a facility removal at any level, a list of diverse circuits can be obtained. Additionally generate a report so that when a planner is considering an equipment bay removal a list of diverse circuits can be obtained.*

Crisis Management Exercises

- *The SNS Committee recommends that network service providers, as a "Best Practice", develop crisis management exercises to become better prepared in the event a disaster strikes.*

Network Reliability Performance Monitoring

- *The SNS Committee recommends the Exchange Carriers Standards Association (ECSA) utilize the FCC's outage data collection (i.e., 30,000 or more customers affected for more than 30 minutes) as a high level metric, supported by an analytical process, as an indicator of network reliability performance.*

Network Architecture Evaluation Recommendation

- *The SNS Committee recommends future architectural proposals be reviewed by the appropriate Committee T1 working group, currently the T1S1.3 working group.*

General Network Survivability Issues Recommendation

- *The SNS Committee recommends that future general network survivability issues be reviewed by the appropriate Committee T1 working group, currently T1A1.2.*

Internetwork Interoperability Test Plan Recommendation

- *The IITP is an industry-wide verification program that has interconnected equipment from U.S. carriers, both local and interexchange, as well as equipment suppliers, to demonstrate and test interoperability. This national verification activity continues to help assure interoperability. The SNS Committee recommends that this activity should be continued on an ongoing basis.*

- *Increased commitment of personnel and resources across the industry for IITP testing.*

- *The IITP should continue development of test scripts to test the network under additional potential failure modes already identified by IITP and others resulting from outage analysis or other sources.*

- *The IITP should enhance the network integrity tests already developed to be more reflective of varied network conditions (e.g., traffic load) and revised Standards/requirements.*

- *The industry should establish a backbone network of dedicated transport facilities to accommodate post-mortem testing on demand without the lengthy start-up time involved in reestablishing a test network.*

- *The scripts developed by the IITP should continue to be used in other stand-alone or bi-lateral testing and results should be reported to the industry via the IITP, in accordance with established NOF Information Sharing Guidelines.*

- *The industry needs to identify a focal point for testing efforts. These responsibilities need to be assigned to assure long-term*

success.

- *High-level support and direction are needed from all segments of the industry for continued IITP success. If an overseer committee is established to coordinate and provide direction to network integrity initiatives. It should include the NOF's IITP activity as one of those initiatives.*

- *The SNS recommends that equipment suppliers align schedules of new software releases.*

10.0 Acknowledgements

The Signaling Network Systems Committee would like to extend their sincerest appreciation to the following individuals/companies for the time and effort dedicated to this project.

- Industry Single Points of Contact and the individuals behind them who actually gathered the data. The SNS Committee recognized that to make meaningful recommendations data must be collected from the industry. The SNS Committee's recommendations are based largely on the invaluable data supplied by the NRC participating companies.

- Massive amounts of data had to be aggregated and then presented in a form that engineers could understand. Eric Tollar (Bellcore) and Chao-Ming Liu (Bellcore) are to be commended for the speed in which they presented the committee with the statistical analysis, but also for their patience in dealing with non-mathematicians (They started with: Pareto is pronounced Pa-re-toe not Pare-to).

- Part of the SNS Committee's vision was to utilize existing industry forums where possible to fulfil our mission. Art Reilly (Chairman, Committee T1) provided the group with excellent recommendations on how to best utilize the resources of Committee T1. Once the work was commissioned, Art provided monthly status reports on the outstanding work at both T1S1.3 and T1A1.2. Art proved to be an invaluable resource without which the team would likely have fallen short of realizing our vision.

- Outage Information Sharing is one example of the essential work being conducted at the Network Operations Forum (NOF). In many instances a committee member would make a proposal and Rick Harrison (Moderator, NOF) would explain that work was either under way or already addressed by the NOF. The SNS Committee extends their appreciation to Rick Harrison and the NOF, in particular the Outage Information Sharing work group for their exceptional work.

- As the saying goes, last but certainly not least - The Signaling Network Systems Committee rolled their sleeves up on June 30, 1992 and began working. When volunteers were needed for a sub-team, there was never any silence. Those who were not on the particular team provided coaching at the monthly SNS Committee meetings. John Seazholtz summed it up best when he said "In my 30 years in the Telecommunications Industry, I have never seen teamwork like this." Individual companies, including competitors worked together to enhance network reliability. Special appreciation is extended to Rich Baseil and Clint Hamilton for their relentless effort in keeping the group focused and aligned with the original issue statement.

11.0 References

1. "Network Switching Element Outage performance Monitoring Procedures" Bellcore Special Report, SR-TSY-000963, Issue 1, April 1989.

2. "Process Quality Management & Improvement Guidelines," AT&T, Issue

B

1.1, 1988.

3. "CCS Network Outages in Bell Atlantic and Pacific Bell, June 10 through July 2, 1991," Bellcore Special Report, SR-NWT-002149, Issue 1, November 1991.

4. "Signaling Transfer Point (STP) Generic Requirements," Bellcore Technical Reference TR-NWT-000082, Issue 4, December 1992.

5. "Bell Communications Research Specification of Signaling System No. 7," Bellcore TR-NWT-000246, Issue 2, Revision 2, December 1992.

6. "CCS Network Interface Specification," Bellcore Technical Reference, TA-TSV-000905, Issue 3, December 1992.

7. "Signaling System 7 (SS7) Protocol - Message Transfer Part (MTP)," ANSI Standard T1.111, 1988.

8. "Reliability - LATA Switching Systems Generic Requirements (LSSGR) Section 12," Bellcore TR-TSY-000512, Issue 3, February 1990.

9. "Signaling Transfer Point (STP) Generic Requirements," Bellcore Technical Reference TR-NWT-000082, Issue 4, December 1992.

10. "AT&T '93 Product Training Catalog," AT&T Product Training Services, 5151 Blazer Memorial Parkway, Dublin, OH 43018-8100.

11. "DSC Technical Education," DSC Communications Corporation, 1000 Coit Road MS-955, Plano, TX 75075.

12. "Ericsson Network Systems Technical Training Course Catalog," Ericsson Network Systems, Inc., 730 International Parkway, Richardson, TX 75082-3875.

13. "1993 Technical Education Course Catalog," Northern Telecom, Sales & Marketing Information Center, Department 4254, PO Box 13010, Research Triangle Park, NC 27709-3010.

14. "1993 Bellcore TEC Training Catalog," Bellcore TEC, 6200 Route 53, Lisle, IL 60532, Issue 7, December 1992.

15. "Service Control Point Node Generic Requirements for IN1," Bellcore Technical Reference, TR-NWT-000029, Issue 1, September 1990.

16. "Network Equipment-Building System Generic Equipment Requirements," Bellcore Technical Reference, TR-EOP-000063, Issue 4, July 1991.

17. "Network Switching Element Outage Performance Monitoring Procedures" Bellcore Special Report, SR-TSY-000963, Issue 1, April 1989.

18. Draft Report on Adoption of a Formal Root Cause Analysis Process from the NRC Switching Committee's Software Design Team, January 14, 1993.

19. "Hardware Reliability Assurance Program (H-RAP) Generic Requirements for Telecommunications Products," Bellcore Technical Advisory, TA-NWT-000942, September 1991.

20. Final Recommendation of the Threshold Reporting Group of the Network Reliability Council, December 15, 1992.

12.0 Appendix

1 - Issue Statement
2 - Data Request - Questionnaire: Carriers
3 - Data Request - Questionnaire: Suppliers
4 - Data Request - Questionnaire: Network Element Population Request Form
5 - U S WEST Training Program Example
6 - NOF Information Exchange

7 - BellSouth Diversity Checklist
8 - AT&T Diversity Requirements for CCS7 Network Interconnect
9 - NYNEX Condition Red Procedures
10 - NOF Emergency Network Restoration Plans
11 - Contribution T1S1.3/93-02113: Signaling Network Systems (SNS) Committee Prioritization of Recent Protocol Enhancements (MTP/OMAP)
12 - IITP Phase 0 Final Report
13 - SNS Industry Network Reliability Initiatives Matrix
14 - IITP Assessment

B