1. Executive Summary

The nationwide Public Switched Telecommunications Network (PSTN) has become, over the years, a highly available and reliable communications medium for a wide range of communications services; voice, data and visual. Statistically, the PSTN, comprising over 20,000 switching systems [Reference 1] averages greater than 99.99% availability [Reference 2]. Nevertheless, the network can experience occasional outages that may create unsatisfactory service conditions for customers, even if only temporarily.

In November 1991, the Network Reliability Council (NRC) was formed by the Federal Communications Commission (FCC) as a federal advisory committee on telecommunications that "would bring together leaders of the telecommunications industry and telecommunications experts from academic and consumer organizations to explore and recommend measures that will enhance network reliability" [Reference 3]. The NRC designated the Network Reliability Steering Team (NO REST) to coordinate the various NRC efforts, including seven focus areas studying specific areas of network reliability.

The Switching System Focus Area (SSFA) was charged with investigating the role of software in the reliability of current switching systems. The nature of the task assigned to the SSFA was to focus on problems and identify solutions that would result in improvements in an already highly reliable network. The analysis did not incorporate other aspects of switching system design such as cost, increase in functionality, etc. The SSFA used the 7-Step Quality Improvement Story Framework [Reference 4] to guide the efforts of the group.

The Switching System Focus Area (SSFA) Team included representatives from service providers, users, and all major switch suppliers. The SSFA was chaired by Will Smith, Senior Vice President and Chief Information & Technology Officer, U S WEST. The NO REST advisor, or champion, for SSFA was Mick McCarthy, Senior Vice President of Service Management, Sprint. Throughout the course of the focus area's efforts, Bellcore Subject Matter Experts performed data aggregation and analysis on behalf of the focus area, and provided guidance and assistance to the sub teams on an as needed basis.

The NRC designated Bellcore as the central point for requesting, collecting, compiling and aggregating data for all focus area teams. Bellcore also assisted the SSFA in determining the scope of the team's data request, designing the content and format and participating in the analysis of the data collected. The data request was issued to the industry single points of contact identified to the NRC.

Through analysis of the data, the SSFA identified four major contributors to switch outages. The major contributors are procedural errors, scheduled events/retrofits, hardware failure and software design. Four sub teams were formed to study these areas in greater detail. The sub teams analyzed available data, as well as data collected through the SSFA data request. Countermeasures to address the frequency and duration of outages in current network the were identified.

Recognizing that the evolving technology of future network configurations may present new issues with respect to ensuring reliability, a fifth sub team was formed to address future network configurations. Finally, the issue of network congestion was addressed. While infrequent, the effects of congestion in the PSTN can be far reaching.

A number of conclusions and key recommendations were identified and became recurring themes across various aspects of switching technology and performance as the group studied outage data and ascertained countermeasures aimed at improving overall switched network reliability.

The major themes and recommendations are as follows:

- In each of the areas studied, there are opportunities for individual service providers and system suppliers to reduce outage frequency and duration.

- The FCC Threshold Report should serve as a indicator of overall switching system reliability.

- An industry manager should collect the outage reports and perfrom quarterly and annual macro

C

analysis of the data. The Exchange Carriers Standards Association (ECSA) is an existing industry organization that is well suited to perform this function.

- Service providers should standardize the process of capturing and reporting timely and complete data on switch outages and share the outage information with system suppliers.

- Should the analysis of the FCC Threshold Reports indicate a downward trend in switching system reliability, the ECSA will determine the need for more specific outage data and further actions. Service providers and systems suppliers should be prepared to submit additional outage data as requested.

- A wide-ranging set of reliability standards and specifications should be developed and made available for use by industry participants, service providers and system suppliers alike.

The FCC's Threshold Report has been chosen by the NRC as the macro level overall indicator of network reliability. It was the task of the SSFA to identify quality indicators for its focus area that, when improved, will lead to improvement in the FCC Threshold Report indicator. The SSFA recommends that the ECSA analysis of the Threshold Report data concentrate on the following quality indicators:

- number of outages/switch/year, for all switches
- duration/outage, for all switches
- lines impacted/outage, for end office switches only

2. Background

In November 1991, the Network Reliability Council (NRC) was formed by the Federal Communications Commission (FCC) as a federal advisory committee on telecommunications that "would bring together leaders of the telecommunications industry and telecommunications experts from academic and consumer organizations to explore and recommend measures that will enhance network reliability" [Reference 3]. The NRC, in turn, formed the Network Reliability Council Steering Committee (NO-REST) to coordinate various NRC efforts.

The NRC, at its April 29, 1992 meeting, identified seven network areas with reliability issues of the highest priority and established seven Focus Area teams to examine these issues in greater depth. The Focus Areas were as follows: E911 Systems, Fire Prevention, Digital Cross-connect Systems, Fiber Cable Systems, Power Systems, Signaling Network Systems and Switching Systems. The NRC also formed the Mutual Aid and Restoration Group to compile a compendium of current knowledge and information on the subject, and the Threshold Reporting Group to provide recommendations on the Threshold Reporting process instituted in FCC Docket 91-273.

NO REST tasked the seven Focus Areas to analyze the existing data, collect additional data, determine root causes, recommend effective industry countermeasures for dealing with the root causes, and develop metrics to measure effectiveness of the recommendations by means of a total quality process. Details regarding each Focus Area's task are found in NRC Issue Statements pertaining to each focus area. Each Issue Statement was written by a NO REST member who was in turn designated as the "champion", or mentor, for the Focus Area. Appendix A contains the Issue Statement for the Switching System Focus Area as provided by NO REST.

2.1. Focus Area Motivation

As noted in Section 1, the PSTN averages greater than 99.99% availability [Reference 2]. Nevertheless, the network can experience occasional outages that can create unsatisfactory service conditions for customers, even if only temporarily.

It is also necessary to recognize that the PSTN is technologically a highly complex, multi-component system constructed of network elements manufactured by a variety of system suppliers and operated by a number of interconnected service providers. There are well over 20,000 switching systems of over 15 types [Reference 1] in operation in the U.S. Therefore, drawing conclusions from the varied and often less than complete data available requires expert analysis.

As shown in the NRC's issue statement, a Bellcore study of 346 switching outage events over a nine

C

month period during 1991 indicated 47% of all outages were the result of software design and/or software release installation and maintenance activities. While initial analysis of these and other available data indicated that software is a major contributor to switching outages, the NRC instructed the SSFA to collect and analyze all available data and confirm or dispute this assumption.

The SSFA was tasked to study existing switching system outage data, with emphasis on software. The SSFA decided to include hardware related outages in order to identify opportunities for the use of software solutions to hardware reliability issues. The nature of the task assigned to the SSFA was to focus on problems and identify solutions that would result in improvements in an already highly reliable network. The analysis did not incorporate other aspects of switching system design such as cost, increase in functionality, etc.

The scope of the SSFA's study includes local, toll, packet, cellular, data, end-office and tandem switches. It also includes adjunct processors and Service Control Points (SCPs). Furthermore, the team has looked at both current and future network configurations. After discussion among NO REST, NRC and focus area team members, it was agreed that the scope of the SSFA's work would not include Signal Transfer Points (STPs) or Digital Cross-connect Systems (DCSs), because they are in the realm of the Signaling Network Systems (SS7) and Digital Cross-connect Systems focus areas, respectively.

In some sections of this report recommendations will be made for industry action. References to "the industry" are generic and do not indicate or imply any forum, association, etc. The SSFA believes that there are various organizations where implementation actions suggested in this report can be initiated and expects that participants in "the industry" will take appropriate actions.

2.2. Organization of Paper

Section 1 provides an overview and summarizes key messages for this report.

Section 2 provides background as to why this focus area was studied.

Section 3 describes the organization of the team responsible for this report, and identifies team members.

Section 4 describes the methodology used to obtain failure data. It also describes the mechanics of the data collection process and the analytic process used to derive conclusions.

Section 5 discusses the types of failures revealed by the data and provides a statistical breakdown, including graphical depiction, of the significant causes. This section also defines each significant cause in depth and provides information on the root causes.

Section 6 summarizes the key learnings and recommends effective countermeasures.

Section 7 describes the metrics proposed for measuring the effectiveness of recommended solutions.

Section 8 discusses recommendations for how the focus area work can be sustained.

Section 9 provides concluding remarks.

Section 10 lists acknowledgments.

Section 11 lists references used in writing this paper.

Section 12 contains all figures referred to in this paper.

Appendix A is the NRC Issue Statement. Appendix B contains the Switching System Focus Area Data Request Questionnaire.

3. Team Membership

The Switching System Focus Area (SSFA) Team included representatives from service providers, users, and all major switch suppliers. Representatives were selected based on their expertise in the area of switching system reliability. In addition, a representative of the Communications Workers of America was kept informed throughout the course of the SSFA efforts. This representation ensured that all stakeholders impacted by system outages were adequately represented. As sub teams were formed

C

to study specific topics, focus area members provided additional subject matter experts from their organizations to staff the sub teams.

3.1. Focus Area Membership

The SSFA was chaired by Will Smith, Senior Vice President and Chief Information & Technology Officer, U S WEST. He was assisted by Larry Kappel, Emily Brooks and Jaye Matthews, also of U S WEST.

The NO REST champion for SSFA was Mick McCarthy, Senior Vice President, Network Organization, Sprint. He provided the group with advice and counsel on questions and concerns that have been raised during the process of data collection, analysis and reporting.

SSFA members were as follows:

John Beagley	Northern Telecom
Ed Bonkowski	Advantis
Emily Brooks	U S WEST
Roshan Chaddha	Bellcore
John Chiang	GTE Mobilnet
Deborah Elsinger	Bellcore
Stu Heffernan	GTE Mobilnet
Peter Jackson	Digital Switch Communications
Bill Jones	AT&T Network Systems
Larry Kappel	U S WEST
Jerry Lind	Siemens Stromberg-Carlson
John O'Rourke	Hewlett Packard
Bo Ohlsson	Ericsson
Dennis Schnack	Sprint
Ken Walling	Pacific Bell
Albert Wood	New York Clearing House

Throughout the course of the focus area's efforts, Bellcore Subject Matter Experts performed data aggregation and analysis on behalf of the focus area, and provided guidance and assistance to the sub teams on an as needed basis. The Bellcore representatives supporting the SSFA were:

Walt Akstulewicz	Ari Jain
Walt Burns	Yana Kane-Esrig
Stu Freidlin	Ming Lai
John Healy	Yang-Wei Wang

3.2. Sub Team Membership

The SSFA used the initial analysis of available Bellcore outage data to guide the formation of sub teams to further study the four major causes in more depth.

The Telco Procedures sub team studied the data regarding all failures classified as caused by procedural errors. Ken Walling (Pacific Bell) chaired the group, which also included the following:

Bill Byard	Ericsson
John Chiang	GTE
Ross Marturano	Northern Telecom
Mark Young	Siemens Stromberg-Carlson

The Scheduled Events & Retrofits sub team examined the outage data concerned with scheduled events/retrofits performed by service providers and system suppliers. Albert Wood (New York Clearing House) chaired this team, and other members included:

Ed Bonkowski	Advantis
Roshan Chadda	Bellcore
Bob Dillon	Northern Telecom
Scott Downs	Ericsson
Tim Dusing	AT&T
Jim Gauthier	New York Telephone
Bill Lee	Siemens Stromberg-Carlson

The Hardware sub team reviewed the data regarding outages attributed to hardware failures. The group was chaired by Bill Jones (AT&T), and included the following members:

Walt Akstulewicz	Bellcore
Elwyn Grant	DSC Communications
Ron Hershberger	Ericsson
John Stewart	Northern Telecom
John Welch	Siemens Stromberg-Carlson

The Software sub team examined the data covering outages described as due to software design. The team was chaired by Jerry Lind (Siemens Stromberg-Carlson). Other members included:

John Beagley	Northern Telecom
John Chiang	GTE Mobilnet
Peter Jackson	Digital Switch Communications

C

Ming Lai Bellcore
Abdel Moharram Ericsson
Dennis Schnack Sprint

A fifth sub team, the Future Network sub team, was also created. This group projected the impact of vulnerabilities of possible future network configurations and the impact of new technologies on the network. This sub team was chaired by Deborah Elsinger (Bellcore). Other members were:

Siva Ananmalay Bell Northern Research
Ed Bonkowski Advantis
Susan Einbinder Bellcore
Stu Heffernan GTE
Gary Herman Bellcore
Bill Jones AT&T
Ming Lai Bellcore
Bob Lund U S WEST
Ross Marturano Northern Telecom
John O'Rourke Hewlett Packard
Larry Schessel Siemens Stromberg-Carlson
Albert Wood New York Clearing House

4. Data Collection and Analysis Methodology

The NRC designated Bellcore as the central point for requesting, collecting, compiling and aggregating data for all focus area teams. All data provided to Bellcore was protected under a non-disclosure agreement. The data were treated as proprietary information, and specific references to individual service providers, central offices, or system suppliers were removed during the aggregation process. Each focus area defined its own data needs.

The Switching System Focus Area (SSFA) started the data collection and analysis process by reviewing existing outage data reported to Bellcore during the first half of 1992. These outage data were primarily provided by three service providers independently of the NRC efforts. All the outage data were provided in the format of "Service Failure Analysis Reports (SFARs)" specified in Bellcore's Special Report entitled "Network Switching Element Outage Performance Monitoring Procedures" (SR-TSY-000963, Issue 1. April 1989). The SFARs were used by the reporting service providers to document the facts and circumstances involved in the outage, the duration and effect on service of the outage, the cause of the outage, and corrective or preventive actions to be taken by involved parties in response to the outage.

After reviewing the existing outage data (see Figure 1), the SSFA decided to form four sub teams with each sub team focusing on one of the four major contributors to these outages as identified from the data. The four major contributors are: (1) Procedural Errors, (2) Hardware Failures, (3) Software Design, and (4) Scheduled Event and Retrofits. To validate the sub teams' initial findings and obtain specific information pertaining to certain types of outages, several sub teams made additional requests for outage data from a wider source, including local and inter-exchange service providers and switching system suppliers. As a result, two data requests were issued separately to the service provider community and the system supplier community.

Bellcore assisted the SSFA in determining the scope of the data request and designing the content and format. The mechanism for collecting the additional outage data was based on the SFAR form, with modifications that requested pertinent information sought by the sub teams. Appendix B contains the data requests issued to the service providers and system suppliers. The data request was issued to the industry single points of contact identified to the NRC.

The SSFA used the following definition of "total outage" in the Data Requests:

> A total outage occurs when the switching system
> 1) loses either originating or terminating services to all its lines,
> 2) loses either incoming or outgoing traffic to all its trunks,
> 3) loses all stable calls, or
> 4) loses CCS signaling capability when the system uses the CCS network to set up inter-switch connections for user traffic.
>
> Outages that did not satisfy any of the above criteria were considered partial outages.

The SSFA Data Request was issued on October 5, 1992. A total of 12 service providers and 6 system suppliers responded with information on more than 5000 outage incidents. Over 90% of these incidents were provided by service providers. Figure 2

C

represents 2Q-3Q1992 outages collected via the data request that were 1 minute or longer in duration and and impacted 1000 or more lines.

All the outage incidents were entered into Bellcore outage data bases made available for the NRC efforts, then reviewed and analyzed by Bellcore analysts. Based on the specific interests of the sub teams, the aggregated results were provided to individual sub teams which made the original requests. These results were used as inputs to the sub teams' efforts in identifying the root causes of outages, proposing effective countermeasures and recommendations to reduce the frequency as well as impact of outages, and establishing long term goals to further improve the reliability performance of switching systems.

Each sub team determined what views of both the existing Bellcore data and the new data collected via the SSFA Data Requests would best enable evaluation of the specific outage areas. The details of the data analysis are provided in Section 5.

5. Types and Causes of Outages

This section presents in-depth analyses of the four major contributors of switching system outages as identified by the outage data. The major contributors are procedural errors, scheduled events/retrofits, hardware failure and software design. Each of these areas is discussed in Sections 5.1 to 5.4, respectively.

Recognizing that future network configurations may present new issues with respect to ensuring reliability, a fifth sub team was formed to address future network configurations. The findings of this sub team are presented in Section 5.5.

Finally, the issue of network congestion was addressed. While infrequent, the effects of congestion in the PSTN can be far reaching. Section 5.6 presents the results of the focus area's study of network congestion outages.

The sub teams used the initial data provided by Bellcore to identify preliminary root causes and determine what additional data would be collected through the process described in Section 4. A common finding across the sub teams was the lack of outage root cause information, in both the initial data provided by Bellcore and the new data collected through the data request process. Each sub team identified this lack of information as a limitation in performing a thorough analysis of the data. Consequently, the recommendations presented address data collection and root cause analysis processes.

5.1 Telco Procedures

As shown in Figure 1, switch outage data collected by Bellcore for the first six months of 1992, Telco Procedural errors account for ten percent of all reported outages and are the second largest contributor to partial outages. In addition, failures classified as "Procedural Telco" have the highest average downtime per incident. In a separate Bellcore study of outages reported to the FCC under the Threshold Reporting Process (i.e., outages affecting more than 30,000 lines for more than 30 minutes) during the period from April 4, 1992 to August 3, 1992, Telco Procedures accounted for 26 percent of the switch related incidents.

A detailed review and analysis was performed on end office switching failures reported to Bellcore during the first six months of 1992 that were classified as caused by telephone company procedural errors. These data included 99 separate incidents collected from several service providers and generated from switching systems manufactured from several suppliers. The outages were first analyzed by time of day to ascertain any relationship to scheduled activities, scheduling of personnel, or system load or capacity. Analysis by duration of outage and by type of failing equipment was performed in an attempt to identify unique patterns of outage. The connection of outages to specific types of activity was also investigated.

In an attempt to obtain definitive failure and root cause information, a data request was issued for all outages with a duration of 10 minutes or longer that occurred in the third quarter of 1992 and any failure reported to the FCC under the new FCC reporting requirements. There were 163 additional Telco Procedural outage reports from 11 service providers and five system providers collected and reviewed.

Because of the similarity of the events reported in both the initial and subsequent data requests, the data were first analyzed separately and then

C

combined. The combined analysis is included in this report.

5.1.1. Outage Analysis and Causes

Figure 3 provides the analysis of switch outage by time of day. The lowest number of procedural errors were reported from 1600 to 2200 hours. There was a high incident of failure between 2300 and 0400 hours. This high rate is due to the scheduling of critical activities during this period of low calling volume. These failures occurred during software change activities, hardware growth, and maintenance procedures. The low incident of failure from 0500 to 0700 hours was evaluated as cessation of critical activity in preparation for the morning call volume increase. The peak between 0800 and 1000 hours appears to be the result of activities performed during the early morning hours or critical activities that were not completed during the light traffic period. No other pattern by time of day was apparent.

Several questions are suggested by the analysis presented in Figure 3. Additional information is needed to make conclusions, however SSFA expertise provides insight.

Are the personnel that work between the 2300 and 0800 hours of a lower skill level, or is the work performed on this shift the primary factor? The primary contributing factor might be the nature of activity occurring during these hours. Is the rate of failure between 0800 and 1000 hours a result of scheduling critical activities during the incorrect time period? This may be partially true. Translation changes and maintenance activity at the start of shifts could be the cause.

Why is there a large difference between the 1900 - 2200 hours and the 2200 - 0000 hours error rates? The 1900-2200 hours period may be a time of preparation for critical activities that will be performed during the light traffic period. Therefore, a lower level of activity in the switch equates to a lower level of failure.

An evaluation by duration of failure (see Figure 4) indicated that there was a high rate of both total and partial short duration failures. The reporting process used to gather this information places emphasis on failures with two minutes or more duration. The data request collected data on failures of 10 minutes or longer duration. It is believed that there could be a much higher number of less than two minute failures than were reported.

An analysis of total outages, represented by Figure 5, indicated that power problems, failure to follow generic program change procedures and improper maintenance procedures were the primary causes of total outages lasting more than 30 minutes. Performing improper maintenance procedures, e.g., forcing failing equipment active, pulling circuit pack from active unit, unconditionally restoring a failing unit, etc., was the major cause of long duration outages and the primary cause of short duration outages. Translation input error is a common cause of reported total system outages. Based on the information provided around these incidents it is believed that the majority of the translation failures were really partial, not total, system outages. Incorrect office parameters were a major cause of short duration total system outages. Most of these failures are the result of an initialization of the switch to activate a new parameter.

Figure 6 illustrates partial outages by duration. By far, translation input error was the largest cause of long duration partial outages. Improper maintenance procedures were identified as the biggest single cause of partial system failures. Power related failure was also identified as a cause of partial system failure.

This analysis of the failure reports suggests three classes of system failure. The first is a failure duration of from zero to five minutes where the switch was manually initialized or it identified the problem and automatically recovered. The second is a duration of five to 20 minutes, where the switch could not recover but manual action successfully invoked recovery. The third, over 20 minutes, occurred where neither the system nor manual action was able to precipitate recovery. This third type of failure required additional investigation before successful recovery. Failures that fell into this category included: loss of power, shorted pins in the back plane, software retrofit procedures not followed, circuit pack removed from the on-line central processor, translation or office parameter errors, forcing a failed unit active, and not applying corrections to known software errors. Each of these conditions placed the system in a state where the normal recovery process was ineffective or inoperable.

C

An evaluation by the failing switch component (Figure 7) indicated that failures were not concentrated in any part of the switch. About 40 percent of the failures were in the central control units and another 40 percent in the peripheral equipment. When reviewed as a specific component, the SS7 units contributed another 10 percent of the failures.

Two factors contributing to the SS7 failures are suggested. First, SS7 is a new technology and it is being installed in many locations for the first time. Errors in manufacturing, implementation and design are still being identified and the technical knowledge level of personnel installing or maintaining this new equipment has not reached the optimum level. Second, because of the interactive nature of this technology, administration and management of SS7 networks are more complicated. There has been a change from a network of individual and mainly isolated intelligent network elements to a network of multiple intelligent switching and signaling network elements interacting in real time. The increasing complexity of the network and network interaction causes it to be nearly impossible to completely test all possible interactions in a laboratory environment. The current design limitations may be human factors and neither hardware nor software.

Finally, the data were evaluated by the type of action being performed when the system failed (see Figure 8). Operating procedures accounted for 45 percent of the failures. Procedural errors while performing hardware maintenance accounted for 22 percent of the failures. Another main cause of failure, accounting for 16 percent, was data entry. The last major category of failure which accounted for eight percent of the failures was forcing unnecessary system initializations or forcing a higher level recovery than necessary. Each of the top sub-causes is discussed in further detail below.

• **Operating Procedures (Figure 9):** The sub cause of 119 procedural errors was a failure to follow proper operating procedures . This included not following correct documentation, skipping documented steps, operating incorrect keys, typing errors, etc. In 48 cases the proper procedure was available but not followed. In 18 cases the generic program change procedure was not followed and in 13 cases standard hardware growth or change procedures were not followed. In 11 cases actions were performed that the switch should not have allowed. These actions included removing the active unit with its mate made busy, removing power from the active unit with its mate in trouble, etc. The sub cause of the remaining 29 outages in this category could not be determined.

• **Hardware Maintenance (Figure 10):** In 57 cases reviewed, hardware maintenance procedures were not followed. In 35 of these 57 cases the incorrect circuit pack or fuse was removed, an incorrect circuit breaker was operated, or a circuit pack or fuse was replaced with an incorrect type. The information provided identified what happened insufficient information was provided to indicate why. In seven cases it appeared that the prescribed maintenance procedures were available but just not followed. In two situations action was allowed by the switch that should have been prevented and in two cases hardware growth procedures were not followed. In this category there was insufficient information to identify what happened in 11 cases.

• **Data Entry (Figure 11):** 41 failures were due to incorrect data entry. 26 of these, or 63 percent of all failures in this category, were due to the switch specific translations. This included entry of incorrect data, procedures not followed, and changes to the wrong system. The information provided indicated the system failed due to installing incorrect translations but did not indicate what caused the error. 7 failures in this category were due to system initialization to resize office parameters. 2 failures were due to incorrect SS7 translations. 3 failures were due to entry of incorrect hardware growth data.

• **Exceeded Required Action (Figure 12):** Action taken exceeded the prescribed recovery methodology in 22 of the failures. These actions were primarily the result of relatively minor system abnormalities that resulted in initializing the switch instead of identifying and correcting the source of the problem. These failures included 14 instances of software corruption and four cases of system alarms where the switch was initialized to clear the situation. In two additional cases the switch was initialized to clear background processes that were running in the switch.

C

5.1.2. Key Learnings

The highest percentage of failure occurred while performing maintenance activities. The second highest occurrence was during system change (hardware growth or software change) procedures. This is due primarily to the performance of data base changes and maintenance tasks from memory. There is not an attempt to use the documented procedure for most maintenance activities or for the more routine software or system hardware growth activities. This problem is exacerbated by the rapid change of the technology and the increasing number of equipment suppliers. Maintenance processes that work in one technology will cause problems if used in another. One example is the replacement of circuit packs without first removing power. This is the normal procedure in some technologies and a sure way to cause a service interruption in others.

Another major cause of failure was not following generic program or software patching procedures. These procedures are generally evaluated and thoroughly tested before being made generally available. The conclusion is that either the procedure was not understood, not customized for the specific location, or not followed at all.

Manual system initialization or forced restoral of defective equipment into service also played a major role. Manually initializing the system to clear software corruption or forced restoral of equipment may be required in some situations to quickly restore service. The problems presented in these data, however, do not appear to have been that serious. There appears to be an attitude, perhaps spawned by the common practice in personal computer use of re-booting: if it is corrupted, initialize it. The symptom of the problem will be alleviated but the problem is still there.

There is a higher comparable rate of failure with new technology than with old. This could be due to a higher rate of installation activity to meet customer commitments, limited experience with the physical hardware and software design, limited knowledge with how the equipment integrates into the switched network, and limited knowledge of maintenance and recovery procedures. The installation, implementation, administration, and maintenance procedures for the new equipment also have not had as much field experience as the same documents associated with old technology. Finally, the capability of the new technology to recover from or disallow improper maintenance actions may not have progressed to the capability of the older technology. It is believed that enhanced design standards or requirements for network element robustness would be beneficial.

Forced restoral of failing equipment, and removal of the active unit or its power while the mate is in trouble suggests two problems. The first is a lack of adherence to maintenance process and the second is a weakness in switch design. The lack of adherence to maintenance process has been previously discussed. Systems currently allow normal removal of active status or power from the active unit when the mate is in trouble.

5.1.3. Telco Procedures Recommendations

1. The elimination of "Telco Procedural Error" as a failure category is recommended as this term makes the failure personal and limits the sharing of information required to identify root cause. A very small percentage of failure reports included data that identified root cause of failure. The failure category "Procedural Error" may be a contributor. This term has overtones that put the craft person on the defensive. All errors, whether they are due to software, hardware, or design, are the result of a procedural error at some point in the product life cycle. It may be as early as the initial design when the requirements are misinterpreted, during manufacturing or software coding, during final product testing or implementation, or when field installation or maintenance is being performed. It is only during this final step when the product is in service that the error is classified as a procedural problem.

By using the term procedural error the outage cause is no longer an abstract problem assigned to a process but a problem with an individual. As soon as this happens, the individual will quite often take the defense. This human defense mechanism prevents the service provider and the system supplier from getting at the real root cause of the failure.

Procedural error should be replaced with an additional layer of problem definition that would include but not be limited to:

- documentation: inadequate, incomplete, not

C

available

- human factors: not clearly marked, equipment layout not consistent, machine to people communication ambiguous, etc.

- system action: allowed improper request, did not warn of severity of requested action, etc.

- management: scheduling, training, etc.

2. To identify the root cause of outages due to procedural errors, an enhancement to the existing service provider data collection process is recommended. A process for analysis of all work error caused failures needs to be established. The process needs to include sharing this information with the associated equipment supplier. This process should be used to identify and eliminate the root cause of these failures. A format similar to the SSFA data request should be established to standardize data collection. The data collection format should be enhanced by expanding the cause codes and adding requirements for key learnings and root cause documentation, countermeasure identification, and action plans for countermeasure implementation. The process should include investigation of the work operation, the resulting failure, the cause of the failure, any temporary work around, and results of the root cause analysis. This analysis process should include the system supplier and be led by an objective service provider work group that was not involved in the failure. This independent work group should be responsible for documenting investigation results, assigning responsibility for resolution of identified issues, and tracking completion of assigned action items. The process should include feed back of investigation results to the system provider and standards and requirements groups. These organizations should use these data to enhance the existing systems, to improve the standards and requirements, and improve Human Factors engineering and design. Pacific Bell's trial of their Customer Service Quality Failure Report (CSQFR) process is one example process that could be employed by all service providers and system suppliers.

A formal process should be established among service providers to share critical information required to prevent similar outage conditions from occurring. This process should include different organizations of a system supplier, service provider, and different service providers. This process should also include feedback of root cause to the robustness standards improvement process. A combination of the aforementioned CSQFR process and the existing National Electronic Switching Assistance Center (NESAC) CSCANS process could meet this need. The CSCANS process is used today by the major system suppliers to electronically share service affecting or procedural information with the seven Regional Bell Operating Companies. This system could be enhanced to include a "Critical" information category and it could be used by all system providers to share information with all of their customers. The CSQFR process could be used to share root cause information with the system providers and Bellcore and other requirements or standards organizations.

3. Methods Of Procedure (MOP) should be prepared for all Hardware and Generic Software growth and change activities. These MOPs should be written as far as is practicable by the people who will execute the work or their management. An approval process should be followed that includes the responsible engineering, line operations, and installation management. Any deviation in the documented process should again be approved by this management team. The MOP should include specific references to detailed information required to perform the work function including name, number, issue and date of issue of handbooks, practices, and recent updates to them, thus ensuring that complex procedures are undertaken with up to data, well designed and thoroughly tested detailed technical procedure information. The MOP should be used as a work operation check list, e.g., as each work function is completed, it should be signed off in the MOP.

4. Manual system initializations to clear alarm indications, back ground processes, or software corruption should not be allowed unless customer service is being drastically impacted. In all other situations the triggering event should be identified and used to enhance the reliability and robustness of the switch. If tools or capability are not currently available to identify the root cause, these investigations should provide data required for their development.

5. System suppliers should strive for simplicity in developing procedures for maintenance,

C

hardware growth and software changes.

6. **System suppliers should enhance existing, or establish new, standards for system robustness to prevent switching systems from accepting or allowing service affecting activity without a positive confirmation.** These robustness standards should be applied to software (e.g., input verification, flow control validation, undo, etc.), hardware (e.g., lighting, labeling, numbering, positioning, warning indication, etc.), and documentation (e.g., layout, numbering, indexing, minimum content, etc.). Requirements published in Bellcore Technical References TR-NWT-001213, "Objectives for the Maintenance User Interface of Switching Systems", should be used as the baseline requirement to guide both standards and user-machine interface robustness improvements.

5.2. Scheduled Events and Retrofits

Scheduled events and retrofits (hereinafter referred to as "scheduled outages") are regular and sometimes necessary outages that take place in the network. As shown in Figure 1, scheduled outages account for 59 percent of all reported outage events in host and remote end office switches reported to Bellcore in the first two quarters of 1992.

The majority of these outages take place in historical low traffic periods (Figure 13) and last for very short average durations. This results in a very low overall customer impact. In fact, Bellcore requires (TR-541) that stable calls be maintained during retrofits, therefore, such calls should not be affected during these scheduled outages. Only transient calls should be negatively impacted by retrofit activity.

Scheduled outages and retrofits are not generally considered to be reliability issues by service providers and system suppliers. However, with the proliferation of communications applications which extend into the traditional low traffic periods (e.g., batch banking transactions and international calling), the root causes of scheduled outages need to be studied with a goal of further minimizing impact on the network. In addition, while scheduled outages are smaller in average duration than the other leading causes of switch failures, the sheer number of these events demands some investigation into whether the number of occurences could be reduced.

5.2.1. Outage Analysis and Causes

To determine the root causes of scheduled outages, service provider and system supplier outage data for the first three quarters of 1992 collected with the SSFA data request was analyzed. The most frequently cited cause of scheduled outages was retrofits to install a new software generic in a switch.

Although outage information for packet switches was requested, very little data were received. Consequently, no conclusions as to the frequency, duration or root causes of packet switch scheduled outages were made, however, it is recommended that future packet switch standards for outage frequency and outage duration be set to the same relative levels as voice switches.

An examination of root cause information for a small sample of outages in which the major cause was error during the scheduled procedure reveals a small number of scheduled outages which turned into "unscheduled" outages. Section 5.1 reported that the second highest percentage of procedural failures are attributable to "system change (hardware growth or software change) procedures". These unscheduled outages would not have occurred if the original scheduled outage could have been eliminated. It is believed that a reduction in scheduled outages should result in a reduction in other outages, mainly procedural.

The SSFA data request generated over 3000 reports for scheduled outages. Section 23 of the Service Provider Data Request (Appendix B) was included to obtain more in-depth information about switch initializations as the listed sub-causes in Section 19 did not get at the reason behind such existing sub-causes as "Software Administration" or "Retrofit". The first question in Section 23 addresses these reasons. The next two questions of Section 23 were included to address a concern that scheduled outages occur too frequently and perhaps unnecessarily. The issue of coordinated retrofits was raised and an attempt was made to quantify the number of switches being retrofitted at the same time. The final question in Section 23 requested any best practices in the industry being followed in order to minimize the number of scheduled outages.

C

Very few responses to Section 23 were received in over 3000 reports attributable to scheduled outages. The team could not identify specific reasons for the lack of information but suspects that it may be due to a lack of in-depth record keeping by service providers for events not necessarily viewed as problems.

To confirm the initial root cause analysis data breakdowns were sought for:

- Outages by major root cause.
- Major root causes broken into sub-causes.
- Duration of outages.
- Outage by time of day.

In order to draw any conclusions regarding frequency of scheduled outages and the average number of scheduled outages per switch per year, the outage data were sorted by Common Language Location Identifier (CLLI) code and data were analyzed for multiple outage reports occurring in the same CLLI (switch). System suppliers supplied information related to switch retrofit activity in 1992 as well as the total switch population supported to calculate average number of scheduled outages per switch per year.

While it is felt that a reduction in both the average number of scheduled outages and the duration of a scheduled outage is needed, to avoid making unreasonable and unattainable recommendations, an additional questionnaire was developed to ask switch suppliers about their plans to effect such changes in their software.

The following are given as the major contributors to scheduled outages and retrofits :

1. Installation of new generics.
2. New feature activation.
3. Parameter changes.
4. Patches to software.
5. Hardware growth.
6. Memory expansion.

It is concluded that these major causes can be further categorized into the following root causes:

- Some switch software requires that a reinitialization be performed in order to change parameters, resize memory tables, activate features, and recognize and gain control of new peripheral devices.

- Software and hardware architecture may also play a role in the excessive amount of time required to perform reinitializations and to prepare for retrofits. Retrofit time requirements are influenced by the complexity of the associated software and the resources (e.g. CPU, memory) being allocated to perform retrofit tasks.

- Software quality influences the number of patches and generic updates issued. No specific data were collected which indicated that software quality was a factor contributing to patching. Since feature activation is treated separately as a sub-cause, there are very few reasons to patch software other than to correct "bugs".

It is worthwhile noting that the current architecture has evolved in an environment that was more tolerant of short duration outages in low traffic periods. This tolerance is changing and most system suppliers indicated that they are making efforts to reduce the need to reinitialize for such reasons as feature and patch activation.

Since very little indication was provided as to whether individual outages could have been avoided through alternative means (Section 23 of the data request), the following procedural causes cannot be substantiated but are nonetheless suspected in some cases.

- Frequent scheduled outages to activate new features can sometimes be a result of poor planning and demand forecasting by the service provider. Engineering plans to install new generics may not always be coordinated with marketing plans to promote a new service. Unexpected growth or customer demand in a service area may force the unanticipated expansion of switching equipment resulting in scheduled outages.

- In order to correct corruption of switch data of unknown origins, service providers sometimes opt for a reinitialization rather than go through a lengthy manual process which would avoid the outage.

- Procedural errors stemming from earlier scheduled outages force service providers to schedule new events to correct those errors.

C

5.2.2 Key Learnings

There are too many scheduled outages taking place. The average number of scheduled outages for the purpose of retrofit activity per switch per year is .9. This figure was obtained from the records of the major switch suppliers for 1992. It is the result of dividing the total number of switches supported by the suppliers into the number of retrofits performed for the year. Considering that scheduled outages other than retrofits also occur, the number of scheduled outages per switch per year is in fact higher and could be at least 1.4.

The duration of scheduled outages is too long (see Figure 14). The current average outage time is over three minutes for retrofits and two minutes for other scheduled outages.

Scheduled events and retrofits are performed as needed and not on any set timetable. External factors are the driving force in performing scheduled events and retrofits. The major external factors involved are the following:

- Providing new features.
- Enhancements to existing features.
- Enhancing overall system performance.
- Consolidating accumulated program corrections (patches).
- Regulatory mandates.
- Growth.

When service providers do not plan retrofits on a regular basis they may be forced to schedule several retrofits in a short period of time. The analysis of data for 140 switches in which the switch had multiple outages shows that the root cause of the outage was system retrofit. An office may be required to sequentially transition through each software release as the office evolves.

Expense is a factor in service providers not performing retrofits on a regular basis. Increased labor costs include pre-conditioning activity and/or equipment growth required for the retrofit, night-of-retrofit support and post retrofit acceptance testing. Higher Right To Use (RTU) fees for new software releases and features also is a factor in increased expenditures.

During a retrofit, switches operate in simplex mode for an extended period of time (up to 24 hours), leaving the switch vulnerable to an unplanned outage. The active side is performing call processing on the old software release while the out-of-service side is loading the new software release. After initialization, switches are kept in a simplex mode during acceptance testing. If the active side experiences a hardware or software error an outage may occur. (There is no data analysis on simplex time or outages due to switches running in a simplex mode.)

The retrofit procedures are long, complex and unique. Many of the procedures are not used in day-to-day operations by the service providers, thus adding to the simplex time.

Analysis has shown that some switches experience a cluster of outages within a plus or minus 45 day window around the retrofit (Figure 16).

5.2.3 Scheduled Events/Retrofits Recommendations

Although SPCS technology is designed with redundant capability, there still exists an opportunity for total breakdown while operating in a simplex state. The probability of failure increases with the frequency and duration of events that mandate system operation in a simplex state. In addition, there is a need for SPCS technology to reduce significantly the duration of these outages. The aforementioned items define the need for goals in these areas as well as tracking mechanisms for conformance measurements and data collection.

1. Reduce the number of scheduled outages per switch per year from the current level of 1.4 to 1.0 by the end of 1995. Scheduled outages are occurring much too frequently in the network. Each scheduled outage has potential to become an unplanned outage as the switch operates in simplex mode during certain lengthy types of maintenance activities on the backup. Any kind of failure on the active (and only available) portion of the switch while in simplex mode can be fatal to the switch and may result in the loss of all call processing capability. Procedural errors occur during scheduled events and retrofits. In some cases these errors cause outages and in other cases result in additional scheduled events. Reducing the number scheduled outages will contribute to a reduction in events in other categories, mainly procedural.

The following objectives are set to eventually

C

reduce the impact of scheduled event outages to the point where service will not be affected:

- By year-end 1995, the objective of 1 minute per event as defined in TR-541 will be achieved for all digital technologies.
- By year-end 1997, this objective should be refined to 30 seconds.
- By year-end 2000, scheduled outages should be non-service affecting.

In order to achieve these goals, the recommendations below address opportunities for system suppliers, service providers and industry to reduce the number of scheduled events.

2. System suppliers should provide a mechanism for feature adding/activation that allows for "Soft" activation rather than re-initialization. This might reduce the number of outages attributed to feature activation (5 % of scheduled outages).

3. System suppliers should provide an on-line memory management capability to reconfigure or expand memory without an impact on stable/transient call processing or the billing process. This should reduce the number of outages attributed to memory expansions and parameter changes (23 % of scheduled outages).

4. As stated clearly in 8.6.4.2 of TR-541, overwrites should currently be implementable without re-initialization (3 % of scheduled outages).

5. Bellcore, industry groups and standards bodies that establish procedures, objectives and requirements should review their technical literature for engineering standards and recommended practices which might inadvertently contribute to the number of scheduled outages. These groups should make appropriate changes in support of this team's recommendations.

6. Service providers should improve service introduction with retrofits. This should permit coordinated reinitializations in which a single outage would serve the objectives of both engineering and marketing.

7. Service providers should improve the accuracy of their manual processes in order to reduce the number of scheduled events which must be repeated due to procedural error.

8. An SFAR-like form should be used to collect data on scheduled outages by service providers and system suppliers. The data collection process should be automated and reports should be filed electronically. Some service providers already keep track of outages in electronic form. The following modifications should be made to the format:

a. Add two new outage cause classifications -
   Scheduled Event - Preventable. This status indicates a scheduled event occurred within 45 days of a previous outage and could have been avoided through proper engineering, planning, or provisioning by including this activity as part of the previous scheduled event.
   Scheduled Event - Corrective. This status indicates that during a low traffic period, generally 0000 to 0600, a scheduled outage occurs which is intended to recover some system capability not recoverable otherwise to which no other root cause may be attributable. The purpose for this sub-cause is to highlight them for further root cause analysis by system suppliers and service providers.

b. Add an entry for amount of time required to perform a scheduled event.

There are four specific metrics which will allow service providers and system suppliers to measure the effectiveness of the above recommendations:

1. Number of scheduled outages per switch per year.
2. Number of preventable and corrective scheduled outages per switch per year.
3. Outage duration in number of minutes of a scheduled outage.
4. Total length of time to perform the retrofit process.

The study of all outages within a 45 day window surrounding a scheduled outage (particularly retrofits) should be conducted to see if there are lessons which could be learned.

It was observed that scheduled event processes that

C

exceed eight hours, or a typical service provider workshift, may not be warranted. The automation of some retrofit activities which are currently manual may reduce not only the amount of time the switch is in a simplex state, but also procedural errors. A reduction in procedural errors associated with scheduled events will also reduce the number of outages.

Currently, some system suppliers are allowing service providers to skip over one or more releases. This provides flexibility and administrative savings to the service provider and reduces the number of scheduled outages.

The issue of scheduled outages must be kept in the proper perspective. While it is believed that too many scheduled outages are occurring today and the above recommendations strive for a reduction in quantity, the reader should not infer that any major network reliability risks exist as a result of this type of outage. Some scheduled outages are and will continue to be necessary. The recommendations contained herein should be considered to be improvements to an already reliable environment. It is encouraging that system suppliers are already addressing some of the architectural recommendations as evidenced by supplier responses to the SSFA data request.

5.3. Hardware

Bellcore provided data for the first half of 1992 (Figure 1) indicates that approximately 12% of total system outages are attributable to hardware failures. These outages accounted for 9% of the total outage time (Figure 18).

An initial review of selected hardware outages from the Bellcore SFAR (Switching Failure Analysis Report) data base proved inconclusive. Limited information on the outages made it difficult to perform a detailed analysis. The only conclusion that could be reached was that the trigger for these outages was a hardware failure. The data did not give an indication of outages resulting from multiple hardware failures. Since switching systems are designed to continue to provide service in the face of faults, i.e., exhibit fault tolerance, questions were raised regarding the accuracy of the root cause analysis for hardware outages.

In order to address this question, detailed Bellcore data for the first three quarters of 1992 were provided for further analysis to the supplier responsible for the particular switch. The data contained over 200 entries classified as hardware, and although not all serivce providers are represented, the data were believed to be representative.

5.3.1 Outage Cause and Analysis

Regardless of system supplier, the conclusions of the analysis were similar. Similarities existed when the outages were examined from the point of view of the trigger, although no single piece of hardware in any system seemed to be triggering an inordinate percentage of outages, as shown in Figure 18. Examination from the root cause point of view indicated that many of the outages were caused by deficient fault isolation and/or recovery software. As shown in Figure 19, over 30% of hardware outages lasted more than five minutes. It may be that inadequate fault isolation and recovery software contributed to the length of those outages.

A more detailed examination of the outage lengths (Figures 20 and 21) shows some interesting points. Almost 75% of the outages are less than 10 minutes in duration, but account for less than 20% of the outage time, while outages over 30 minutes are 15% of the incidents but account for more than 60% of the outage time. The median outage time is about 2.5 minutes, while the average time is 11.5 minutes. Thus, the distribution of outages times is clearly skewed and has a significant tail.

An examination of the outages by time of day (Figure 22) shows a relatively flat distribution (which might be expected) except for the periods from Midnight to 3am, and from 3pm to 6pm. A detailed look at Midnight to 3am showed a number of instances where offices experienced a relatively short outage in conjunction with Routine Exercises. There were other cases where central office activity triggered some type of hardware failure resulting in a service interruption. An examination of the outage incidents in the 3pm to 6pm time period does not provide any specific reason(s) for the increase in number or outage time, although it should be noted that the two longest outages both started in this time period. Additional data need to be studied to determine if this is a repeating pattern or merely an anomaly in this particular data set.

C

There were a number of cases in data where the outage was classified as total, but an examination of the details revealed that this was not accurate. Specifically, one extremely long outage is shown as total, when there was a complete loss of billing for the period covered, but no service impairment. There were a number of outages where SS7 connectivity to the network was lost, but the switch continued to provide intraoffice service. While not all that common, there were sufficient numbers of these cases to have had an impact on the data analysis. For this analysis, these cases were reclassified as partial and will be discussed below.

An examination of the data on partial outages revealed a somewhat different outage pattern from above. Since, as noted, the definition of a partial outage is not clear this category included the four cases mentioned before - loss of peripheral equipment, loss of SS7 connectivity, loss of the umbilical to a remote location, loss of billing - and instances where a particular call function was inoperable but all other services were operating properly, and instances where various call progress tones were inoperable. It should be noted that as network interconnection becomes more widespread, loss of SS7 connectivity at an end office will result in total isolation, exactly as the loss of the umbilical to a remote unit does today. There is clearly a need for clarification of types of outages.

Figure 23 portrays the partial outage entries by the type (or impact) of the outage. Since the Billing loss and the individual Call Function loss have such an effect on outage time, Figure 24 eliminates them from the data analysis, in order to show more clearly the relative weights of peripheral failures, SS7 isolations, remote isolations, and tone failures. Even with this simplification, it is somewhat of an apples-to-oranges comparison. In general, an SS7 or remote isolation, or a tone failure has an impact on most of the subscribers in a central office, while a peripheral failure usually affects a small percentage of the subscribers, although the effect for those subcribers is a total loss of service.

Basically, the analysis shows that most outages classified as partial are loss of peripheral equipment and typically affect 500 to 2000 subscribers. Since the peripheral outages are the dominant part of partial outages, the outage lengths are broken out in Figures 25 and 26.

One last piece of analysis from the data shows that only 5% of these hardware outages would have generated an FCC report under the current threshold reporting guidelines.

5.3.2 Key Learnings

From the above, several conclusions can be drawn. First of all, the vast majority of switch outages characterized as hardware could be attributed to some other category (typically fault isolation and recovery) when put in the correct cause category. In some cases, especially the very short outages, it is clear that the system has been designed to take a low level boot as a part of the system recovery strategy.

There is an inconsistency in reporting partial hardware outages as total outages. Not only is there a need for a good definition of outage,but also additional categories such as billing failure, or office isolation (by loss of SS7, or in the case of a remote switch unit, by loss of umbilical). What is also required is a better definition of what constitutes a partial outage. Clearly, malfunction of a piece of peripheral gear that isolates some portion of the subscribers in a central office is a partial outage, but the definition has been used to cover loss of SS7 connectivity, loss of umbilical to a remote unit, and other malfunctions that don't seem to fit into the total category.

From these data it can be seen that peripheral outages are different from total outages in that they tend to be significantly longer. Whereas only 15% of the total outages were >30 minutes, almost 30% of the peripheral outages were >30 minutes. While total outages >30 minutes account for 80% of the outage time, peripheral outages >30 minutes account for 95% of the outage time. The inclusion of the other partial outage types does not change this result significantly. The conclusion one reaches after examining the data is that partial outages, when they occur, are somewhat less likely to be resolved by automatic recovery means, and are more likely to require craft intervention. Given that partial outages of 30 minutes or more are approximately twice as likely as total outages of 30 minutes or more (30% vs. 15%), there is a possibility that they are actually more difficult to resolve. This is open to argument, since the longer outage time may be due in part to dispatch times,

C

etc. It is not always clear from the data whether a craftperson was present in the office at the time of the incident or not.

5.3.3 Hardware Recommendations

1. In order to properly characterize the cause of the outage, and follow up with appropriate corrections, it is necessary to modify the data collection form so that organizations responsible for filling it out are strongly encouraged to examine the outage from a root cause point of view. This will require close communication between the service provider and the system suppplier. This communication is crucial, since it is far more likely that a proper determination of root cause will be made by the system supplier and service provider jointly, rather than each one acting independently and with limited knowledge.

2. An industry definition of outage(s) needs to be determined with performance and reporting standards agreed upon and implemented. This will enable an analysis of service failures and highlight the areas requiring proactive measure.

3. Hardware outage reports should include specific information about the type of outage. Specific categories should include at the least, A) Complete loss of all service, B) Loss of connectivity to the network, by reason of loss of SS7 or the remote umbilical, C) Loss of billing function, D) Loss of peripheral equipment affecting >500 lines, E) Loss of a significant call function, e.g., loss of IEC dialing capability, or loss of all voice mail capabilities, etc., and F) severe overload, e.g., 20% DTD >3 seconds, or 20% Receiver Attachment Delays >3 seconds. For offices which serve as access tandems, and whose failure may have more severe consequences on the network, there are probably other categories to be added. Additionally, in the case of manual intervention for recovery information should be provided indicating whether technical personnel were present or had to be dispatched.

4. Service interruptions of two minutes or more, affecting a significant number of lines (>500), where there is a evidence that the problem was triggered by a single hardware failure should be reported immediately to the supplier of the equipment, as well as documented by way of an outage report. Failures of unduplicated hardware that affect a relatively small number of lines (<100) should be handled similar to other individual circuit pack failures. The system supplier should perform root cause analysis of all outages triggered by a single hardware failure.

5. Hardware and software fault recovery design processes should converge early in the development cycle. It is impossible to tell from the data why the recovery software does not function properly in all cases of single hardware failures, but there is a general feeling that an earlier convergence of hardware designers and software fault recovery developers would go a long way to eliminating this problem. Additionally, continued effort to improve the hardware reliability itself will minimize the need for activation of the fault recovery software and lead to more reliable operation of the entire system.

5.4. Software Design

The analysis of outages caused by software design began with the Bellcore 1H92 data covering outages during 1H92. The primary causes of the outages are summarized in Figure 27.

In order to validate the conclusions drawn from this initial data set, additional data were requested. Because of delays in obtaining all these data, other available outage data collected in response to the SSFA data request and covering software design outages were analyzed. These data consisted of information from service providers, both LEC and IXC, for outages which occurred during 1Q92-3Q92. Outages which occurred during 3Q92 were primarily longer than 10 minutes and are summarized separately.

5.4.1 Outage Cause and Analysis

Based on available data, data corruptions of various types are the leading cause of "software design" outages. This category includes corruption of both static (i.e., permanent or semi-permanent) and dynamic (i.e., per call or transient) data. In terms of both number of incidents and duration, this is the leading cause of software design outages. In many cases system wide initializations are called (either manually or automatically) to clean up these data base corruptions. In some cases, the system went through several initializations, presumably following an initialization escalation strategy of

C

increasingly more severe initializations on each subsequent incident.

Delayed and defective patches were the next most significant cause of software design outages, although not significant for the SSFA data. Delayed patch indicates that the outage was caused by a known fault but a failure or delay in the patch delivery process left the switch vulnerable. The data did not indicate how responsibility for this process failure was divided between service provider and system supplier.

A review of the patch delivery process by both system suppliers and service providers to identify causes for delays in patch delivery and installation would be warranted in those cases where missing patches were a significant factor. Defective patches are primarily a design and/or coding issue, but it was felt that bad patches should have been detected in testing before delivery to the field, if properly tested in conditions that simulate the field environment.

Other errors include problems in routine exercise or maintenance tests and several incidents where the exact nature of the problem could not be determined from the descriptions available.

5.4.2 Key Learnings

Figures 28 and 29 show average duration of outages for each sub-cause for the Bellcore data and the SSFA data, respectively. The Bellcore data show that for this particular sample, defective and delayed patches resulted on average in the longest outages. This was followed by outages due to routine exercises and static and dynamic data base errors. The SSFA data indicate that static data base errors have the longest duration by far, followed by defective patches, data synchronization errors and routine exercise errors. Although differences appear between the two sets of data, it is clear that data base errors, defective patches and missing patches are leading outage problems.

Figures 30 and 31 show the outage duration by time of day for the Bellcore data and SSFA data respectively. Both figures indicate there is a higher rate of outages during off-peak hours from midnight to 7 a.m., than during the rest of the day. The distribution of outages into the off-peak hours is interesting. Certainly many maintenance activities occur during this period. Yet figures 28 and 29 indicate that routine exercise problems are not a major source of outages. Although there is an increase in outages during the morning and afternoon, there is no strong correlation with daytime traffic. The off-peak hours correspond to periods when much activity is occurring in the switch; routine maintenance (both manual & automatic), data base administration activities, patch loading and perhaps clean-up activities which are deferred outside of the busy daytime hours.

The data indicate that outages associated with the running of routine exercises are not a major contributor to outage incidents. Thus, the peak in outage occurrence seen during the early morning hours (midnight - 6:00 a.m.), when routine exercise programs are often run, must be attributable to other activities within the switch. These activities may include OA&M functions which fail, clean-up activities, i.e., work deferred from heavy traffic periods to clean up problems encountered in the switch or other routine activities that fail to complete as expected. The team concluded that in many cases the system failed to contain the original problem or reacted in too severe a manner to failures in routine procedures. In other words, the system's fault tolerance was deficient.

This finding was confirmed from the descriptions available for some of the outages. Many of these descriptions described events where the problem was specific to a specific area or sub-system of the switch, yet the fix required a total switch outage, or the switch's response to manual or automatic actions was more severe than expected. The conclusion reached after reviewing these data is that the fault tolerance of switching systems needs improvement. For example, an error in the data base for a system component might require a system re-configuration. Because of some fault related to the initial conditions, this configuration fails to complete properly, leading to an unexpected system outage. Repeatedly, data base problems, specific to a subscriber or feature, caused the switch to initialize. The analysis of available data resulted in varying opinions as to which outages indicated a failure or problem with fault tolerance. This lack of consensus as to what constitutes s failure in fault tolerance may be indicative of a lack of standards in this area.

The importance of a robust software life-cycle process for the development and delivery of quality

C

software is recognized. The available outage data did not provide insight on whether the software faults being studied were associated with any particular phase of the software development life-cycle. Information of this type is viewed as sensitive by most system suppliers and is treated as proprietary. Although it was not possible to get detailed information of this type, the software development and delivery process was studied.

The question of steps to reduce the occurrence of outages attributable to software design problems was discussed. System suppliers participating in the SSFA shared their internal root cause analysis processes as well as various proactive steps being taken to reduce outage frequency and duration. To support these activities, each system supplier supplied a written statement to Bellcore of its formal root cause analysis process. These statements were compiled, with supplier identifications removed. They provided a basis for discussions of the root cause analysis process and the recommendations that follow. As a complementary activity, system suppliers also provided statements of their proactive activities being undertaken to reduce the number and duration of outages due to software design. These statements serve as a basis for the recommendations that follow.

Naturally, many of these steps are architecture dependent and may not be directly applicable to switching systems with differing architectures. Other suggestions are directly applicable to any system.

As stated above, it was decided that in dealing with software design errors, it would be most productive to address the software design and delivery process to see how errors leading to outages were being introduced into products and what could be done to eliminate or reduce outage causing faults. Thus there was a focus on the software development and delivery process and not on supplier specific switching system architectural issues; this is not to eliminate recommendations for design changes as appropriate, but rather to recognize that evolutionary changes to existing switching system design are the most likely to be implemented and that process changes will result in significant improvement in delivered product quality.

5.4.3 Software Design Recommendations

1. Switching system suppliers should enhance their software development methodology to insure effectiveness and a modern process of self-assessment and continual improvement. General software engineering practices, though not specific to system outage or reliability issues, would obviously be important in improving switch performance in these areas. While all system suppliers use formal methodologies in the development of their software systems, the effectiveness of their methodologies needs to be improved. In particular, procedures need to be established to assure application of the complete methodology in all aspects of software development, e.g., fault correction as well as new feature development. In addition, there needs to be a process put in place of self-assessment of the effectiveness of different development activities and self-improvement where warranted. This self-assessment process needs to be made an integral part of the development methodology.

Several methods and practices are commonly in use. Variations in system architecture, development environments and practices will allow different specific formulations of development practices. Published and widely accepted standards for the Software Development Process include:

- Bellcore TR-NWT-000179, Issue 1, 7/89, Software Quality Program Generic Requirements (SQPR).
- Carnegie-Mellon University/Software Engineering Institute, Capability Maturity Model.
- ISO 9000-3 "Quality management and quality assurance standards: guidelines for selection and use".
- Bellcore TA-NWT-000179, Issue 3, 1/93 updates TR-179 in conformance with ISO 9000-3. The TA is planned to be converted into TR-179, Issue 2 in 6/93.

There is also a pressing need for wider use of electronic media/CASE tools and object-oriented techniques in the specification and in the analysis of requirements, in order to adequately account for complex inter-actions and inter-dependencies, *at*

C

the requirements level, i.e. very early in the software life-cycle. This would also make it much easier to effect requirements traceability and verification. This need encompasses the entire process starting from customer/service provider requirements, through Bellcore, and including system suppliers.

2. Formal design and code inspections should be performed as a part of the software development methodology. Although design and code inspections are part of all formal methodologies, it was felt that they are such critical parts of the development process to warrant special attention. Improvements in software performance can be achieved through two means - better designs and testing. It is generally more effective to capture the design problems and insure the fault tolerance of the design early in the process. Testing of software, through fault insertion or functionality test cases, can assist in the final stages of software design. However, it is not a substitute for a properly designed software product.

Due to many identified problems associated with software and associated data, it is suggested that the design process integrate early design reviews against specific requirements for functionality of design and fault tolerance. Formal reviews should include - a description of the logical structure and data flow (module/feature) followed by an execution (walk-through) of selected feature scenarios or test cases. These feature scenarios should include at a minimum, valid inputs and failure modes of inputs. Specifically, the scenarios should be used to insure the design and external systems follow the least service-affecting path. For example, rigorous application of formal design techniques and reviews can go a long way in eliminating the primary cause of design errors such as those which lead to data base errors, a leading cause of outages attributable to software design. When coupled with the results of the root cause analysis process, as described below, it should also be possible to eliminate improper error handling which may lead to outages. Proper application of reviews, in conjunction with the results of root cause analysis should also help to reduce the number of bad patches which lead to outages.

3. A formal root cause analysis process is needed to investigate outage root causes and recommend corrective actions. Root cause analysis of the outage starts only after the immediate technical problem has been resolved with a fix. The purpose of this analysis is to determine where in the software development process the fault was introduced; how and why it was introduced; and why it was not discovered prior to delivery of the software to the customer. Root cause analysis should also identify or recommend steps to prevent similar faults from being introduced and delivered in the future. Crucial to the success of the root cause analysis process is the close cooperation of system supplier and service provider to assure that the outage information needed for the analysis is collected and provided to the system supplier. A formalized process to deliver such information should be in place. Service providers should report data for all partial and total outages to the appropriate system supplier. Characteristics of the process should include:

- Characterization of the source of the fault with respect to the software development methodology stages of the system supplier.

- Identify both software development process and design changes, as appropriate, which might prevent similar problems from being introduced in the future. The process changes should cover both software design as well as test/validation aspects of the development process.

- Where appropriate, internal development support tooling should be enhanced to help capture data needed in the root cause analysis, e.g., fault report data can include an initial designation of the root cause of the fault.

- Recommendations need to be publicized throughout the organization, and where appropriate, training material, design guidelines, etc., need to be updated. There should be sufficient follow-up to assure that recommendations are implemented.

- Reports should be made on an on-going basis to management and management should provide support for this activity to assure the needed focus. Timely feedback to customers is also needed.

The root cause analysis process is potentially one of the most powerful tools available to help

C

eliminate software design outages of all types. In addition to helping identify the primarily design faults leading to data base corruptions or design errors in patches, as described above, it can also help identify weaknesses in switch error handling and fault tolerance as well as process problems which result in delays to patch delivery. Thus root cause analysis can help to address all of the major causes associated with software design outages.

4. Test environments and scenarios should be enhanced to provide more realistic settings. Many problems turn out to be configuration and data base dependent, and realistic test configurations need to be available. Programs should be developed that provide for continual evolution of testing environments that accurately represent the way the software is configured and used by customers. The more closely the test bed emulates the "real world" scenario, the more accurately the field performance of the software can be assessed and predicted, resulting in higher quality software at initial delivery. This type of test configuration is especially beneficial for regression and software patch testing and should be utilized as early as in the development cycle as possible. The Root Cause Analysis process described above will help in analyzing field failures to determine root causes for test escapes and will help ensure test configurations are continually evolved. Also, the ongoing work and recommendation from the ECSA sponsored Network Operations Forum (NOF) will provide for future testing enhancements/ recommendations in areas that need to be addressed.

5. Software fault insertion testing should be performed. This should include data base corruption as well as program corruption. The most direct benefit of this type of testing is a direct check of the switching system's fault tolerance to corruptions/faults in the data base. Since data base corruptions have been identified as a leading cause of software design errors, and fault tolerance has been identified as an area needing further enhancement, a systematic approach to Software Fault Insertion Testing is particularly appropriate.

6. Fault tolerance requirements and standards need to be clarified. Fault Tolerance is the system's software safety-net -- how to maintain system stability or sanity in the face of an underlying primary fault, with minimum impact to services. The available data suggest that many outages were prolonged or caused by failures or deficiencies in the system's fault tolerance or ability to contain a fault to one part of the system. On further analysis, it became clear that in many cases standards or requirements may be implicit rather than explicit. Often there are trade-offs between switch down time and other performance criteria. For example, a data base corruption affecting a single subscriber, group of subscribers or a feature may leave the subscribers without service or without a particular feature. In many cases this condition can be corrected by an initialization of the data base which can result in a switch outage. On the other hand, avoiding the outage leaves the subscriber with impaired service for a potentially extended time since it will probably be longer and more expensive in terms of personnel time to manually troubleshoot and repair this one data base corruption. The longer the subscriber remains with the service affecting corruption in the data base, the greater the probability of receiving a customer complaint. By necessity, these clarifications of fault tolerance have both a uniform standards aspect and also individual switching system aspect, i.e., they are both system requirements which is standard across the industry or at least standard for a given type of switching system (local, toll, packet, for example) and individual switch (manufacturer) specific.

In addition to the above recommendations the following outage reduction best practices have been identified as part of the responses by system suppliers to the request for proactive steps for outage reduction. Each item has been applied successfully on one or more specific switching systems. They should be evaluated within the framework of other switching systems as to their usefulness.

7. Rigorous self-enforcement of design guidelines as they relate to system initializations. Initializations are called by software when a program designer makes an explicit call to an initialization routine in response to some unrecoverable program condition. These calls should be subject to some type of impedance: The designer should be able to support their use as absolutely necessary and consistent with the switch's design guidelines for error handling. These error handling design guidelines must be current and reviewed periodically for completeness and effectiveness, i.e.: Do they adequately handle the situation? Can the situation be handled with less

C

severe system impact? This scrutiny should apply to all requests for a system initialization, whether in the software of a new program, or in a patch which may require an initialization for activation. This review can be part of the standard review process of the software or it can be a separate step, as long as the proper scrutiny is applied.

8. Isolation of Faults/Containment of System Responses. Faulty software or processes need to be isolated as far as possible from the rest of the system and the impacts to the system contained to the smallest system components possible. If the impact of a fault can be contained within a system component or subsystem, it should be possible to clear the fault by proper initialization of just that component or subsystem. Where warranted, new levels of initialization limited to these system components should be developed.

9. Continuous review of escalation strategy effectiveness based on field performance. When a low-level initialization does not correct a problem or repeated calls to a particular level of initialization are made within a certain time period, the system will typically attempt a higher level initialization to correct the problem. These higher levels of initialization have broader system impact and typically will take longer to complete. Both the escalation path through various levels of initialization and the conditions which cause an escalation (repetition rate or period of repetition) should be reviewed for effectiveness. It may turn out, for example, that an intermediate level of initialization is not effective in resolving a problem, i.e., the system almost always continues to escalate to a higher level initialization. In this case, it may be appropriate to by-pass this intermediate level of initialization, reducing the total outage time. It also may be appropriate to adjust the repetition time required to escalate. If this time is set for too long a period, the system will go through a high level initialization, and a longer outage, too often.

10. Reduce initialization execution times. It may be possible to reduce the time it takes to complete particular initializations. In this case, although outages are not eliminated, their durations are reduced.

The service standards and performance measurements contained in Section 12 of the LSSGR (Reliability) as well as Bellcore TR-TSY-000929, Reliability and Quality Measurements for Telecommunication Systems (RQMS) are widely used and adequately measure switching system performance. Performance improvements achieved by adopting the recommendations above can be tracked through the on going use of these measurements.

In conclusion, it is believed that significant improvement in switch performance can be achieved by changes to the software development and delivery process. Process recommendations include adoption of a modern, formalized development methodology, and enhancements to test environments and strategies. A formal, continuing root cause analysis process with cooperation by service providers to provide complete outage data, will allow system suppliers to identify specific areas in their own systems and/or processes that require improvement.

5.5. Future Networks

The Issue Statement in Appendix A noted the transition of switching systems from electro-mechanical to today's stored program control environment and the increasing complexity of interoperability and synchronization. As this technology evolution continues, the level of complexity associated with network switching will increase. In addition, it is expected that the current multiple-provider environment will be even more prevalent in the future. End-user services will be provided through combinations of suppliers' products, service providers, and network providers. It is believed that the larger the number of providers, the more complex the reliability problem becomes, because of the difficulty of isolating the responsible element or entity and containing the problem so that it does not affect other parts of the network.

In today's networks, many reliability problems can be prevented by having simple and/or unambiguous interfaces between elements and between providers. It is believed that these same principles must be followed in the network of the future as different elements and more providers are involved in the provision of end-user services. The reliability of future networks causes some concern if preventative measures are not taken up front, and it deserves serious consideration to ensure that customers' reliability needs are met.

C

The vision for the network of the future (depicted in Figure 32) is one that provides;

- •a rich set of features for customers, including voice, data, and eventually multi-media,
- •the ability to customize services for particular customers or markets,
- •rapid availability of new services, and
- •interoperability between different network/service providers as well as between elements manufactured by different suppliers.

Two significant additions to today's network are expected in the 1995-1997 time frame. The first is Advanced Intelligent Network (AIN) control of new circuit-switched services. Current AIN arrangements consist of digital switches with AIN capabilities and Service Control Points (SCPs) providing service control of those AIN capabilities; future releases will support switch-to-adjunct or switch-to-Intelligent Peripheral interfaces using ISDN. Second, wide scale data capabilities will be provided by X.25 networks and fast-packet switches supporting X.25, Frame Relay and/or SMDS. Additional changes will include the introduction of broadband video capabilities and the replacement of copper with fiber.

A two-phased approach was adopted to analyze this future network. First, a single-provider network was modeled and issues associated with individual elements in that network as well as those that arise when different suppliers are used to provide the elements identified . The intent in this first phase was to simplify assumptions to focus on software reliability issues in a simple single-provider (but multi-supplier) environment.

The second analysis phase addressed the added complexity inherent in multiple-provider network environments and the special issues that arise with multiple network providers and service providers involved in offering services.

Some specific reliability concerns associated with the network environment of the future were identified. These concerns and recommendations for addressing them are discussed in the sections that follow. A generic model is proposed for mapping network components to a platform/software layer matrix to determine future issues. Sample recommendations generated using this methodology are also included.

5.5.1 Single Provider Network Model

As mentioned above, the first step was to simplify the network of the future into a single-provider (but not single element supplier) environment. It was assumed that this provider could be any telecommunications network provider. The analysis was not expanded to fundamentally different kinds of networks; different environments would raise additional issues.

Five categories of reliability issues were identified based on this view of the network of the future;

1. concerns associated with the introduction of AIN and open network architectures in general,
2. concerns associated with the wide scale introduction of data and multimedia capabilities,
3. concerns associated with interoperability between multiple suppliers' products,
4. concerns associated with operations capabilities, and
5. concerns related to future trends.

These issues are mapped by issue number to the elements and interfaces of the single-provider environment shown in Figure 32, and are discussed in more detail below.

5.5.1.1 Open Network Architectures and AIN

One characteristic of future networks is the ability to respond quickly to customers' possibly unique service needs. Advanced Intelligent Network capabilities currently in the early deployment stages in the telecommunications network will make it possible to create services rapidly that meet customers' needs. In addition, open network architectures could enable third parties (other than the network provider; for example, information providers) to offer their services to end users.

In AIN, by design, the rate of change and variability of services across network elements and customers is planned to increase relative to today's network. Network providers and/or third-party service providers may be able to create some new services, without needing to update switch software generics. In the future, service software can be placed in a variety of elements throughout the network - Adjuncts, Intelligent Peripherals, SCPs, and even switches. Both in AIN and open network

C

architectures, switches must be able to interwork with the elements that house service software to provide services to the end users.

The inherent complexity in future AIN configurations will exacerbate two factors that adversely affect software reliability. First, the number of software components (and their associated rate of change) that must interact correctly to provide a network function will increase. Second, the complexity of the actual operating environment of software exceeds what is reasonably possible to simulate in a testing environment.

AIN Service Creation

A specific issue with AIN is service creation. To discuss the AIN software reliability implications in more detail, a brief overview of an illustrative process to create and deploy new service software in the AIN is helpful. A five-step AIN service creation and deployment overview is presented, with comments highlighting possible future process advances also included. (Note that this description refers to the term "feature package," which is not yet a universally-accepted term. Groups of features could be handled differently in future Adjuncts, SCPs, and IPs.)

1. Some form of service creation environment will be used to create a new feature or set of features. In the future, the service creator could be a network provider, a service provider, or even the customer.

2. This feature (or set of features) plus perhaps other existing features may be assembled into a feature package associated with a subscribers' line or lines. Currently, feature creation is done in the context of an existing feature package. In other words, if Feature X is to be added to packages A and B, two development efforts are required, one to add feature functionality X to package A and one to add the functionality to package B. There is no physical realization of Feature X independent of the package. In the future, it is envisioned that features could be created as independent entities that can be used (and re-used) in feature packages as necessary. In this environment, features could be assembled like building blocks into feature packages.

3. The feature package software may be loaded into an SCP, Adjunct, or Intelligent Peripheral attached to the switch(es) terminating the lines or trunks over which calls will use the service software. In the future, when individual features are available as independent entities, features may be loaded into feature packages already resident in SCPs and/or Adjuncts.

4. Subscriber-independent data associated with the users of the feature package, the features and the feature package will be loaded into the SCP or Adjunct as well as the subtending switches.

5. The feature functionality associated with the feature package will then be available for use, assuming appropriate operations capabilities are in place.

AIN Feature Testing

A second specific area of concern associated with AIN is rigorous testing of features and/or feature packages created and deployed. This rigorous testing is required to ensure both that the features work and that reliability problems in features or feature packages do not affect other features on the network. Assuming the aforementioned process, a number of scenarios to illustrate potential software reliability testing challenges in future AIN configurations are envisioned.

The following three examples are provided for illustrative purposes:

1. A feature package may potentially be assigned to a variety of subscribers (and therefore lines) associated with different supplier's switches, each with potentially different generic loads. Furthermore, each line accessing the feature package may, in general, have different switch-based functionality associated with it. Although inter-supplier testing is being performed today, it does not seem practical to expect to replicate in totality the wide variety of network configurations in a lab setting to exhaustively test a feature package. Suppliers may wish to consider automated testing methods, if they don't use them already, to solve the problem of the large number of tests required. The implication is

C

that the network itself will end up being used to perform some portion of what has heretofore been lab system testing. Therefore, new testing procedures, most likely using a layered approach, will be needed. It is critical that firewalls are built to ensure that feature failures are contained and don't affect the performance of the network.

2. As feature software grows in complexity, the likelihood of uncovering all functional errors through exhaustive regression testing, whether in a lab or a network, may diminish. Software complexity is largely proportional to the number of independently-created software components that interact. It seems likely that an increasing number of functional errors will find their way into the AIN. This implies that the network will require new software diagnostic and maintenance capabilities not present today, and as discussed above, new testing procedures.

3. When and if independent, reusable feature software exists, a new testing step will be required when features are packaged together. One alternative is to test the new feature in every package prior to deployment. In a mature AIN with even a moderate number of features, testing prior to deployment will not only be an enormous task but will also restrict the flexibility of using that feature once it is deployed to those combinations tested. The alternative is to test features in the context of the particular feature package when the feature package using that feature is deployed. Again, this implies some degree of testing in the network as well as software diagnostic and maintenance capabilities not present today.

The above scenarios are not intended as an exhaustive list. They are meant to demonstrate by example how the dynamics of the AIN will require new network capabilities if reasonable network reliability is to be maintained.

Open Network Architectures

As the telecommunications networks evolve in the directions of AIN, open network architectures, standard protocols (e.g., Switch-Computer Application Interface (SCAI), CCITT IN Capability Set-1, OSI/CMAP), and distributed processing (e.g., INA and OSF), telecommunications services may involve more and more software systems produced by many suppliers and run on heterogeneous machines. For example, an AIN service may involve multiple switches, intelligent peripherals (e.g., voice mail systems), SCPs, and Service Management Systems. These could be manufactured by multiple suppliers, and may also use many software systems (such as the operating system, service creation environment, service software, and billing system) running on these machines and developed by various network element suppliers, computer suppliers, service providers, advanced users, and third-party software houses. By design, a wide variability of programs and associated data will exist across a mature network in the future. Correct management of the different versions of the software will require a level of software control not currently found in today's network.

The traditional way of ensuring network integrity by analyzing and testing new or evolving products on a single node is a reasonable approach as long as the number of products (machines and software systems) is manageable from the analysis and testing perspective. Interoperability testing involving more than one machine is gaining well-deserved attention. However, even for a manageable number of products, the possible combinations of configurations that need to be tested is very large. In future open networks with many inter-related software systems developed by different system suppliers and changed frequently, using the current approach for network integrity is becoming increasingly intractable under the demand for controlled costs and increasing quality.

5.5.1.2 Future Data and Multimedia Networks

As telecommunications networks evolve to satisfy customer needs for multiple media (e.g., voice, data, video, image, or mixed), telecommunications services may involve various types of circuit switches, ISDN switches, mobile phone switches, packet switches, signaling points, and fast-packet switches (e.g., frame relay, SMDS, ATM) in some overlay networks. Currently, there are stringent reliability criteria for voice networks and circuit switches and looser reliability criteria for packet switches and data networks. Different types of fast-

C

packet switches now have different reliability requirements. The robustness design and experience in new fast-packet switches are not as extensive as for the existing circuit switches, and the reliability implications of fast-packet switches already deployed have not yet been analyzed.

5.5.1.3 Multi-Supplier Interoperability

Networks of the future will continue to be built of equipment from multiple suppliers. For network elements from different suppliers to work together smoothly, the network elements must be rigorously designed to meet a set of unambiguous interface requirements. There is little opportunity to resolve interpretation of requirements issues before products are put into service, so these requirements need to be very clear. As long as we continue to use the English language for requirements, we will continue to have ambiguities. Some suppliers already use formal requirements languages, but the overall standards and/or requirements are still being written in English.

Furthermore, as new versions of the requirements are issued or new features are introduced into the network, requirements must recognize that not all elements will be able to support the feature at the same time. Typically, this means that the feature is not turned on until all elements are equipped to handle it. However, as extensions to a feature are introduced, it may not be possible to coordinate the introduction of the enhancement simultaneously in all elements. Smooth evolution of services in the future network must be part of all services planning.

5.5.1.4 Operations Considerations

Operations will play a critical role in the reliability of the network of the future. First, new technologies will bring with them some significant operations challenges, which if not addressed, could have a negative impact on network reliability. Second, some new technologies have the ability to improve network reliability significantly; e.g., SONET's self-healing capability. To illustrate these points, the operations area of Service Negotiation and Management is discussed below.

Service Negotiation and Management (SN&M) includes those functions that are needed to negotiate, configure, monitor, and control network services and the subscription of customers to those services. These functions include the operations systems aspects of network services, and the systems realizing these functions are not reflected in Figure 33, for simplicity. However, these functions are essential for reliable operation of services from the customer viewpoint and for timely and effective response to service troubles and outages, particularly as service control is distributed and involves more sources of service logic and more service providers.

In service negotiation, the goal is to provide the customer with a set of compatible features; the assignment of conflicting or incompatible features to the same customer may result in incorrect service operation. Proper assignment necessitates (1) pre-analysis of possible features; (2) analysis of inter-feature compatibility for the desired feature set (3) knowledge of the features currently active for a customer; and (4) the ability to install the new feature(s) and verify the total set of active features.

To achieve the above, service negotiators may require access to data base(s) recording all possibly conflicting features to which a customer subscribes (e.g., Customer Record Information Systems or Service Management Systems). These information systems would accurately reflect the features or triggers activated in SCPs and/or network elements (e.g., memory administration data bases). For final verification, service activation systems should verify that the resulting feature set is the intended feature set. Once service is activated, service management requires access, again, to the total state of features associated with customers. Service management also requires the ability to observe the operation of service logic and its execution platform through network surveillance systems.

Effective avoidance of assignment of conflicting features to the same customer is more difficult when a customer may obtain a feature from more than one provider, as is likely with third-party service provider scenarios. In such situations, various options are worth consideration. For example, a single negotiator may represent all service providers. Another possibility is independent negotiation and activation of features or feature packages than are known a priori to be non-interfering. As previously mentioned, when troubles arise in a multiple-provider environment, a major issue will be to trace the source of the trouble, particularly since customers may have no way to determine which network provider or third-

C

party service provider to approach.

In summary, operations systems will need to spot trends as well as discrete events, and take steps automatically for assuring reliability.

5.5.1.5 Future Trends

Suppliers are continually working to modernize their switches, to reduce costs and improve efficiency. Reliability and performance improvements are included in these programs. However, it is possible for "old" reliability problems to crop back up again as software is revised to improve efficiency (and patches are removed). Switch suppliers are continually addressing new technology opportunities; the reliability implications of these must always be analyzed as part of the evaluation. The benefits of any new technology must be weighed with the costs of that technology.

Some local exchange network providers have expressed an interest in moving toward larger central offices. This trend toward large central offices could be an attempt to satisfy one of two needs, each of which results in a different configuration. The first is the need for more access lines; in this case, the resulting central office would be much like the central offices of today, with a larger number of access lines. The second is the desire to limit the number of switches that require software changes to deploy new services. This reduction in the number of switches requiring software changes could decrease the cost of deployment. This need could result in a different configuration in which the desired service is deployed on one switch and other switches behave in some sense as remotes of that switch. This could be thought of as a "foreign exchange"-like arrangement, in which customers don't need to be directly connected to the switch providing the service.

Failures associated with larger switches are very likely to impact a larger customer base; therefore, a larger risk is assumed as switches grow in number of access lines. There is some debate regarding whether partitioning the switch into stand-alone modules improves the reliability of the switch. Supporters claim that experience has demonstrated better reliability; detractors feel that this has not been demonstrated practically and that the result is dependent on the type of failure.

There are cost and reliability benefits of larger switches; for example, there could be fewer procedures and less training of maintenance engineers required per access line. For the second configuration, there is the added potential of reliability problems because of the second switch and the transmission path to that switch. Failures on each of these would affect a larger number of customers. Past experience has found that the trunks linking remotes with the host switch are the primary cause of remote failures. If this is the case, then a highly-reliable connection is required between the linked central offices. All offices in this scenario need to be able to isolate and contain failures.

Network providers are designing new specifications for the software structure of their networks that would increase reusability and decrease cost through distributed processing and layering concepts. This architecture, called Information Networking Architecture (INA), could affect reliability in the future. Distributed processing makes redundancy more feasible, allowing less complex recovery from failures by using other elements. However, if the same software, with the same bug, is running in different places in the network, the reliability implications could be significant. Distributed processing within an element makes fault isolation more difficult; among multiple elements it will be even harder. Data management, or the knowledge of where data are located and how the data are accessed and updated, also needs further study in distributed processing environments. Finally, the speed at which elements in a distributed network respond to requests could have an impact on the reliability of the network/services.

Some local exchange network providers are moving in the direction of reducing the number of different switch software loads through the use of common sets of features. It has been suggested that the reliability of the network would improve by this practice, since the compatibility of various software loads and interworking network products is difficult to maintain. In addition to uniform feature sets, some providers are also attempting to maintain switches at roughly the same generic level. These can help to reduce the testing nightmare for manufacturers and network providers.

Since it would be impractical as well as risky to

C

"flash cut" all switches at the same time to the same generic level, differences of one generic level among the various switches in the network would be expected. This variance, however, would be kept to a minimum number of switches at any time. Rapid propagation of a problem into a network-wide problem could occur when a single generic is used. By permitting several generic loads to exist in the network, the chance of a single fault contaminating the network can be reduced. Further, the upgrades could be spaced over time and the technical staff would be more knowledgeable about the upgrade process and the details of a particular load. This could reduce the chance of aborts or reloads.

There are reliability issues which argue both for and against this kind of switch management strategy.

- Data have shown that upgrades to the network are responsible to some degree for a number of network outages. A few local exchange network providers have maintained their network at about the same generic software level and have found that it does improve the reliability.

- Uniform feature sets would minimize the need to retrofit a switch with new software containing features not in the existing system, but unexpectedly required for a customer. Assuming that features can be enabled without reinitializing the switch, common feature sets would reduce the number of outages. However, to avoid frequent retrofits as new features are introduced, long product lead times could occur. In an industry with rapidly-evolving technology, this may be impossible.

- As switches interoperate and communicate control information more frequently, compatibility among the communicating entities becomes increasingly important. Assuring compatibility between a wide range of generic levels can be difficult. Software developers must make sure that each subsequent level of software is "backward compatible" with a large number of earlier levels. Testing this compatibility can produce a matrix of test combinations that can be unwieldy and difficult to manage. Limiting the extent of backward compatibility eases this burden and therefore improves the likelihood of proper interoperability.

- By keeping generics at the same level (or within one level of each other), support efforts by service provider second-tier support groups such as the Electronic Switching Assistance Centers (ESAC) as well as switch suppliers can be more focused. This focused support can translate into cost savings in support personnel and deeper expertise in each supported generic level, and therefore fewer procedural errors.

- The practice of interdependent "flash cuts" to keep all switches at the same level is potentially risky and should be avoided. It is unlikely that adequate personnel (both service provider and switch supplier) exist to support widespread simultaneous retrofit activity. This increases the potential of error and long outages.

- If new software is installed on all switches in a network in a relatively short time frame, it is possible that an undetected bug could be introduced which could take down the entire network rather than just a few nodes.

5.5.2 Multiple-Provider Network Model

Having addressed the single-provider-network issues, the analysis is expanded to the more complex environment of multiple providers. It is possible to use a very simple model since single-provider issues were already depicted in the single-provider model. All new issues associated with multiple providers are depicted by the interfaces between providers. The rule of thumb to improve reliability appears to be to keep these interfaces as simple as possible without constraining the functionality available. The model, depicted in Figure 33, focuses on the reliability considerations associated with a switch resident in Provider A's network and its relationship with other providers, and to relationships between STPs. Note that the issues discussed in the previous section are still applicable; however, we added three new categories of concerns to reflect the additional complexity inherent in the multiple-provider model.

These three new categories are 1) concerns

C

associated with the coordination of software across network providers, 2) inter-provider mediation, and 3) concerns related to fault isolation and diagnostic messages. Benefits of multiple-provider networks are discussed below.

First, multiple-provider networks imply well-defined network interfaces and demarcation between service providers; this can improve network reliability. Also, multiple-provider networks represent alternative routes or services for customers. For example, cellular, as part of the overall telecommunications network, has provided vital communications means during recent natural disasters that took down wireline networks. Finally, the availability of Advanced Intelligent Network capabilities will allow customers to specify a primary routing destination, a secondary one, etc. The network will then be able to hunt through this prioritized list to reach the subscriber for incoming calls. These destinations may belong to different service providers and are therefore unlikely to all fail at the same time.

5.5.2.1 Coordination of Software Across Network Providers

In the multiple-provider network, each interface is defined by public standard protocols, such as CCS7, ISDN, or MF trunking. The additional challenge that this network architecture implies is that each such component may be designed by different manufacturers and administered by different companies. So while the basic components of the architecture are similar to the single-provider model, the service assurance is made more complex because two additional dimensions are added. At a purely functional level, the coordination of software across network providers can be quite simply defined as ensuring protocol conformance at each level of interface. While this definition is simple to state, in practice it is quite difficult to ensure. Networks today use a wide range of protocols to exchange information. Conformance to those specifications has proven challenging in today's networks. Key reasons for this are:

- Each manufacturer may interpret aspects of the protocol differently. This can lead to cases of incompatibilities, even when manufacturers claim conformance to the specifications.
- There is limited multi-supplier testing until products are deployed. Any incompatibilities are typically found in an in-service environment, with potential customer impact.

5.5.2.2 Inter-provider Mediation

Interfaces that network providers may make available to third-party service providers in the future may include (1) an application programming interface through which a third-party executes its own service logic on a service logic execution environment provided by the network provider, or (2) an application protocol interface through which a third party connects its common channel signaling network into the signaling network of the network provider. A fundamental issue in supporting the addition of third-party services to telecommunications networks is the trade-off between service functionality and network reliability. Can we enable third parties to add new services to a telecommunications network without endangering the correctness, reliability, or performance of existing services? Such interfaces exist today, but they are clearly defined and the amount and type of information passed through these interfaces is limited.

However, even in today's relatively simple environment, a service provided by a third party can disrupt network performance, e.g., media-stimulated calling offered by a third party can cause overloads in the access network. The specific design problem for the interfaces that are opened up is to simultaneously (1) export enough functionality so that all useful third-party services are supported, and (2) export a sufficiently-constrained functionality so that no third-party service can disrupt the public network, other services, or other users. As more general interfaces are made available, some very difficult problems arise.

Three examples are discussed below:

1. A third party may use an open interface in a way which, although it is neither an error nor illegal, the network provider finds objectionable. Examples would be: initiating automatic repeat dial on busy every second for a period of hours, using some personal-number calling interface to track continually the physical location of a subscriber (e.g., one could imagine the

C

news media wishing to track the location of some political candidate), or sending, from a travel agent's computer, queries every minute for a month to an airline reservation system in an effort to secure cheap seats on a heavily-booked flight. This aggressive access could result in a network overload situation, affecting other services using the network.

2. When multiple players are involved in a service, it is desirable but may not be possible to be able to assign responsibility for failures unambiguously. When a failure is clearly the responsibility of one party or the other, the responsible party can respond in the usual way by taking corrective action. Unfortunately, there may be many failures where the responsibility for correcting the problem is somewhat ambiguous, e.g., suppose a faulty third-party ACD erroneously delivers some huge number of calls to some innocent, uninvolved customers. In this situation, the network provider may feel pressure to take some corrective action, although the source of the trouble is clearly within the third-party service provider's equipment.

3. Bugs in the service logic of a third-party service provider (e.g., commanding an unreasonable amount of resources for a single call) may have an impact the network providers' network.

Two categories of services in the multiple-provider environment are envisioned. The first category is those services that will involve multiple service/network providers transparently to the different providers involved. For example, a network provider may provide access and routing to an information service provided by another provider. The network provider might not even be aware that this service was using its network to complete. For this category of services, reliability implications are no different from those of a single-provider network. The service provider's service could be affected by any failures or congestion of the underlying network used; this cannot be prevented. (The service provider may wish to have alternate facilities available to prevent a network failure from affecting its service). The network provider can use its standard measures for controlling congestion and failures, including, if necessary, blocking the service provider's traffic. One exception to this is media-stimulated, or mass calling events, which can and do cause widespread service interruptions.

The second category of multiple-provider services is those for which negotiations are needed between providers. In this case, a service cannot be offered without the agreement of each provider, i.e., tariffs and/or contracts are needed between providers, to share information or to offer certain interfaces to each other. Part of the process of providing this category of services in a multiple-provider environment is the negotiation of each provider's level of participation in that service. A key concern for this category of services is the need to ensure that a provider involved in the offering of a service cannot affect the reliability of another provider's network or service in directions that violate the recommendations described below.

Other key concerns in a multiple-provider network are those related to the coordination of services and capabilities across those providers. From a customer's perspective, transparency across the different providers is almost always required.

5.5.2.3 Fault Isolation and Diagnostic Messages Across Multiple Providers

In multiple-provider networks, the issue of identification, isolation, and resolution of problems becomes much more complex. This is mostly attributable to the lack of common jurisdiction over any given problem. When an end customer (telephone or data user) is unable to use a given service, in the single-provider network there is a very clear responsibility for problem resolution. From the protocol perspective, this challenge of accountability can begin to be addressed by building verification capabilities into network components. Real-time identification and isolation of problems will help speed ownership and identification of the responsible provider. Protocols must be built for all eventualities. This means that specification must include performance both at normal (engineered) loads as well as overloads. This provides a clear, defined mechanism for dealing with problems and isolating problems from different network elements.

C

5.5.3 Future Network Recommendations

Recommendations to address the issues raised in Sections 5.5.1 and 5.5.2 are provided in this section.

1. A holistic industry view of total network reliability is advocated, to prevent each supplier from developing controls and solutions that could conflict with others' attempts. Reliability requirements must be developed and followed in the network of the future for all new technologies, integrated with the design of new features and capabilities.

Increased industry cooperation in the form of reliability forums is recommended, e.g., workshops on fault-tolerant systems. In addition, chartering an objective network monitoring body is recommended. This monitoring function could also be extended to help delineate and resolve areas of potential dispute when service outages impact multiple suppliers' equipment and transcend single-provider boundaries.

2. A generic model should be used for mapping network components, analyzing them, and making recommendations. This matrix proposal addresses the software reliability issue with more formality, rather than the inherent randomness associated with brainstorming reliability issues. The benefits of this method are: (1) by studying the generic network model, you can define rules which generally govern reliability of any network, current or future, and (2) by studying a specific network architecture and failure, you can identify specific network architecture or network component weaknesses.

The proposed generic network model consists of two major components; a network component (including CPE, Access Platform, Network Platform, and Service Platform) and a software component broken out into logical software layers (including hardware and controlling software, system software, and application/feature software). These items can be represented in matrix form as presented in Figure 34. Each matrix "box" represents a logical network component and related software component. Common borders between boxes represent signaling protocols, both proprietary (e.g., communication between software layers within a single network component) or standard (e.g., communication between network components). Examples of elements found in today's networks are mapped to their respective "box" and signaling interface in Figure 35.

It is now possible to define different fault types and fault scopes/impacts from this generic network model. Below are some examples of faults. Refer to Figure 38 for graphical representation of the faults.

Fault Type 1: Error in the feature software of a single Access Platform (e.g., Class 5 switch). Fault Scope/Impact: At most, the operation of that single feature should be impacted within that single Access Platform. No other software on the Access Platform nor any other network element should be impacted. Network impact is low.

Fault Type 2: A service platform goes out of service. Fault Scope/Impact: At most, the operation of features on the single service platform are affected. Network impact is low.

Fault Type 3: Network platform basic software layer finals (e.g., OS). Fault Scope/Impact: New calls requesting setup through the failing Network Platform will not complete. Network impact is high.

The more serious errors, for example Fault 3 above, may need further investigations to determine how the scope can be minimized. In the case of the Network Platform failures, it may be necessary to add signaling scheme enhancements to provide routing capabilities which minimize the fault scope/impact. These rules can be defined independently of specific network configurations. In addition to general fault definition, the matrix could be used to help report and study field faults. Field faults, for example, could be reported in terms of network scope/impact (e.g., Three-Way Calling was not operational for 3 hours, or an access platform was not operational for 5 minutes causing loss of service). Actual fault cause would then need to be determined and mapped onto the matrix in terms of Network Component and Software Component. These data could be studied to determine how well the fault type matched the fault scope/impact and to identify signaling or platform deficiencies.

This model provides an abstract platform on which to study reliability issues and complements the current, more detailed team work. The sub team

C

recommends that this model be further analyzed to determine its merits. If accepted, this model should then be used as the basis for generic reliability recommendations such as:

- Failures should not propagate down the columns of the matrix. For example, a failure in an application should not have an impact on the basic software or basic hardware layers. In addition, failures should not propagate to the left in any row; that is, an error in a service platform should be prevented from affecting the network platform, and so on.

- More information needs to be passed vertically between the software layers and horizontally between platforms to improve fault isolation and verify the functional integrity of the network.

- Industry-wide standards should be developed for fault-typing. This methodology could be used. Then fault requirements (or reliability requirements) should be developed for each fault type.

- Requirements for each aspect of each protocol should have a pre-defined test case(s) to validate the functionality. This would provide a benchmark of compliance for the entire industry, and would further enable each manufacturer to execute a common test suite on a per-release basis, identifying any potential incompatibilities. This also minimizes the different interpretations that can arise to each specification. The definition of that test suite must be part of the specifications themselves, so that any changes to the specification will result in changes to the test suites. A common set of test cases would also allow specification writers (which includes the entire industry for public protocols) a critical analysis of every aspect of the protocol. This may further identify untestable or poorly-defined specifications.

3. The following recommendations should be incorporated immediately into future requirements, standards, and/or specifications:

- Industry requirements being developed for data and multimedia switches should include reliability requirements that are consistent with customer needs. In addition, the reliability implications of fast-packet switches currently being deployed should be analyzed.

- Requirements should be written using unambiguous specification languages that can also produce test scripts quickly.

- All requirements should include pre-defined test case(s) to validate the functionality.

- Requirements developed should also be backward-compatible when appropriate.

- Operations requirements for new technologies should include means for ensuring high reliability, including data collection, measurements, and tools. Methods and procedures should be identified to ensure that any failures that do occur are contained and quickly remedied. In addition, operations requirements must always attempt to eliminate the need for human intervention.

- Requirements should specify that switches are insulated from impairments in elements that house service software (whether third-party software or not) and that service software should not be able to impair network elements. The methodology proposed in the previous section could be used to understand the firewalls that need to be established.

- Both in AIN and in open network architectures, requirements should specify that switches must be able to interwork with the elements that house service software to provide services to the end users. The activation of new features must not impair the network.

- Requirements being developed for data and multimedia switches should include reliability requirements that are consistent with customer needs. Input for these requirements can be obtained by analyzing fast-packet switches currently being deployed. Analysis of the applicability of mature fault-handling technologies in circuit switches and new distributed fault-tolerant schemes to the design of new and

C

evolving fast-packet switches must be done.

- Requirements should specify that the structure of generic loads be flexible and permit the layering of applications and features without exposing the customer to disruptions in the network when changing the underlying generic software.

- Requirements for each aspect of each protocol should have a pre-defined test case(s) to validate the functionality. This would provide the entire industry a benchmark of compliance. This would further enable each manufacturer to execute a common test suite on a per-relase basis, identifying any potential incompatibilities. This also minimizes the different interpretations that can arise to each specification. The definition of that test suite must be art of the specifications themselves, so that any changes to the specification will result in changes to the test suites. A common set of test cases would also allow specification writers (which includes the entire industry for public protocols) a critical analysis of every aspect of the protocol. This may further identify untestable, or poorly-defined specifications.

4. The following recommendations should be considered when multiple providers are involved in the provision of service to customers:

- The network provider and the third-party service provider negotiations must ensure that reliability concerns are addressed. This may go a long way toward solving the problem of assertive use of an open interface. Generally, a network provider who is fully recovering its costs can be indifferent to extremely heavy use of some open interface; however, there are exceptions, such as when the heavy user can impair other network traffic. Network and service provider negotiations could also include a more expansive notion of access to cover not just the correct use of a single invocation of an open interface, but rather to cover an overall pattern of access.

- Service providers should negotiate and plan media-stimulated events with network providers prior to the event. While there is no single solution to neutralize the vulnerabilities associated with such events, the sub team recommends notification and planning in advance of the event. An example of this is Pacific Bell's efforts to: (1) provide detailed methods and procedures, process control, and account team/customer educational material designed to enhance and support event notification and planning, and, (2) implement a performance-based treatment policy. This policy has clearly-defined expectations regarding media-stimulated calling generators, such that successive service impairment incidents, absent event notification and planning, result in progressively grave responses (up to permanent disconnection of media-stimulated calling service).

- Service and network providers should design the necessary firewalls, preventing failures from spreading to the other provider's network/service, be part of the negotiation between providers prior to the offering of the service.

- All participants in the provision of services that use the telecommunications network should be required to meet the same standards for network/service management.

- The providers should also agree during the negotiation process on how failures will be identified and isolated when there is a service problem, including who is responsible for taking action when necessary. This isolation of a service problem is expected to be difficult in multiple-provider environments.

- The providers will also need to recognize which software release upgrades will affect other providers in the arrangement and will need to determine a process for scheduling upgrades.

- Customers should have a single point of contact for any particular service for service provision, questions about the service, billing, failure-reporting, etc. (Note that this implies that a customer could have many single points of contact.) This coordination

should be negotiated in advance of service deployment.

- Any interface that is created must not adversely impact the integrity, reliability, security, and privacy of the network or services provided in the network. This protection that is needed can be accomplished through mediation, either internally at various points within networks, within administrative systems, through manual procedures, and at access points to third parties. Currently, many of the mediation functions are done manually and many of the automated functions are typically performed outside of call processing. Generic interfaces must be developed to address application-independent needs.

- Complementary fault isolation and diagnostics processes need to be developed to manage services involving multiple providers.

5. An industry group should be asked to work these issues which will have an unknown impact on reliability or those for which no solution has been determined:

- Service creation implications on reliability should be analyzed by organizations developing Intelligent Network specifications. (Priority = high)

- Alternatives for the management of interoperability testing should be identified and analyzed. The proposal that follows consists of five steps that require the cooperation of the telecommunications industry: (1) A product (machine or software) to be deployed in a network needs to pass some process standards, such as ISO 9000. (2) The product needs to pass some measurable product-oriented acceptance criteria in functionality, performance and reliability (e.g., measurements in RQMS, software failure density and test coverage, capacity to handle traffic). (3) The product needs to pass some measurable network interface and system integration criteria (e.g., conformance to standard protocols, firewall and failure localization mechanisms, trap and trace utilities, degree of release independence). (4) Effective testing on service providers' sites for node and network integrity needs to be conducted before deployment. (5) Overall network performance as well as single-provider performance needs to be monitored and analyzed for continuous improvement in acceptance criteria, product quality, and network integrity. Implementing this process will establish a proactive approach to ensuring network integrity as network complexity increases in future open network configurations. (Priority = high)

- Procedures need to be identified and established to identify and isolate faults in the network, send diagnostic messages between providers, and collect error information for network-wide problems. (Priority = high)

- Fault-typing, as proposed in the previous section, could be evaluated as a means for identifying where firewalls need to be established for current and future technologies. (Priority = medium)

6. Hardware and software designers must work together to synergistically perform system design. This recommendation is submitted for consideration although not directly discussed with respect as to future networks.

5.6. Network Congestion

A review and analysis of network outages by Bellcore reveals that of 5025 events reported only 34 or .7% involved an overload situation. Thus, overload does not represent a significant portion of network outages.

Most end office switches have automatic overload controls which have been designed to limit the overload impact on customers served by the end office affected. Service providers have network management tools which allow for fast reaction to an overload condition when it does occur. They are able to detect most conditions early enough to prevent the impact from spreading beyond the local area.

However, at least three events have demonstrated the impact that a failure, due to congestion, of the SS7 networks in a local network, can have on the

C

national network. The preventions for this type of congestion are: the safeguards that are being designed by the system suppliers providing and installing the network components, the service providers utilizing effective methods for operating and maintaining their SS7 networks and close coordination and interoperability of the SS7 network, and joint efforts between telephone companies and customers to manage Media Stimulated Events. The NRC's Signaling Systems Focus Area is making recommendations on this area. The Network Operations Forum (NOF) is also continuing efforts to ensure the reliability of the SS7 network.

Examples of the events that can cause network overload are: high volume traffic, civil disturbances, natural disasters, weather conditions, equipment trouble, power failure, and media stimulated call generation. Natural disasters are responsible for a high percentage of the network congestion events that do occur. Hurricane Andrew in Florida and Louisiana and the earthquakes in California are recent examples. The application of Network Management both locally where calling originates and in the end offices where traffic is being directed prevents the overload impact from spreading beyond the local area.

The only cause that falls in the category of a "planned event" is media generated mass calling. This may be a radio talk show call in, ticket selling by phone for a high attraction event like Garth Brooks, telepolling and lotteries for something valuable advertised in the print media. These mass calling events have been an "overload" issue for the telephone service providers for over ten years but have been growing in volume during the past five years. In general, they have been managed by telephone companies with a great deal of success.

5.6.1 Network Congestion Recommendations

Most service providers have policies relating to mass calling service. Many providers put mass calling lines on a choke network which automatically limits the calls and limits the service impact. Others rely on cooperative event notification and planning to prevent network overload; if the mass callers follow the guidelines and notify the service provider in advance of their plans, service impact is minimized and the network is protected. The potential overload problem occurs when the service provider does not have enough information about a media stimulated mass call in to implement network management controls before the event occurs. The only protection of the network becomes the network management controls which must be initiated after the overload has occurred. These situations are usually contained within the calling area; in large cities like New York the originating calls are spread over may offices. The terminating office is impacted until controls are in place.

The protection of dial tone in originating and terminating switches affected by media stimulated calling incidents is important. Standard engineering practices tend to balance central office resources (digit receivers, memory blocks, network paths, etc.) such that excessive originating demands for service are denied early on in call processing. Returning dial tone to a customer's bid for service, then, is contingent upon an adequate supply of switch resources to handle the call. Dial tone is denied if switch resources are unavailable.

In addition, all switches employ defensive strategies to protect the essential health of their processors and critical components during system overload. Automatic overload controls in response to switch congestion include three strategies: (1) Improve the availability of scarce resources; (2) prioritize the system's processing tasks to make resources available for new calls; (3) limit the rate that new calls are entered into the system (delay dial tone).

Essential Service Protection strategies are involved during periods of severe switch congestion. Essential Service Protection is aimed at assuring that a number of lines designated by the service provider as "essential" receive priority originating service during periods of extreme overloads, in order to assure continuation of critical community services (e.g., 911).

A nationwide, inter-industry Media Stimulated Calling (MSC) Task Force was chartered in March of 1991 to discuss and identify key issues and to draft problem statements regarding MSC events. These issues were brought to the attention of existing national forums, who acknowledged responsibility to address and resolve the issues.

The MSC Task Force was chaired by Bellcore and

C

consisted of members from Ameritech, AT&T, ECSA and its sponsored forum, the NOF, Call Interactive, Clarion Marketing, Exchange Carrier Standards Association, GTE, MCI, Sprint Telemedia, Nynex, US Sprint and USTA.

After a series of meetings and conference calls the following accomplishments were reported:

- MSC event logistics have been significantly influenced due to increased communication amongst industry participants and better understanding of the impact that an MSC event can have on the network.

- MSC network data and national planning guideline issues were thoroughly discussed. Key issues and addenda to existing issues were introduces and accepted by the NOF (i.e.,: NOF Issue 131 800/900 call blocking data and NOF Issue 124 Prior Notification of MSC events). An MSC Program Evaluator and an MSC Event Profile document were designed as tools to facilitate successful planning and implementation of MSC events.

In follow-up to the above, the NOF has solidified and codified the exchange of information relating to MSC events between Local Exchange Carriers and Interexchange Carriers. This resolution of NOF Issue 124 defines the event parameters and the time notification requirements prior to a mass calling event.

A recent study of mass calling incidents by some service provider subject matter experts identified three media stimulated calling serving arrangements that carry an exceptionally high risk of service impairment:

- arrangements using SS7 trunk signaling
- arrangements that use 800 numbers
- arrangements that provide mass calling services at E911 tandems

The high volume call-in network is better suited for mass calling events.

Service impact is minimized or even eliminated when the mass calling event is known about and planned for. Therefore, service providers are:

- Putting great emphasis and stress on customer education by providing detailed methods and procedures, process control and internal/external customer education material to enhance and support event notification and planning.

- Implementing policies with clearly defined expectations regarding MSC Generator notification and planning responsibilities.

With a policy in place, service providers will become even more successful at minimizing the number of unplanned media stimulated calling events that result in network congestion.

6. Key Learnings and Best Practices

Section 5 presented the data analysis and recommendations in specific areas related to switching system reliability. Service providers and system suppliers should make use of the information in Section 5 in identifying best practices that may be effective for their use in improving switching system reliability.

The expression "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 SSFA, and concurred by the Network Reliability Steering Team (NO REST), to be especially effective are designated in the Technical Papers 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.

The recommendations listed below were common across two or more of the individual areas studied by the SSFA and should be implemented on a global basis.

1. Individual service providers should standardize their processes for capturing and reporting timely and complete data on switch outages.

C

A finding common to all the sub teams efforts is the necessity for service providers to standardize the process of capturing and reporting timely and complete data on switch outages and to share the information with their system suppliers. Such a data capturing and reporting process will provide early warning signals that are especially critical as new technologies are introduced. This process will also allow for trends to be observed for tracking the effectiveness of implemented countermeasures. A requirement of such a process is that it be easy to use for the reporting organizations and that in turn value is provided back to them as a result of such reporting. A standard, electronic data collection format will facilitate the collection of timely and complete information.

2. A wide ranging set of industry standards and specifications should be created and made available for use by industry participants, service providers and system suppliers alike.

The SSFA identified the need for a wide ranging set of industry standards and specifications that would be created and available for use by industry participants, service providers and system suppliers alike. Areas needing such specifications and standards include (but are not limited to) the following topical areas: fault tolerance, human factors, minimum operations specifications for new technology and the resolution of reliability issues concurrent with the development and commercialization of new features/functionality. In addition, reliability specifications and standards for the various subsystems of switches (hardware, software etc.) need to be established and used early in the design process of new switching products.

7. Metrics

The FCC's Threshold Report has been chosen by the NRC as the macro level overall indicator of network reliability. The challenge for the various focus areas is to identify quality indicators for their respective areas that, when improved, will lead to improvement in the FCC Threshold Report indicator.

The SSFA has selected the following quality indicators for the purpose of improving switching system reliability :

a) **number of outages/switch/year, for all switches**
b) **duration/outage, for all switches**
c) **lines impacted/outage, for end office switches only**

The SSFA sub teams have suggested objectives for improving specific areas of network reliability. Measurement of the above metrics should be a good indicator of achievement with respect to those objectives. These metrics should be used by individual service providers and system suppliers in analyzing the effectiveness of steps taken to improve switching system reliability. They should also be used in summarizing the data provided in the FCC Threshold Reports.

8. Recommendations for Sustaining Work

As was stated in Section 6, the SSFA identified the need for a wide ranging set of industry standards and specifications that would be created and made available for use by industry participants. Additionally, in Section 7, three quality indicators are proposed to monitor and track switching performance in the network. An obvious question arises, "who or what body, if any, should be charged with analyzing the FCC Threshold Reports and any additional data determined necessary?"

There are many existing efforts sponsored by the telecommunications industry members aimed at improving overall network performance and reliability. Appendix C summarizes current industry initiatives that pertain to switching systems reliability. Among these efforts are various forums sponsored by the Exchange Carrier Standards Association (ECSA) such as the Carrier Liaison Committee (CLC), Network Operations Forum (NOF), Committee T1, etc. Bellcore, the research and development consortium owned by the seven Regional Bell Operating Companies (RBOCs) conducts network integrity and quality assurance studies to support service standards and procurement policies of its client companies and issues technical standards of performance to industry at large to further enable service reliability and network integrity. In short, there are many efforts in place that are effective in working toward a more reliable network infrastructure.

In determining an organization for sustaining the

C

focus area work, the SSFA developed the following criteria for evaluating the organization to be charged with such a responsibility.

a) Broad based industry participation and support.

b) Must operate effectively and with a sense of urgency in the establishment of standards and requirements yet must not be perceived as running roughshod over segments of the industry.

c) Must not be Ad Hoc; this function must reside in a well-established organization.

d) Must have technical competency or sufficient technical knowledge to effectively contract for technical work needed to discharge it's responsibilities.

e) Must be funded by all industry participants in an appropriate manner.

Given these criteria, the SSFA believes that the ECSA is well suited to carry out the following recommendations.

1. The ECSA should collect and monitor the FCC's Threshold Reports and provide a quarterly summary of the results to the FCC.

The recommendation of the SSFA is that the ECSA be responsible for collecting and monitoring the FCC's Threshold Reports, performing macro analysis and providing quarterly summaries of the results. If the results indicate a negative trend in switching system reliability, the ECSA will determine the need for additional outage data and further action.

2. If necessary, based on analysis of FCC Threshold Report data, additional outage data should be provided by service providers and system suppliers for root cause analysis and identification process.

To facilitate this possible need for additional data, a standard format, similar to the SSFA data request and modified as necessary based on earlier recommendations in this report, should be made available for use by service providers and system suppliers. In addition, an electronic means of reporting the additional data should be made available. Service providers and system suppliers will therefore need to implement internal procedures that will ensure the availability of the necessary data should a need arise.

9. Conclusions

While the recommendations in Sections 6, 7 and 8 of the SSFA are focused on collective industry efforts, service providers and system suppliers have the opportunity to implement many of these recommendations on an individual basis. Most, if not all, industry participants have ongoing quality improvement processes into which these recommendations can be incorporated.

The SSFA has examined current causes of switching outages and possible future reliability issues within this report. Given the level of interest and participation in this effort, other industry efforts noted herein, and the many other forums addressing similar topics, it is reasonable to expect that the current high level of reliability will continue and improve.

10. Acknowledgments

The SSFA wishes to thank Mick McCarthy for his ongoing counsel and support of the team's efforts. The team also wishes to thank Ross Ireland, and Eva Low, both of Pacific Bell, for their advice and instruction provided in their respective roles as Chair and Technical Assistant of the NRC Steering Team.

The team would like to extend a special thanks to Roshan Chaddha, John Healy, Yangwei Wang and all the Bellcore Subject Matter Experts noted in Section 3.1 for their efforts in collecting and analyzing the information requested by the SSFA sub teams.

The team would also like to express its appreciation to Roy Sheldon, Northern Telecom Inc., for his contribution on network congestion included in this report.

The SSFA discussion on metrics included the work of John C. McDonald, MBX Inc. (formerly of Contel Corp.) and Dennis Adams, NYNEX.

The SSFA appreciates the diligence of all the industry single points of contact in collecting and

C

supplying the information required for this investigation.

This report itself is evidence of the significant level of cooperation and involvement of the SSFA and its sub teams in all team activities. The results reflect the incorporation of the user, service provider and system supplier perspectives combined with the vast experience of the individuals on the team.

11. References

[1]*The Central Office Switch Databook* (1992), Lynda Starr, Probe Research, Inc.

[2]*The Reliability of the Telephone Network*, Richard Fagerstrom and John Healy, Bellcore, to be published.

[3]Minutes of the Network Reliability Council Meeting of November, 1991.

[4]*Team Leader Course Participant Workbook, Second Edition*, Qualtec Quality Services, Inc., 1987.

C

C

12. Figures

C

12. Figures

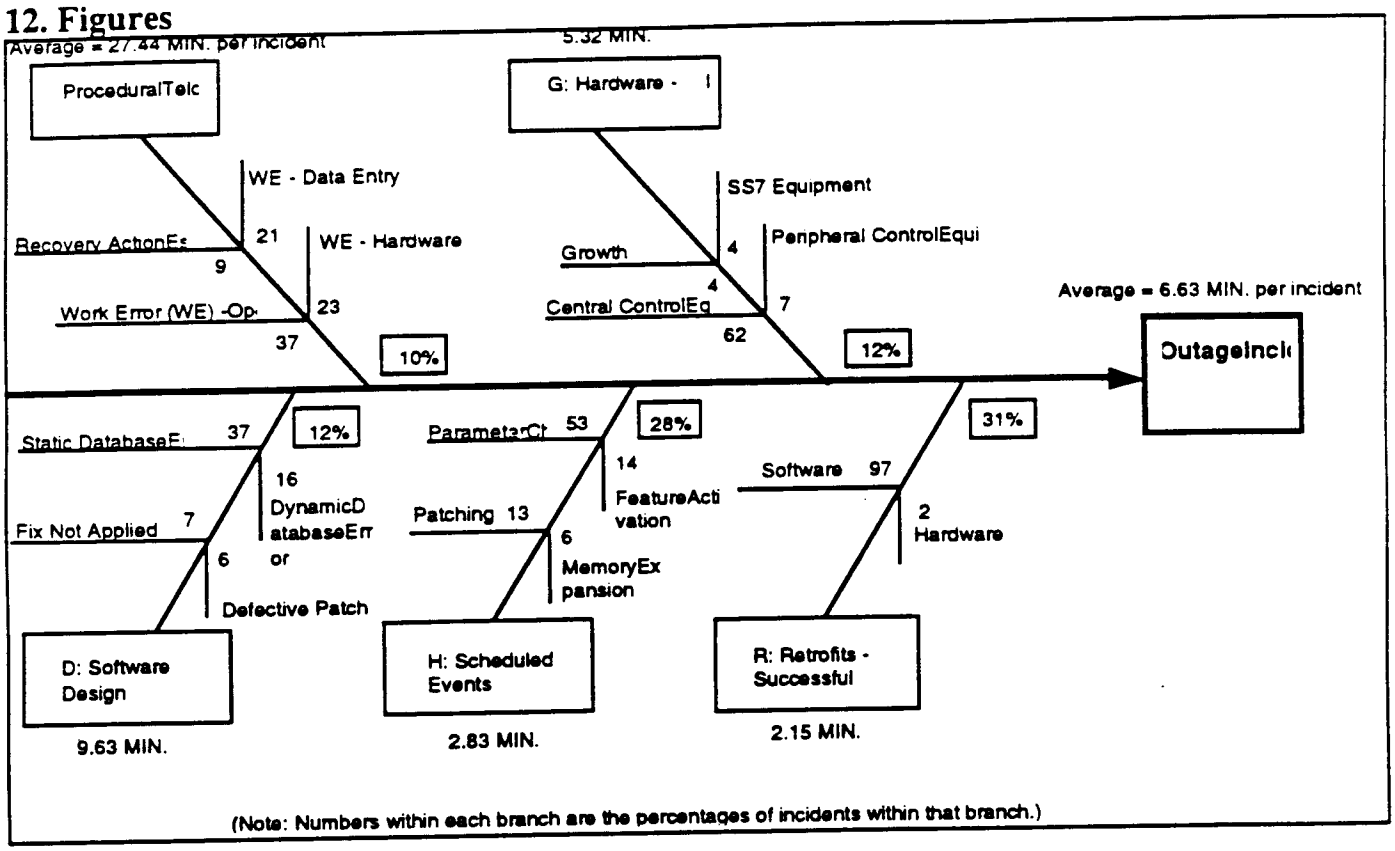

Figure 1a: Causes of Total Outage Incidents (Bellcore 1H92 data)

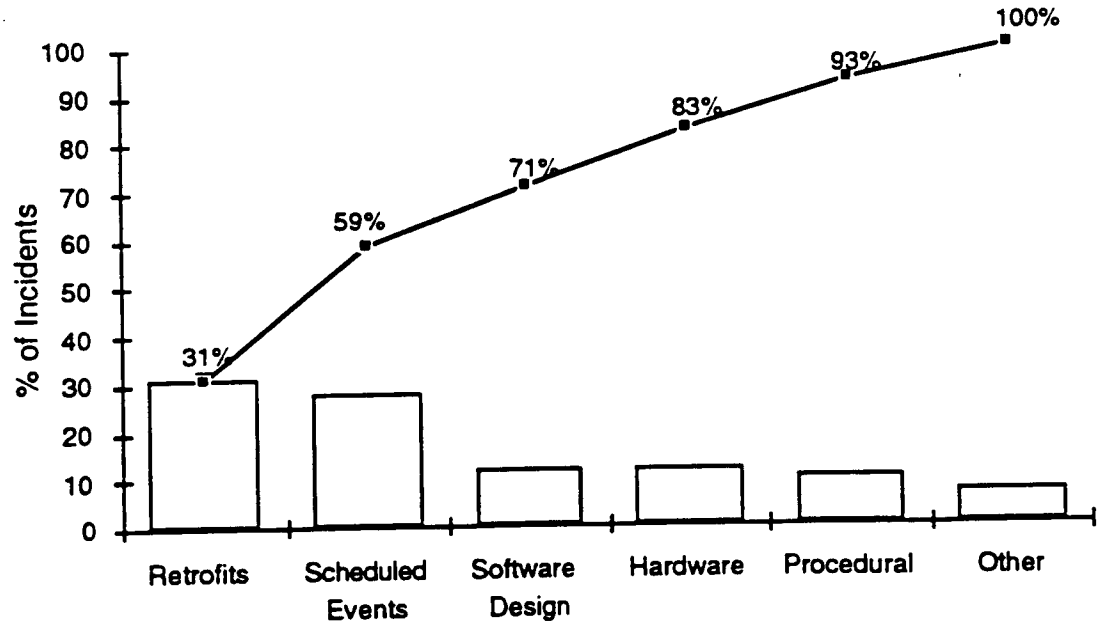

Figure 1b: Causes of Total Outage Incidents (Bellcore 1H92 data)

C

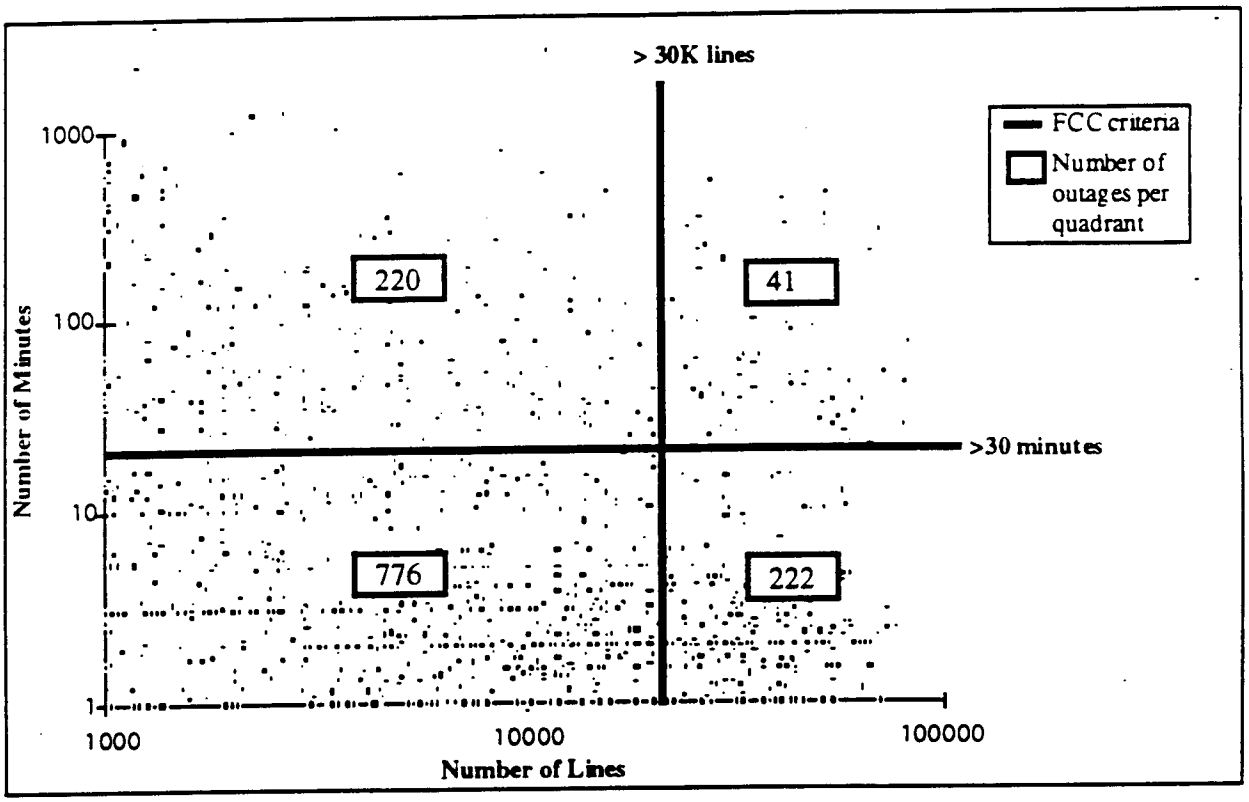

Figure 2: 2Q and 3Q SSFA Outage Data

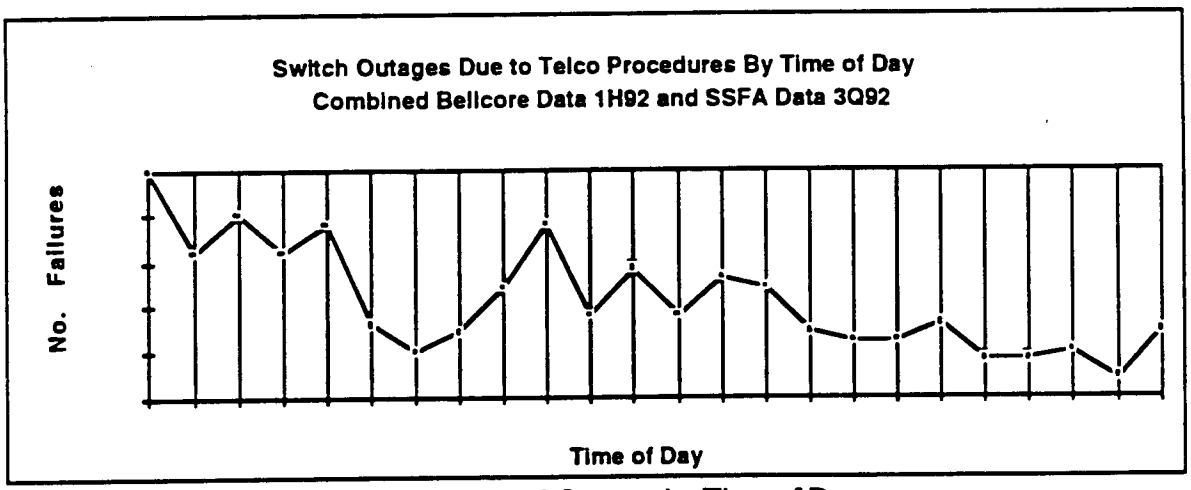

Figure 3: Procedural Outages by Time of Day

C

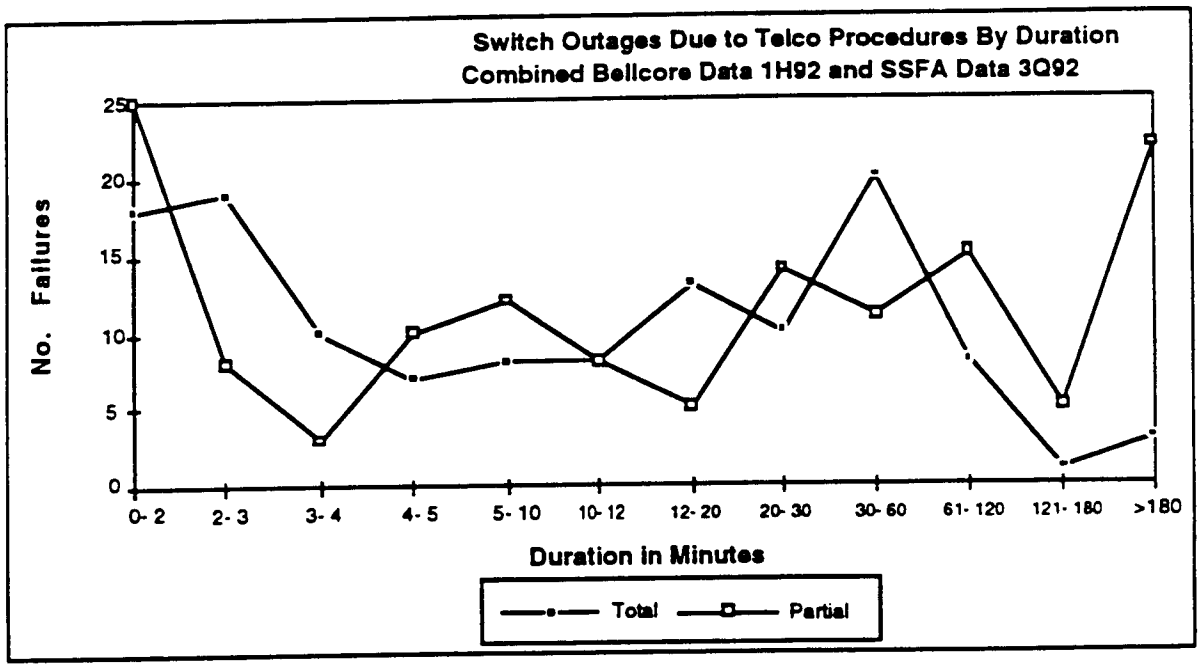

Figure 4: Procedural Outages by Duration

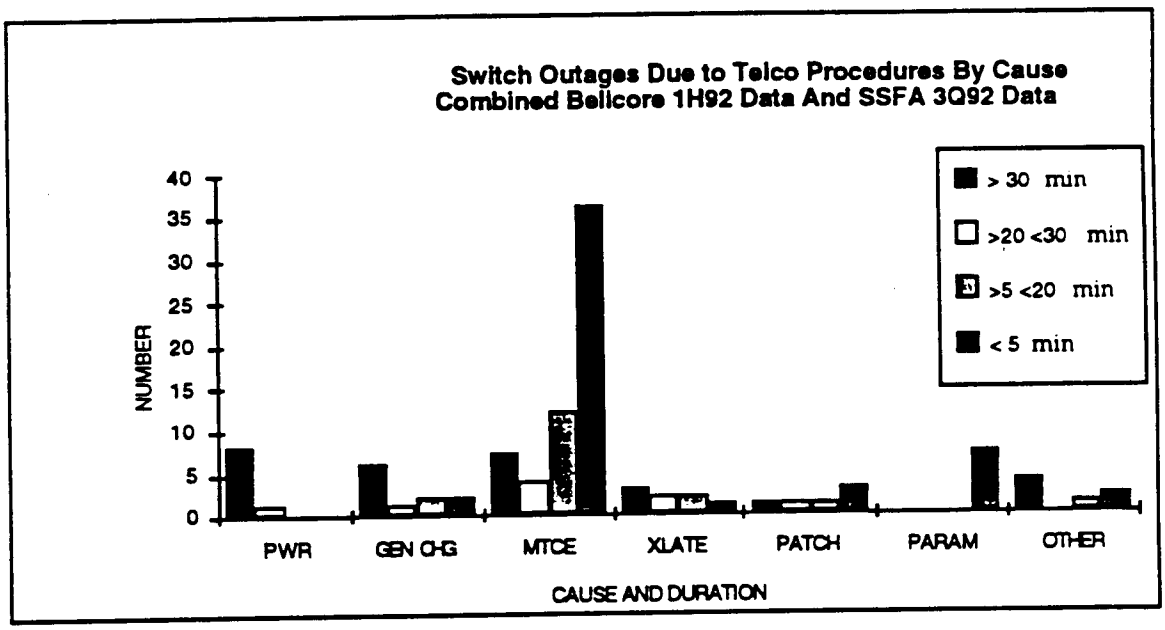

Figure 5: Total Procedural Outages by Cause

C

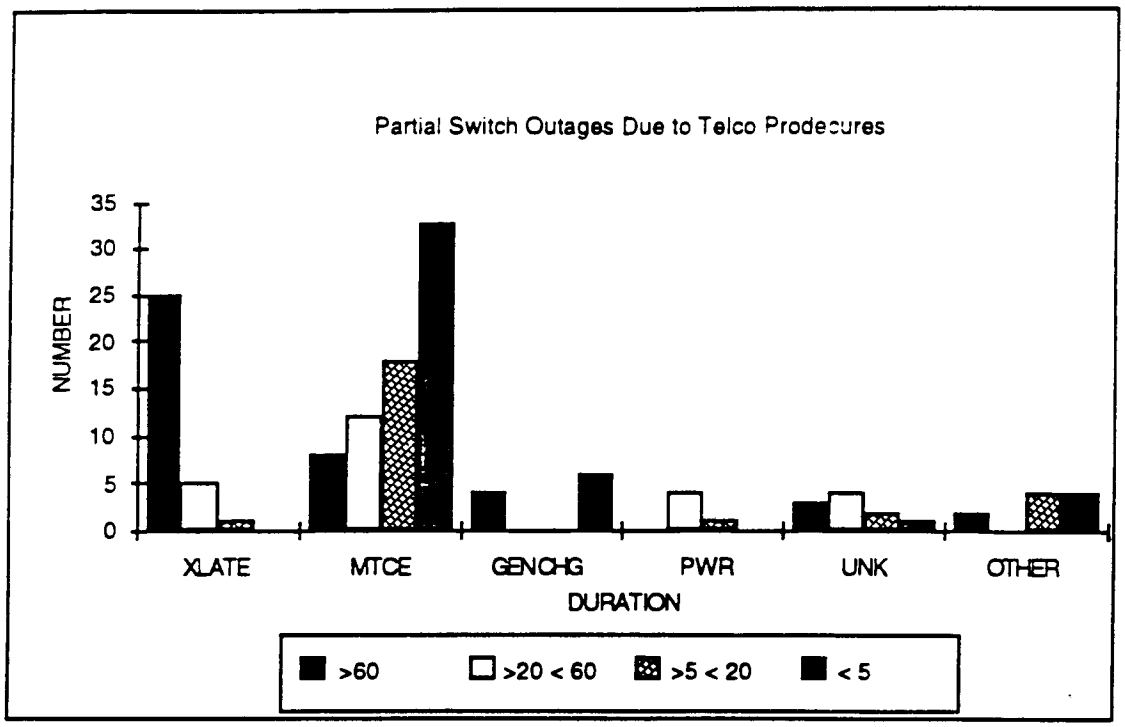

Figure 6: Partial Outages by Cause

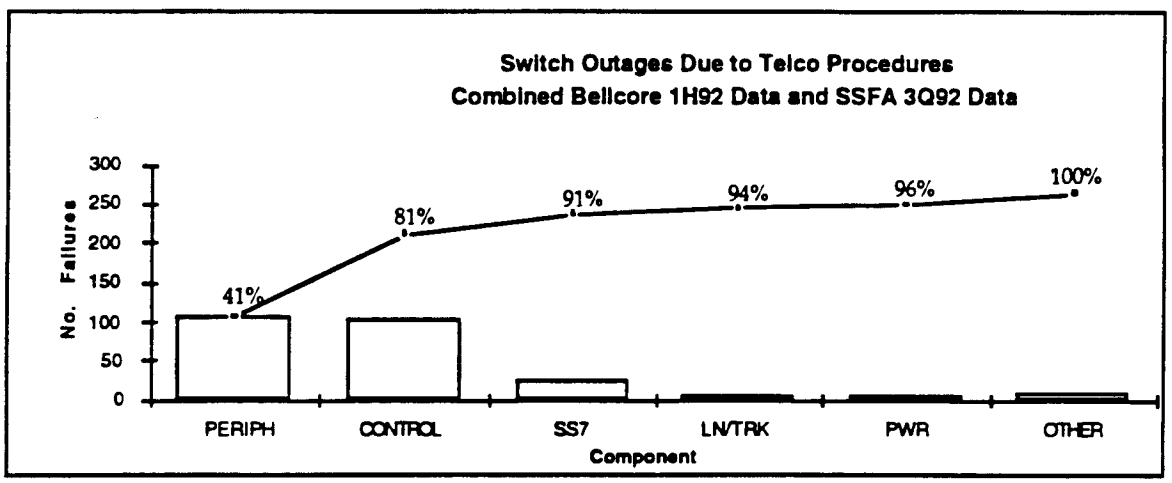

Figure 7: Procedural Outages by Failed Component

C

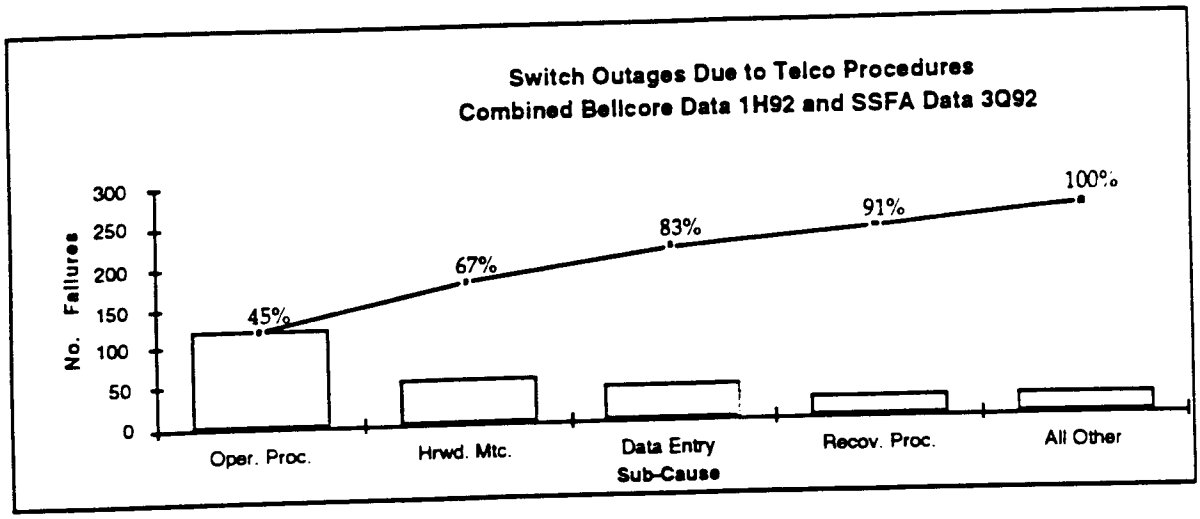

Figure 8: Procedural Failures by Sub-cause

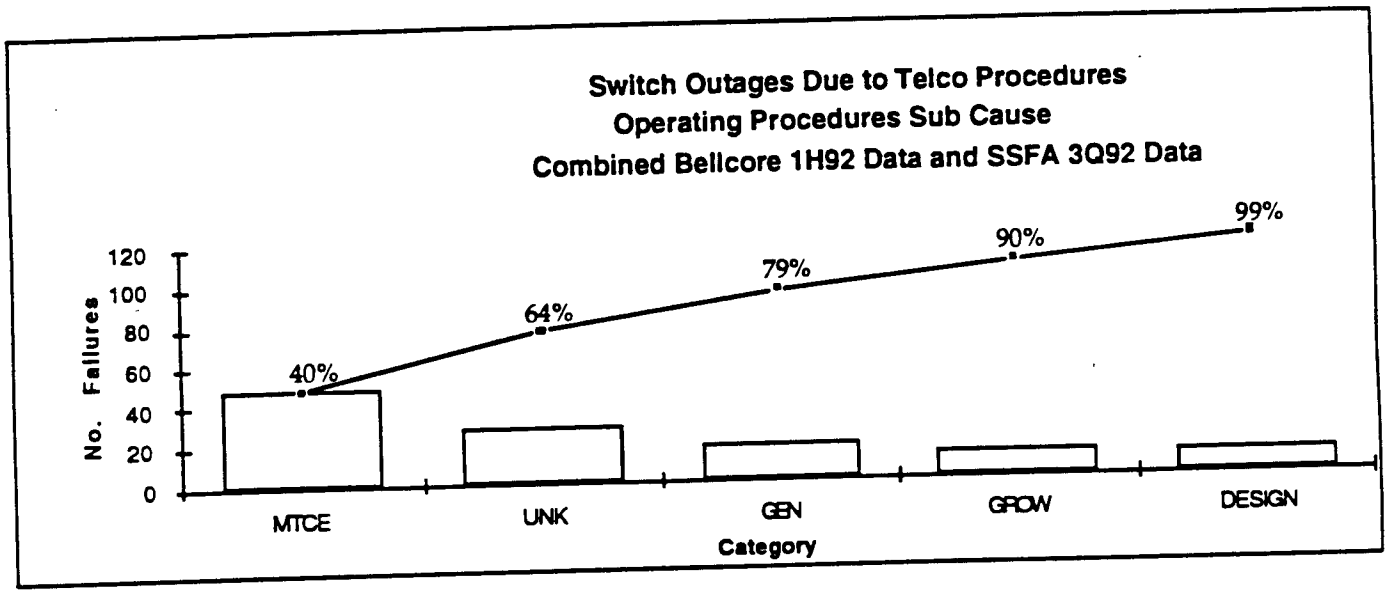

Figure 9: Operating Procedures Sub-cause

C

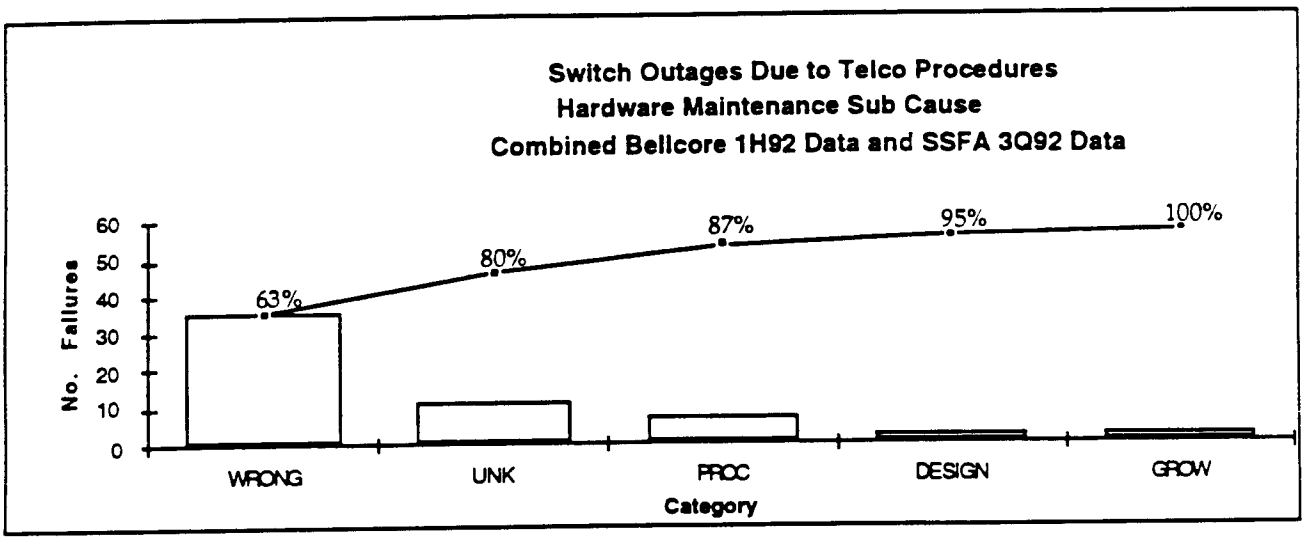

Figure 10: Hardware Maintenance Sub-cause

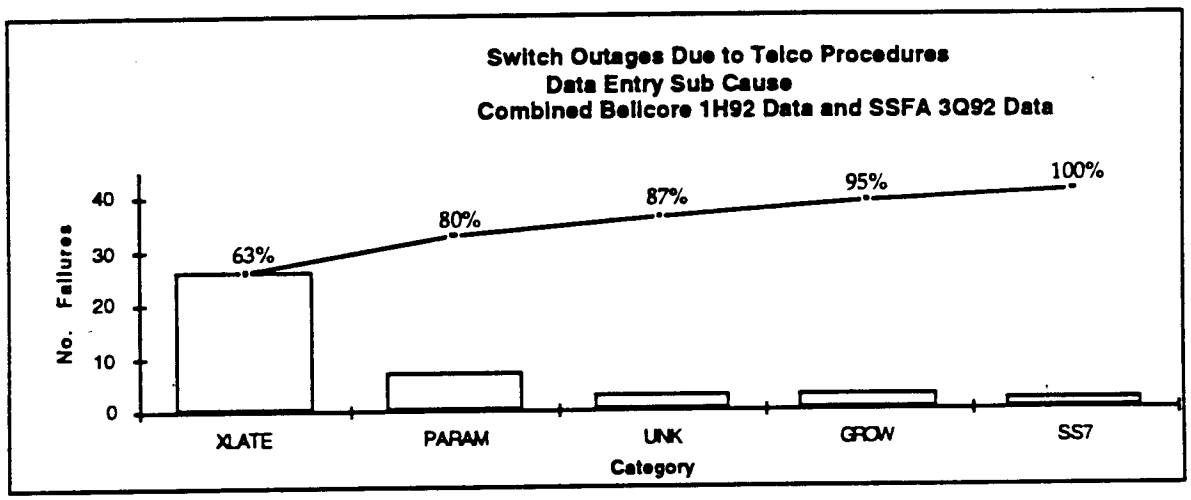

Figure 11: Data Entry Sub-cause

C

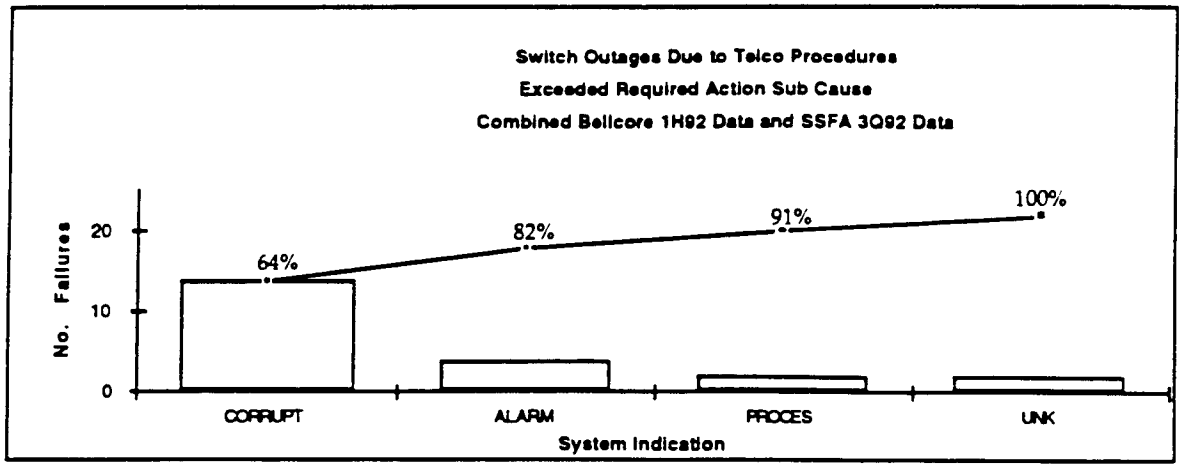

Figure 12: Exceeded Required Action Sub-cause

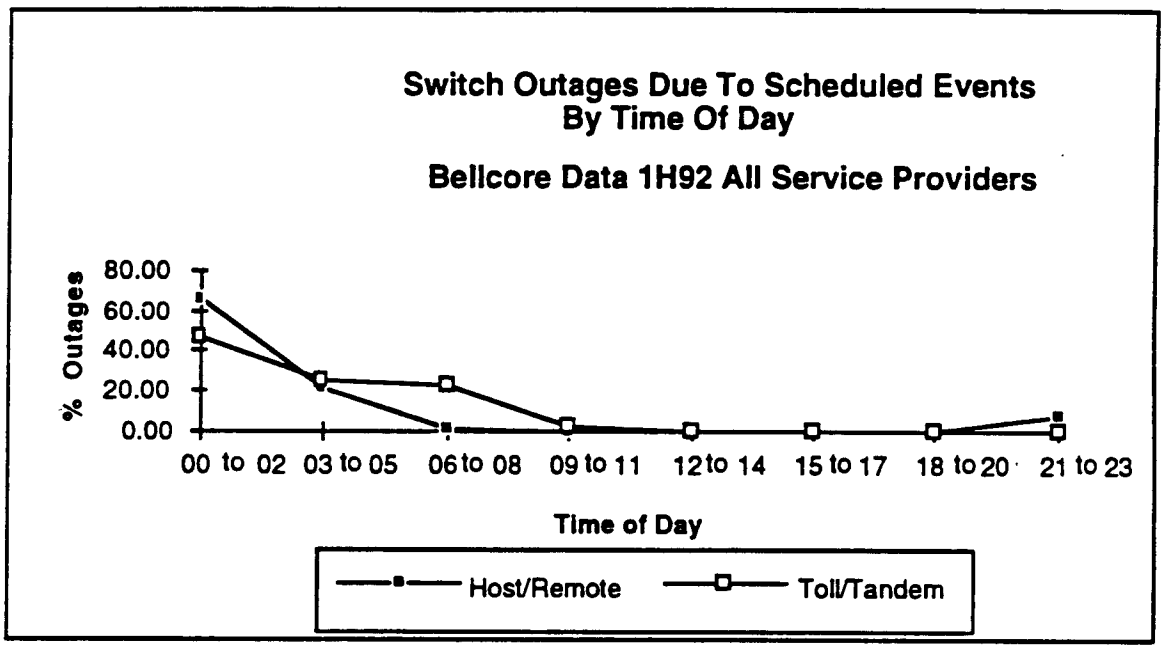

Figure 13: Outages Due to Scheduled Events by Time of Day

C

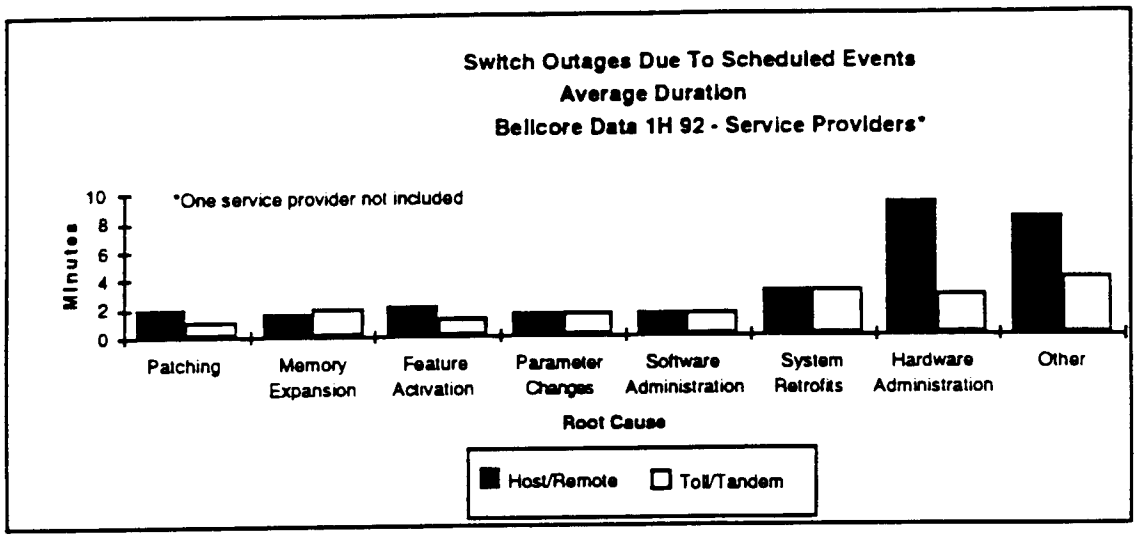

Figure 14: Outages Due to Scheduled Events by Duration

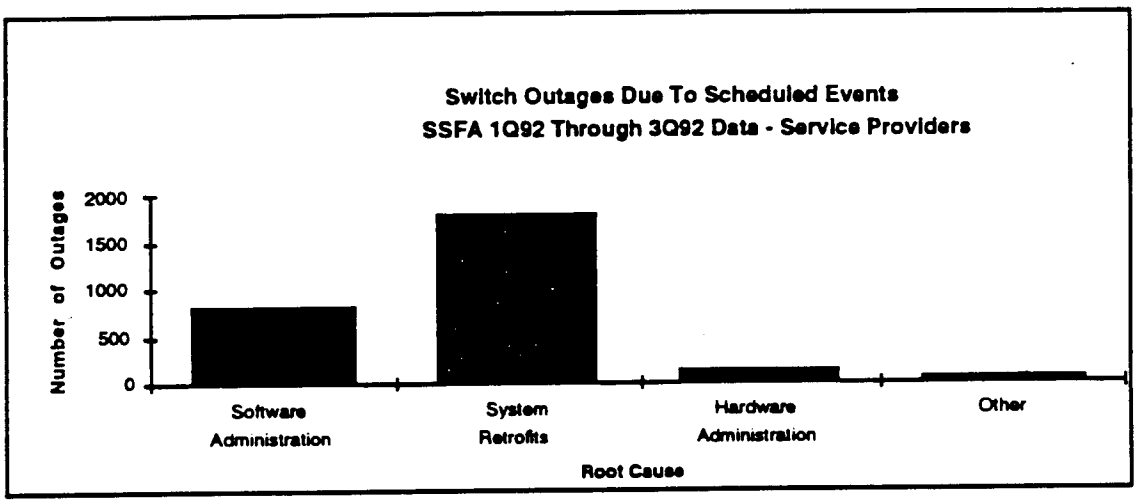

Figure 15: Root Causes for Scheduled Event Outages

C

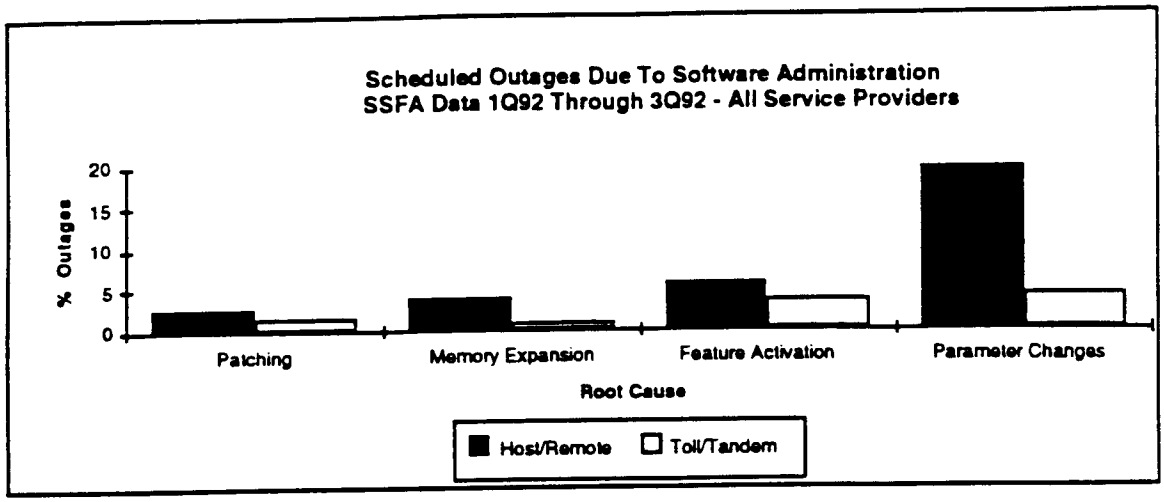

Figure 16: Scheduled Outages Due to Software Administration

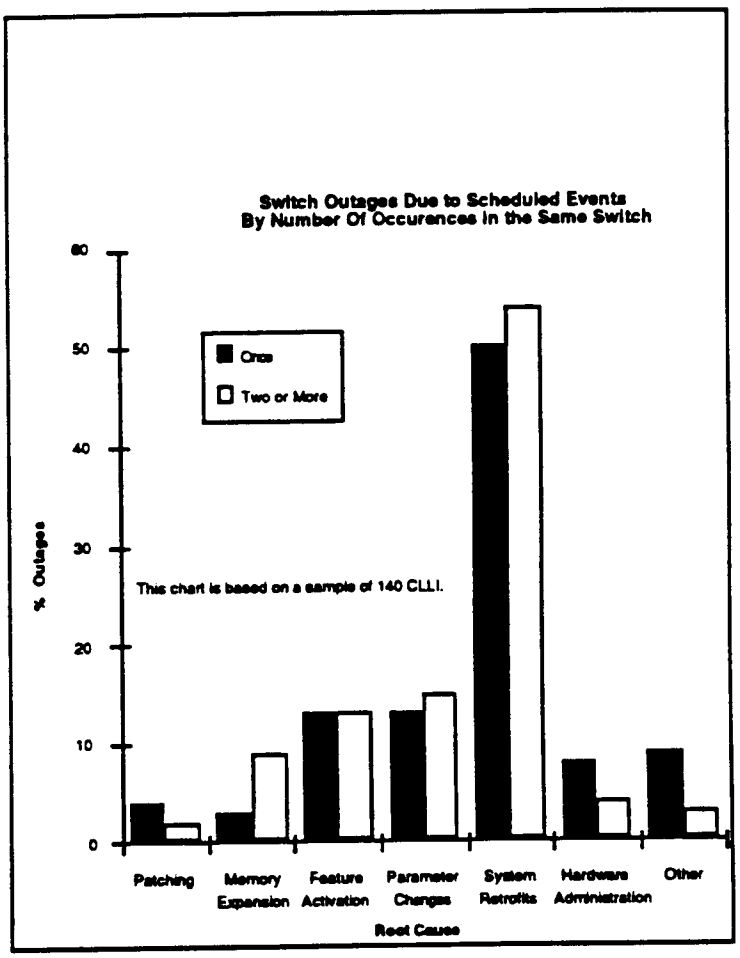

Figure 17: Scheduled Outages by Number of Occurrences in the Same Switch

C

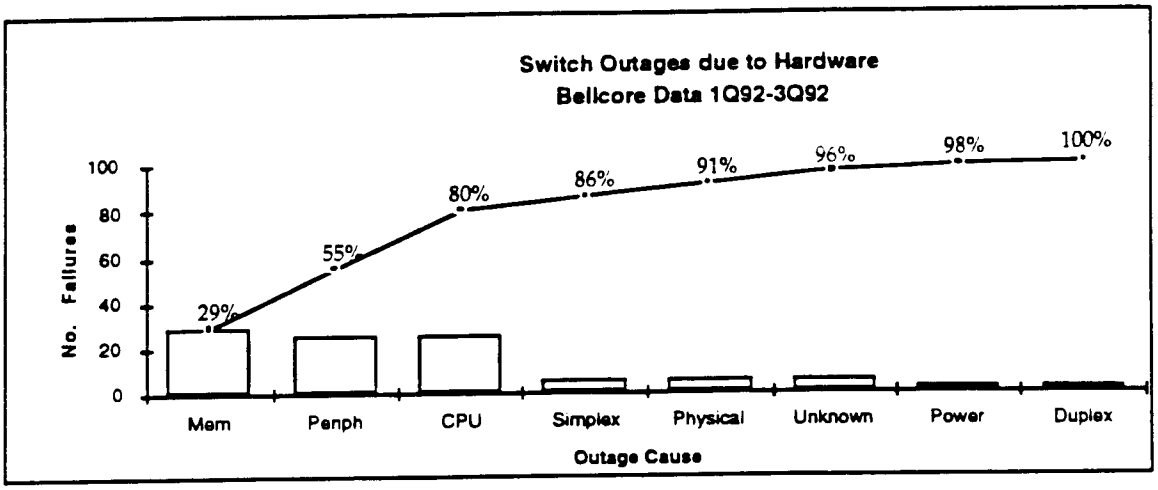

Figure 18: Outages Due to Hardware (Bellcore Data)

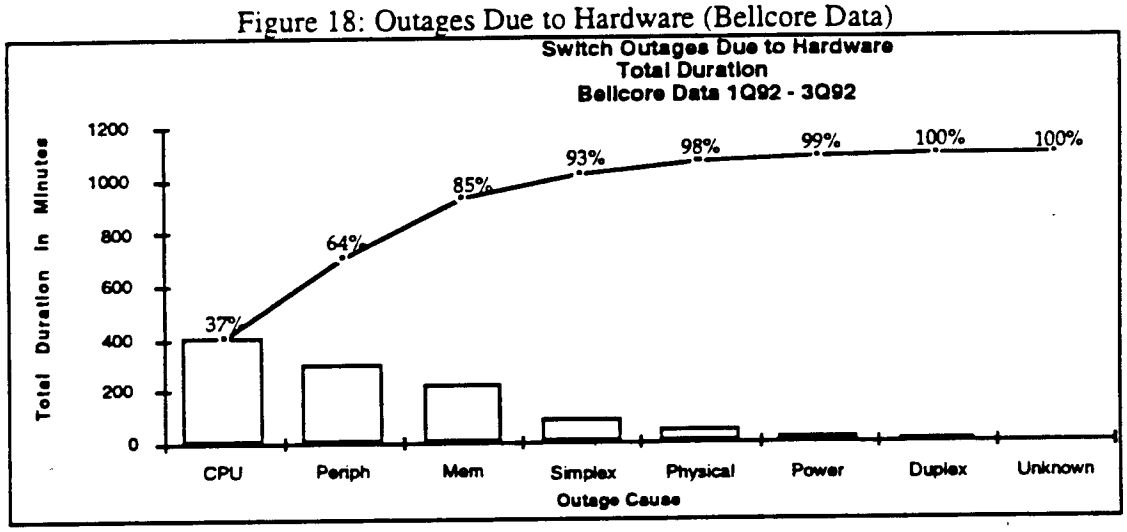

Figure 19: Outages Due to Hardware by Sub-cause

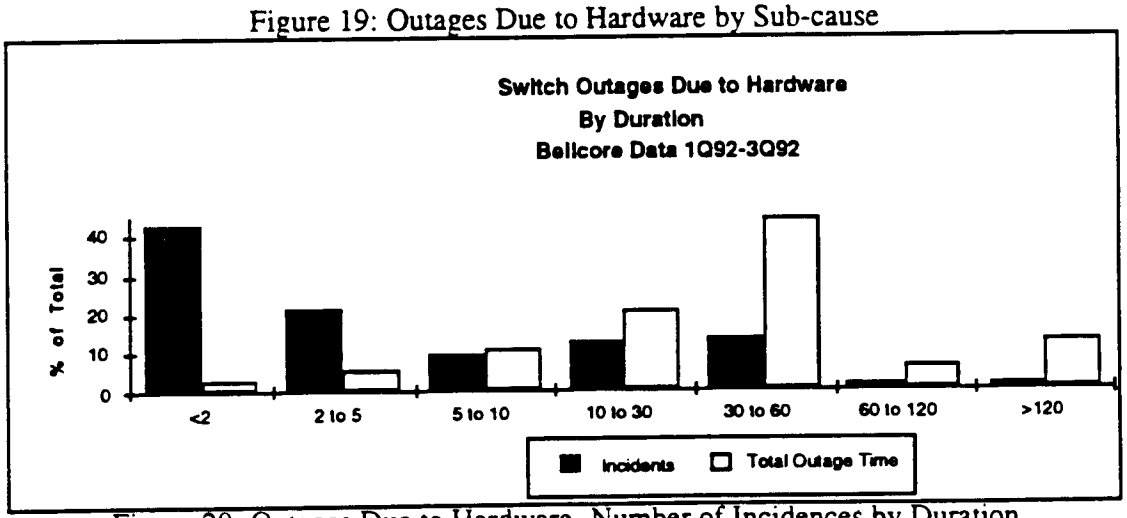

Figure 20: Outages Due to Hardware- Number of Incidences by Duration

C

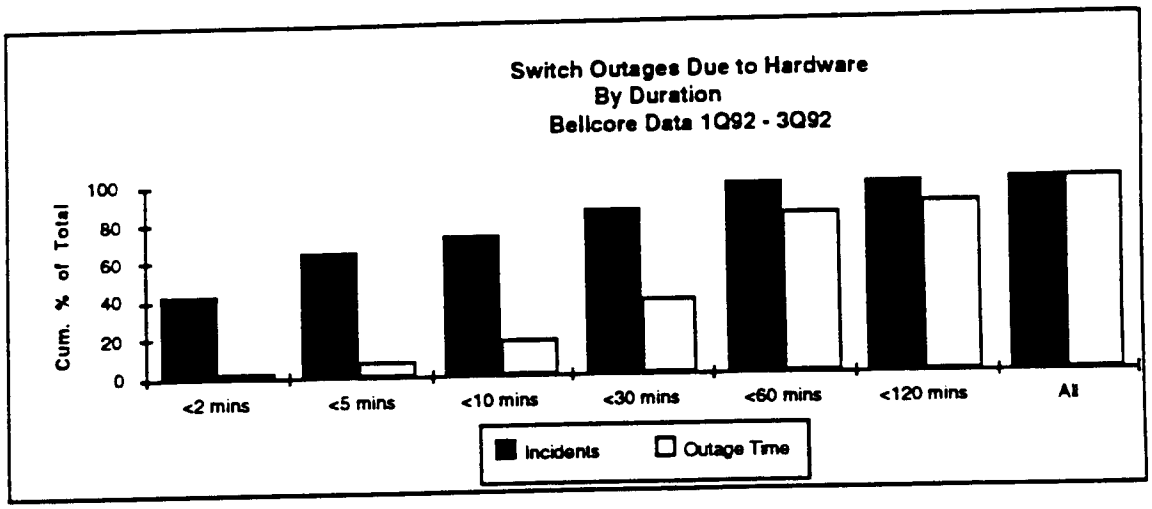

Figure 21: Outages Due to Hardware - Total Outage Time by Duration

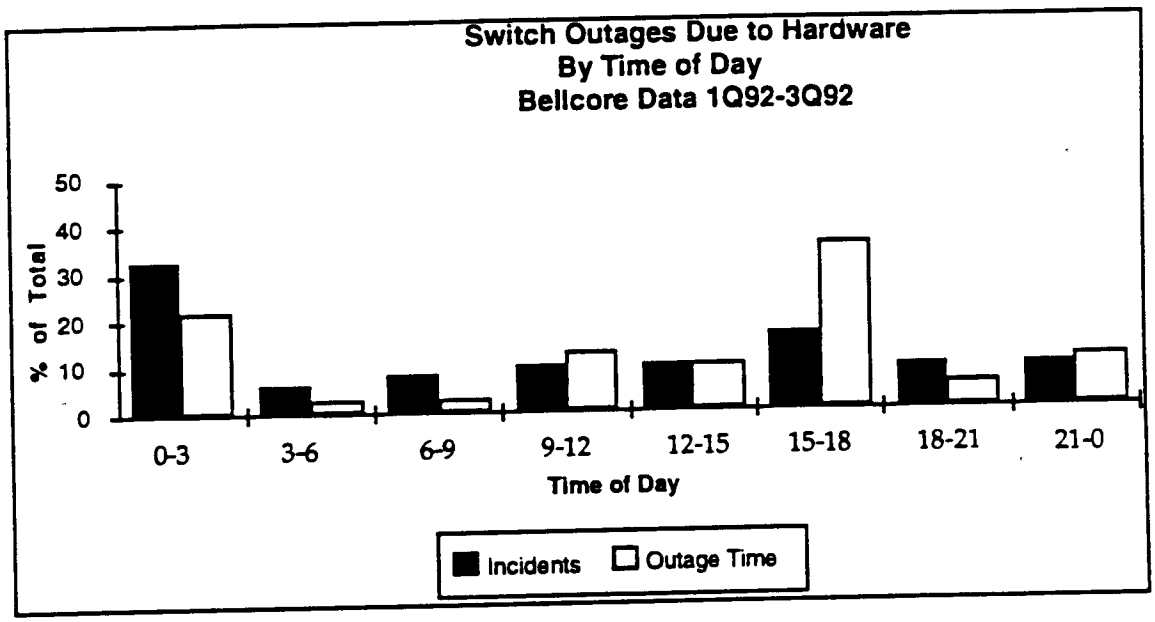

Figure 22: Outages Due to Hardware by Time of Day

C

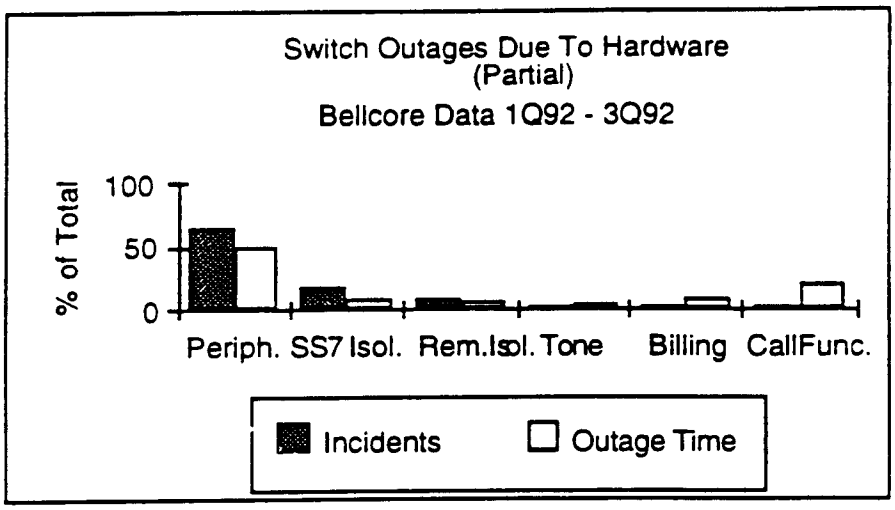

Figure 23: Partial Outages Due to Hardware by Sub-cause

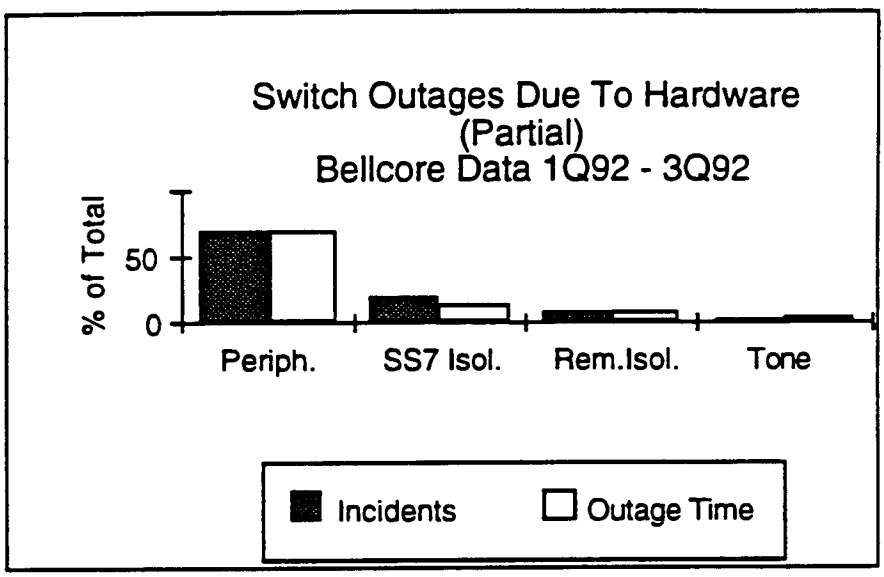

Figure 24: Partial Outages Due to Hardware by Sub-cause
(not including Billing or Call Function Loss)

C

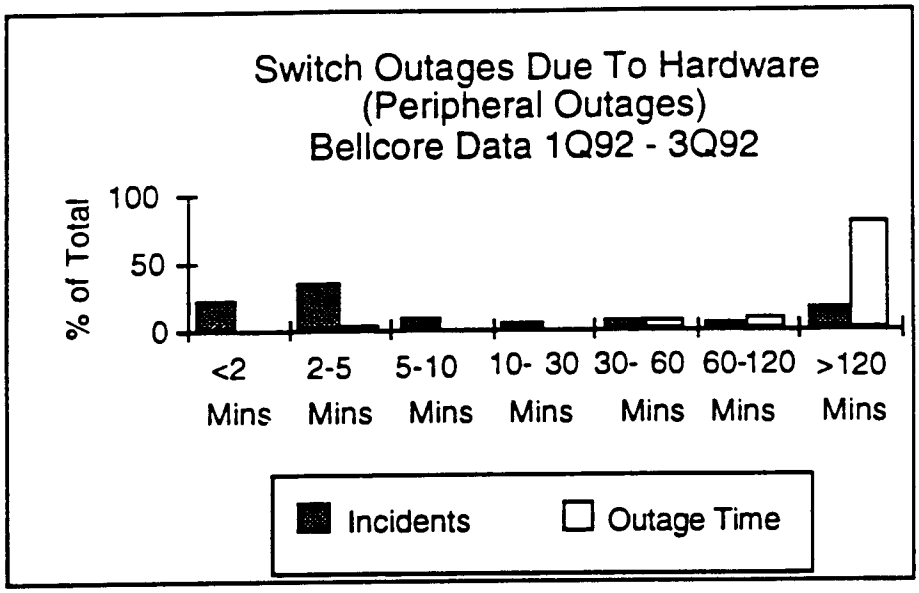

Figure 25: Peripheral Outages - Number of Incidences by Duration

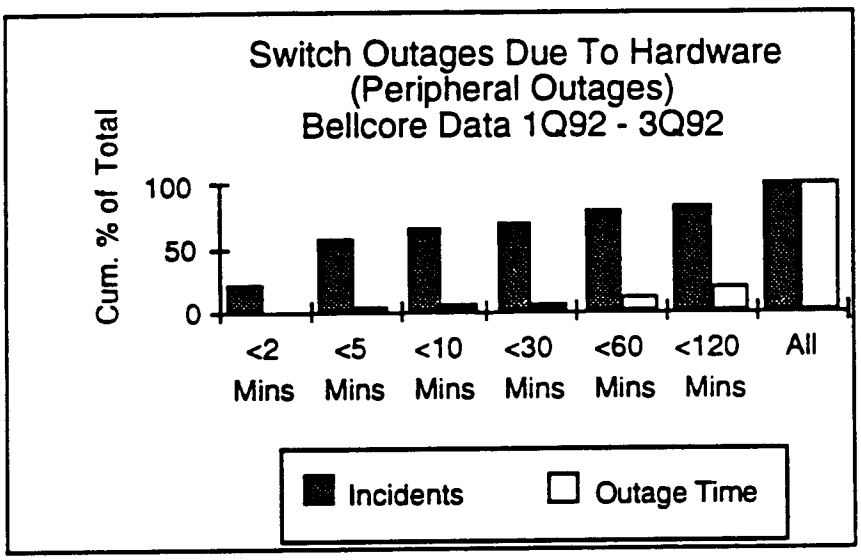

Figure 26: Peripheral Outages - Total Outage Time by Duration

C

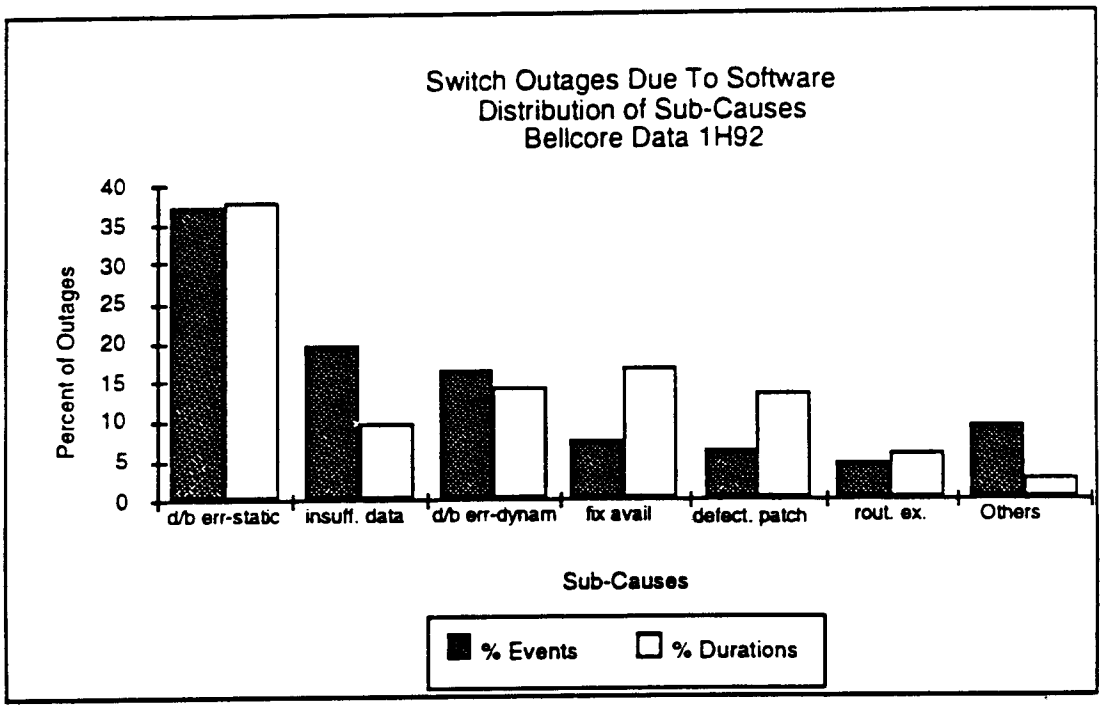

Figure 27: Outages Due to Software by Sub-cause (Bellcore Data 1H92)

C

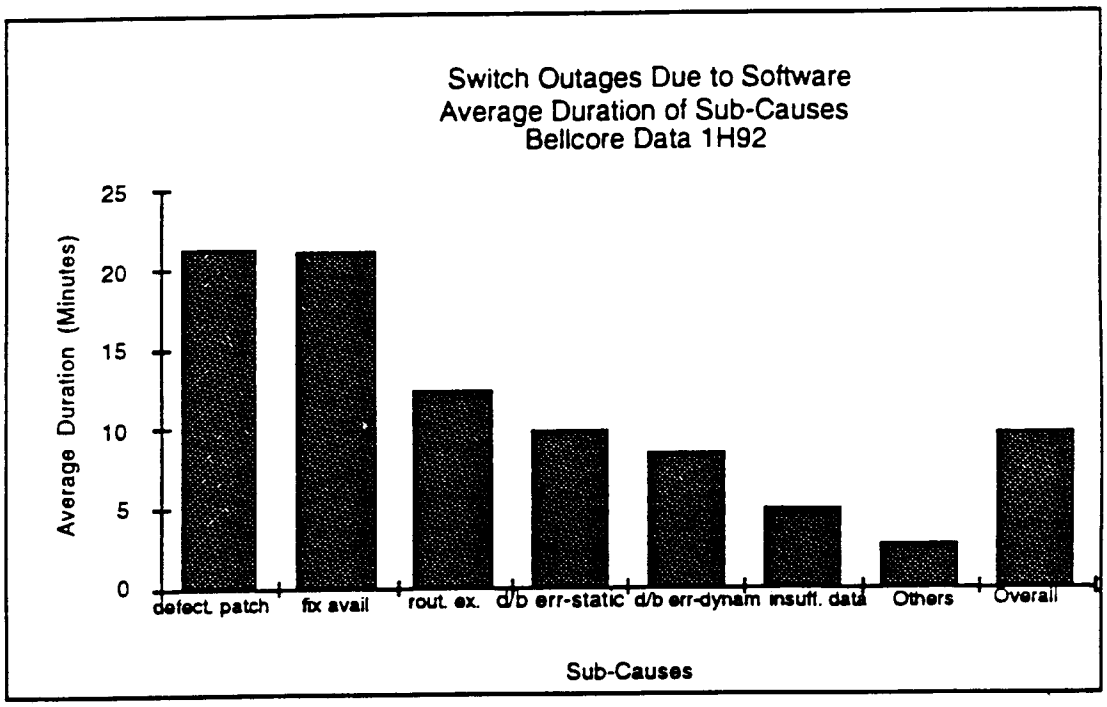

Figure 28: Outages Due to Software by Duration (Bellcore Data)

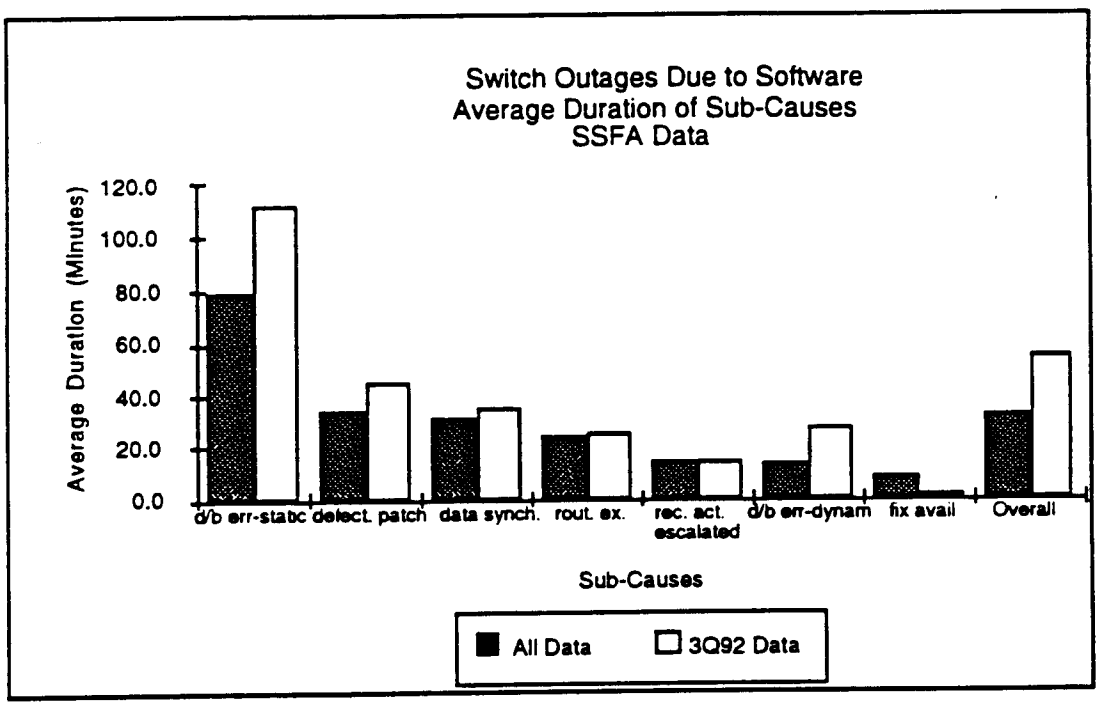

Figure 29: Outages Due to Software by Duration (SSFA Data)

C

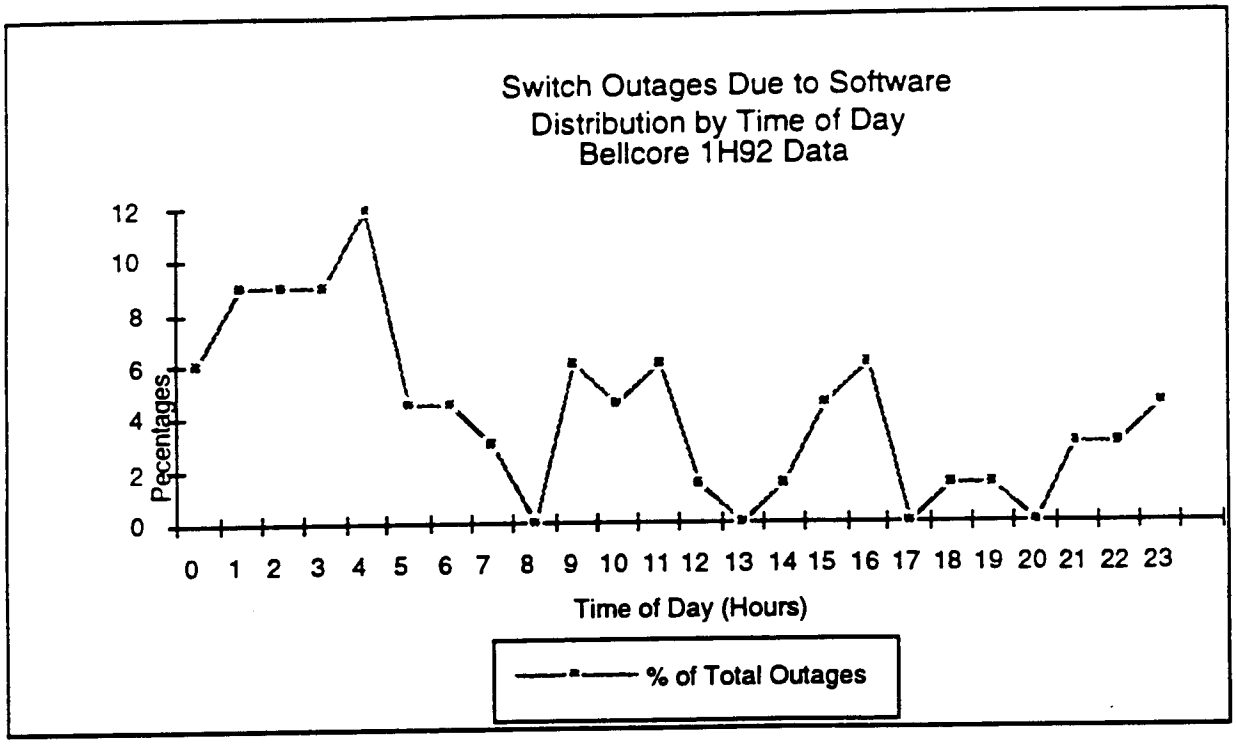

Figure 30: Outages Due to Software by Time of Day (Bellcore Data)

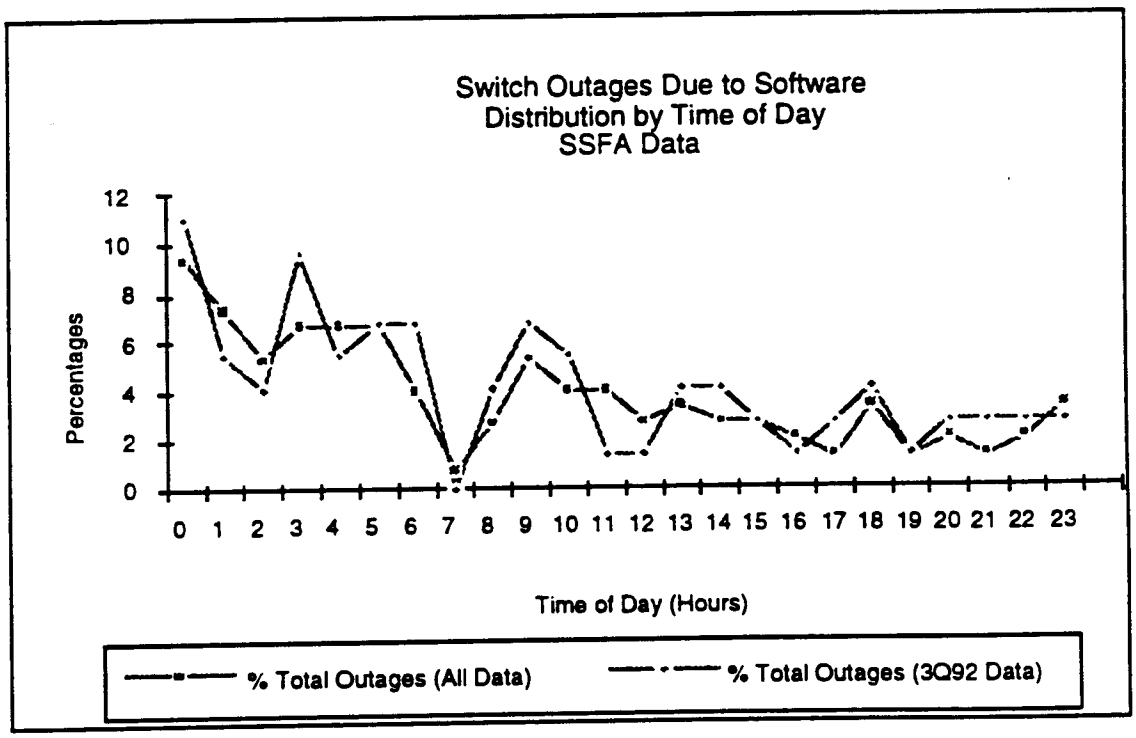

Figure 31: Outages Due to Software by Time of Day (SSFA Data)

C

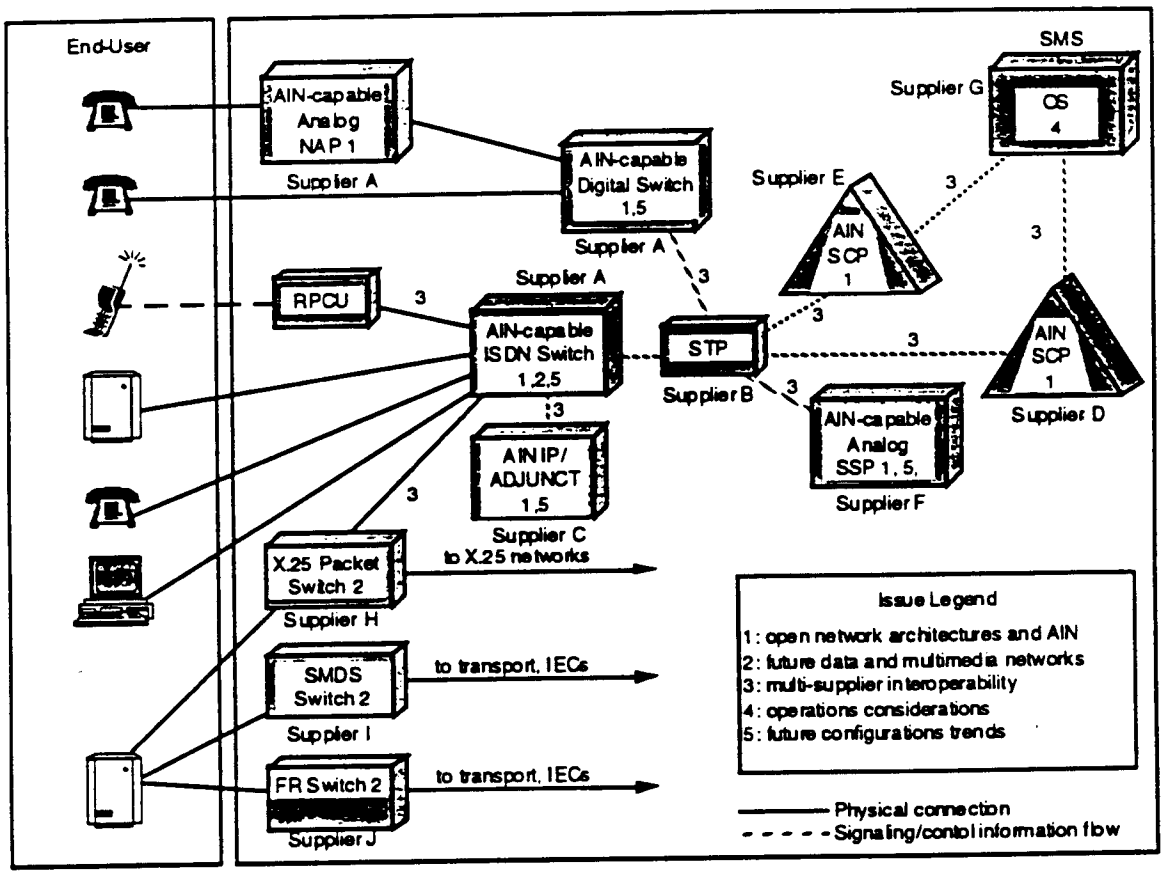

Figure 32: Single Provider Model (1995 - 1997)

C

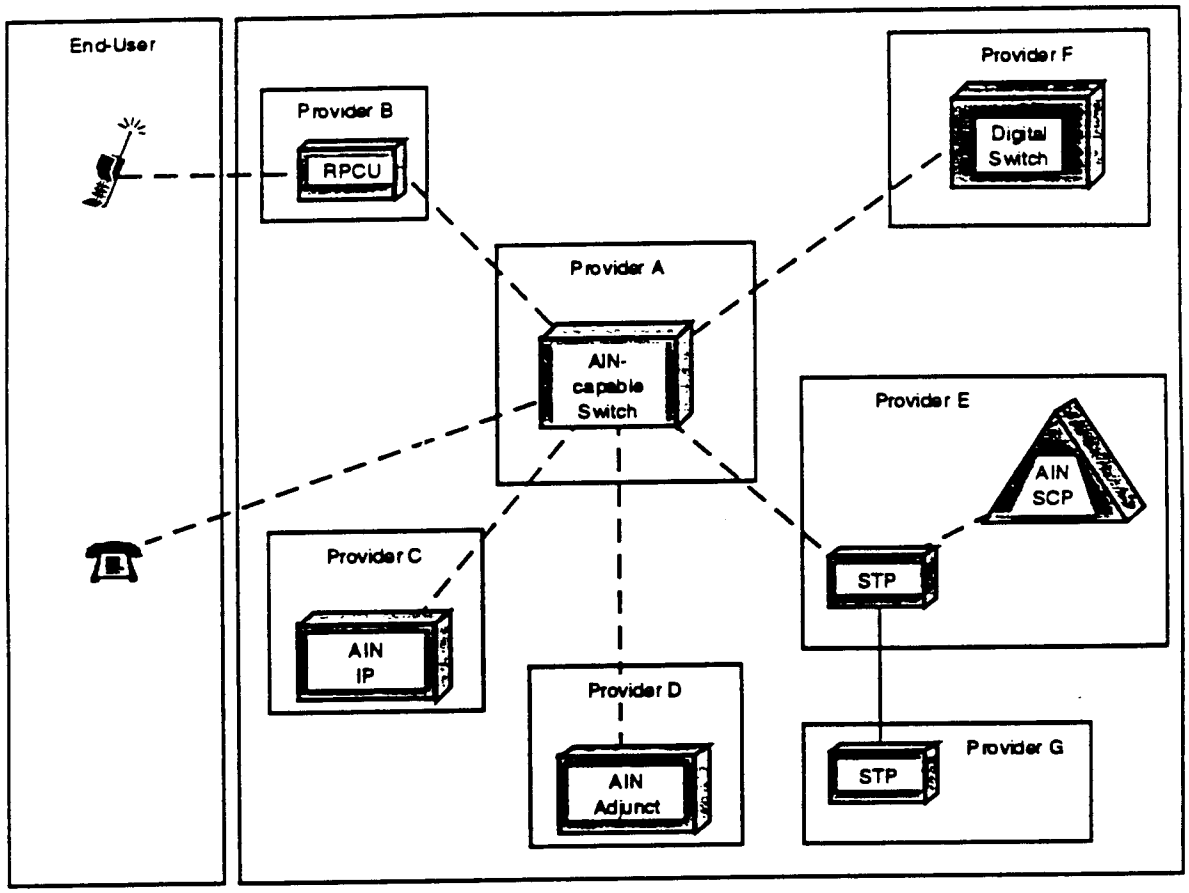

Figure 33: Multiple Provider Model (1995 - 1997)

	Network Component			
Software Component	CPE Platform	Access Platform	Network Platform	Service Platform
Application Layer				
Basic Layer				
Hardware/Controlling Software Layer				

Figure 34: Generic Network Model

C

Network Component

Software Component	CPE Platform: Analog Tele ISDN Teleph Computer PBX Cellular Tel	Access Platform: Analog NAP Digital Switch X.25 Packet Sw SMDS Switch FR Switch RPCU	Network Platform: Digital Switch Analog SSP STP X.25 Packet Sw SMDS Switch FR Switch	Service Platform: AIN SCP SMS OS AIN Adjunct AIN IP
Application Layer	ADSI Features Speed Calling PBX Features	Call Forwarding Speed Calling Packet Features	Class Features Reverse Charging FX Line Features	SLP Features 800 Service Operator Services
Basic Layer	DTMF Signaling Q.931 Signalling Analog/ADSI Sig	Call Control Connection Control Line Signalling Operating System	Trunk Signaling	SLEE Software Operating System
Hardware/Controlling Software Layer	Terminal Computers Router/Bridges Telephones	Switching Fabric Line Access Tone Generator Announcement	Switching Fabric Trunk Access Tone Generator Announcement	Access Ports Announcement Processor Disk

Represents Inter-Platform Protocol Interfaces (e.g., CCS7, Analog Line, ISDN Line, MF Trunk)

Represents Intra-Platform Protocol Interfaces (e.g., API and Proprietary Interfaces)

Figure 35: Examples of Elements Mapped to "Boxes"

Network Component

Software Component	CPE Platform	Access Platform	Network Platform	Service Platform
Application Layer		Fault Type 1		Fault Type 2
Basic Layer			Fault Type 3	
Hardware/Controlling Software Layer				

Fault Type 1: Error in the feature software of a single Access Platform

Fault Type 2: A Service Platform goes out of service

Fault Type 3: Network Platform basic software layer fails

Figure 36: Graphical Representation of Faults

C