PROCEDURAL OUTAGE REDUCTION

Addressing the Human Part

May 31, 1999

Authors:
P.J. Aduskevicz (AT&T)
Kathleen Atwater Peterson (Nortel Networks)
Jay Bennett (Telcordia)
Rick Canaday (AT&T)
Tom Chillemi (Bell Atlantic)
Norm Fischman (Bell Atlantic)
Anita Flintall (Nortel Networks)
Bill Klein (ATIS)
Anil Macwan (Lucent)
Spilios Makris (Telcordia)
Clyde Miller (Nortel Networks)
Denny Miller (Nortel Networks)
Eve Perris (Telcordia)
Karl Rauscher (Lucent)
Scott Taylor (BellSouth)
Whitey Thayer (FCC)
Erwin Van Allen (Southwestern Bell)
Sandy Wallace (Sprint)
Ken Walling (Pacific Bell)

Table of Contents

PROCEDURAL OUTAGE REDUCTION

Addressing the Human Part

ABSTRACT

While it is impossible to apply one counter measure that will prevent procedural errors, we have found that some standardization in the design of the environment reduces the possibility of failure. The concept of human-centric design for telecommunications products and documentation has potential for reducing the impact and/or frequency of procedural errors. This design approach is presently being implemented on new network elements. For the existing network, universal applications of Good ("Best") Practices provide a valuable solution for reversing the rising trend of outages attributed to procedural errors. Although as an industry we are moving in the right direction, our efforts need to be more aggressive. Best practices, generic requirements and existing legislation should be embraced and implemented to minimize procedural errors and improve network reliability.

EXECUTIVE SUMMARY

Background

Starting with the third quarter of 1992, the Federal Communication Commission (FCC) required reporting of large service outages by telecommunications service providers. Reporting requirements are specified in Part 63.100 of the FCC's Rules (see Appendix D). In an effort to monitor reliability of the nation's telecommunications network, the Alliance for Telecommunications Industry Solutions /Network Reliability Steering Committee (ATIS/NRSC) has performed various statistical analyses of these FCC-reportable service outages. The results of these analyses are published in quarterly and annual reports.

The analyses focus, not only on total numbers of incidents and their impacts across the network, but also delve deeper into various areas of the network. The analyses are performed separately for different failure locations such as local switches and facilities. In particular, the analyses of FCC-reportable facility outages identified an increasing trend in facility incidents. The NRSC established a Facilities Solution Team to investigate how this trend could be reversed. The team's findings were published in reports in February 1996 and November 1997.

Earlier in 1997, the NRSC analyzed the root causes of FCC-reportable service outages (any outage greater than 30,000 lines and lasting for 30 or more minutes). Initial exploratory investigations indicated an increasing trend in outages caused by procedural errors. The NRSC classifies an outage as having a procedural error root cause if the source of the outage was a problem with documentation, training, supervision, maintenance, or some kind of human error. It should be made clear that cable damage is not considered a procedural error root cause category and is in the Facilities Solution Team analysis. The special nature of cable damage problems required the establishment of a separate root cause category. These problems were addressed in an earlier Facilities Solution Team Report. While cable damage is often the result of human error, cable damage is not included in the procedural errors addressed in this report.

A subsequent study performed in early 1998 confirmed the increasing trend in Procedural Error FCC-reportable service outages. The NRSC formed a Procedural Error Team to investigate this trend and provide recommendations for its reduction.

Status of Outages Attributed to Procedural Errors

This section presents major findings from "FCC-Reportable Service Outages (3Q92-4Q98) with Procedural Errors as Root Cause." The complete text of this document is provided in Appendix A.

A procedural error is the root cause for 33% of reported service outages. The frequency of procedural error outages has increased about 3% per quarter since July 1992, while outages from other root causes (Non-Procedural Error outages) demonstrate a decreasing—but not statistically significant—trend over the same time period. Figure 1 presents a plot of the number of Procedural Error and Non-Procedural Error FCC-reportable outages in each quarter from 3Q92 through 4Q98. The lines plot the trends in outage frequency for both root cause types.

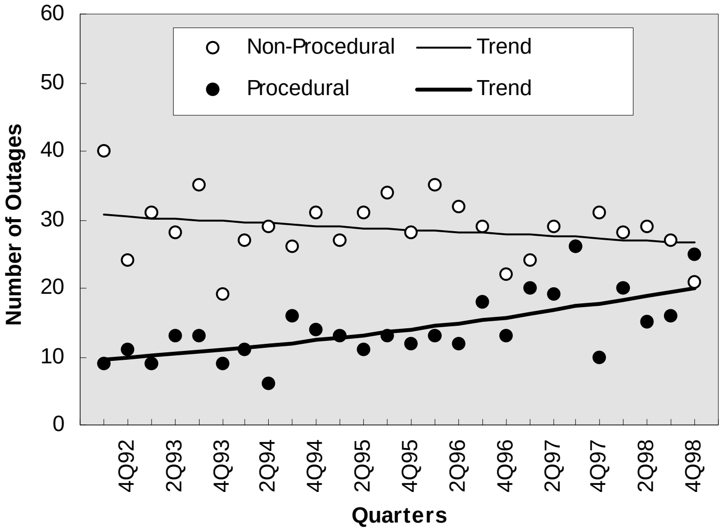

Figure 1. Procedure Error and Non-Procedure Error Outage Frequency by Quarter*

* Bennett, J., *FCC-Reportable Service Outages (3Q92 – 4Q98) with Procedural Errors as Root Cause*, Telcordia White Paper, February 23, 1998. See Appendix A.

Documentation/procedure problems (38%), insufficient supervision (28%), and insufficient training (27%) are the major root cause subcategories. Almost half of all outages caused by insufficient supervision occurred in 1998. Almost half of procedural error outages occur at switches (28% at Local Switches and 17% at Tandem Switches). While procedural errors are not the root cause of a statistically significant majority of outages within any single failure category, the proportion of procedural error outages is significantly lower among facility outages than it is among virtually all other failure locations. The frequency of procedural error outages peaks near noon and midnight, although the noon peak is significantly less pronounced than that for outages from other root causes. On average, each procedural error outage has significantly less impact as measured by the Committee T1 Outage Index than an outage from another root cause. The number of customers potentially affected by procedural error outages is significantly less than by outages from another root cause. Overall, the average duration of procedural error outages is significantly less than those outages from other root causes.

Comparison of Large vs. Small Outages

One of the first questions raised was whether FCC-reportable service outages provided a representative sample for the purposes of the study. A special study was commissioned in response to FCC and consumer group questions concerning service quality in large and small service outages. Five companies provided data sets of switch outages caused by procedural errors. Within each company's data set, distributions of "Large" outages (Large with respect to duration and number of customers affected) were different from those of "Small outages". While some differences were found, they were not significant. After extensive review, it was concluded that outages reported to the FCC appear to provide a reasonably representative sample of the general reliability of the whole network for the purpose of this study (Appendix B contains the details of this study). Consequently, the major source of data analyzed by the team was the collection of reports of FCC-reportable service outages.

Since the investigation of procedural outages is basically moving into uncharted waters, the team's approach to this study was to attack the problem from a comprehensive viewpoint. This view includes:

- improved product design to reduce the possibility of incorrect actions causing service interruptions,
- simplified documentation to reduce misinterpretation,
- methods of training verification to decrease the possibility of skill level problems, and
- processes to determine the true root cause for network outages.

The intent of this publication is to provide information that:

- identifies the problem,
- shows industry direction,
- provides a list of good practices, and
- proposes new concepts that could address some of the long-term issues hindering network reliability.

Findings/Conclusions (Eighteen Points of Light)

1. While numerous industry initiatives have enhanced the overall quality of software and hardware used in most major network elements, there has not been sufficient focus on procedural issues to drive improvement trends.
2. On average, 33% of outages reported to the FCC are attributed to procedural error. An all time high in this category was reached in 4Q98 with 53% of FCC reported outages being procedural in nature.
3. The distribution of outages attributed to procedural errors is 79% service provider and 21% vendor.
4. Outages attributed to procedural error are of lesser duration and impact than outages not attributed to procedural error.
5. Industry internal reports of outages attributed to procedural error lack consistent categorization and root cause identification. The industry could be more effective in reducing procedural outages and enhancing network reliability if a common language and a consistent mechanism for reporting were implemented.
6. Review of reports submitted to the FCC by service providers uncovered different formats and levels of detail, which created difficulty in understanding and categorizing some reports.
7. While some differences exist between the causes of Large and Small outages, they do not appear to be of such a magnitude as to influence prioritization of solutions to procedural errors.

8. The Network Reliability Councils (NRC-1 and NRC-2) and their successors, the Network Reliability and Interoperability Councils (NRIC-3 and NRIC-4), were established as Federal Advisory Committees to the FCC. They have all published a number of documents that would imporve network reliability if fully implemented. ATIS established the NRSC at the request of NRC-1. A collection of telecommunications industry best practices can be found in the following publications:

   - *Network Reliability: A Report to the Nation (NRC-1)*
   - *Network Reliability: The Path Forward (NRC-2)*
   - *Keeping the Network Alive and Well: Solving the Problem of Cable Dig-Ups (NRSC)*
   - *Fixing Facility Outages: Building the Tools to Make it Happen (NRSC)*
   - *Network Interoperability: The Key to Competition (NRIC-3).*

9. Although no domestic or international standards body has addressed procedural errors specifically, a number of human factors standards bodies have made contributions that have the potential to reduce procedural errors if implemented. Standards such as ISO9241 focus on designing user interfaces from a human-centric perspective and should be considered for use by the industry.

10. There are two generic requirements documents written specifically to mitigate procedural errors:

    - *GR-2914-CORE, Human Factors Requirements for Equipment to Improve Network Reliability* focuses on designing equipment from a user's perspective.

    - *GR-454-CORE, General Requirements for Supplier Provided Documentation* provides information on how to develop complete and comprehensive documentation.

11. Good (Best) Practices aimed at reducing procedural errors tend to be focused on process, capability, and sensitivity. The primary factors, which contribute to these practices, are clarity, simplicity, and adherence.

12. A Critical Event Management process is an effective method for duration reduction when an outage occurs. Critical Event Management mandates that when an outage occurs, all focus should be on time to recover and minimization of damage.

13. Evaluation of procedural failures shows that people have different perspectives and habits. Thus a single countermeasure will not work for everyone. Some standardization in the design of the environment reduces the possibility for failure.

14. One of the primary mitigators in reducing outages attributed to procedural errors is to design network user-interfaces from a human-centric perspective (e.g., network elements, software, documentation). For any user-interface to be used easily and efficiently, designs must be meaningful and understandable and have a coherent structure to the user.

15. Ability to design documentation to minimize human error centers on the language used within the documentation. A restricted language system that limits language to a set of core vocabulary words and company – or industry-defined technical words enforces the use of words with only a single meaning. This system also consists of a set of writing guidelines for grammar, mechanics, and style.

16. As the demand for greater network reliability is tested against growing network complexity, business cases should examine the introduction of Expert System technology.

17. Future mitigators to improve network reliability can be categorized in two major groups:

    - Introduction of technology and process improvements today to both existing networks and new products to minimize human involvement
    - Rigorous implementation of current best practices and sharing knowledge at the industry level to prevent and eliminate procedural outages

18. While diverse facilities are recommended for all critical services, numerous inventory control systems do not or can not ensure initial or ongoing diversity of critical circuit facilities.

Best Practices (The Eleven Commandments)

Listed below is a summary of the best practices that are included in this report. There is a later list of more specific best practices that we call for short "Good Practices." If all these practices are followed, we believe that there would be a significant reduction in the number and impact of procedural outages. The best practices are:

1. The Procedural Errors Study Team recommends that the NRSC develop a standard format template for recording of outages reported to the FCC. Additionally, a review of root cause subcategories should be initiated for inclusion in any new template. Timely reporting and formatting of outages would be enhanced if the template were available via Internet access.
2. Much good work has been done over time to capture best practices around the design and operations of the network for maximal reliability. Many of today's outages attributed to procedural error are the result of not following these documented best practices. All service providers and vendors should reaffirm their organization's commitment to these best practices.
3. Service suppliers and vendors should review the included list of good practices aimed at reducing the number of procedural outages. This list is focused on procedural errors only and spans the seven areas previously identified by NRC-1 as being potentially vulnerable to outages.
4. All telecommunication equipment vendors should design equipment that meets the requirements set forward in GR-2914-CORE, *Human Factors Requirements for Equipment to Improve Network Reliability*.
5. Telecommunications service suppliers and vendors should ensure that all product/service documentation meets requirements specified in GR-454-CORE*, General Requirements for Supplier-Provided Documentation*.
6. Telecom service suppliers and vendors should adopt the concept of a simplified language system, which controls vocabulary, grammar, mechanics, and style for better user understanding.
7. Suppliers and service providers should establish a comprehensive method for performing root cause analysis on all outages attributed to procedural error. Included in this

document in Appendix C is a sample root cause analysis template used by one of the nations telecommunications companies.

8. Inventory control systems should be reviewed to ensure the system's ability to track and maintain diverse assignment of critical facilities.
9. Telecommunication suppliers and vendors should adopt uniform methods of electronic documentation distribution and usage. Electronic access to documentation will allow better version control and ease of access for field personnel. Additionally, electronic access allows future enhancements such as inter-active methods and information.
10. Telecommunications suppliers and vendors should provide specialized training for critical event management. This non-traditional approach to reducing the outage interval requires a mindset change for many industry personnel. The emphasis must be placed on restoring the service first, then fixing the problem.
11. Periodic testing of critical event systems and processes should be performed on a regular basis (i.e., monthly). Examples of these systems/processes are emergency generator (system) and spare circuit pack central warehousing (process). These systems/processes should be certified as being compliant to meet overall network reliability requirements.

Additional More Specific Best Practices - Good Practices

In this document, there is an entire section aimed at providing more specific best practices. For short, we call these practices "Good Practices." A summary of these practices is given below. The *Future Mitigators* section contains several, more general best practices allowing application of practices across a wider segment of the network.

1. Mandatory use of a detailed Method of Procedure (MOP) should be required for all hardware and software growth and change procedures.

2. The Maintenance Window should be adhered to for all “Hot Power” work and for all installation, change, or maintenance activities that are critical in nature. To be effective, senior management must also support this process.

3. “Ask Yourself” programs should be established that focus on human factors and provide a process for identification of limitations, omissions, or errors before starting the work. The “Ask Yourself” programs require demonstrated support from senior management. These programs define a list of questions to be answered before any work activity begins.

4. A “Critical Event Management” process should be in place to manage the event.

5. Technicians performing critical work should be isolated from day-to-day activity and its distraction of telephone calls and peer questions.

6. Dedicated groups should be established to perform critical tasks where possible—i.e., all 911, growth, change, maintenance, or major modification to a central processor.

7. There should be regular weekly or daily communication with the service team(s) to share performance, detail from any failure or outage, time between outages, a reminder of identified trouble areas, the triggering event, the root cause, and

associated counter measure. Management should be committed to and enforce these processes.

8. Each technician should be properly prepared to complete his or her work without impacting the health of the network.

9. Periodic audits should be performed to assure that facility diversification is maintained. Previous NRC Best Practices have recommended that all 911 trunks, SS7 Signaling Links, Remote Office Umbilicals, and Network Timing Circuits should be diversified. While diverse routing can not completely stop procedural outages, in can greatly affect the frequency by changing the odds of multiple events occurring at the same time. But the investment in diversity is to no avail if it is lost due to procedural errors.

10. An “Approval for Use” process should be established. This process is used to ensure that equipment placed in the network meets both design and technology management requirements and that it works as specified.

11. A physical verification of both local and remote alarms and of remote network element maintenance access should be performed on all new equipment installed in the network before it is placed into service. Periodic re-verification of these alarms and access should be scheduled.

12. When a new Central Office (CO) is installed or an old switching system replaced, the diversified Foreign Exchange (FX) telephone line for the office should also be verified. Periodic re-verification of FX lines should be scheduled.

13. A process should be established to track the location of all spare equipment.

14. All removable covers that have equipment designations should have those designations removed and the designations placed on the permanent portion of the unit or frame.

15. The most effective practice when performing complex translation changes is to test the translations before and after the change to ensure the appropriate and expected results.

Providing the Industry a Means of Preventing/Reducing Procedural Outages

As the data has clearly indicated, procedural errors significantly impact the integrity of the network. Recent studies demonstrate that procedural errors represent an average of 33% of FCC-reported service outages per Part 63.100 (See Appendix D). In the fourth quarter of 1998, FCC outages attributed to procedural errors rose to 50% (Bennett, 1999). This chapter investigates what industry initiatives have already been taken to mitigate procedural errors and what needs to be implemented going forward.

The Federal Communications Commission's (FCC) Initiatives

The FCC was the initial "catalyst" for identifying the significance of network outages. Following a number of major telecommunications network outages, the FCC established the Network Reliability Council (NRC-1). The NRC-1 identified seven areas as being potentially vulnerable to outages.

- Fiber Cable Cuts
- Signaling Network Systems
- Digital Cross-connect Systems (DCS)
- 911
- Fire
- Power
- Switching.

A subcommittee for each area was formed to identify the vulnerabilities and address issues of concern, determine the on-going work efforts, and to propose recommendations to prevent or minimize potential outages. In June 1993, the NRC-1 published *Network Reliability: A Report to the Nation*, a compendium of technical papers, which became known as the Purple Book. The findings demonstrated that procedural errors play a significant role in network service interruptions and outages. This compendium of technical papers provided industry members, legislators, regulators, academia, and the general public with a complete reference of findings and recommendations to improve network reliability. These recommendations became "Best Practices." See Appendix F for many of these practices.

In 1996, the NRC conducted a follow-up study entitled, *Network Reliability: The Path Forward* (a.k.a. the Red Book). The objective of this study was to assess the reliability of the public network and, at the same time, make recommendations on how to increase interconnection and introduce new technologies into the network. Five areas were addressed in this work effort:

- Network Reliability Reporting
- Increased Interconnection
- New Technology Introduction
- Essential Services Reliability
- Use of Telecommuting in Disasters.

At the request of the NRC, the Alliance for Telecommunications Industry Solutions (ATIS) established the Network Reliability Steering Committee (NRSC) in May of 1993. The NRSC was formed to monitor network reliability, utilizing major outage reports filed with the FCC pursuant to Docket 91-273. One of the NRSC's standing committees is the Facilities Solution Team (FST). It was chartered to determine the causes of the high rate of facility outages and to recommend ways to reduce their frequency and impact. The Facilities Solution Team released two reports on Facilities Reliability; (1) *Keeping the Network Alive and Well: Solving the Problem of Cable Dig-ups,* and *(2) Fixing Facility Outages: Building the Tools to Make it Happen*. These reports provide recommendations on how to reduce facility outages. Some of the recommendations that were proposed in both the work efforts under the NRC and the NRSC's FST could reduce the likelihood of service interruptions and outages attributed to procedural errors.

The NRC continues to be the driving force in industry initiatives to reduce network outages. Through the years, the NRCs (NRC-1 and NRC-2) have evolved to become the Network Reliability and Interoperability Councils (NRIC-3 and NRIC-4). NRIC-3 was primarily commissioned to advise the FCC on what would be necessary to implement the new Section 256 of the Telecommunications Act of 1996. The NRIC-3 released a report entitled *"Network Interoperability: The Key to Competition"* in 1997 (a.k.a. the Blue Book). The recommendations in this document provide optimal reliability and interoperability of, and accessibility to, public telecommunications networks.

Currently, Focus Group 3, Subcommittee 1 of the NRIC-4, is updating the Best Practices that have been proposed for improving network reliability. This subcommittee is particularly focused on Best Practices for mitigating power, procedural, and facilities outages. This work effort includes examining the Best Practices that have been proposed, surveying companies that have implemented these recommendations to determine if they have been effective, modifying practices if needed, and eliminating those practices which have become obsolete due to the evolution of technology. This work effort is expected to be completed in 1999 and will represent a useful contribution towards reducing the number of overall outages, which includes those attributed to procedural errors. The telecommunications industry Best Practices that have been proposed can be found in the following documents:

- *Network Reliability: A Report to the Nation (NRC-1)*
- *Network Reliability: The Path Forward (NRC-2)*
- *Keeping the Network Alive and Well: Solving the Problem of Cable Dig-ups* (NRSC)
- *Fixing Facility Outages: Building the Tools to Make it Happen (NRSC)*
- *Network Interoperability: The Key to Competition (NRIC-3).*

Legislative Initiatives

The legislative initiative to mitigate outages has been focused on facilities. In 1995, Rep. Frank Pallone introduced “Comprehensive One-Call Notification Act,” H.R. 2482, in the House. The bill required States to consider adopting mandatory, comprehensive, statewide one-call notification systems to protect underground facilities from being damaged by any excavations. This legislation outlines a process for construction workers, telecommunications service providers, and other utility companies to set up a single location to call before digging. This process will simplify and coordinate efforts so that appropriate companies can be notified to mark utility lines, and those who are digging will have the information they need to avoid facility dig-ups. Similar legislation was also introduced in the Senate.

In June of 1998, the Transportation Equity Act for the 21st Century (TEA21) bill that was passed included the One-Call Notification Act. Although this bill focuses on allocating funds for federal highway related projects, the issue of One-Call Notification on a national scale was addressed. In this bill, the Department of Transportation’s Office of Pipeline Safety (OPS) has been asked by Congress to conduct an extensive study and compile a list of best practices for One-Call Notification Systems. The completion of this study is expected June of 1999. The OPS has created sub-teams to address damage prevention practices in the following eight industry segments: Planning & Design, One-Call Centers, Locating & Marking, Mapping, Compliance, Reporting & Evaluation, Public Education, and Excavation Practices & Emerging Technologies. The NRSC’s Facilities Solution Team was a long time advocate and champion of One-Call Legislation at both the federal and state level and is a participant in this effort.

While such One-Call legislation will certainly assist in reducing the number of facilities outages, the impact on the overall number of outages currently attributed to procedural errors is uncertain. As indicated earlier, the proportion of procedural error outages is significantly lower among facility outages than it is among virtually all other categories. This occurs in part because one cause category of facility outage is identified as cable damage, rather than a procedural error. Although one could argue that a portion of the outages caused by cable damage do represent a procedural error, these categories are mutually exclusive in the reporting of facility outages.

Standards Initiatives

In both the international (International Telecommunications Union – Telecom [ITU-T]) and domestic (American National Standards Institute [ANSI] accredited Committee T1-Telecommunications) standards arenas, numerous standards have been developed and approved which, if implemented, would significantly reduce network outages and related procedural errors. A prime example are the standards for SS7 which discuss in depth the underlying architecture of the network and the necessity of providing two-way diversity for A-link sets in order to achieve network reliability and unavailability (downtime) objectives[1]. Analysis of numerous network outages reported to the FCC shows that the failure to implement and/or maintain diverse routing for SS7 A-links has significantly increases the impact of those outages.

In addition, Committee T1, and, in particular, its T1A1.2 Working Group on Network Survivability Performance, developed an index to determine the impact of service outages (see Committee T1 Technical Report No. 42, August 1995). This "Outage Index" is currently used by the NRSC in its quarterly and annual reports to assess the severity of FCC-reportable service outages. To date, T1A1.2 has not had any formal discussions or proposals related specifically to outages attributed to procedural errors. T1A1.2 and other industry forums should consider addressing the impact of procedural errors.

Although no domestic or international standards body has addressed procedural errors specifically, a number of human factors standards bodies have made contributions that have the potential to reduce procedural errors if they are implemented. These standards focus on designing user interfaces from a human-centric perspective. An example of such a standard is ISO 9241, Ergonomics requirements for office work with visual display terminals (VDTs). ISO 9241 consists of the following parts:

- Part 1: General Introduction
- Part 2: Guidance on task requirements
- Part 3: Visual display requirements
- Part 4: Keyboard requirements
- Part 5: Workstation layout and postural requirements
- Part 6: Environmental requirements
- Part 7: Display requirements with reflections
- Part 8: Requirements for displayed colors
- Part 9: Requirements for on-keyed input devices
- Part 10: Dialogue principles
- Part 11: Guidance in usability specifications and measures
- Part 12: Presentation of information
- Part 13: User guidance
- Part 14: Menu dialogues
- Part 15: Command dialogues
- Part 16: Direct manipulation dialogues
- Part 17: Form filling dialogues.

[1] See Bellcore Notes on the Networks, SR-2275, Issue 3, December 1997 sections 4.6.4, 6.23, 8.3, 14.2, 14.6, and 14.7 as well as ANSI T1.111-1988, Section 7.2.1.

Generic Requirements

There are two (Telcordia) generic requirements documents that were written specifically to mitigate procedural errors. The first of these documents is GR-2914-CORE*, Human Factors Requirements for Equipment to Improve Network Reliability.* This document focuses on designing equipment from a user's perspective. The objective of these proposed generic requirements is to improve the design of the Maintenance User Interface of network equipment by focusing on design implementations that would most likely have a significant impact on reducing procedural errors. The proposed generic requirements in this document pertain to both hardware and software interfaces between network equipment and the technicians who perform maintenance activity on the equipment. The proposed generic requirements in this document are intended to apply to new equipment manufactured as of December 1998 and may also be applied to new sub-components or additions to existing equipment in which the hardware and software interfaces are evolving.

The spirit of GR-2914-CORE was to develop proposed generic requirements to ensure network reliability, but at the same time, allow flexibility for product differentiation. The emphasis on the requirements in this document is to ensure that the design of network elements provides the necessary information for technicians to do their job and prevent confusion.

GR-454-CORE*, Generic Requirements for Supplier-Provided Documentation,* presents proposed generic requirements for preparing network element documentation that will ensure that technicians have easy to use documentation which provides unambiguous information needed to successfully complete a task. These proposed generic requirements emphasize the importance of creating documentation from the user's perspective and assists in promoting consistency in the content, format and style of the documentation provided by different suppliers for similar network elements.

Both GR-2914-CORE and GR-454-CORE were industry initiatives and were motivated by the high frequency of outages attributed to procedural errors. The proposed generic requirements in these documents have been developed to assist in preventing the types of procedural errors that exist in the field today or that are likely to occur due to the evolution of technology. As noted, these proposed generic requirements take into account the technician, the technician's current environment, and task requirements. The emphasis on the requirements in GR-2914-CORE and GR-454-CORE is to ensure that the design of network elements and their accompanying documentation provide, unambiguously, the necessary information for a technician to do his required job successfully and reduce the probability of the occurrence of a procedural error.

Currently, both of these proposed generic requirements documents are gaining industry recognition. Some suppliers are beginning to adopt these proposed requirements in their network element designs and their equipment documentation. Some service providers have identified these documents as mitigators for reducing outages attributed to procedural errors in their FCC outage reports. In addition, some of the service providers are asking for suppliers to comply with these requirements and have included them in contract negotiations.

There are other generic requirements documents that are noteworthy for their contribution to ensuring network reliability and minimizing procedural errors. Reliable equipment minimizes human intervention, which in turn reduces the likelihood of a procedural error. GR-929-CORE*, Reliability and Quality Measurements for Telecommunications Systems (RQMS),* proposes generic requirements for Reliability and Quality Measurements for Telecommunications Systems (RQMS). RQMS provides performance objectives by product type for selected network telecommunications equipment. The objectives and measurements set for any product type furnish service providers the data necessary to evaluate network performance. Although GR-929-CORE currently does not address the measurement of outages attributed to procedural errors, an industry initiative from the GR-2914-CORE Technical Forum proposed that such a measure should be included.

In 1998, it was proposed that an RQMS metric be added for switching equipment that measures outages attributable to procedural errors. The objective of this metric would be to track these types of outages. The metric will focus on total and partial outage duration (e.g. minutes or events per system per year). This metric will include all procedural errors, regardless of whether they were attributed to telco, vendor, or other. It was proposed that this metric be included in the Switching Element Measurements under Required Reliability & Quality Measurements. The proposal focused on switching as an initial attempt to track procedural errors. The intent would be to expand this metric to all equipment types, if this procedural error metric provided added value to the RQMS process. A technical sub-committee from GR-929-CORE will be meeting during the third quarter of 1999 to discuss the criteria of such a metric and its value in the RQMS process. The tracking of outages attributed to procedural errors can assist service providers and suppliers in addressing the factors that contribute to the occurrence of these errors.

There are a number of generic requirements documents that focus on the reliability of network elements. For example, GR-512-CORE, *LSSGR: Reliability, Section 12,* provides proposed hardware reliability modeling requirements and field reliability performance requirements for Local Access and Transport Area (LATA) switching systems. These proposed generic requirements apply to LATA end office and tandem switching systems, both Integrated Services Digital Network (ISDN) and non-ISDN. Field reliability performance measures and the root causes that impact performance are noted in this document. Examples of reliability requirements for other switching technologies include GR-301-CORE, *Public Packet Switched Network Generic Requirements* and GR-110-CORE, *Broadband Switching System (BSS) Generic Requirements*. The objective of these documents is to ensure network reliability, rather than impact outages attributed to procedural error. However, as noted, reliable hardware reduces the need for human intervention and, therefore, indirectly reduces the probability of a human error.

GR-929-CORE and GR-512-CORE focus on the overall reliability of the network. GR-2914-CORE and GR-454-CORE attempt to minimize the probability of the occurrence of procedural errors through the interface to technicians. All of these proposed generic requirements could have an impact on reducing outages attributed to procedural errors. The success of these documents in improving network reliability will depend on the degree to which they are implemented. Service providers and suppliers should embrace these requirements to reduce the frequency of procedural errors and improve network reliability. All of these generic requirements documents are funded and co-authored by a cross section of industry representatives that include service providers, Telcordia, and vendors.

Common Reporting Methods

When examining outage data from various companies, it becomes apparent that there is a lack of consistency in the industry on how outages and their root causes are categorized. As an industry, we may be more effective in reducing outages attributed to procedural errors and improving network reliability if we are talking the same language and attacking the same problems. To assist in achieving this goal, a common language and a consistent mechanism for reporting should be implemented.

Industry initiatives have already moved in this direction. The FCC has clearly defined the term “outage” and has outlined the rules and regulations of reporting such events. “Outage” is defined as “a significant degradation in the ability of a customer to establish and maintain a channel of communications as a result of failure or degradation in the performance of a carrier’s network.” (See Appendix D).

In Part 63.100 of the Commissions Rules and Regulations (Chapter 1 of title 47 of the Code of Federal Regulations, Part 63), the rules for required reporting are identified. Generally those rules are as follows:

- Outages potentially affecting 30,000 or more customers and lasting 30 or more minutes
- Outages lasting 30 or more minutes and affecting certain special facilities regardless of the number of customers affected
- Fire-related incidents affecting 1000 or more lines and continuing for 30 or more minutes.

Outage reports must include an analysis of the root cause of the incident and evaluate the effectiveness and application of best practices as identified by the NRC-1. (See Appendix D).

Although the FCC clearly defines when an outage must be reported and identifies what information should be included in that report, it does not appear that all reporting parties provide an equal level of data or information on root cause and preventative measures addressing an outage.

In response to Part 63.100 of the Commission's Rules, the NRSC has provided definitions and examples of Direct Cause and Root Cause of outages so that these components of the outage reports will represent consistently defined elements. It is recommended that these definitions be implemented when determining the Direct and Root cause of an outage. These definitions are included in Appendix E.

Example of Direct Cause is defined as follows:

Procedural-Service Provider: Failure to follow standard procedures/documentation
"Work error by telco personnel; correct procedures exist and were generally available, however, the procedure/documentation was not used or was used incorrectly. Includes use of out-of-date or incorrect procedures or documentation when current or corrected documentation was generally available."

Example of Root Cause is defined as follows:

Procedural-System Vendor: Insufficient staffing
"Unexpected conditions depleted available resources; predictable but unavoidable shortage (unreasonable demand); ineffective/inadequate roll-down or centralization arrangement; resource-intensive (new) technology outside scope/reach of existing automatic/remote administration systems, etc."

If the industry relies on these NRSC definitions, there will be a common language, but a common approach is still lacking. A consistent reporting mechanism, which is based on common definitions, may assist the industry in gaining a better understanding of outages attributed to procedural errors. By clearly understanding the root causes of outages attributed to procedural errors, there is a greater chance of reducing their frequency and impact.

The procedural error outage sub-team perceives a need for consistent categorizing and reporting procedural error outages. Electronic accessibility of a standard reporting format would enhance the industry's ability to achieve consistency. While input will be needed from multiple network reliability committees to finalize a standardized methodology, the Procedural Error Outage sub-team recommends that the following types of information be included in any standardized reporting methodology, which may be developed for reporting outages attributed to procedural errors:

- Date of Incident
- Time of Incident
- Incident Duration
- Nature of Failure
- Equipment Type
- CLLI & Release
- Total Facility Size
- Outage Type
- Customer Trouble Reports
- No. of Affected Lines/Circuits/etc.
- Blocked Call Impact on Network
- Root Cause Category
- Background of Event
- Chronological Sequence of Events
- Other Contributing Factors
- Factors Contributing to the Duration of the Incident
- Quick Fix Actions

- Triggering Event
- Outage Cause
- Best Practice to Mitigate.

Conclusions

From reviewing the existing industry initiatives, it is evident that strides are being taken to address the impact of procedural errors on the public network. Some of these efforts have the potential of having a significant impact on outages, while others may indirectly effect the frequency of these errors. Although for the industry this is a move in the right direction, outages attributed to procedural errors continue to increase. Industry efforts need to be more aggressive. Legislation, Best Practices, and Generic Requirements should be embraced and implemented to achieve the goal of minimizing procedural errors and improving network reliability.

References

Amendment of Part 63 of the Commission's Rules to Provide for Notification by Common Carriers of Service Disruptions. Federal Communications Commission. CC Docket No. 91-273 (August 1, 1994).

Bennett, J. FCC-Reportable Service Outages (3Q92-4Q98) with Procedural Errors as Root Cause: A Bellcore White Paper. February 18, 1999.

Fixing Facility Outages: Building the Tools to Make it Happen. Facilities Solution Team of the Network Reliability Steering Committee of the Alliance for Telecommunications Industry Solutions. November 1997.

Committee T1 Technical Report No. 42 on Enhanced Analysis Of FCC-Reportable Service Outage data, August 1995.

GR-110-CORE, Broadband Switching Systems (BBS) Generic Requirements, Issue 1 (Bellcore, September 1994); plus Revisions.

GR-301-CORE, Public Packet Switched Network Generic Requirements (PPSNGR), Issue 2 (Bellcore, December 1997).

GR-454-CORE, Generic Requirements for Supplier-Provided Documentation (a module of LSSGR, FR-64; OTGR, FR-439; and TSGR, FR-440), Issue 1 (Bellcore, December 1997).

GR-512-CORE, LSSGR: Reliability, Section 12 (a module of LSSGR, FR-64), Issue 2, (Bellcore, January 1998).

GR-929-CORE, Reliability and Quality Measurements for Telecommunications Systems (RQMS) (a module of RQGR, FR-796), Issue 4 (Bellcore, December 1998).

GR-2914-CORE, Human Factors Requirements for Equipment to Improve Network Reliability, Issue 4 (Bellcore, December 1998).

Keeping the Network Alive and Well: Solving the Problem of Cable Dig-Ups. Facilities Solution Team of the Network Reliability Steering Committee of the Alliance for Telecommunications Industry Solutions. February 1996.

Network Reliability: A Report to the Nation. Network Reliability Council of the Federal Communications Commission. June 1993.

Network Interoperability: The Key to Competition. Network Reliability and Interoperability Council. December 1997.

Network Reliability: The Path Forward. Network Reliability Council of the Federal Communications Commission, April 1996.

Introduction

The Human Factors Good Practice sub-team reviewed those FCC ('97-'98) Final Service Disruption Reports with the Root Cause identified as procedural. From this data, the team identified the following good practices. These good practices are focused on process, capability, and sensitivity. Primary factors in each of these good practices are clarity, simplicity, and adherence. The process should be concise and complete, and there should be no tolerance for deviation.

To identify good practices, we first need accurate data on the root causes of the failures and network performance after the identified counter measures are implemented. Many of the reports did not include root cause or corrective action. The change in the number of reports by type was used to analyze the effects of the countermeasures. Widespread use of a countermeasure also classified it as a good practice.

Several good practices focused on equipment installation-related failures. These failures were caused by failure to protect areas around the work area, not following documented procedure, not having a documented procedure, not informing all associated centers or organizations of the work activity, and not performing critical activity during low risk hours.

Method of Procedure (MOP)

To alleviate failures, mandatory use of a detailed Method of Procedure (MOP)[2] [3] is recommended for all hardware and software growth and change procedures. The MOP should include a description of the work activity, emergency back out procedures, escalation procedures with telephone numbers, detailed environmental or miscellaneous work items, i.e., fire stopping, “Ask Yourself”, coordinated MOPs, etc., plus the detailed step-by-step procedure that will be used to perform the work. The people performing the work should prepare the MOP, and they should perform a walk through (dry run) of the procedure to ensure understanding and completeness. The MOP approval list should include the responsible engineer, the installation manager, and the line operations manager. After approval, there should be no deviation from the work steps, including work sequence, without approval of all these managers.

The MOP should include steps for every work item and the sequence in which they should be performed. These steps should include preparation for the work—verification of hardware and software stability, backing up software, tool availability, capability of technicians, technician review of the “Ask Yourself” questions, protection around work area, etc. It should also include customer and internal group notification and the establishment of emergency communications before starting the work. The installation steps should include step-by-step

[2] TP 76300MP, Installation Requirements SBC Local Exchange Carriers, July 1, 1998

[3] GR-1275-CORE, Central Office Environment Installation/Removal Generic Requirements, Revision 1 (Bellcore, March 1998)

work items, expected responses (including alerts, alarms, failures, etc.), tests required to verify correct installation, and the post-work completion activities.

For all critical activities, these MOPs should identify “Safe Stop” points and should include “Emergency Back Out” and “Emergency Escalation” procedures. Safe Stop points are points during the execution of the detailed work steps where work can be stopped with minimum potential risk to service. This is the point of retreat when a work item that is later in the sequence of work does not successfully complete. Emergency Escalation procedures should include names, telephone numbers, and a conference bridge to be used if things do not go as planned.

The detailed Installation steps for repetitive work (frame growth procedure, generic program load procedure, etc., should be documented, laboratory tested, and standardized prior to use. MOPs that are site specific (hot power, cable removal, etc.) should include detailed installation steps that are jointly developed, reviewed, and verified by the supplier and customer.

The MOP should be used as a work item checklist with work items initialed and dated by the person performing the work as it is completed. If, during performance of the work activity, a problem is encountered that requires deviation from the approved process, the work should be backed up to a Safe Stop Point and halted. At that time, the problem or procedure should be corrected, and the management team should again approve the changed MOP.

Maintenance Window

A minor error during the performance of some activities can result in catastrophic service impact. These critical work activities should be performed during the office-specific lowest traffic hours. Without more definitive data, this period is generally defined as 2200 hours to 0600 hours. For hot power work, it is defined as 0000 hours to 0600 hours. This period is commonly called the “Maintenance Window” or “Safe Time”[4]. The maintenance window should be adhered to for all hot power work and for all installation, change, or maintenance activities that are critical in nature. For this process to be effective, senior management should also provide support.

The use of a maintenance window itself does not prevent procedural outages. However, it does reduce the potential service impact and the duration of recovery.

“Ask Yourself”

Many network failures occur because the proper tools or procedures are not available prior to starting the work. Others occur because the technician is not skilled or prepared for the work activity. Ask Yourself programs can be established to focus on these deficiencies and provide a process for identification of limitations, omissions, or errors before starting the work. These programs are general in nature but have also been customized for specific work functions. A typical list of Ask Yourself questions would include:

[4] BA 002-300-100, Bell Atlantic Regional Operations Staff Safe Time Practice, Issue D (Bell Atlantic, December, 1997)

- Do I know why I am doing this work?
- Have I identified and notified everybody—customers and internal groups—who will be directly affected by this work?
- Can I prevent or control service interruptions?
- Is this the right time to do this work?
- Am I trained and qualified to do this work?
- Have I considered all the Maintenance Do's and Don'ts that apply to this procedure?
- Are the work orders, MOP, and supporting documentation detailed, current, error free and approved?
- Do I have everything I need to quickly back out or restore service if something goes wrong?
- Do I know whom to call if something goes wrong?
- Have I walked through and do I understand the procedure?
- If you have answered NO to any of these questions, STOP: contact your supervisor or next level of support.

Effective Ask Yourself programs require demonstrated support from senior management. When a technician answers one of these questions with NO and stops a work function that may be critical to a project or to a customer due date, he or she should be supported even if they are wrong. If they are not supported, this proactive process will not work. This process requires continued review, re-affirmation, recommendation, and certification of all people working in or around the network. The maximum duration between certification and re-certification should be no more than six months. Each certified person should display evidence of certification. If a person does not have a current certification, they should not be allowed to work in the network.

Critical Event Management

When failures occur, the duration of the service impact is shortened when a "Critical Event Management"[5] process is in place to manage the event. This process should include command and control of the event, communications requirements for both recovery and problem resolution, and communications requirements for managing the event. It should include requirements for escalation within the tiers of technical support, and it should include requirements to periodically critique and upgrade the process. This process should include by type of event, to whom to escalate to within what timeframe. The type of event could range from a simple condition to a full network element failure. For simple or partial network failures, the time for escalation will be of longer duration than for a total failure, which should be immediate.

The Critical Event Management process should define the communication processes. It should include a communication process for those performing the network restoration and another for those managing the environment created by the event. The establishment of two conference bridges may effectively provide these communications.

[5] 190-130-147PT, Trouble Escalation Procedures, issue D (Pacific Bell, August 1996)

To be effective, the Critical Event Management process should be followed for each applicable event, reviewed periodically with all technicians and supervisors, and critiqued following major events to identify and eliminate faults or to improve use of the process.

Awareness

One of the most pervasive causes of failure is loss of concentration on the in-progress task.

- Technicians following detailed MOPs become distracted and miss a step.
- Technicians working together on a task assume their partner completed a step.
- Technicians making translation or data base changes get distracted by telephone calls or questions from peers and make input errors.
- Technicians perform the correct task in the wrong office or remove packs or wiring in the wrong place in the correct office.

There have been many attempts to resolve this issue. *The Human Factors Requirements for Equipment to Improve Network Reliability* (GR-2914-CORE)[6] established standards for labeling and color-coding duplicated equipment, circuit packs, and cables. It established requirements for warnings during critical work operations and requirements for data base interaction and changes. When implemented, these requirements should reduce the possibility of error, but we still need to maintain the awareness and sensitivity of the technician.

The following good practices have been established to reduce vulnerability in this area. Technicians performing critical work should be isolated from day-to-day activity and the distraction of telephone calls and peer questions. Establishment of a dedicated sub group to perform a task can also accomplish this. This approach should be applied for performance of critical hardware or software modification to groups that are dedicated to the surveillance, maintenance, and management of 911 services.

Even with dedicated teams, the sensitivity to risk must be maintained. Maintaining sensitivity requires communication. First those performing the work should understand the risk of the work operation. Expectations of caution, attention to work, test calls, and professionalism need to be communicated and understood. Performance metrics should be established for the work group. The group should understand these metrics and know how they are performing. Regular weekly or daily communication with the team(s) should share performance detail from any failure or outage, time between outages, and a reminder of identified trouble areas. Finally, management should be committed to and enforce these processes.

The sensitivity to critical operations is enhanced through weekly conference calls with all work groups and support staffs. These conference calls are used to share all network failures, the network impact, the triggering event(s), the root cause, and associated countermeasures. This expands awareness to related work groups, provides a forum to

[6] GR-2914-CORE, The Human Factors Requirements for Equipment to Improve Network Reliability, Issue 4 (Bellcore, December 1998)

share improvement ideas, and provides a forum for tracking countermeasure implementation.

Training and experience modify technician performance. Their opportunity for initiating network failure is reduced when they are adequately trained. Added experience reduces the probability of failure but it also adds a risk of complacency. Highly skilled and experienced technicians are involved with more critical work operations. Because of their knowledge, they are also more likely to ignore a documented procedure and perform, what appears to them, a common and perhaps simple task.

Each technician should be properly prepared to complete his or her work without impacting the health of the network. They should each have a training track that is customized to their work function. The training track should include both formal and on-the-job training. This training should include “Critical Event Management,” “Maintenance Window,” and “Ask Yourself” training.

911 Emergency Services

911 related failures continue to be of major concern. The triggers for these events range from cut facilities, wet facilities, power failures, translation errors, CCS failures, 911 tandem switch failures, and work errors. In addition to all the good practices already discussed, two additional good practices should be implemented to reduce these failures.

First, all 911 work should be performed in a dedicated work group where possible. The group should be responsible for all provisioning, maintenance, and surveillance of the 911 network. The technicians should have a specialized training track, and they should have certification or qualification requirements to ensure technical expertise. Technicians should be required to re-certify annually.

Second, a periodic audit of all critical circuits should be performed to ensure continued diversification of 911 trunks, CCS Links, Remote Office Umbilicals, and Network Timing. Diversification is only effective if it is maintained.

Prevention

Every opportunity should be taken to identify and eliminate the cause of failure before implementing new or changed hardware or software into the network.

One way to do this is through the use of an “Approval for Use” process. This process is used to ensure that equipment placed in the network meets both design and technology management requirements and works as designed and advertised. The process incorporates test plans to verify interoperability with Operations Support Systems (OSS) and other network elements that may not be readily available at the supplier location. The tests should include verification of all growth, change, and implementation procedures and should verify documentation functionality and completeness. These tests should be performed jointly with the manufacturer, or, if not, a manufacturer feedback loop should be maintained that ensures any identified deficiency and its root cause is properly addressed.

A physical verification of both local and remote alarms and of remote network element maintenance access should be performed on all new equipment installed in the network before it is placed into service. When these functions are not performed, the probability of failure without notification is greatly increased. Likewise, if remote network element access is not verified, a simple restoration process may require technician dispatch to the site, resulting in further delay in service restoral. If a new CO is installed or an old switching system replaced, the integrity of the diversified FX telephone line for the office should also be verified.

A number of outages are of extended duration because the technician does not have the tools nor test equipment to implement the restoration. The most common cause is unavailability of spare circuit packs. This results in a delay until the spares are located and shipped from some other location. To prevent these delays, a process should be established to track the location of all spare equipment. This process should align with network performance and reliability requirements and should include procedures for allocating, procuring, delivering, and deploying spare equipment. When spares are not locally available, the process should also provide a method to expedite identification and delivery of the required equipment.

Removal from service of the incorrect network element, controller, processor, connector, or circuit pack continues to be a problem. Many of these issues are addressed by the Human Factors Design Requirements in GR-2914-CORE. These design requirements were developed to affect the design of new network elements. Some problems are so pervasive that countermeasures should be revised to reflect existing technology. One of these is the process of labeling removable cabinet or frame covers with frame, network element, controller, or circuit numbers. These covers are interchangeable and can be installed in an incorrect location. As a result, another technician at a later date may remove the incorrect equipment from service. All removable covers that have equipment designations should have those designations removed and the designations placed on the permanent portion of the unit or frame.

Translation errors continue to be one of the most pervasive areas of procedural failure. There have been many root causes identified including technical skill level, complexity of work operations, work environment, distraction, multitasking, etc. In some areas, dedicated groups have been established to perform the critical translation functions. Dedicated 911 groups are one example. In other areas, technicians performing critical translation changes are isolated from the normal interaction of the work place including incoming calls. Still other efforts have been undertaken to mechanize the translation function. After implementing all of these countermeasures, the most effective practice when performing complex translation changes is to test the translations before and after the change to ensure the appropriate and expected results. A test of the translations before making a change can verify that the work is being done in the correct office and the current translation agrees with the records. A test after the translation change will verify that the change works as planned. If the test returns the same results as the pretest, it is an indication that an error has occurred. If the appropriate test results are not received, perform an investigation and correction before continuing the work activity. This procedure is critical when a change is entered and the test indicates the targeted translator has not changed. This is normally an indication that an error has been made in the input, and this testing process has captured it.

Conclusions

Evaluation of procedural failures has shown that people have different perspectives and habits. It is, therefore, impossible to implement one countermeasure that will work for everyone. Some standardization in the design of the environment reduces the possibility for failure. The most frequent areas of failure have been identified and Human Factors Design requirements have been prepared and documented in GR-2914-CORE. An in-depth analysis of procedural failures that includes the experience of the people involved in the failure is required to get to the root cause(s) of the event. The results of these in-depth investigations should be tested against the GR-2914-CORE requirements to validate effectiveness and to identify additional areas that require standardization or improvement.

Introduction

There are industry initiatives underway and identified good practices focused on network reliability. However, due to the growth in network suppliers, network owners, and network complexity, there is a need to look further ahead to assure continued improvement. This chapter's focus is on providing both insight and encouragement for companies to examine and embrace new technologies and processes that can further improve future network reliability. Investment priorities and business cases should assure that the right expenditures are planned to improve network dependability into the next millennium.

Three areas for advancement are:

- providing an environment to minimize human error
- designing our networks to minimize human involvement
- keeping errors from becoming outages.

Providing an Environment to Minimize Human Error

Human-centric product design

One of the primary mitigators in reducing outages attributed to procedural errors is to design network user-interfaces from a human-centric perspective (e.g., network elements, software, documentation). For any user-interface to be used easily and efficiently, designs should be meaningful, understandable, and have a coherent structure to the user[7]. The technology design should provide the user with situations that minimize error, minimize the impact of error, and maximize the chance of discovering an error once it has occurred[8]. By designing network tools, machines, systems, tasks, jobs and environments that take into account human capabilities and limitations, as well as the advantages of the human's cognitive ability to process information, the potential for human error is minimized[9]. Minimizing the probability of human error minimizes the resulting procedural errors, which currently plague the network.

Currently, two (Telcordia) Generic Requirements documents address the human-centric perspective to specifically mitigate the probability of the occurrence of procedural error.

[7] Norman, D. Things That Make US Smart; Defending Human Attributes in the Age of the Machine. Reading: Addison Wesley Longman, Inc., January 1994. 304 p.

[8] Norman, D. Things That Make US Smart; Defending Human Attributes in the Age of the Machine. Reading: Addison Wesley Longman, Inc., January 1994. 304 p.

[9] Chapanis, A. (1991). Human Factors Society Bulletin Number 34(11), "To communicate the human factors message, you have to know what the message is and how to communicate it." Pgs.1-4.

These generic requirements documents are GR-2914-CORE[10], *Human Factors Requirements for Equipment to Improve Network Reliability, Issue 4* and GR-454-CORE[11], *Generic Requirements for Supplier-Provided Documentation, Issue 1.* Both of these documents are industry driven and data based on procedural errors that have occurred or exist in the field today. They take into account the technician, the technician's current environment, and task requirements.

GR-2914-CORE proposes generic requirements to ensure network reliability, but at the same time, allow flexibility for product differentiation. Each proposed requirement is preceded by its intent, which clearly identifies the objective of that particular requirement (i.e., the procedural error it proposed to mitigate). Test methods are provided for some of the requirements to ensure reliability of design implementations, as well as to encourage the use of standardized procedures.

The following examples from GR-2914-CORE show the emphasis placed on ensuring that the design of network elements provides the necessary information for the technicians to do their job and assist in preventing confusion.

1. The intent of Requirement [137] is to minimize the use of color as the only indication to the technician of status information.

   R6-8 [137] - When a Maintenance User Interface uses color to convey status information, the Network Element (NE) shall provide accompanying text to clearly identify the meaning of color.

2. The intent of Requirement [57] is to ensure that a technician updating the on-line memory to the storage memory is aware of any existing corruption that has occurred since the last update.

   R8-3 [57] - If a read/write error occurs in the system, an alarmed error message shall be provided in a separate log. When a technician initiates a memory update, a summary of the alarmed messages shall be provided, since the last update.

   - These error messages shall be alarmed and in a readable format that can be interpreted by the technician with minimal effort (i.e., message should be readable text or, at most, should require referring to one document).
   - Input shall be required from the technician for the update to continue.

3. The intent of Requirement [63] is to prevent a technician from mistakenly carrying out an activity that will be service affecting. The requirement ensures that technicians will be given a clear and concise indication of the outcome of initiating specific commands.

   R9-6 [63] - Command execution shall be a two-stage process when the context of an action or command suggests the possibility of service-affecting consequences.

[10] GR-2914-CORE, Human Factors Requirements for Equipment to Improve Network Reliability, Issue 4 (Bellcore, December 1998).

[11] GR-454-CORE, Generic Requirements for Supplier-Provided Documentation (a module of LSSGR, FR-64; OTGR, FR-439; and TSGR, FR-440), Issue 1 (Bellcore, December 1997).

Examples of service-affecting consequences include files being deleted, units being removed from service with no automatic transfer of function, or service being disrupted or degraded. The first stage would provide relevant information and describe the potential consequences to the user before execution of the command, and the second stage actually would serve to execute the command. The input needed for command execution shall be descriptive of the consequences and be presented in the prompt verbiage. For example, to execute a specific command, a technician shall enter "Yes. Take out trunk group members 1-10."

Documentation also plays a critical role in the mitigation of procedural errors. The following examples from GR-454-CORE, *Generic Requirements for Supplier-Provided Documentation*, demonstrate the human-centric approach of these requirements and how they ensure that the technician is provided with clear, concise, and well organized information to assist him in completing a task successfully.

1. R2-5 [5] - Strict consistency in terminology, format, abbreviations, acronyms, numbering schemes, and markings shall be observed between documentation associated with the supplier's product (equipment, system) and physical aspects of the product such as various electronic or mechanical displays of information on, in, or by the product. That is, what is shown in the documentation should match what the user sees when operating the equipment.
2. R2-6 [6] - The document shall have a glossary that defines abbreviations, acronyms, and any other special or unique terms used in the document.

Designing equipment, documentation, software or any Maintenance User Interface from a human-centric perspective will assist in ensuring that the user interfaces technicians encounter will be unambiguous and provide the necessary information they need to successfully complete a task. This in turn will reduce the likelihood of procedural errors. Human-centric designs can only assist in reducing outages attributed to procedural errors if they are implemented. The implementation of industry driven human-centric design requirements such as GR-2914-CORE and GR-454-CORE represent a means to mitigate procedural errors as we move forward.

Language Simplification

Another aspect of designing the documentation to minimize human error centers is the language used within the documentation. Many industries and individual companies are introducing a restricted language system that limits language to a set of core vocabulary words and company- or industry-defined technical words to enforce the use of words with only a single meaning. This system also consists of a set of writing guidelines for grammar, mechanics, and style. The airline industry took the lead in 1990 with the adoption of a national simplified English program under the Association Europeene des Constructeurs de Material Aerospatial (AECMA). Other companies including Caterpillar, NCR, Xerox, Nortel Networks, and IBM have also embraced controlled language as important to customers' successful operation and maintenance of their equipment.

The use of a standard "telecommunication's industry" English with a restricted lexicon would attempt to reduce ambiguities, colloquialisms, and synonyms and improve clarity. Together with the writing guidelines, the restricted lexicon limits the author's use of words and suggests clear, concise, and logically organized sentences.

In theory, providing consistent language eliminates lexical, syntactic, and semantic ambiguities for people using documents written to this standard. The restricted vocabulary keeps the user from wondering whether SS7 (Signaling System 7) is the same as CCS7 (Common Channel Signaling 7), for example, and subsequently improves navigation through a document by limiting variations that need to be entered into a search engine to find the correct information. For users with English as a second language, different words can mean different things even though they may be synonyms in English. Consistency drives both universal understanding accessibility of the information.

Another benefit of simplified English is that it helps to control the reading level of documents developed for native and non-native English speakers by restricting the words that can be used. Standard English writing guidelines should encompass the indicators that drive standard readability statistics from elimination of passive voice, number of words per sentence, sentences per paragraph or Flesch Reading Ease, Flesch Kincaid Grade Level, Coleman-Liau Grade Level or Bormuth Grade Level. The combination lowers the grade-level education required by readers.

On-Product Help

While GR-2914-CORE addresses human factors requirements in the product interfaces, a further advancement is to assure that the product is designed with help for the interfaces embedded in the product itself. Advantages of on-line information in further reducing service outages include:

- information is located with the product (on-line help) or is available throughout the product (on-line information that can be called from the product)
- information is always current, updated with the software itself
- pertinent on-line information is easier to find (especially in context-sensitive help scenarios)
- on-line information tends to be more direct and simpler to use
- on-line help can provide consistency in interface design
- on-line information can make use of multimedia elements which enhances understanding through appropriate animation, video snippets or sound
- on-line information can make use of colors and textures to imply different connotations to information elements.

Electronic Information

For products where embedded help cannot be introduced, the access to information should be moved from paper to electronic access through either the Web or in a client/server arrangement. Maintenance and operations centers should be designed to allow all craftsperson's access to real-time information. Companies need to reinforce the evolution away from the dependency on paper. Paper information introduces errors with poor version control on documentation, allowing accidental use of out-dated information, craftsperson reliance on training manuals rather than actual, comprehensive product documentation, and separate systems for Warnings and Bulletins not integrated into documentation.

Adequate Lead-Time for Network System Changes

The last aspect recommended to minimize human error is recognition that the Operations Support Systems are not synchronized with the changing architectural requirements. The OSSs are developed for and used by the service providers to connect various network components to provide specific services to customers. While the problem is beyond the control of the manufacturers of the network components, suppliers need to provide early and comprehensive views on changes that will affect downstream OSSs. This will decrease errors introduced with short lead-times, avoid product deployment records not matching product functional reality, and/or avoid not capturing full functional requirements to identify administrative software gaps.

Designing Networks To Minimize Human Involvement

While the first step to improving network reliability is to provide an environment to minimize the possibility of human error, the next is to introduce automation where possible to minimize human involvement in executing procedures. As the demand for increased network reliability is tested against increased network complexity, business cases are examining the introduction of Expert System technology. While the penetration of early expert systems was slow from the 1980s through 1995[12], the emphasis on new advancements and the proliferation of information access now has a vast amount of time and energy pouring into these systems. A Delphi Group survey indicated that 90.2% of Information Technology professionals said they would invest in knowledge management in the next four years[13]. Independent consultants estimate investment in analysis-based applications for Network Management to grow to $2B+ annually by the year 2002.

Intelligent operator behavior can be modeled and integrated into an automated operations and maintenance management system with expert system technology and artificial intelligence. The objective is to reproduce some of the contextual reasoning applied by the operator to resolve error conditions or perform routine administrative procedures.

The operations and maintenance procedures comprise large numbers of commands and massive volumes of alarm messages that currently need to be interpreted by a human operator to customize the generic procedures described in the manuals to a specific situation or problem at hand. This customization usually revolves around the identification of appropriate command parameters and the proper navigation throughout the procedure’s decision network. In addition, this on-the-fly customization can be error-prone, since the operator may inadvertently make keyboard entry mistakes or misinterpret alarm data causing erroneous command sequences to be entered. Furthermore, the large volume of alarms and the frequent need to put procedures on hold to tend to more critical ones easily creates a serious usability problem resulting from operator information overload.

The expert system module can restrict procedure application depending on time or event analysis, proactively identify appropriate fault resolution, remove the task of customizing the

[12] New Ways to Make data Pay: Knowledge Management Technology Improves Analysis and decision-Making. Christy Walker, PC Week, v15, n34, p14, August 24, 1998

[13] Measuring the Impact of Expert Systems. Luvai Motiwalla; James Fairfield-Sonn, Journal of Business & Economic Studies, v4n2, p1-17, Fall 1998

procedures on-the-fly while monitoring and validating expected system feedback from the operator's workload, reduce the need for documentation, and ultimately insure faster operator performance. High-level messages can be displayed with optional access to compiled contextual information. In addition, the stacking of partially completed procedures with all data saved for later completion can be easily managed.

Artificial intelligence provides tools and techniques that allow complex knowledge and procedures to be modeled:

- to capture and model intelligent operator behavior
- to integrate it in an automated system
- to reproduce it repeatedly on-the-fly with the variations required by the context.

The design and development of intelligent systems can off-load the operator by transforming otherwise massive unmanageable data into high-level and easily understandable monitoring and auto-diagnostic messages as well as proactive context-sensitive and on-line intelligent advice originating from the product itself. In this manner, the product becomes more intelligent, more automated, and to a larger extent more self-sufficient. The majority of normal maintenance activities are candidates for Expert Systems.

Keeping Errors From Becoming Outages

Even with more automated environment and improvement in human intervention, retained errors will still ultimately occur. What can be done to mitigate errors turning into outages?

Layering Fault Protection

One way to prevent human errors from propagating through a complex system such as the telecommunications network is to design multiple layers of protection. Broadly, human errors can be classified into intentional and unintentional. Asking questions to confirm whether the task is the one that the persone really intended to start on the system can prevent unintentional errors. This involves a series of prompts to be triggered by the system and subsequent warnings regarding the consequences of the action. Intentional errors are tougher to handle using techniques for unintentional errors. However, giving controlled access to sensitive service-affecting operations can minimize them. Access is controlled through password protection or requiring social security number or by similar identification.

Improving Emergency Operating Procedures

When an error or outage occurs, the importance transfers to the time required recovering and minimizing damage.

The nuclear power industry reviewed and changed its emergency operating procedures (EOPs) following the Three Mile Island (TMI) incident. Prior to the TMI incident, EOPs used to be "event based," i.e., the procedures attempted to identify the event that caused the emergency before resolving it. After the TMI incident, the EOPs were changed to "symptom based." Using a hospital emergency room as a benchmark, these procedures now attempt to identify the values of critical operating parameters and assure that the plant is within safe operating parameters. If not, the EOPs will bring the plant to a safe operating condition before doing further investigation into the original event.

It is of interest for the telecommunications industry to examine operating procedures to identify whether the procedures are adequate to handle the types of outages that have been observed over the past few years. Such an investigation can also include reviewing changes to the procedures either on a local or global scale. Operating procedures for the aviation industry can also be examined for effectiveness in handling emergencies.

Assuring Diversity in Network Design

The underlying architecture of the circuit-switched telephone network has undergone significant changes in the past decade. Prior to the introduction of SS7, the switches and the trunks between them handled almost all calls without external assistance. Today, with SS7, most calls cannot be properly completed without the assistance of many signaling messages passed between the switches and, in some cases, between the switch and a centralized database (i.e. Service Control Point).

A review of the network outages reported to the FCC identified a number of outages where the required diversity did not exist. These outages break down into three broad categories. These categories are listed below with examples:

- <u>Diverse facilities and equipment did not exist</u>
  The final reports on several network outages indicate that the service provider was aware of the applicable best practices, but chose not to construct the route diverse cable or 911 tandem. Compounding this particular problem is the development of dense wave division multiplexing, which enables a single fiber cable to carry a virtually unlimited amount of traffic. Once a fiber cable exists in a given route, about the only justification for constructing a physically diverse alternate route is diversity.
- <u>Diverse facilities and equipment exist, but were not assigned</u>
  There are two aspects of this problem which have existed for many years in the telecommunications industry. The primary problem is lack of synchronization of the administrative software, hardware, and documentation. The second aspect of diversity is that inventory control systems do not nor cannot track ongoing system/product introduction resulting in circuits originally assigned with diversity changing to a non-diverse arrangement.
- <u>Single point of failure</u>
  SS7 and/or 911 Service circuits from many different locations were all assigned to the same network component, such as a power supply, digital cross-connect, or interoffice facility.
- <u>Multiple Locations</u>
  During 1998, over half the reported network outages impacted customers in two or more buildings. This happens when a large number of circuits from many different buildings pass through a common network component.

The primary responsibility for diversification and provisioning of the required facilities and equipment rests with the top management of each service provider. In addition, discussions with subject matter experts suggest that a quarterly check is required to make sure that circuits that should be diverse have not been inadvertently moved to a common network component.

Therefore, a fundamental future mitigator is a review of the existing network design for compliance with existing diversity recommendations and strict attention to diversity in future network expansion.

Commitment to "Best Practices"

Much good work has been done over time to capture "Best Practices" for design and operations of our network for maximal reliability. All are captured in *Network Reliability: A Report to the Nation* published June 1993. Many of today's procedural outages are the result of not following these documented Best Practices. All service providers should reaffirm their organization's commitment to these Best Practices. The following, recommended for immediate priority, represent a compendium of "Good Practices" to reduce the number of FCC-reported Procedural Outages in the network:

- Conduct periodic audit on all critical circuits to ensure that diverse routing has not been compromised.
- Provide a tracking process for all spare equipment and procedures for allocating and procuring. When spares are not readily available, provide a method to expedite a timely response.
- Develop an "Approval for Use" procedure to ensure equipment placed in the network works as designed and advertised. Incorporate test plans to provide interoperability testing with OSSs and other network elements that may not be readily available at the supplier location.
- Confirm/Conduct Physical verification of alarms on all new equipment installed in the network.
- Provide MOPs with specific step-by-step procedures, in addition to expected alerts, alarms, and failures, which can be tracked and signed off as technicians complete each step.
- Maintain work procedure sensitivity. Take steps to ensure workers' minds are on the task at hand. Avoid interruptions that may cause lack of concentration. Technicians need to be frequently reminded of the importance of their tasks and the impact of failure.
- Develop a Critical Management Work Process defining steps to take to get out of trouble. If a procedure fails, how do I recover?
- Establish communications between work groups before, during, and after procedural work. Ensure that other work groups are aware of work in progress.
- When providing complex network routing/configuration changes, test the before and after to ensure appropriate and expected results.
- Review company-wide Maintenance Window Policy.
- Develop an "Ask Yourself" program and tailor it to specific work groups where possible. Periodically review the program.
- Assemble 911 Service dedicated work groups to provide 911 Services. The group should be responsible for all provisioning, maintenance, and surveillance of the 911

network. The organization should have certification requirements to ensure technical expertise. Technical support teams should be required to re-certify annually.

- Assure that all technicians have an appropriate “Training Track” for their specific responsibility.
- Provide critique (Event Analysis) on all outages to determine GR-2914 CORE (Human Factors) compliance and whether the outage would have been avoided if compliant.

Conclusions

There is much to be learned from history. A key practice to improving network reliability is to learn from experience. We need to increase communication of outages reported to the FCC to industry members. Vendors and service providers should be committed to reviewing the root causes of the procedural outages and subsequently investigating their own companies to assure similar circumstances are eliminated before a similar outage can occur.

In summary, future mitigators for improved network reliability can be categorized into two major groups:

- Introduction of technology and process improvements today to both existing networks and with new products to minimize human involvement
- Rigorous implementation of current best practices and sharing knowledge at the industry level to prevent and eliminate procedural outages.

Human-centric design of products and documentation hold great promise for future reduction of procedural errors. This relatively new concept, coupled with the stringent use of standards and universal application of (good) “Best Practices,” provides a complete solution for reversing the rising trend of outages attributed to procedural errors. In the future, the same concepts that make traffic signals clearly understood and air travel the safest mode of transportation available should be applied to the telecommunications industry. The degree of success realized will be directly linked to the industry's readiness to embrace the application of these concepts.

APPENDICES

APPENDIX A—FCC REPORTABLE SERVICE OUTAGES: PROCEDURAL ERRORS

FCC-Reportable Service Outages (3Q92 – 4Q98)
with Procedural Errors as Root Cause

A Telcordia White Paper by Jay Bennett

Executive Summary

This paper provides a statistical analysis of FCC-Reportable Service Outages, which occurred between July 1, 1992 and December 31, 1998 as a result of procedural errors. The analysis was restricted primarily to outages reported on the basis of customers potentially affected (greater than or equal to 30,000) and outage duration (greater than or equal to 30 minutes) per CC Docket 91-273. Noteworthy results include:

- A Procedural Error is the root cause for 33% of reported service outages.
- Procedural Service Provider is the root cause of 79% of Procedural Error outages while Procedural System Vendor or Procedural Other Vendor is the root cause of the remaining 21%.
- Documentation/procedure problems (38%), insufficient supervision (28%), and insufficient training (27%) are the major root cause subcategories. Almost half of all outages caused by insufficient supervision occurred in 1998.
- Almost half of Procedural Error outages occur at switches (28% at Local Switches and 17% at Tandem Switches). The remaining Procedural Error outages are divided primarily (and almost equally) among Facility, CCS, and CO Power outages.
- Procedural errors are not the root cause of a statistically significant majority of outages within any single failure category. Non-procedural errors are the root cause of a statistically significant majority of Facility, CCS, Natural Disaster, and Overload outages. The proportion of Procedural Error outages is significantly lower among Facility outages than it is among virtually all other categories.
- The frequency of Procedural Error outages peaks near noon and midnight although the noon peak is significantly less pronounced than that for Non-Procedural Error outages.
- The frequency of Procedural Error outages has increased about 3% per quarter since July 1992 while Non-Procedural Error outages demonstrate no such trend over the same time period.
- Each Report Year after the Baseline Year (July 1, 1992 - June 30, 1993) had a higher aggregated outage index attributable to procedural errors than in the Baseline Year.
- Each Procedural Error outage on average has significantly less impact (as measured by the outage index) than a Non-Procedural Error outage.
- The number of customers potentially affected by Procedural Error outages is significantly less than by Non-Procedural Error outages.

- Overall, the average duration of Procedural Error outages is significantly less than that of Non-Procedural Error outages. This is especially true for Facility outages while Tandem Switch outages are longer when caused by procedural errors.

Introduction

This paper provides a statistical analysis of FCC-Reportable Service Outages, which occurred between July 1, 1992 and December 31, 1998 as a result of procedural errors. The analysis is based on data collected by the Alliance for Telecommunications Industry Solutions (ATIS) Network Reliability Steering Committee (NRSC) from reports made to the FCC by telecommunications carriers per CC Docket 91-273. Unless specified otherwise, all outage categorizations are those specified by ATIS/NRSC. The paper updates and extends analyses presented in an earlier version of this White Paper.

ATIS/NRSC categorizes each outage according to its root cause. Three of these categories can be grouped as *Procedural Errors (PE)*:

1. Procedural Service Provider,
2. Procedural System Vendor, and
3. Procedural Other Vendor.

All other outages will be referred to as *Non-Procedural Error (NPE)* outages.

The total number of Procedural Error outages through 4Q98 is 431 out of 1307 outages (33%). ATIS/NRSC categorizes each outage as “Regular” (outage meeting or exceeding the 30,000-customer and 30-minute duration thresholds) or “Special” (outage reported to the FCC with respect to other criteria such as affecting major airports, nuclear plants, and 911 tandems). Of the 431 PE outages, 367 were Regular and 64 were Special. Unless noted otherwise, this paper analyzes *only* Regular FCC-Reportable Service Outages. The 367 Regular PE outages represent 33% of the 1110 Regular outages from all root causes while the 64 PE outages represent 32% of the 197 Special outages from all root causes; the difference in these percentages is not statistically significant.[1]

Root Cause Category/Subcategory

As shown in Figure 1, Service Providers have a statistically significantly higher share of PE outages than that of Vendors (System and Other combined).

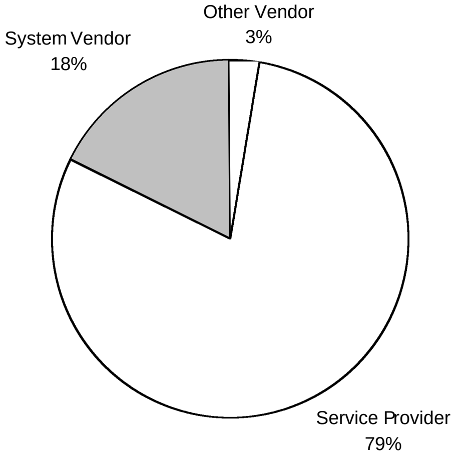

Figure 1. Distribution of Root Cause Categories for PE Outages

Figure 2 presents the distribution of PE outages over Root Cause Subcategories:

- *No Documentation*: Documentation/procedures unavailable, unclear, incomplete
- *Poor Documentation*: Documentation/procedures out-of-date, unusable, impractical
- *Training*: Insufficient training
- *Supervision*: Insufficient supervision/control
- *Maintenance*: Inadequate routine maintenance/memory back-up
- *Other*: Other or Unknown.

No Documentation/Procedures (32%), Insufficient Supervision (28%), and Insufficient Training (27%) dominate the root cause subcategories of PE outages equally. Note that when Poor Documentation/Procedures are included, documentation/procedure problems account for 38% of PE outages.

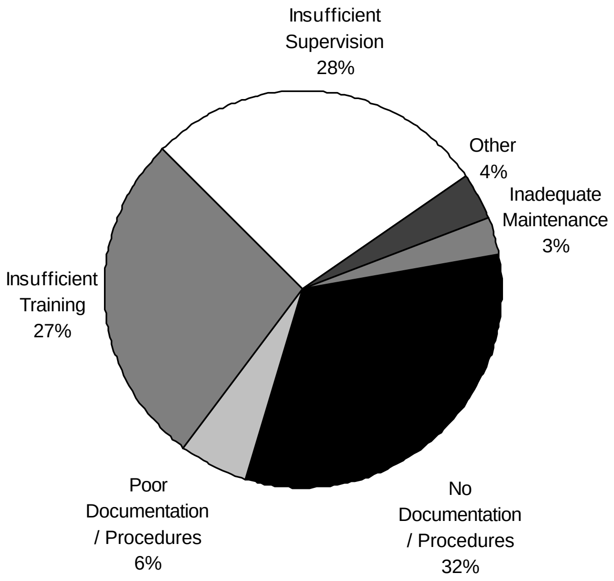

Figure 2. Distribution of Root Cause Subcategories for PE Outages

Figure 3 shows the number of PE outages by Root Cause Subcategory within each Root Cause Category. Note that the System Vendor and Other Vendor categories have been collapsed into a single Root Cause Category (called Vendor). The figure shows that documentation problems are dominant within each Root Cause Category, 52% and 35% for the Vendor and Service Provider categories respectively. Within the Service Provider category, Insufficient Training (31%) and Insufficient Supervision (28%) are equally notable Root Cause Subcategories. Almost half (42%) of all outages caused by Insufficient Supervision since 3Q92 occurred in 1998 alone; this difference between 1998 and previous years is statistically significant.

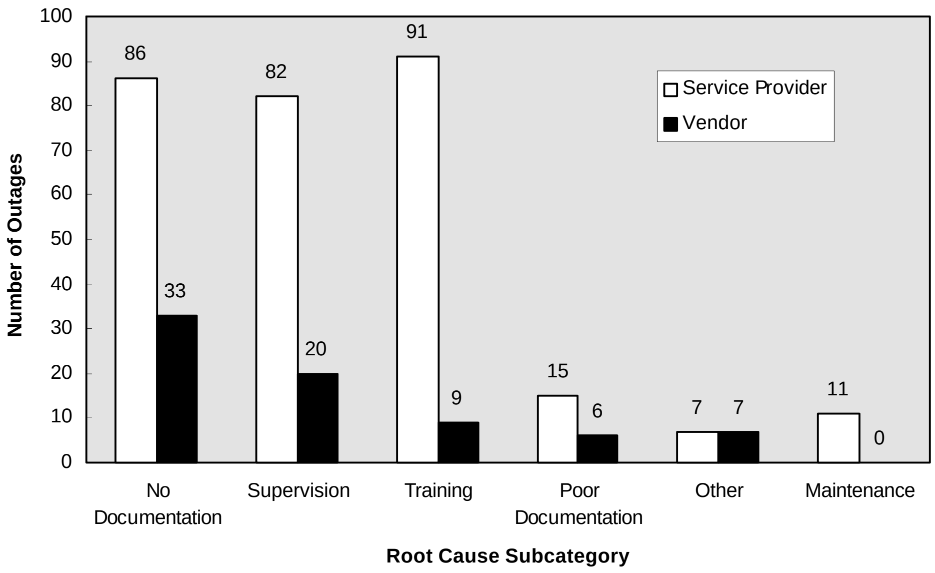

Figure 3. Distribution of PE Outages across Root Cause Subcategories for Service Provider and Vendor (System and Other Combined)

Failure Category

Table 1 shows the distribution of Procedural Error and Non-Procedural Error outages within each Failure Category. There is no category in which the proportion of Procedural Error outages is significantly higher than 50%. The proportion of Procedural Error outages is significantly lower than 50% in the Facility, CCS, Natural Disaster, and Overload categories. The proportion of Procedural Error outages is significantly lower among Facility outages than it is among all other categories (other than Natural Disaster and Overload).

Table 1. Procedural and Non-Procedural Error Outages By Failure Category

Outage Type	CO Power	Tandem Switch	Local Switch	DCS	Other	CCS	Facility	Natural Disaster	Overload
NPE	37	56	91	17	8	82	430	13	9
PE	49	63	102	18	8	59	68	0	0
Total	86	119	193	35	16	141	498	13	9
PE %	57%	53%	53%	51%	50%	42%	14%	0%	0%

Figure 4 shows the distribution of PE outages across Failure Categories. Almost half (45%) of PE outages involve Switches (Local or Tandem).

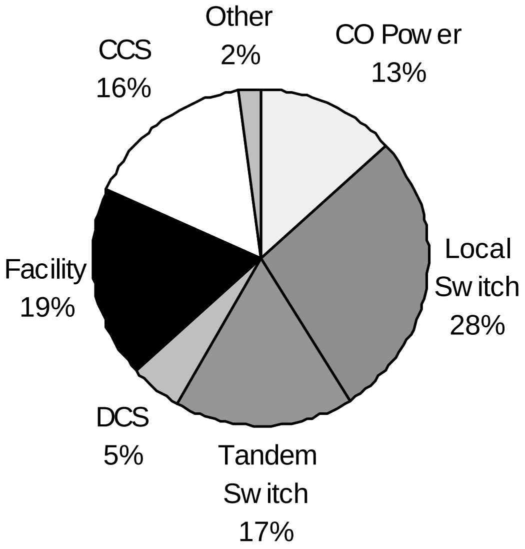

Figure 4. Distribution of Failure Categories for PE Outages

As shown in Figure 5, Translation problems account for the majority (52%) of Tandem Switch PE outages. Hardware and Translations are equally notable subcategories for Local Switch PE outages. A chi-square test indicates that these differences in subcategory distributions are not statistically significant. The following results were found for other Failure Categories:

- *Facility*: Different forms of cable cuts or damage accounted for 37% of Facility PE outages. 41% involved cable electronics while 7% involved splices or connectors.

- *CCS*: Most (76%) of the CCS PE outages had the Isolation Failure Subcategory. STP and Link(set)s accounted for 14% and 5% respectively.
- *CO Power*: Over half were located at DC Plant (35%) and DC Distribution (24%). A relatively large fraction (22%) had the other subcategory.
- *DCS*: Of the 18 DCS PE outages, 8 were Hardware and 5 were Software.

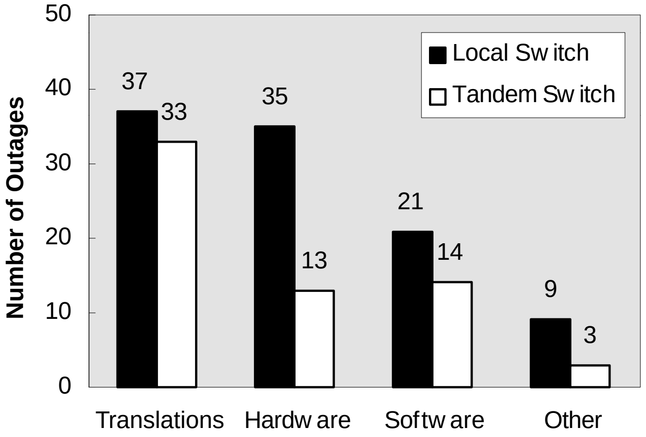

Figure 5. Failure Subcategory Distributions for PE Outages of Switches

Geographic Location of Failure

The failures causing 354 PE outages were identified as occurring in a specific state in the United States. The state with the highest number of PE outages is California (56). Based on 1995-96 FCC data on presubscribed lines by state, this number is higher than expected (44.5) with an upper tail *p*-value of .04 (barely not "statistically significant" by our assumed .05 two-tailed level of significance). Texas had the second greatest number of PE outages (34); based on its share of lines, the state was expected to have only 22.3 PE outages; this difference is statistically significant (one-tailed *p*-value of .010). Other states of note with higher than expected PE outages:

- Colorado: Actual/Expected 11/5.3 (statistically significant one-tailed *p*-value of .018),
- Arizona: Actual/Expected 10/5.3 (one-tailed *p*-value of .043),
- North Dakota: Actual/Expected 3/0.8 (one-tailed *p*-value of .050).

States with noteworthy lower than expected PE outage frequencies were:

- Kentucky: Actual/Expected 0/4.4 (statistically significant one-tailed *p*-value of .012)
- Tennessee: Actual/Expected 2/6.9 (one-tailed *p*-value of .031) and
- Alabama: Actual/Expected 1/5.0 (one-tailed *p*-value of .038).

Time of Day

NPE and PE outages have a statistically significant difference in frequency per time of day. Figure 6 shows the outage frequency in each hour with an indication of the trend. The plot indicates that PE and NPE outage frequencies each have two peaks: near noon and near midnight. The NPE peak at noon is the most pronounced.

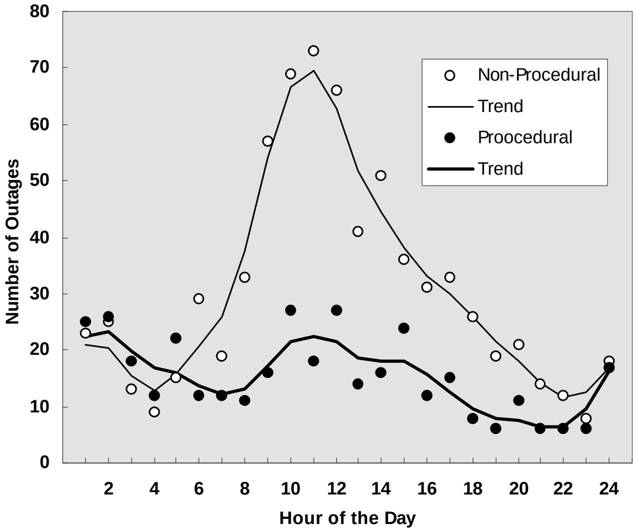

Figure 6. Procedural and Non-Procedural Outage Counts as a Function of Time of Day

Figure 7 shows the percentage of PE outages throughout the day. The percentages were calculated by taking the number of PE outages that occurred in each hour and dividing by the total number of outages that occurred in that hour. The percentage ranges from a low near 20% during the daytime hours to a high near 60% in the early morning hours.

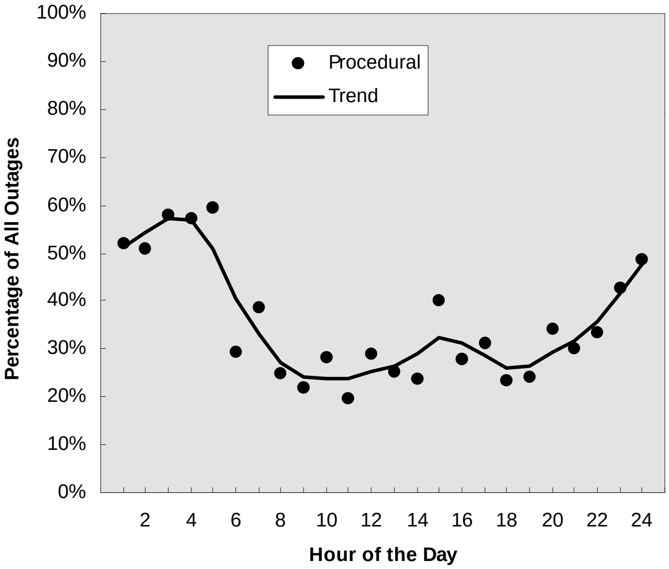

Figure 7. Procedural Error Outage Percentage as a Function of Time of Day

Frequency by Time

Figure 8 presents the total number of PE and NPE outages reported in each Report Year.[1] Note that the Report Year 6 total was estimated based on the totals from 3Q98 and 4Q98. Report Year 4, Report Year 5, and Report Year 6 (i.e., 3Q98 and 4Q98) have statistically significant higher PE outage frequencies than the Baseline Year.

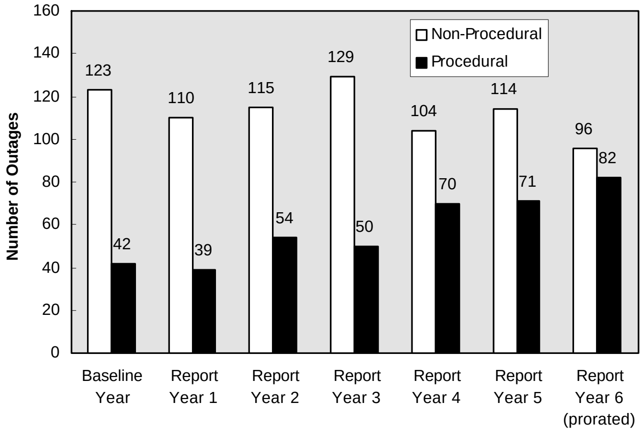

Figure 8. Procedural Error and Non-Procedural Error Outages by Report Year

Figure 9 is a quarterly control chart for Procedural outage frequency with control limits derived from the Baseline Year PE data. Every quarter (except one) since 3Q94 has had a PE outage frequency greater than the Baseline Year average. Six quarters since 3Q96 have had PE outage frequencies in the Yellow region (i.e., probability of 0.025 at the Baseline Year rate) or the Red region (i.e., probability of 0.005 at the Baseline Year rate).

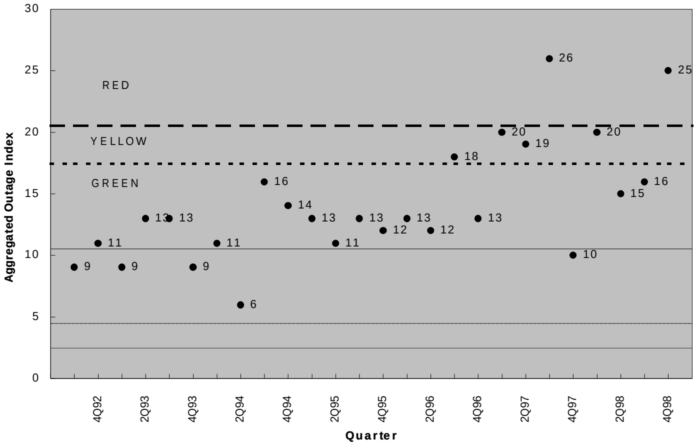

Figure 9. Procedural Error Outage Frequency Control Chart

Figure 10 plots the number of NPE and PE outages for each quarter from 3Q92 through 4Q98. The frequency of PE outages has been increasing at the statistically significant rate of 3% per quarter. The frequency of NPE outages shows a slight decline that is not statistically significant. 4Q98 is the first quarter in which PE outages exceeded NPE outages.

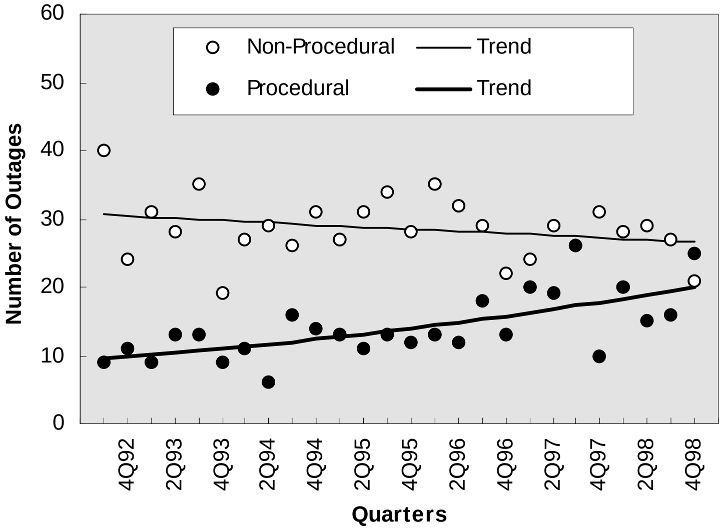

Figure 10. PE and NPE Outage Frequency by Quarter

Figure 11 plots the PE percentage of all outages for each quarter. A logistic regression (shown by the Trend line) indicated that the increasing PE share of outages is statistically significant.

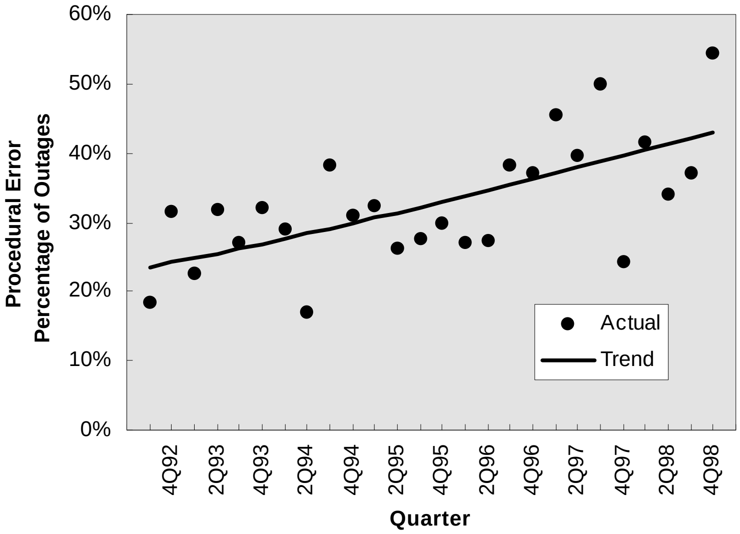

Figure 11. PE Percentage of Outage Frequency by Quarter

Outage Index

In order to measure the impact of FCC-reportable service outages, ATIS/NRSC employs the Outage Index developed by the Standards T1A1.2 Working Group. PE outages have accounted for 28% of the aggregated outage index from July 1, 1992 through December 31, 1998. This percentage is lower than the PE share (33%) of all outage reports. Thus, PE outages have had a lower mean outage index (8.1) than NPE outages (10.1). This difference is statistically significant.

Figure 12 presents the aggregated outage indexes of PE and NPE outages for each Report Year. Note that the Report Year 6 total was estimated based on the totals from 3Q98 and 4Q98. Every Report Year after the Baseline Year (July 1, 1992 - June 30, 1993) has had a higher aggregated outage index attributable to procedural errors than in the Baseline Year.

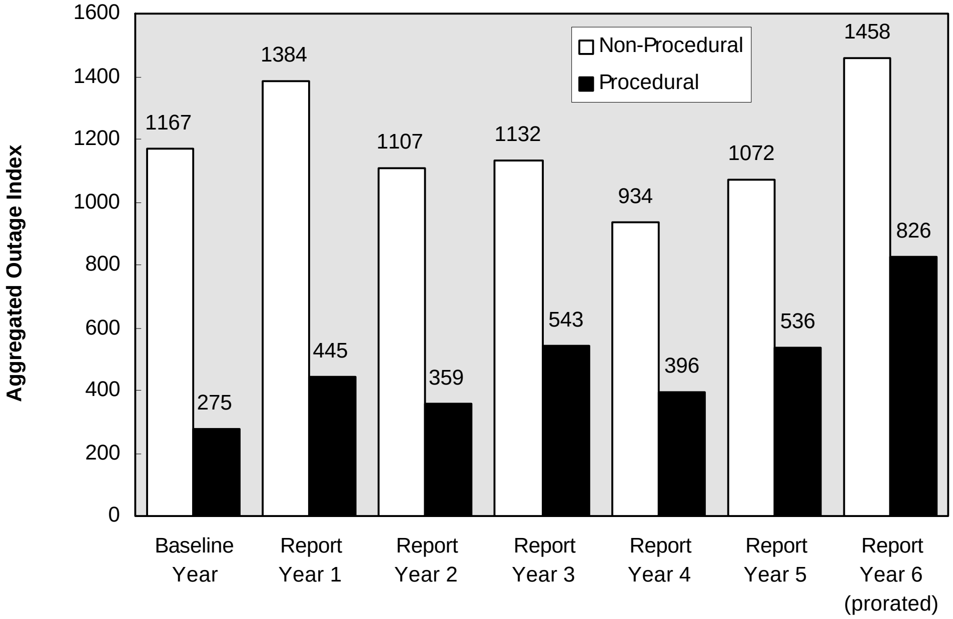

Figure 12. Procedural Error and Non-Procedural Error Aggregated Outage Indexes by Report Year

Figure 13 is a quarterly control chart for Procedural aggregated outage index with control limits derived from the Baseline Year PE data. Three quarters (including the two most recent ones) had an aggregated outage index in the Yellow region. Every quarter since 3Q94 (except 3Q96 and 4Q96) has had a PE aggregated outage index greater than the Baseline Year average. With eight consecutive quarters above the Baseline Year average, this current increase above the Baseline Year level is statistically significant.

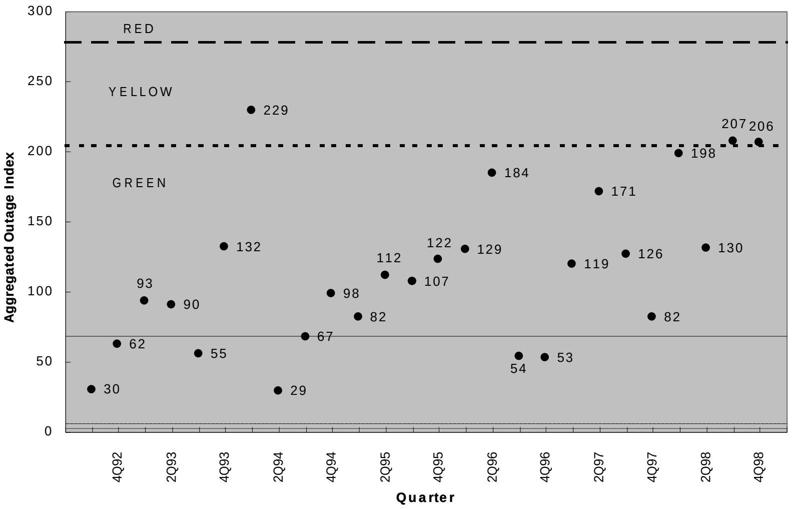

Figure 13. Procedural Error Aggregated Outage Index Control Chart

Figure 14 plots the aggregated outage indexes for PE and NPE outages by quarter. The trend lines in the graph provide indications similar to those for outage frequency (i.e., PE aggregated outage index per quarter is increasing while that of NPE outages is decreasing). Only the trend for PE quarterly aggregated outage index is statistically significant, increasing 3.9 per quarter.

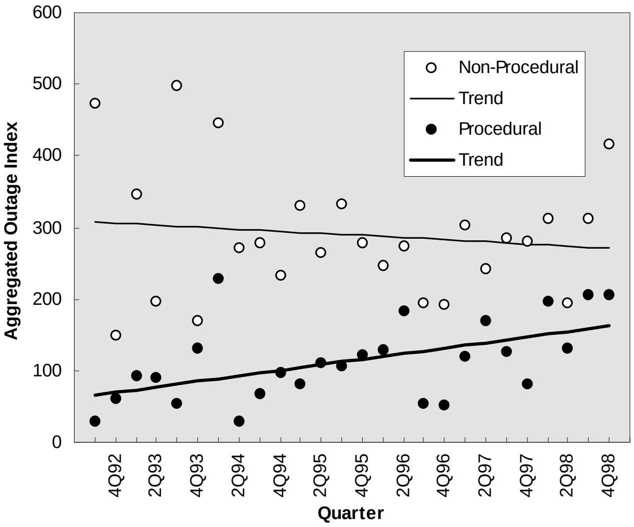

Figure 14. PE and NPE Aggregated Outage Index by Quarter

Figure 15 plots the percentage of aggregated outage index in each quarter that is attributable to PE outages. The trend (based on a logic transformation) is statistically significant. The trend indicates that while PE outages have a minority share of the aggregated outage index, this share has been increasing from about 18% to about 37%.

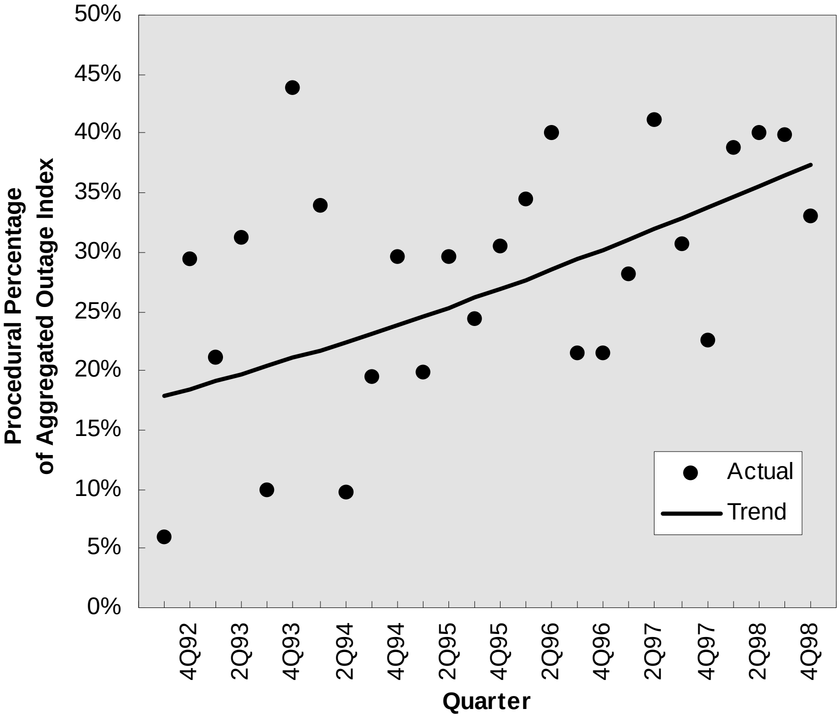

Figure 15. PE Percentage of Aggregated Outage Index by Quarter

Table 2 presents the average aggregated outage index per quarter for each of the four quarters in a year. The table shows that the percentage from PE outages is near the 33% average in every quarter except the Third Quarter where it drops to 21%. The differences in average aggregated outage index between quarters are statistically significant for NPE outages, but not for PE outages.

Table 2. Average Aggregated Outage Index per Quarter
(July 1, 1992 through December 31, 1998)

Quarter	NPE	PE	All	PE%
1	331	142	472	30%
2	241	119	360	33%
3	339	92	432	21%
4	246	108	354	30%

Customers Potentially Affected

Table 3 provides the mean and median customers affected by PE and NPE outages. The median number of customers affected is less for PE outages than for NPE outages; this difference is statistically significant.

Table 3. Thousands of Customers Potentially Affected by Service Outages
(July 1, 1992 through December 31, 1998)

Outage Type	Mean	Median	90th Percentile
NPE	124	58	236
PE	138	50	229

Table 4 presents similar summary information broken down by failure category. The significance level in the bottom row is the result of a non-parametric Wilcoxon test comparing the NPE and PE means within each failure category. Among Facility and CO Power outages, PE outages potentially affect fewer customers than NPE outages do; the differences within these two failure categories are statistically significant.

Table 4. Thousands of Customers Potentially Affected by Service Outages
for Each Failure Category (July 1, 1992 through December 31, 1998)

Outage	DCS		Tandem Switch		Facility		CO Power		CCS		Local Switch	
Type	Mean	Median	Mean	Median	Mean	Median	Mean	Median	Mean	Median	Mean	Median
NPE	256	77	211	75	108	69	194	55	114	46	76	45
PE	253	121	271	88	130	54	78	46	167	48	67	43
Sig. Level	.29		.67		.03		.02		.42		.96	

Duration

Table 5 provides the mean and median duration of PE and NPE outages. The average duration for PE outages is less than that of NPE outages; this difference is statistically significant.

Table 5. Duration of Service Outage (Minutes)
(July 1, 1992 through December 31, 1998)

Outage Type	Mean	Median	90th Percentile
NPE	512	210	712
PE	206	111	484

In Table 6, this analysis is performed for each failure category. PE outages have significantly shorter duration in the Facility failure category while PE outages are significantly longer in Tandem Switch outages. While PE outages appear to be shorter in the remaining categories, the differences are not statistically significant.

Table 6. Duration of Service Outage (Minutes)
for Each Failure Category (July 1, 1992 through December 31, 1998)

Outage	DCS		Tandem Switch		Facility		CO Power		CCS		Local Switch	
Type	Mean	Median	Mean	Median	Mean	Median	Mean	Median	Mean	Median	Mean	Median
NPE	194	141	237	109	481	304	240	189	149	83	143	80
PE	150	123	309	160	271	152	223	135	99	70	157	68
Sig. Level	.56		.05		<.0001		.25		.22		.48	

Future Work

This paper provides a broad survey of important statistical characteristics of Procedural Error outages reported to the FCC. It has been provided as input to the NRSC Procedural Errors Team. The goals and priorities of the NRSC Data Assembly and Analysis Team should guide the types of analysis for future work.

References

A Technical Report on Enhanced Analysis of FCC-Reportable Service Outage Data, T1 Technical Report No. 42, August 1995.

Bennett, J., FCC-Reportable Service Outages (3Q92 – 4Q98) with Procedural Errors as Root Cause, Telcordia White Paper, February 23, 1998.

FCC Report and Order 92-58, CC Docket No. 91-273 (7 FCC Record 2010), Federal Communications Commission, Washington, DC, adopted February 13, 1992, released February 27, 1992.

FCC Report and Order 94-189, CC Docket No. 91-273 (9 FCC Record 3911), Federal Communications Commission, Washington, DC, adopted July 14, 1994, released August 1, 1994.

Makris, S., Analysis of FCC-Reportable Outages: Procedural Errors (7/1/92 - 12/31/96), presentation to the NRSC Data Assembly & Analysis Team, February 27, 1997.

Statistics of Communications Common Carriers, Federal Communications Commission, Washington, DC, 1995/1996 Edition.

APPENDIX B—UNIVERSE COMPARISONS OF LARGE AND SMALL OUTAGES

Introduction

Five member companies of NRSC submitted data sets of network outages caused by a procedural error. While all companies provided data on switch outages, only one provided data on transport outages. For this reason, subsequent analysis was restricted only to switch outages. The data sets included outages below FCC-reportable thresholds (per FCC Docket 91-273), as well as those above the thresholds. The goal of the analysis was to determine whether large outages (on the order of FCC-reportable outages) provided a useful representation of the distribution of root causes among procedural error outages of all sizes. Following the lead of FCC-reportable criteria, four criteria of "large" were used:

Study Approach

1. <u>Duration ≥ 30 minutes</u>
   Outages were placed into two groups, one in which the duration of the outage was less than 30 minutes and one in which the duration of the outage was greater than or equal to 30 minutes.
2. <u>Lines ≥ 30,000</u>
   Outages were placed into two groups, one in which the "equivalent lines" affected by the outage were less than 30,000 and one in which the equivalent lines affected by the outage were greater than or equal to 30,000. The following rules were used to define "equivalent lines" for the purposes of this criterion:
   a. If an outage had data on equivalent lines affected, that number was used.
   b. If an outage had data only on lines affected, that number was used.
   c. If an outage had data only on trunks affected, the number of equivalent lines was defined as 10 times the number of trunks.
   d. If an outage had data on lines and trunks affected, the number of equivalent lines was defined as the maximum of the number of lines or 10 times the number of trunks.
3. <u>Lines ≥ 30,000 AND Duration ≥ 30 minutes</u>
   This criterion is similar to the FCC reporting criterion. Outages were placed into two groups; one in which the equivalent lines affected by the outage were greater than or equal to 30,000 and duration of the outage was greater than or equal to 30 minutes, and one in which the equivalent lines were less than 30,000 or duration was less than 30 minutes.
4. <u>Lines ≥ 30,000 OR Duration ≥ 30 minutes</u>
   Outages were placed into two groups; one in which the equivalent lines affected by the outage were greater than or equal to 30,000 or duration of the outage was greater than or equal to 30 minutes, and one in which the equivalent lines were less than 30,000 and duration was less than 30 minutes.

The less restrictive criterion of “Large” was used to obtain more substantial samples in the Large category. Table 1 summarizes the number of outages in the Large and Small groups for each company. An examination of the bottom row of Table 1 indicates that the criterion requiring both duration and lines affected to be large results in small sample sizes in the Large category for four of the five companies.

Data Analysis

Table 1. Number of Outage Reports for Each Company by Outage Size,

Using Four Different Criteria for Outage Size

Large	Company A		Company B		Company C		Company D		Company E	
Criterion	Large	Small	Large	Small	Large	Small	Large	Small	Large	Small
Lines ≥30,000	9	20	42	55	11	115	100	158	22	289
Duration ≥30 minutes	9	20	74	42	46	80	38	220	83	228
Either Threshold	16	13	86	21	55	71	123	135	99	212
Both Thresholds	2	27	30	76	2	124	15	243	6	305

Each company had its own set of cause categories in which the outages were classified. For this reason, each company was analyzed separately. Table 2 summarizes the results for each company individually. Only those categories in which 10 or more outage reports were reported are given; the remaining reports were placed in the “Other” category. In the case of Company A, the reports were grouped into two categories—root causes with a vendor responsibility and root causes with a carrier responsibility.

Table 2. Distribution of Outage Reports by Cause

Company A		Company B		Company C		Company D		Company E	
Cause	%	Cause	%	Cause	%	Cause	%	Cause	%
Carrier	66%	Work Error - Operational	50%	Customer	43%	Procedures	63%	Installer Error	35%
Vendor	34%	Work Error - Data Entry	22%	Installation	30%	Human Engineering	16%	Tech Error	27%
		Work Error - Hardware	15%	Other	27%	Training	6%	Customer Install	6%
		Other	13%			Unexpected Failure	4%	Ad Hoc Activities	5%
						Other	11%	Inst Manual	4%
								Patch	4%
								Parm Or Table	3%
								Other	15%
Outages	29	Outages	116	Outages	126	Outages	258	Outages	311

Statistical tests for significant differences in cause distributions between Small and Large outages were performed. For these tests, the definition of Large based on either threshold exceeded was the primary definition used. Statistically significant differences in the distributions were found for three of the five companies.

- Company B: Data Entry Work Errors were a higher percentage (28% versus 5%) and Hardware Work Errors were a lower percentage (7% versus 38%) among Large outages than among Small outages.
- Company C: Customer Errors were a higher percentage (56% versus 32%) and Vendor Installation Errors were a lower percentage (20% versus 38%) among Large outages than among Small outages.
- Company E: Parameter/Table Errors were a higher percentage (9% versus 0%) and Vendor Installation Errors were a lower percentage (26% versus 40%) among Large outages than among Small outages.

Across these three companies, indications of two commonalities can be noted:

- Installation errors produce smaller outages.
- Errors involving data, tables, or parameters produce larger outages.

These differences have a relatively small effect on prioritizing causes. For all three companies, the two largest causes of outages—which together accounted for a majority of outages in all three companies—were the same among Large outages as among all outages. For Company E, the two largest causes reverse positions using the definition of Large outages; however, since the percentages are relatively close, this is a minor difference. For Company B, the two largest causes reverse positions if the Both Thresholds definition of Large outage is used instead of the Either Threshold definition.

Summary

In summary, while some differences do exist between the causes of large and small outages, they do not appear to be of such a magnitude as to influence prioritization of solutions to procedural errors. Large outages appear to provide a reasonably representative sample for this purpose. Nevertheless, the study provides some indication that procedural errors of a more centralized nature (e.g., data errors) have a greater chance of producing large outages than those of a localized nature (e.g., hardware work errors). In addition, the disparity in root cause categories used by different companies indicates that a review of current classification of procedural error root causes may be productive.

APPENDIX C—ROOT CAUSE ANALYSIS (RCA)

Introduction

RCA is a new mindset. It is a cultural change that is often difficult to grasp initially. We have all been trained—as far back as grade school—to solve problems or to find the cause of a problem. We generally were not trained to go back and find out what caused the cause.

True RCA not only challenges us to ask what caused the cause but to do this several times. The rule of thumb is to do this five times. This is referred to as the “5 Why's” (although in reality “Why” should be replaced or supplemented by asking how, when, and where, as well).

RCA is a methodology that allows detailed and progressive investigation into major “single-incident” problems/outages or recurring problems. In today's technology, RCA rarely involves individual hardware, software, or procedural issues; generally two or more types of issues are closely linked and require detailed investigation. Many times, the immediate preventive or pro-active troubleshooting techniques and fixes are misinterpreted as being a root cause analysis. While troubleshooting and quick fix may turn out to be a true root cause, it is usually only an analysis of what happened. Root cause should identify how, why, where and when the trouble manifested itself.

Root cause IS NOT about assigning blame! It should be done objectively, with a desire to prevent a similar condition from occurring again. The true test of the identity of a root cause is that once corrected this problem can not recur.

The sample template that follows is used by one of the nation’s telecommunications companies. If adopted, it can provide consistency in an organization’s approach to data capture.

Sample Template

RNSA-RCA-9-

ROOT CAUSE ANALYSIS
FOR

(A) Summary:

Date of Incident:	Time of Incident:
Nature of Failure:	Equipment Type:
CLLI & Release:	FCC Reportable under Docket 91-273:
Total Facility Size:	Outage Type:
Subscriber Reports:	Incident Duration:
No. of Affected lines/circuits/etc.:	Root Cause Category:
Blocked Call Impact on Network:	Associated Reports:

(B) LESSONS LEARNED:

(C) IMPACT ON SERVICE:

(D) BACKGROUND OF EVENT:

(E) How Did Network LOB Become Aware:

(F) Chronological Sequence of Events:

(G) Quick Fix Actions:

(H) Other Contributing Factors:

(I) Factors Contributing to the Duration of the Incident:

(J) Root Cause Analysis:

Triggering Event:

Affected Element:

Outage Cause:

Root Cause Findings:

(K) Network Reliability Council "Best Practices" that relate to this incident:

(L) Describe how the NRC Recommendations could have prevented this outage:

(M) Additional Comments or Recommendations:

(N) Corrective Action Items:

Action Item Description/Requirement:	Dates:	Accountable Team Member:
1 Local Regional	Due Date:	
	Completed:	
2 Local Regional	Due Date:	
	Completed:	
3 Local Regional	Due Date:	
	Completed:	
4 Local Regional	Due Date:	
	Completed:	
5 Local Regional	Due Date:	
	Completed:	

(O) PONC:

(P) Costs to be Recovered:

(Q) Date and Location of Root Cause Analysis Meeting:

# A = Attended I = Invited R = Required (ex. I,A,R)

(Q) Analysis Team:
***** Designates Chairperson

#	Name:	Organization:	Tel #:	Fax #:
*				

This RCA report is considered to be a final analysis of the outage and the underlying circumstances and as such, is not scheduled to be revised or updated unless further investigation yields substantially or significantly new data. All progress and status updates for the Action Items shall be directed to the undersigned Chairperson for review, tracking and implementation follow-up.

Chairperson: Signature:____________________________ Date:___________________

Mgr. Mtce Engr. Signature:____________________________ Date:___________________
Anyone needing to know the current status of an Action Item may contact the Regional Operations-Network Service Assurance Center: 8 a.m. to 5p.m.

APPENDIX D—63.100 NOTIFICATION OF SERVICE OUTAGE

Recent studies demonstrate that procedural errors represent an average of 33% of FCC-reported service outages as defined in Part 63.100 of the FCC's rules.

CHAPTER I – FEDERAL COMMUNICATIONS COMMISSION

PART 63 – EXTENSION OF LINES AND DISCONTINUANCE, REDUCTION, OUTAGE AND IMPAIRMENT OF AGENCY STATUS

Sec. 63.100 Notification of Service Outage

(a) As used in this section:

(1) Outage is defined as a significant degradation in the ability of a customer to establish and maintain a channel of communications as a result of failure or degradation in the performance of a carrier's network.

(2) Customer is defined as a user purchasing telecommunications service from a common carrier.

(3) Special offices and facilities are defined as major airports, major military installations, key government facilities, and nuclear power plants. 911 special facilities are addressed separately in paragraph (a) (4) of this section.

(4) An outage which potentially affects a 911 special facility is defined as a significant service degradation, switch or transport, where rerouting to the same or an alternative answering location was not implemented, and involves one or more of the following situations:

(I) Isolation of one or more Public Service Answering Points (PSAPs) for 24 hours or more, if the isolated PSAPs collectively serve less than 30,000 or more access lines, based on the carrier's database of lines served by each PSAP; or

(ii) Loss of call processing capabilities in the E911 tandem(s), for 30 minutes or more, regardless of the number of customers affected; or

(iii) Isolation of one or more PSAP(s), for 30 or more minutes, if the isolated PSAPs collectively serve 30,000 or more access lines, based on the carrier's database of lines served by each PSAP; or

(iv) Isolation of an end office switch or host/remote cluster, for 30 minutes or more, if the switches collectively serve, 30,000 or more access lines.

(5) Major airports are defined as those airports described by the Federal Aviation Administration as large or medium hubs. The member agencies of the National Communications System (NCS) will determine which of their locations are "major military installations" and "key government facilities."

(6) An outage which "potentially affects" a major airport is defined as an outage that disrupts 50% or more of the air traffic control links or other FAA communications links

to any major airport, any outage that has caused an Air Route Traffic Control Center (ARTCC) or major airport to lose it radar, any ARTCC or major airport outage that has received any media attention of which the carrier's reporting personnel are aware, any outage that causes a loss of both primary and backup facilities at any ARTCC or major airport, and any outage to an ARTCC or major airport that is deemed important by the FAA as indicated by FAA inquiry to the carrier management personnel.

(7) A mission-affecting outage is defined as an outage that is deemed critical to national security/emergency preparedness (NS/EP) operations of the affected facility by the National Communications System member agency operating the affected facility.

(b) Any local exchange or interexchange common carrier or competitive access provider that operates transmission or switching facilities and provides access service or interstate or international telecommunications service, that experiences an outage which potentially affects 50,000 or more of its customers on any facilities which it owns, operates or leases, must notify the Commission if such outage continues for 30 or more minutes. Satellite carriers and cellular carriers are exempt from this reporting requirement. Notification must be served on the Commission's Duty Officer, on duty 24 hours a day in the FCC's Communications and Crisis Management Center in Washington, DC. Notification may be served on the Commission's Watch Officer on duty at the FCC's Columbia Operations Center in Columbia, MD, or at such other facility designated by the Commission by regulation or (at the time of the emergency) by public announcement only if there is a telephone outage or similar emergency in Washington, DC. The notification must be by facsimile or other record means delivered within 120 minutes of the carrier's first knowledge that the service outage potentially affects 50,000 or more customers, if the outage continues for 30 or more minutes. Notification shall identify a contact person who can provide further information, the telephone number at which the contact person can be reached, and what information is known at the time about the service outage including: the date and estimated time (local time at the location of the outage) of commencement of the outage; the geographic area affected; the estimated number of customers affected; the types of services affected (e.g. interexchange, local, cellular); the duration of the outage, i.e. time elapsed from the estimated commencement of the outage until restoration of full service; the estimated number of blocked calls during the outage; the apparent or known cause of the incident, including the name and type of equipment involved and the specific part of the network affected; methods used to restore service; and the steps taken to prevent recurrences of the outage. When specifying the types of services affected by any reportable outage, carriers must indicate when 911 service was disrupted and rerouting to alternative answering locations was not implemented. The report shall be captioned Initial Service Disruption Report. Lack of any of the above information shall not delay the filing of this report. Not later than thirty days after the outage, the carrier shall file with the Chief, Office of Engineering and Technology, a Final Service Disruption Report providing all available information on the service outage, including any information not contained in its Initial Service Disruption Report and detailing specifically the root cause of the outage and listing and evaluating the effectiveness and application in the immediate case of any best practices or industry standards identified by the Network Reliability Council to eliminate or ameliorate outages of the reported type.

(c) Any local exchange or interexchange common carrier or competitive access provider that operates transmission or switching facilities and provides access service or interstate or international telecommunications service, that experiences an outage which potentially affects at least 30,000 and less than 50,000 of its customers on any facilities which it owns, operates or leases, must notify the Commission if such outage continues for 30 or more minutes. Satellite carriers and cellular carriers are exempt from this reporting requirement. Notification must be served on the Commission's Duty Officer, on duty 24 hours a day in the FCC's Communications and Crisis Management Center in Washington, DC. Notification may be served on the Commission's Watch Officer on duty at the FCC's Columbia Operations Center in Columbia, MD, or at such other facility designated by the Commission by regulation or (at the time of the emergency) by public announcement only if there is a telephone outage or similar emergency in Washington, DC. The notification must be by facsimile or other record means delivered within 3 days of the carrier's first knowledge that the service outage potentially affects at least 30,000 but less than 50,000 customers, if the outage continues for 30 or more minutes. Notification shall identify the carrier and a contact person who can provide further information, the telephone number at which the contact person can be reached, and what information is known at the time about the service outage including: the date and estimated time (local time at the location of the outage) of commencement of the outage; the geographic area affected; the estimated number of customers affected; the types of services affected (e.g. interexchange, local, cellular); the duration of the outage, i.e. time elapsed from the estimated commencement of the outage until restoration of full service; the estimated number of blocked calls during the outage; the apparent or known cause of the incident, including the name and type of equipment involved and the specific part of the network affected; methods used to restore service; and the steps taken to prevent recurrences of the outage. When specifying the types of services affected by any reportable outage, carriers must indicate when 911 service was disrupted and rerouting to alternative answering locations was not implemented. The report shall be captioned Initial Service Disruption Report. Lack of any of the above information shall not delay the filing of this report. Not later than thirty days after the outage, the carrier shall file with the Chief, Office of Engineering and Technology, a Final Service Disruption Report providing all available information on the service outage, including any information not contained in its Initial Service Disruption Report and detailing specifically the root cause of the outage and listing and evaluating the effectiveness and application in the immediate case of any best practices or industry standards identified by the Network Reliability Council to eliminate or ameliorate outages of the reported type.

(d) Any local exchange or interexchange carrier or competitive access provider that operates transmission or switching facilities and provides access service or interstate or international telecommunications service that experiences a fire-related incident in any facilities which it owns, operates or leases that impacts 1000 or more service lines must notify the Commission if the incident continues for a period of 30 minutes or longer. Satellite carriers and cellular carriers are exempt from this reporting requirement. Notification must be served on the Commission's Duty Officer, on duty 24 hours a day in the FCC's Communications and Crisis Management Center in Washington, DC. Notification may be served on the Commission's Watch Officer on duty in the FCC's Columbia Operations Center in Columbia, MD, or at such other facility designated by the Commission by regulation or (at the time of the emergency) by public announcement only if there is a telephone outage or similar emergency in Washington, DC. The notification must be by facsimile or other recorded means delivered within 3 days of the carrier's first knowledge that the incident is fire-related, impacting 1000 or more lines for thirty or more minutes. Notification shall identify the carrier and a contact person who can provide further information, the telephone number at which the contact person can be reached, and what information is known at the time about the service outage including: the date and estimated time (local time at the location of the outage) of commencement of the outage; the geographic area affected; the estimated number of customers affected; the types of services affected (e.g. interexchange, local cellular); the duration of the outage, i.e. time elapsed from the estimated commencement of the outage until restoration of full service; the estimated number of blocked calls during the outage; the apparent or known cause of the incident, including the name and type of equipment involved and the specific part of the network affected; methods used to restore service; and the steps taken to prevent recurrences of the outage. When specifying the types of services affected by any reportable outage, carriers must indicate when 911 service was disrupted and rerouting to alternative answering locations was not implemented. The report shall be captioned Initial Service Disruption Report. Lack of any of the above information shall not delay the filing of this report. Not later than thirty days after the outage, the carrier shall file with the Chief, Office of Engineering and Technology, a Final Service Disruption Report providing all available information on the service outage, including any information not contained in its Initial Service Disruption Report and detailing specifically the root cause of the outage and listing and evaluating the effectiveness and application in the immediate case of any best practices or industry standards identified by the Network Reliability Council to eliminate or ameliorate outages of the reported type.

(e) Any local exchange or interexchange common carrier or competitive access provider that operates transmission or switching facilities and provides access service or interstate or international telecommunications service, that experiences an outage on any facilities which it owns, operates or leases which potentially affects special offices and facilities must notify the Commission if such outage continues for 30 or more minutes regardless of the number of customers affected. Satellite carriers and cellular carriers are exempt from this reporting requirement. Notification must be served on the Commission's Duty Officer, on duty 24 hours a day in the FCC's Communications and Crisis Management Center in Washington, DC. Notification may be served on the Commission's Watch Officer on duty at the Columbia Operations Center in Columbia, MD, or at such other facility designated by the Commission by regulation or (at the time of the emergency) by public announcement only if there is a telephone outage or similar emergency in Washington, DC. The notification must be by facsimile or other record means delivered within 120 minutes of the carrier's first knowledge that the service outage potentially affects a special facility, if the outage continues for 30 or more minutes. Notification shall identify a contact person who can provide further information, the telephone number at which the contact person can be reached, and what information is known at the time about the service outage including: the date and estimated time (local time at the location of the outage) of commencement of the outage; the geographic area affected; the estimated number of customers affected; the types of services affected (e.g. 911 emergency services, major airports); the duration of the outage, i.e. time elapsed from the estimated commencement of the outage until restoration of full service; the estimated number of blocked calls during the outage; the apparent or known cause of the incident, including the name and type of equipment involved and the specific part of the network affected; methods used to restore service; and the steps taken to prevent recurrences of the outage. When specifying the types of services affected by any reportable outage, carriers must indicate when 911 service was disrupted and rerouting to alternative answering locations was not implemented. The report shall be captioned Initial Service Disruption Report. Lack of any of the above information shall not delay the filing of this report. Not later than thirty days after the outage, the carrier shall file with the Chief, Office of Engineering and Technology, a Final Service Disruption Report providing all available information on the service outage, including any information not contained in its Initial Service Disruption Report and detailing specifically the root cause of the outage and listing and evaluating the effectiveness and application in the immediate case of any best practices or industry standards identified by the Network Reliability Council to eliminate or ameliorate outages of the reported type. Under this rule, carriers are not required to report outages affecting nuclear power plants, major military installations and key government facilities to the Commission. Report at these facilities will be made according to the following procedures:

(1) When there is a mission-affecting outage, the affected facility will report the outage to the National Communications System (NCS) and call the service provider in order to determine if the outage is expected to last 30 minutes. If the outage is not expected to, and does not, last 30 minutes, it will not be reported to the FCC. If it is expected to last 30 minutes or does last 30 minutes, the NCS, on the advice of the affected special facility, will either:

(i) Forward a report of the outage to the Commission, supplying the information for initial reports affecting special facilities specified in this section of the Commission's Rules;

(ii) Forward a report of the outage to the Commission, designating the outage as one affecting "special facilities," but reporting it at a level of detail that precludes identification of the particular facility involved; or

(iii) Hold the report at the NCS due to the critical nature of the application.

(2) If there is to be a report to the Commission, a written or oral report will be given by the NCS within 120 minutes of an outage to the Commission's Duty Officer, on duty 24 hours a day in the FCC's Communications and Crisis Management Center in Washington, DC. Notification may be served on the Commission's Watch Officer on duty at the FCC's Columbia Operations Center in Columbia, MD, or at such other facility designated by the Commission by regulation or (at the time of the emergency) by public announcement only if there is a telephone outage or similar emergency in Washington, DC. If the report is oral, it is to be followed by a written report the next business day. Those carriers whose service failures are in any way responsible for the outage must consult with NCS upon its request for information.

(3) If there is to be a report to the Commission, the service provider will provide a written report to the NCS, supplying the information for final reports for special facilities required by this section of the Commission's rules. The service provider's final report to the NCS will be filed within 28 days after the outage, allowing the NCS to then file the report with the Commission within 30 days after the outage. If the outage is reportable as described in paragraph (e) (2) of this section, and the NCS determines that the final report can be presented to the Commission without jeopardizing matters of national security or emergency preparedness, the NCS will forward the report as provided in either paragraphs (e) (1) (i) or (e) (1) (ii) of this section to the Commission.

(f) If an outage is determined to have affected a 911 facility so as to be reportable as a special facilities outage, the carrier whose duty it is to report the outage to the FCC shall as soon as possible by telephone or other electronic means notify any official who has been designated by the management of the affected 911 facility as the official to be contacted by the carrier in case of a telecommunications outage at that facility. The carrier shall convey all available information to the designated official that will be useful to the management of the affected facility in mitigating the affects of the outage on callers to that facility.

(g) In the case of LEC end offices, carriers will use the number of lines terminating at the office for determining whether the criteria for reporting an outage has been reached. In the case of IXC or LEC tandem facilities, carriers must, if technically possible, use real-time blocked calls to determine whether criteria for reporting an outage have been reached. Carriers must report IXC and LEC tandem outages where more than 150,000 calls are blocked during a period of 30 or more minutes for purposes of complying with the required 50,000 potentially affected customers threshold and must report such outages where more than 90,000 calls are blocked during a period of 30 or more minutes for purposes of complying with the 30,000 potentially affected customers threshold. Carriers may use historical data to estimate blocked calls when required real-time blocked call counts are not possible. When using historical data, carriers must report incidents where more than 50,000 calls are blocked during a period of 30 or more minutes for purposes of complying with the required 50,000 potentially affected customers threshold and must report incidents where more than 30,000 calls are blocked during a period of 30 or more minutes for purposes of complying with the 30,000 potentially affected customers threshold.

(h) (1) Any local exchange or interexchange common carrier or competitive access provider that operates transmission or switching facilities and provides access services or interstate or international telecommunications services, the experiences an outage on any facilities that it owns, operates or leases that potentially affects 911 services must notify the Commission within the applicable period shown in the chart in this paragraph (h) (1) if such outage meets one of the following conditions, as defined in paragraph (a) (4) of this section:

Condition	Lines affected	Duration
Loss of E911 Tandem capability	No limit	30 minutes or more....
Isolation of PSAP(s)	Under 30,000 access lines served.	24 hours or more…….
Isolation of PSAP(s)	50,000 or more access lines served.	30 minutes or more....
Isolation of PSAP(s)	30,000 to 50,000 access lines served.	30 minutes or more.…
Isolation of EO switch, host/remotes from 911.	50,000 or more access lines served.	30 minutes or more....
Isolation of EO switch, host/remotes from 911	30,000 to 50,000 access lines served.	30 minutes or more....

(2) Satellite carriers and cellular carriers are exempted from the reporting requirement in this paragraph (h). Notification must be served on the Commission's Duty Officer, on duty 24 hours a day in the FCC's Communicaitons and Crisis Management Center in Washington, DC. Notification may be served on the Commission's Watch Officer on duty at the Columbia Operations Center in Columbia, MD, or at such other facility designated by the Commission by regulation or (at the time of thee emergency) by public announcement only if there is a telephone outage or similar emergency in Washington, DC. The notification must be by facsimile or other record means delivered within the notification period indicated above from the time of the carrier's first knowledge that the service outage “potentially affects a 911 special facility” as described in paragraph (a) (4) of this section and summarized in the chart in paragraph (h) (1) of this section and the service outage has continued for the duration indicated in paragraph (a) (4) of this section and summarized in the chart in paragraph (h) (1) of this section. Notification shall identify a contact person who can provide further information, the telephone number at which the contact person can be reached, and the information known at the time notification is made about the service outage including: the date and estimated time (local time at the location of the outage) of commencement of the outage; the geographic area affected; the estimated number of customers affected; the types of services affected; the duration of the outage, i.e. time elapsed from the estimated commencement of the outage until restoration of full service; the estimated number of blocked calls during the outage; the apparent or known cause of the incident, including the name and type of equipment involved and the specific part of the network affected; methods used to restore service; and the steps taken to prevent recurrences of the outage. The report shall be captioned Initial Service Disruption Report. Lack of any of the information in this paragraph (h) (2) shall not delay the filing of this report. Not later than thirty days after the outage, the carrier shall file with the Chief, Office of Engineering and Technology, a Final Service Disruption Report providing all available information on

the service outage, including any information not contained in its Initial Service Disruption Report and detailing specifically the root cause of the outage and listing and evaluating the effectiveness and application in the immediate case of any best practices or industry standards identified by the Network Reliability Council to eliminate or ameliorate outages of the reported type.

Analysis Component Definitions & Examples
Direct and Root Cause

DIRECT CAUSE

Procedural - Service Provider

Failure to follow standard procedures/documentation

Work error by telco personnel; correct procedures exist and were generally available, but correct procedures/documentation were not used or were used incorrectly. Includes use of out-of-date or incorrect procedures or documentation when current or corrected documentation was generally available.

Followed procedures/documentation that were incorrect
Flawed documentation or procedures used by telco personnel include errors in vendor documentation (i.e., faulty or unclear procedures or typographical errors); errors in telco approved documentation (i.e., inadequate or inaccurate MOPs, in-house technical M&P, local drawings); use of out-of-date or incorrect procedures where current or corrected documentation were not generally available. Includes failures where standard (vendor) procedures/documentation did not exist or were not generally available.

Procedural - System Vendor

Failure to follow standard procedures/documentation
Work error by system vendor personnel; correct procedures exist and were generally available, but correct procedures/documentation were not used or were used incorrectly. Includes use of out-of-date or incorrect procedures or documentation when current or corrected documentation was generally available.

Followed procedures/documentation that were incorrect
Flawed documentation or procedures used by system vendor personnel include errors in vendor documentation (i.e., faulty or unclear procedures or typographical errors); errors in telco approved documentation (i.e., inadequate or inaccurate MOPs, in-house technical M&P, local drawings); use of out-of-date or incorrect procedures where current or corrected documentation were not generally available. Includes failures where standard (vendor) procedures or documentation did not exist or were not generally available.

Procedural - Other Vendor

Failure to follow standard procedures/documentation
Work error by other vendor personnel; correct procedures exist and were generally available, but correct procedures/documentation were not used or were used incorrectly. Includes use of out-of-date or incorrect procedures or documentation when current or corrected documentation was generally available.

Followed procedures/documentation that were incorrect
Flawed documentation or procedures used by other vendor personnel; includes errors in vendor documentation (i.e., faulty or unclear procedures or typographical errors); errors in telco approved documentation (i.e., inadequate or inaccurate MOPs, in-house technical M&P, local drawings); use of out-of-date or incorrect procedures where current or corrected documentation were not generally available. Includes failures where standard (vendor) procedures/documentation did not exist or were not generally available.

Design - Software

Faulty or defective software design; includes inadequate fault recovery strategies or failures; ineffective software fault isolation performance that triggers system re-initializations, or requires manual system recovery action for resolution. Includes insufficient software/memory capacity allocation problems.

Design - Firmware

Faulty or defective firmware design; includes inadequate fault recovery strategies or failures and ineffective fault isolation performance that require manual recovery action for resolution. Includes problems associated with incomplete firmware restoral (with or without accurate state indicators) following re-initialization.

Design - Hardware

Faulty or defective system hardware design; includes problems with component independence and single-point-of-failure problems between otherwise-duplex components, as well as physical hardware design problems (i.e., bad connectors, inadequate grounding techniques). If failure was the result of a product change notice (PCN) inappropriately delayed by the vendor or telco, or the PCN was waived by the telco, consider root cause procedural fault.

Hardware Failure

Random hardware failure not related to design but due to the inherent unreliability of the system components. If (single) hardware failure causes loss of duplicated critical systems, consider procedural or design fault. If system outage resulted from hardware failure occurring during simplex operation, consider root cause procedural fault if simplex mode resulted from inappropriate deferral of normal maintenance.

External Environment

Natural (storms, lightning)
External environmental conditions that exceed limitations documented in the vendor's technical specifications; includes direct effects of flooding, freezing, excessive temperature or rate of temperature changes; includes outages resulting from lightning or external high voltage transients introduced into the system. If bonding and grounding violations caused the entry of lightning into the system, consider root cause procedural or design fault. If water damage was the result of cable pressurization failure, consider root cause procedural fault.

Man-made (vandalism, accidents)

External man-made conditions that exceed documented (or reasonable) technical specifications; includes direct effects of water system ruptures, fires, vehicular accidents, vandalism, and explosions. If incident was the result of inadequate security precautions, consider root cause procedural fault.

Cable Damage

Cable damage caused by dig-ups, (fiber) micro-bending, rodent damage, falling trees, etc.; includes underground and aerial cable failures associated with natural and man-made external environments. If incident was the result of faulty cable installation, or of cable locating activities, consider root cause procedural fault.

Internal Environment

Water
Entry of water into the system, including roof leaks, air conditioning leaks, excessive humidity, fire suppression activities, flooding, etc. If failure was the result of environmental systems failure (e.g., AC leaks, pressurization failures), or inadequate property management (e.g., unreasonable delay in repair or roof leak, predictable flooding), consider root cause procedural fault.

Temperature
Excessive ambient temperatures, excessive rate of temperature changes. If failure was the result of environmental systems failure and a more effective response to the failure would have prevented/minimized impact of incident, consider root cause procedural fault.

Corrosion/contamination
Corrosive contamination that enters the system from surrounding environment; includes dust, airborne dirt, and smoke and/or fire suppression chemicals. If failure was the result of inadequate air filtration strategies or maintenance, consider root cause procedural or design fault.

Fire

Fires within the telecommunications facility environment; includes fires in test sets, peripheral equipment, power equipment, and building systems. If incident was the result of telco/others' activities, consider root cause procedural fault.

Traffic/System Overload

Reduced capacity due to system trouble
System overload or congestion associated with decreased system throughput or trouble-caused resource limitation; does not include system congestion associated with simple high-volume traffic conditions. If failure was the result of excessive out-of-service conditions, consider root cause procedural fault. If failure was a result of overload triggered by moderate increase in traffic/attempts, or recovery-associated activities, consider root cause design fault.

High call volume
S*ystem overload or congestion associated with high traffic or load conditions that exceed the engineered capacity of the system;* includes unexpected traffic that was the result of media-stimulated calling, natural disasters, political or social activities, or other external conditions. If failure was the result of poor event notification and planning, or network management response to media-stimulated call-in, or a result of inadequate capacity engineering, consider root cause procedural fault.

Commercial and/or Back-up Power Failure

Instances of outage directly related to failure of the external power system, or failures of telco back-up power systems; includes failures associated with commercial power, standby generators, building electrical systems, Direct Current (DC) power plants, DC distribution systems, and alarms/monitoring systems. Does not include failures of dc/dc converters or fuses embedded in switches and transmission equipment, unless the problem was caused by the power plant. If the failure was the result of inadequate/no response to (alarmed/un-alarmed) failures, consider root power alarm fault. If the failure was the result of overloaded or undersized power equipment, consider root cause procedural or design fault.

Other/Unknown

The cause of the outage cannot be determined, or the cause does not match any of the classifications above; does not include cases where outage data was insufficient or missing or where direct cause is still under investigation. When direct cause cannot be proven, it is usually still possible to determine probable cause, which is preferred to the use of “unknown.” When classifications provided do not match direct cause, approximate match is preferred to the use of “other.”

Insufficient Data

Failure report (and subsequent investigation, if any) did not provide enough information to determine direct cause of failure.

ROOT CAUSE

Procedural - Service Provider

Insufficient training
Training not available from vendor; training not available from telco; training available but not attended; training attended but inadequate or out-of-date; training adequate but insufficient application followed; training need never identified, etc.

Insufficient staffing
Unexpected conditions depleted available resources; predictable but unavoidable shortage (unreasonable demand); ineffective/inadequate roll-down or centralization arrangement; resource-intensive (new) technology outside scope/reach of existing automatic/remote administration systems, etc.

Insufficient supervision/control
Insufficient oversight or leadership; ineffective administration and/or maintenance strategies; process or communication failures; conflicting priorities, etc.

Documentation/procedures unavailable
Documentation or procedures (vendor or telco) not published; published, but not distributed; distributed, but not available on-site, etc.

Documentation/procedures unclear or incomplete
Documentation/procedures obscure/oblique; too general—insufficient specificity; too detailed/technical for practical use, etc.

Documentation/procedures out-of-date
Documentation/procedures not updated; correction/update available but not incorporated locally, etc.

Documentation/procedures unusable or impractical
Documentation/procedures unwieldy; inadequate indexing or cross-referencing; bits and pieces of information difficult to integrate; ineffective delivery vehicle, etc.

Inadequate routine maintenance/memory back-up
Failure would have been prevented/minimized by simple maintenance routines; recovery action was delayed/complicated by old or missing program/office data tapes or disks, etc.

Other

Procedural - System Vendor

Insufficient training

Training not available from vendor; training not available from telco; training available but not attended; training attended but inadequate or out-of-date; training adequate but insufficient application followed; training need never identified, etc.

Insufficient staffing
Unexpected conditions depleted available resources; predictable but unavoidable shortage (unreasonable demand); ineffective/inadequate roll-down or centralization arrangement; resource-intensive (new) technology outside scope/reach of existing automatic/remote administration systems, etc.

Insufficient supervision/control
Insufficient oversight or leadership; ineffective administration and/or maintenance strategies; process or communication failures; conflicting priorities, etc.

Documentation/procedures unavailable, unclear, incomplete
Documentation or procedures (vendor or telco) not published; published, but not distributed; distributed, but not available on-site. Documentation obscure/oblique; too general—insufficient specificity; too detailed/technical for practical use, etc.

Documentation/procedures out-of-date, unusable, impractical
Documentation/procedures not updated; correction/update available but not incorporated locally. Documentation unwieldy; inadequate indexing or cross-referencing; bits and pieces of information difficult to integrate; ineffective delivery vehicle, etc.

Ad hoc activities, outside scope of MOP
Unapproved, unauthorized work or changes in agreed-to procedures.

Other

Procedural - Other Vendor

Insufficient training
Training not available from vendor; training not available from telco; training available but not attended; training attended but inadequate or out-of-date; training adequate but insufficient application followed; training need never identified, etc.

Insufficient supervision/control
Insufficient oversight or leadership; ineffective administration and/or maintenance strategies; process or communication failures; conflicting priorities, etc.

Documentation/procedures unavailable, incomplete
Documentation or procedures (vendor or telco) not published; published, but not distributed; distributed, but not available on-site. Documentation obscure/oblique; too general - insufficient specificity; too detailed/technical for practical use, etc.

Documentation/procedures out-of-date, unusable, impractical

Documentation/procedures not updated; correction/update available but not incorporated locally. Documentation unwieldy; inadequate indexing or cross-referencing; bits and pieces of information difficult to integrate; ineffective delivery vehicle, etc.

Ad hoc activities, outside scope of MOP
Unapproved, unauthorized work or changes in agreed-to procedures.

Other

Design - Software

Inadequate defensive checks
Changes to critical or protected memory were allowed without system challenge; contradictory or ambiguous system input commands were interpreted/responded to without system challenge; failure of system to recognize or communicate query/warning in response to commands with obvious major system/network impact.

Ineffective fault recovery or re-initialization action
Simple, single-point failure resulting in total system outage; failure of system diagnostics that resulted in removal of good unit with restoral of faulty mate; failure to switch/protection switch to standby/spare/mate component(s).

Faulty software load - program date
Bad program code/instructions; logical errors/incompatibility between features/sets; software quality control failure; wrong/defective program load supplied.

Faulty software load - office date
Inaccurate/mismatched office configuration data used/applied; wrong/defective office load supplied.

Other

Design - Firmware

Insufficient software state indications
Failure to communicate or display out-of-service firmware states; failure to identify, communicate or display indolent or “sleepy” firmware states.

Ineffective fault recovery or re-initialization action
Failure to reset/restore following general/system restoral/initialization.

Other

Design - Hardware

Inadequate grounding strategy
Insufficient component grounding design; duplex components/systems sharing common power feeds/fusing.

Poor backplane or pin arrangement
Non-standard/confusing pin arrangements or pin numbering schemes; insufficient room or clearance between pins; backplane/pin crowding.

Poor card/frame mechanisms (latches, slots, jacks, etc.)
Mechanical/physical design problems.

Insufficient component/network redundancy/diversity
System or network design with unnecessary aggregation of components or features; system or network deployment with readily avoidable single-point-of-failure configurations.

Other

Hardware Failure

Processor community failure
Memory unit failure
Peripheral unit failure
Other

External Environment

Lightning/transient voltage
Component destruction or fault associated with surges and over-voltages caused by (electrical) atmospheric disturbances.

Storm - wind/trees
Component destruction or fault associated with wind-borne debris or falling trees/limbs.

Storm - water/ice
Component destruction or fault associated with fog, rain, hail, sleet, snow, or the accumulation of water/ice (flooding, collapse under weight of snow, etc.).

Vehicular accident
Component destruction or fault associated with motor vehicle (car, truck, train, etc.) collision.

Vandalism/theft
Component loss, destruction, or fault associated with larceny, mischief, or other malicious acts.

Earthquake

Component destruction or fault associated directly or indirectly with seismic shock (if damage was the result of inadequate earthquake bracing, consider hardware design fault).

Fire
Component destruction or fault associated with fire occurring/starting outside telco plant, including brush fires, pole fires, etc.

Other

Cable Damage

Digging error
Excavator error during digging (contractor provided accurate notification, route was accurately located and marked, and cable was buried at a proper depth with sufficient clearance from other sub-surface structures).

Inadequate/no notification
Excavator failed to provide any notification prior to digging, or did not accurately describe the location of the digging work to be performed. (Because of the success in avoiding dig-ups by acting upon prior notification, the lack of notification is considered to be the root cause of every dig-up in which prior notification was not provided.)

Cable unlocated
The excavator provided prior notification, but the facility owner or locating company failed to establish the presence of a cable that was then eventually damaged.

Inaccurate cable locate
The cables' presence was determined, but their locations were inaccurately identified.

Shallow cable
The cable was buried at too shallow a depth (notification was adequate, location was accurate, excavator followed standard procedures).

Other

Internal Environment

Roof/air conditioning leak
Component destruction or fault associated with water damage (direct or electrolytic) caused by roof or environmental systems leaks into/in central office environment.

Manhole/cable vault leak
Component destruction or fault associated with water entering manholes cable vaults, Containerized Environmental Vaults (CEVs), etc.

Cable pressurization failure
Component destruction of fault associated with cable damage resulting from cable pressurization failure.

Environmental system failure (heat/humidity)
Component loss or fault associated with extreme temperature, rapid temperature changes, or high humidity due to loss/malfunction of environmental control(s). If the failure was the result of inadequate/no response to (alarmed/un-alarmed) environmental failures or due to incorrect manual control of environmental systems, consider procedural fault.

Fire suppression (water, chemicals) damage
Component loss or fault associated with corrosion (electrolytic or other) caused by fire suppression activities; root cause assumes no substantial failure was directly associated with the smoke/fire that triggered suppression.

Fire, arcing, smoke damage
Component loss or fault associated with damage directly related to central office or equipment fires (open flame or smoldering), corrosive smoke emissions, or electrical arcing (whether or not ignition of surrounding material occurs).

Direct, dust contamination
Component loss or fault associated with dirt or dust, typically resulting in component overheating or loss of connectivity.

Other

Traffic/System Overload

Media-stimulated calling - insufficient notification
System/network overload/congestion directly associated with media-stimulated calling event where event sponsor/generator failed to provide adequate advance notice or provided inaccurate (underestimated) notification.

Mass calling—focused/diffuse network overload
System/network overload/congestion directly associated with unplanned, external trigger(s) causing a significant, unmanageable traffic load.

Common channel signaling network overload
CCS system/network overload associated with (true) high traffic loads congesting STP/SCP processors or CCS link network. If overload was associated with STP/SCP message handling congestion, false or reactivated link congestion, inappropriate or incorrect CCS network management message(s), protocol errors, etc., consider software design fault.

Inappropriate/insufficient Network Management (NM) control(s)
System/network overload/congestion associated with ineffective NM system/switch response, either because no effective NM control was available, system/switch response to control was inappropriate, or its implementation was flawed. If failure was related to inappropriate control strategy or execution by NM organization, consider procedural fault.

Ineffective engineering/engineering tools
System/network overload/congestion directly associated with under-engineering of the system/network due to rapidly changing network demand, or introduction of new network components and/or technologies. If failure was associated with simple under-engineering (absent changing environment), consider procedural fault.

Other

Commercial and/or Back-Up Power Failure

Inadequate/missing power alarm
System failure associated un-alarmed (or under-alarmed) power failure; alarm not provided initially due to inadequate standards or failure to implement standards; alarm/alarm system failure (broken or modified). (Because of the success in avoiding severe, battery-depletion failure where power alarms are effective and effectively responded to, system failures directly associated with power alarms should be classified as such, instead of as procedural faults.)

Insufficient response to power alarm
System failure associated response to power failure; alarm system worked but support personnel did not respond properly. Because of the success in avoiding severe, battery-depletion failure where power alarms are effective and effectively responded to, system failures directly associated with power alarms should be classified as such, instead of as procedural faults.

Lack of routine maintenance/testing
System failure that could have been avoided if periodic power system testing, maintenance and/or detailed inspection had been performed.

Overloaded/undersized power equipment
System failure attributable to insufficient sizing/design of power configuration.

Faulty power diversification

System failure directly associated with insufficient diversification among power system components, including ac rectifiers/chargers, battery power plant, dc distribution facilities, etc.

Faulty power redundance
System failure directly associated with insufficient redundancy among power system components, including ac rectifiers/chargers, battery power plan, dc distribution facilities, etc.

Inadequate site-specific power contingency plans
System failure that could have been avoided/minimized if emergency operating procedures and contingency plans had been available; outage was prolonged because of lack of site-specific data including equipment engineering data, portable engine hook-up hardware/procedures, load shedding plans, etc.

Other

Operations Support/Strategy

Insufficient surveillance capability
System failure that could have been avoided/minimized if remote operations had been able to better "see" system performance; total/comprehensive view of system not available. Surveillance system/links unavailable/out-of-service.

Inadequate control capability
System failure that could have been avoided/minimized if remote operations had been able to better control system performance; comprehensive controls only available on-site; control system/links unavailable/out-of-service.

Ineffective roll-down or hand-off activity
System failure that could have been avoided/minimized if better communication and/or process control had been in place between/among operations organizations.

Ineffective alarm threshold/display
System failure that could have been avoided/minimized if user-programmed threshold/display indicators/messages had been more effective/explicit.

Impractical trouble-correlation among Operating Systems (OS)
System failure that could have been avoided/minimized if output of disparate operations systems had been better integrated/intelligible—unreasonable output language/naming convention differences among OSs.

Other

Other/Unknown

The cause of the outage cannot be determined, or the cause does not match any of the classifications above. Does not include cases where outage data was insufficient or missing, or where root cause is still under investigation. When root cause cannot be proven, it is usually still possible to determine probable cause, which is preferred to the use of “unknown.” When classifications provided do not match root cause, approximate match is preferred to the use of “other.”

Insufficient Data

Failure report—and subsequent investigation, if any—did not provide enough information to determine direct cause of failure.

References

Chapanis, A. (1991). Human Factors Society Bulletin Number 34(11), “To communicate the human factors message, you have to know what the message is and how to communicate it.” Pgs.1-4.

GR-2914-CORE, Human Factors Requirements for Equipment to Improve Network Reliability, Issue 4 (Bellcore, December 1998).

GR-454-CORE, *Generic Requirements for Supplier-Provided Documentation* (a module of LSSGR, FR-64; OTGR, FR-439; and TSGR, FR-440), Issue 1 (Bellcore, December 1997).

AECMA, Association Europeane Des Constructeurs De Material Aerospatial

New Ways to Make Data Pay: Knowledge Management Technology Improves Analysis and Decision-Making. Christy Walker, PC Week, v15, n34, p14, August 24, 1998

Measuring the Impact of Expert Systems. Luvai Motiwalla; James Fairfield-Sonn, Journal of Business & Economic Studies, v4n2, p1-17, Fall 1998

Root Cause Analysis Template

Federal Communication Commission Rules
63.100 Notification of Service Outage

NRSC Outage Reporting

Analysis Component Definition and Examples Direct and Root Cause

APPENDIX F—COMPENDIUM OF ADDITIONAL BEST PRACTICES

These best practices were collected from several sources, with the intent of validating the good practice list. Many like comparisons can be made between the list of good practices and previously recommended best practices. Many of the recommended best practices identify the use of duplicated or diverse components or facilities. While duplication or diversification can not prevent a procedural error, it can prevent a single error from becoming an outage.

Procedural

- The definition of "Best Practices" as used in the technical papers presented in *Network Reliability: A Report to the Nation (NRC-1)* is as follows: "Best Practices" are those countermeasures (but not the only countermeasures) which go furthest in eliminating the root cause(s) of outages. None of the practices are construed to be mandatory; however, a very small number of countermeasures that are deemed by the Focus Team and concurred by the Network Reliability Steering Team (NO REST) to be especially effective countermeasures will be designated as "recommended."
- Service providers and suppliers are strongly encouraged to study and assess the applicability of all countermeasures for implementation in their companies and products, respectively. It is understood that all countermeasures, including those designated as "recommended" may not be applied universally. The following "Best Practices" recommendations are provided from *Network Reliability, A Report to the Nation – Compendium of Technical Papers*. (Also referred to as the Purple Book).

SP/SSP (Signaling Point/Service Switching Point)

- Inadvertent Maintenance of Redundant Active Units - To minimize human errors related to misidentification of active Common Channel Signaling (CCS) units as failed units requiring repair, network service providers should conduct an "Awareness Training Program" for all maintenance persons who work on SP/SSP (Signaling Point/Service Switching Point) CCS equipment. The training should emphasize the importance of end-to-end communications when maintenance is being performed. The training should also highlight the functionality, identification of active and alternated/redundant units, and the network impact of failure of redundant equipment in link processors, link interfaces, link peripheral power supplier, and other link related components.
- While not specifically switch related, use dedicated DS1 facilities for links to reduce the frequency of procedural activity on links.
- Use quad A-links (i.e., four diverse A-links to a SP).
- Crisis Management exercises should be developed in order to become well prepared in the event a disaster strikes.
- Carriers and suppliers should improve their own failure data collection and analysis procedures for better root cause analysis. Carriers and suppliers should form partnerships to jointly perform these analyses.

Software and Switching System Reliability

- Individual service providers should standardize their processes for capturing and reporting timely and complete data on switch outages. 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 for such a process is that it be easy to use for the reporting organizations and derive value back for reporting.

DCS (Digital Cross-Connect Systems)

- DCS Awareness Program patterned after Pacific Bell's and AT&T's efforts as an industry "best practice" should be developed and deployed.
- Provisioning technicians should be restricted from all commands except those that are needed for their work. Technicians should avoid any "global" command that may have the potential for significant impact.

911 (Emergency Services)

- Periodic audits should be performed to ensure that if Diverse Routing for Interoffice Facilities was provided, it is maintained.
- Alternate Public Safety Answering Point (PSAP).
- Red Tagged, Diverse Equipment – Split circuits between similar pieces of equipment and mark that equipment at the plug-in level with red tags. The red tags alert the central office personnel that the equipment is used for essential services and is to be treated with care.
- Network Management Center – These centers contain equipment and personnel that can monitor and manage the 911 network as a unique and separate entity from the rest of the network.

Power-Generator Failures

- Many standby generator systems are designed for fully automatic operation. Clear instructions should be provided for emergency manual operation of stand-by generators in case of failure of the automatic systems.
- Adequate fuel should be maintained on-site, and there should be a well-defined re-supply plan.

ACRONYMS

AECMA	Association Europeene des Constructeurs de Material Aerospatial
ARTCC	Air Route Traffic Control Center
ANSI	American National Standards Institute
ATIS	Alliance for Telecommunications Industry Solutions
BBS	Broadband Switching Systems
CCS	Common Channel Signaling
CEV	Containerized Environmental Vault
CO	Central Office
DCS	Digital Cross-Connect Systems
EOPs	Emergency Operating Procedures
FAA	Federal Aviation Association
FCC	Federal Communication Commission
FST	Facilities Solution Team
FX	Foreign Exchange
ISDN	Integrated Services Digital Network
ITU-T	International Telecommunications Union – Telecom
LATA	Local Access and Transport Area
MOP	Method of Procedure
NCS	National Communications System
NE	Network Element
NM	Network Management
NPE	Non Procedural Errors
NRC-1	The Network Reliability Council-1
NRC-2	The Network Reliability Council-2
NRIC-3	Network Reliability and Interoperability Council
NRSC	Network Reliability Steering Committee
NS/EP	National Security/Emergency Preparedness S
OPS	Office of Pipeline Safety
OS	Operating System
OSS	Operations Support System
PCN	Product Change Notice
PE	Procedural Errors
RCA	Root Cause Analysis
RQMS	Reliability and Quality Measurements for Telecommunications Systems
SP	Signaling Point
SS7	Signaling System 7
SSP	Service Switching Point
STP/SCP	Signaling Transfer Point/Signaling Control Point

TMI	Three Mile Island
VDT	Visual Display Terminals