NRIC VII

December 2005

FOCUS GROUP 1C

Analysis of the Effectiveness of Best Practices Aimed at E9-1-1 and Public Safety

Final Report

Table of Contents

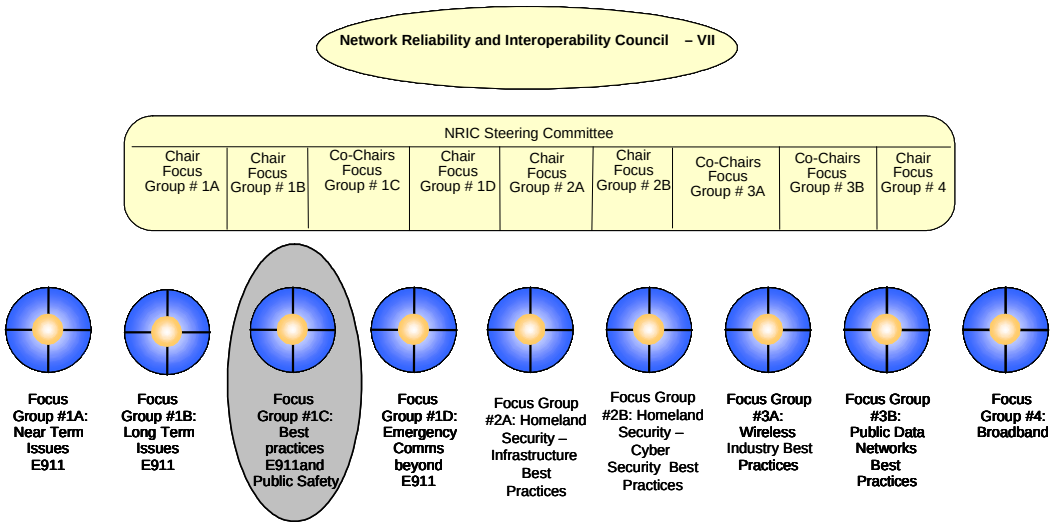
1 Introduction

The NRIC VII Council has been charged with reporting on ways to improve emergency communications networks. This report documents the efforts undertaken by Focus Group 1C with respect to the following:

- Analysis of 9-1-1 / E9-1-1 outages
- Identification of E9-1-1 architecture vulnerabilities
- Definition of information to be provided to callers when 9-1-1 network elements fail
- Enumeration and evaluation of factors to be considered in determining whether redundant E9-1-1 selective routers and alternate PSAPs should be provided
- Determination of effectiveness and modification of Best Practices for the E9-1-1 network, Public Safety and emergency communications in general

1.1 Structure of NRIC VII

The structure of the Network Reliability and Interoperability Council is as follows:



1.2 Focus Group 1C Members

Over the course of NRIC VII, Focus Group 1C has had a number of dedicated professionals contribute to its activities. Below is the list of members who participated on Focus Group 1C at various times during the two years of the NRIC VII Charter.

Focus Group 1C Members

Name	Company
Bonnie Amann	Sprint
Michael Anderson	Ericsson
Jay Bennett	Telcordia Technologies
Robert Burkhardt	Independent Consultant
Jim Beutelspacher	State of Minnesota 9-1-1
Rick Canaday	AT&T
Doug Edmonds	Northwest Central Dispatch
Darryl Foster	Cox Communication
Ann Gasperich	TAG Consulting
Bob Iwaszko	Verizon Wireless
Percy Kimbrough	SBC
Bill Klein	ATIS
Richard Krock	Lucent Technologies
Gail Lassiter	BellSouth
Marc Linsner	Cisco Systems, Inc.
Ben Lightner	BellSouth
Spilios Makris	Telcordia Technologies
Jeng Mao	NTIA
Ron Mathis	Intrado
Bob Oenning	Washington State E9-1-1
Brad McManus	Sprint
Janice Partyka	TechnoCom Corp.
Nancy Pollock	Metropolitan Emergency Services Board
Karl Rauscher	Lucent Technologies
John Rollins	Verizon
John Rosnick	Sprint
Jim Runyon	Lucent Technologies
Fran Ryan	Sprint
Robert Schafer	MCI
Thom Selleck	AT&T
Kevin Smith	Nortel
Whitey Thayer	FCC
Rachel Torrence	Qwest
Carla Wirths	Sprint

A subgroup of the above list is responsible for the development of this Focus Group 1C Final Report.

Final Report Contributors

Name	Company
Michael Anderson	Ericsson
Jim Beutelspacher	State of Minnesota 9-1-1
Doug Edmonds	Northwest Central Dispatch
Bob Iwaszko	Verizon Wireless
Percy Kimbrough	SBC
Richard Krock	Lucent Technologies
Ben Lightner	BellSouth
Spilios Makris	Telcordia Technologies
Ron Mathis	Intrado
Bob Oenning – Co-Chair	Washington State E9-1-1
Nancy Pollock- Co-Chair	Metropolitan Emergency Services Board
John Rollins	Verizon
John Rosnick	Sprint
Fran Ryan	Sprint
Thom Selleck	AT&T
Kevin Smith	Nortel Networks
Whitey Thayer	FCC
Rachel Torrence	Qwest
Carla Wirths	Sprint

2 Results in Brief

Focus Group 1C was chartered to analyze the effectiveness of Best Practices aimed at 9-1-1 and Public Safety. Under the initial NRIC charter, Focus Group 1C was assigned the following:

- Analysis of 9-1-1/E9-1-1 outages
- Identification of E9-1-1 architecture vulnerabilities
- Determination of effectiveness and modification of Best Practices for the E9-1-1 network, Public Safety and emergency communications in general

Over time, additional tasks were reassigned from Focus Group 1A to Focus Group 1C. Those tasks were:

- Definition of information to be provided to callers when 9-1-1 network elements fail

- Enumeration and evaluation of factors to be considered in deciding whether redundant E9-1-1 selective routers and alternate PSAPs should be provided

This was done through a number of assigned tasks, the key findings of which are outlined, in brief, below.

9-1-1/E9-1-1 Outage Analysis

- A large portion of 9-1-1/E9-1-1 outages were caused by cable damage.
- Implementation of diverse routing and/or automatic re-route would have eliminated or mitigated the effect of 37% of 9-1-1/E9-1-1 outages.
- In most cases, broad network infrastructure outages (e.g., damaged facilities, switch outage) caused an impact to multiple services, including 9-1-1 service. In only 12% of the analyzed outages was 9-1-1 the only service affected.
- NRIC Best Practices aimed at restoration and survivability of the overall network also benefit 9-1-1.
- NRIC Best Practices are effective in mitigating 911/E911 outages when followed.

E9-1-1 Architecture Vulnerabilities

- Four components of the 9-1-1/E9-1-1 architecture were identified as the most likely causes of 9-1-1 affecting failures:
  - Facility
  - Common Control Signal (CCS)
  - Power Elements
  - Switches (local and selective router)

E9-1-1 Network Failure Notification for Callers

Enhanced 9-1-1 (E9-1-1) network failure notifications are necessary to inform the public that the system is unavailable, and also to inform the public as to what actions can be taken to ensure access to available public safety services until such time as E9-1-1 services can be restored. There is no current network capability which provides for the delivery of messages to individual callers concerning a major failure within the E9-1-1 networks beyond tones indicating the unavailability of the network. Currently, the most effective way to inform the calling public of E9-1-1 outages due to network failures is by utilizing public notification systems.

Consideration of Redundant E9-1-1 Selective Routers and Alternate PSAPs

Focus Group 1C was asked to enumerate and evaluate the factors for consideration in deciding whether redundant E9-1-1 selective routers and

alternate PSAPs should be deployed as mitigation measures to preclude E9-1-1 service impacting outages.

In general, both of these options are considered Best Practices (see NRIC Best Practices 6-6-0568 and 6-6-0571) and an analysis of their impact on reviewed outages confirmed their value. However, the decision to deploy either alternative should be made on an individual basis after all relative factors are considered.

Focus Group 1C developed a list of 16 factors that should be considered in deciding whether redundant selective routers should be provided. All factors fell under one of the following categories:

- Cost
- Vulnerabilities
- Network Issues

Focus Group 1C also developed a list of 8 factors that should be considered in deciding whether alternate PSAPs should be provided. All factors fell under one of the following categories:

- Network Vulnerabilities
- Coordination and Capabilities
- Alternatives

These factors should be assessed by the expert performing the evaluation, and those factors that are relevant should be considered in each individual case.

Best Practices for 9-1-1/E9-1-1, Public Safety and Emergency Communications

Initially, Focus Group 1C identified a total of 58 existing NRIC Best Practices that were seen as directly impacting E9-1-1 and Public Safety. Through continued evaluation of existing Best Practices and coordination with other NRIC VII Focus Groups, Focus Group 1C identified one additional Best Practice that also met this criterion, bringing the total number of Best Practices examined to 59.

A qualitative survey was conducted among the members of the Focus Group to determine how effective these Best Practices are in addressing emergency communications in general, and by extension E9-1-1 networks and Public Safety. Again, after much coordination across Focus Groups and thorough discussion within Focus Group 1C, the final results are as follows:

- 7 of these Best Practices were rated as effective
- 43 of these Best Practices were rated as generally effective, but were deemed to require some degree of modification or updating

- 9 of these Best Practices were rated as no longer effective and are recommended for deletion
- In addition, Focus Group 1C is proposing 2 new Best Practices to address gaps identified by the Focus Group

Recommended modifications to the Best Practices and new Best Practices are included in Section 8.4 of this report.

3 Background

The Network Reliability and Interoperability Council was originally established to study the causes of service outages within and between the nation's telecommunications networks and to develop recommendations to reduce their number and mitigate their effect on consumers.[1] NRIC I-IV concentrated on reliability concerns in a number of areas including signaling (SS7), fiber cuts, switching systems, power failures, fires, 9-1-1 outages, and digital cross-connect systems. Reports and trends in these areas were studied and recommendations on what level of service outages should be reported to the FCC were made. A limited number of Best Practices to address these areas of concern were also developed.

NRIC V implemented a "voluntary one-year trial with participation by Internet Service Providers, CMRS, satellite, cable, and data networking service providers to alert National Communications System / National Coordinating Center for Telecommunications (NCS / NCC) of outages that are likely to have significant public impact."[2] This was the first step NRIC took in expanding its review of outages beyond wireline service providers.

The focus through NRIC V remained predominantly on telecommunications service and equipment providers. The focus was consistent with the ongoing evolution of technology and introduction of new players in the industry. However, the September 11, 2001 terrorist attacks highlighted the need to include the participation of the Public Safety and Emergency Management Sectors in the NRIC deliberations.

In the wake of the attacks, in March 2002 NRIC VI chartered a Homeland Security Focus Group to develop Best Practices to prevent disruptions of public telecommunications services and the Internet and to effectively restore those

[1] www.nric.org

[2] Ibid.

services in the case of disruptions. Under this Focus Group a Public Safety subcommittee was formed to identify the needs of the Public Safety sector and to make recommendations that would ensure that commercial telecommunications services networks could continue to meet the special needs of public safety emergency communications. The subcommittee addressed issues such as the means to prioritize, as appropriate, Public Safety usage of commercial services during emergencies.[3]

The Public Safety subcommittee identified commercial communications service needs in times of crisis by conducting a nationwide survey of numerous Public Safety entities, and then made Best Practice recommendations to address issues identified in the survey. Included among the recommendations were suggested changes to existing Best Practices and the creation of several new Best Practices specifically developed to address the emergency communications needs of the Public Safety sector.

NRIC VII Focus Group 1C used these Public Safety Best Practices developed during NRIC VI, as well as existing Best Practices that address the E9-1-1 network, the Public Safety Answering Points ("PSAPs") and/or other emergency communications, as a baseline in determining the impact of Best Practices on emergency communications. (Best Practices that address general network infrastructure, while they might support emergency services, do not address the E9-1-1 network or emergency service directly and were, therefore, not included in this analysis.)

NRIC VII combines previous work on Public Safety and outage reporting, as Focus Group 1C focuses on the reportable outages that affect 9-1-1/E9-1-1 services specifically, notification and prevention of 9-1-1/E9-1-1 outages, potential vulnerabilities in the E9-1-1 network, and the Best Practices applicable to E9-1-1 and Public Safety. We expect that future NRICs may continue the analysis of outages, expanding that focus to include wireless and data network outages, which are now reportable under FCC 04-188,[4] although current FCC regulations on outage reporting may preclude this (see section 4.3).

[3] Homeland Security Public Safety Final Report, NRIC VI, www.nric.org
[4] New Part 4 of the Commission's Rules Concerning Disruptions to Communications, FCC 04-188 http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-04-188A1.doc

4 Objective, Scope, and Methodology

4.1 Objective

The NRIC VII Council has been chartered with reporting on ways to improve emergency communications networks. Per the NRIC VII Charter, Focus Group 1C is responsible for performing an analysis of the effectiveness of Best Practices aimed at E9-1-1 and Public Safety.

4.2 Scope

This report contains the findings of Focus Group 1C regarding the following issues:

9-1-1/E9-1-1 Outage Analysis

The scope of this analysis is limited to outages related to 9-1-1/E9-1-1 that have been reported pursuant to 47 C.F.R. § 63.100[5]. The Focus Group did not review data from outages that were not reportable or that did not impact 9-1-1/E9-1-1 services.

The Focus Group noted that virtually any telephone service outage can impact the capability to dial 9-1-1, but only those outages where carriers had indicated a direct 9-1-1 impact were analyzed. Also not included were any reports that were initially filed pursuant to 47 C.F.R. § 63.100, but then were later withdrawn by the filing company because the company later determined that the outage did not meet the criteria requiring it to be reported.

E9-1-1 Architecture Vulnerabilities

For purposes of this document, the 9-1-1 network is defined as the end-to-end connectivity from the caller, through the Public Switched Telephone Network (PSTN), including both wireline and wireless networks, to a PSAP and including components unique to 9-1-1 services. These are the bounds of the network that were analyzed for possible vulnerabilities. IP-enabled networks were not considered in this analysis.

E9-1-1 Network Failure Notification for Callers

The Focus Group assumed that the information being sought is over and above the current reorder and busy signals commonly sent by the network during an outage. The Focus Group also assumed that notification included not only

[5] 47 C.F.R. § 63.100
http://a257.g.akamaitech.net/7/257/2422/05dec20031700/edocket.access.gpo.gov/cfr_2003/octqtr/47cfr63.100.htm

verbal messages but various network tones. These messages are limited only to voice/audible message and do not include data.

Consideration of Redundant E9-1-1 Selective Routers and Alternate PSAPs

While the NRIC VII Charter refers to E9-1-1 Tandems, Focus Group 1C believes that E9-1-1 Selective Routers is a more appropriate term and therefore uses this terminology throughout the report.

The scope of this deliverable is limited to identifying and explaining factors that should be considered in deciding whether redundant E9-1-1 selective routers and alternate PSAPs should be provided. The analysis does not include evaluation of implementation methods or network configuration once the decision to implement is made.

Best Practices for 9-1-1/E9-1-1, Public Safety and Emergency Communications

The scope of Focus Group 1C's work effort is limited to Best Practices that directly address E9-1-1 networks, Public Safety or emergency communications. It does not address those Best Practices which have a broader scope and whose implications reach beyond E9-1-1 and Public Safety (i.e., BP's addressing general PSTN supporting infrastructure). The scope includes Best Practices developed by previous NRIC's as well as existing industry best practices that are not currently documented in the NRIC database.

This report contains the results of a qualitative survey conducted by Focus Group 1C among its members who applied consistent evaluation criteria to determine the effectiveness of Best Practices pertaining to emergency communications. It also contains recommended modifications for existing Best Practices and suggested new Best Practices to maximize the effectiveness of NRIC Best Practices.

Finally, and by way of clarification, in a number of cases throughout this report and the Best Practices addressed within, the term Public Safety Authority (PSA) is used. This term is defined as the administrative entities associated with Emergency Communications, which can be a Public Safety Answering Point (PSAP), or entities at the Federal, State, County or City governmental level.

4.3 Methodology

Described below is the methodology used to address each of the key issues in the report.

9-1-1/E9-1-1 Outage Analysis

To perform the outage analysis, the Focus Group identified the timeframe of the data it would use for the outage analysis. Prior to NRIC VI, the focus of Best Practices was on the traditional wireline networks. NRIC VI changed the landscape by developing and incorporating Best Practices addressing wireless networks. Consequently, when determining what time frame would be used in the outage analysis, Focus Group 1C chose to analyze outage data for 2002, 2003, and the first quarter of 2004 as this was the time frame during which a significant number of Best Practices were developed. The Focus Group also felt that Best Practices that impact 9-1-1 have evolved significantly due to the efforts of previous NRIC's, making earlier outage data less relevant to current Best Practices.

Outage data was then compiled by obtaining two sets of data:

- The FCC data on outages related to 9-1-1/E9-1-1 that were reported pursuant to 47 C.F.R. § 63.100 from January 2002 through March of 2004. The initial number of outage incidents received from the FCC for this purpose was 84. These incidents contained raw data as reported to the FCC by the carriers

- 80 NRSC summary data outage incidents based on E9-1-1 outages that were reported pursuant to 47 C.F.R. § 63.100 from January 2002 through March of 2004. These reports summarized the same FCC data and categorized each outage within three primary categories (Failure, Direct Cause, Root Cause). In all cases, these reports summarized outages that were reported to the FCC. These reports were reconciled with the FCC data to ensure consistency.

An Outage Analysis subgroup reviewed the individual outage reports from both sources to determine which outages affected 9-1-1/E9-1-1 services. Through this review and reconciliation process, the subgroup determined that 76 of the outage incidents provided to the Focus Group by the FCC and NRSC affected 9-1-1/E9-1-1 services and should be included in the analysis.

The Focus Group decided that to maintain consistency with the work being done by other reporting groups, the NRSC definitions would be used in identifying the root cause, direct cause, failure category, and all related sub-categories.

These definitions can be found in Section 9.2. Using these definitions, the compiled outage data was then analyzed by the Outage Analysis subgroup to identify trends, key findings, and areas of concern. Graphs depicting the findings are located in the Analysis and Findings section of this report.

Beginning in 2005, outage data is unavailable due to new FCC regulations which prohibit the availability of outage records to the public. The new rules, available in Part 4 of the Commission rules[6], in Section 4.2 state "Reports filed under this part will be considered confidential. Public access to reports filed under this part may be sought only pursuant to the procedures set forth in 47 CFR 0.461." Under these new rules, access to these reports are restricted due to Homeland Security considerations.

E9-1-1 Architecture Vulnerabilities

As per NRIC VI, vulnerability is defined as a characteristic of any aspect of the communications infrastructure that renders it, or some portion of it, susceptible to damage or compromise.[7]

In order to identify potential architecture vulnerabilities, a 9-1-1 Network Topology Reference Diagram was developed to "level-set" the Focus Group. This reference diagram is a high-level graphic illustration of network components and architectures that facilitated the analysis by comparing "apples to apples" when dealing with differing technologies and functionalities. (See Section 8.2.)

The Architecture Vulnerability subgroup referred to each of the 76 outages contained in the outage analysis, and using the reference diagram as a map, identified in which area of the network each outage occurred. This data was aggregated and analyzed for trends identifying the most vulnerable areas of the 9-1-1 / E9-1-1 network.

E9-1-1 Network Failure Notification for Callers

As in the vulnerability identification process, the 9-1-1 Network Topology Reference Diagram was used as a starting point in determining where and if notification could be generated and what type of notification should be provided to callers when 9-1-1 network elements fail. A technical feasibility analysis was performed with all elements of the 9-1-1 network being evaluated. Points within the network with the potential for experiencing a major failure that could preclude delivery of the dialed 9-1-1 call to the PSAP were identified. Once

[6] New Part 4 of the Commission's Rules Concerning Disruptions to Communications, FCC 04-188 http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-04-188A1.doc

[7] Network Reliability and Interoperability Council VI, Homeland Security - Physical Security (Focus Group 1A) Final Report, Issue 3, December 2003

identified, each point or network element was further examined regarding the feasibility of introducing a notification function. Section 8.1 contains a table cataloging the various network elements, cross-referenced with potential options for notification delivery, as well as an illustration of the E9-1-1 Network topology used in this analysis.

Consideration of Redundant E9-1-1 Selective Routers and Alternate PSAPs

The Focus Group first identified the factors that should be considered when deciding whether to deploy redundant E9-1-1 selective routers and alternate PSAPs. Through a brainstorming session during a face-to-face meeting, these factors were identified for both the deployment of selective routers and the implementation of alternate PSAPs. These factors were further evaluated and expanded to include multiple areas of consideration for each factor.

Best Practices for 9-1-1/E9-1-1, Public Safety and Emergency Communications

Best Practices related to Outage Analysis

The full list of existing NRIC Best Practices totaling 776 were obtained from the NRIC website[8], and the Best Practices were sorted to identify those practices related to 9-1-1/E9-1-1 and emergency communications using key word searches for words such as Public Safety, 9-1-1, and Emergency Services.
A total of 97 of the existing NRIC Best Practices were initially identified by the Best Practices subgroup as being applicable to 9-1-1/E9-1-1 outages. These are the Best Practices listed in the Focus Group's September, 2004 report.

Survey to determine effectiveness of Best Practices

For its second report, the Focus Group was chartered to conduct a survey on the effectiveness of Best Practices for emergency communications. After reviewing the initial list of Best Practices from its first report, the Focus Group removed those Best Practices that were both a) not developed specifically to address E9-1-1 and Public Safety (i.e., had broader implications across other networks) and b) under known review by other Focus Groups.

The Focus Group then reviewed the NRIC VI final report from the Public Safety subcommittee and identified one additional Best Practice that it deemed relevant to emergency communications. This Best Practice was added to the survey list, leaving the Focus Group with 59 Best Practices to be evaluated for their effectiveness for emergency communications.

[8] www.nric.org

In order to more effectively manage the amount of data being evaluated, the Focus Group split up into two subgroups, each focusing on a different set of Best Practices, and the survey was conducted among the subject matter experts on each subgroup. Each Best Practice was evaluated using the following criteria:

- The extent and frequency of implementation
- The contribution to emergency communications (whether through reduced 9-1-1 outages, improved emergency response, or delivery of critical information)
- The technical feasibility, relative to cost

Overall effectiveness for each of the identified Best Practices was judged based on application of the stated criteria, as well as the expertise of both subject matter experts in the subgroup, and those solicited for input by members of the subgroup. The existence of other possibly more effective Best Practices was also explored and noted.

The full Focus Group met during a two-day session to review the work of each subgroup, to compile the final list of relevant Best Practices, and to finalize the results to be included in its report. All analyzed Best Practices were placed into one of the following categories:

- Effective
- Effective – Needs Modification
- No Longer Effective – Recommend for Deletion

While conducting the analysis of its survey results, the Focus Group made the following assumptions and decisions.

- The Best Practices selected for the survey were directly applicable to 9-1-1 and Public Safety. Other Best Practices that support 9-1-1 and Public Safety as part of the general reliability of the PSTN were not included in this analysis.
- Every Best Practice was assumed to have been implemented and effective at some point in time. When determining that a Best Practice was no longer effective, the Focus Group sought an indication of what circumstances had changed or how the promise of the Best Practice had otherwise failed to develop.
- The Focus Group used materials outlining the approach used across other NRIC VII Focus Groups to develop the survey criteria.

- Best Practices were evaluated in terms of cost based on technical feasibility and implementation criteria.[9]
- The criteria were used as a facilitation tool to drive discussion around the effectiveness of Best Practices. Ratings for each Best Practice were predicated on informal evaluations based on subject matter expertise, experience and industry knowledge.

Best Practice Modifications

Based on the results of the survey, the Focus Group reviewed those Best Practices that were determined as requiring modification or recommended for deletion. In addition, the outage analysis subgroup identified several additional Best Practices that were deemed relevant to 9-1-1 and Public Safety. These Best Practices were added to the list for review and potential modification. The Focus Group developed the necessary modifications to make each of the identified Best Practices more effective. Additionally, the Focus Group developed the rationale for those Best Practices it is recommending for deletion.

In the course of making recommended modifications, the Focus Group reviewed any recommendations made by other Focus Groups for the same Best Practices that had been evaluated in this survey. In some cases, Focus Group 1C decided that the other Focus Group had more expertise to review the Best Practice and therefore removed the Best Practice from Focus Group 1C's final review. In other cases, Focus Group 1C agreed with the changes made by other Focus Groups, in which case Focus Group 1C supported the recommendations made by the other Focus Group. In cases where Focus Group 1C was not in agreement with changes made by other Focus Groups, or vice versa, the groups discussed conflicts until consensus was reached.

In the end, 59 existing Best Practices are included in Focus Group 1C's final review, and two new Best Practices are recommended for addition to the NRIC Best Practice database.

[9] Cost in this case was not identified as a specified monetary amount, but as a general cost level (e.g., high cost, low cost)

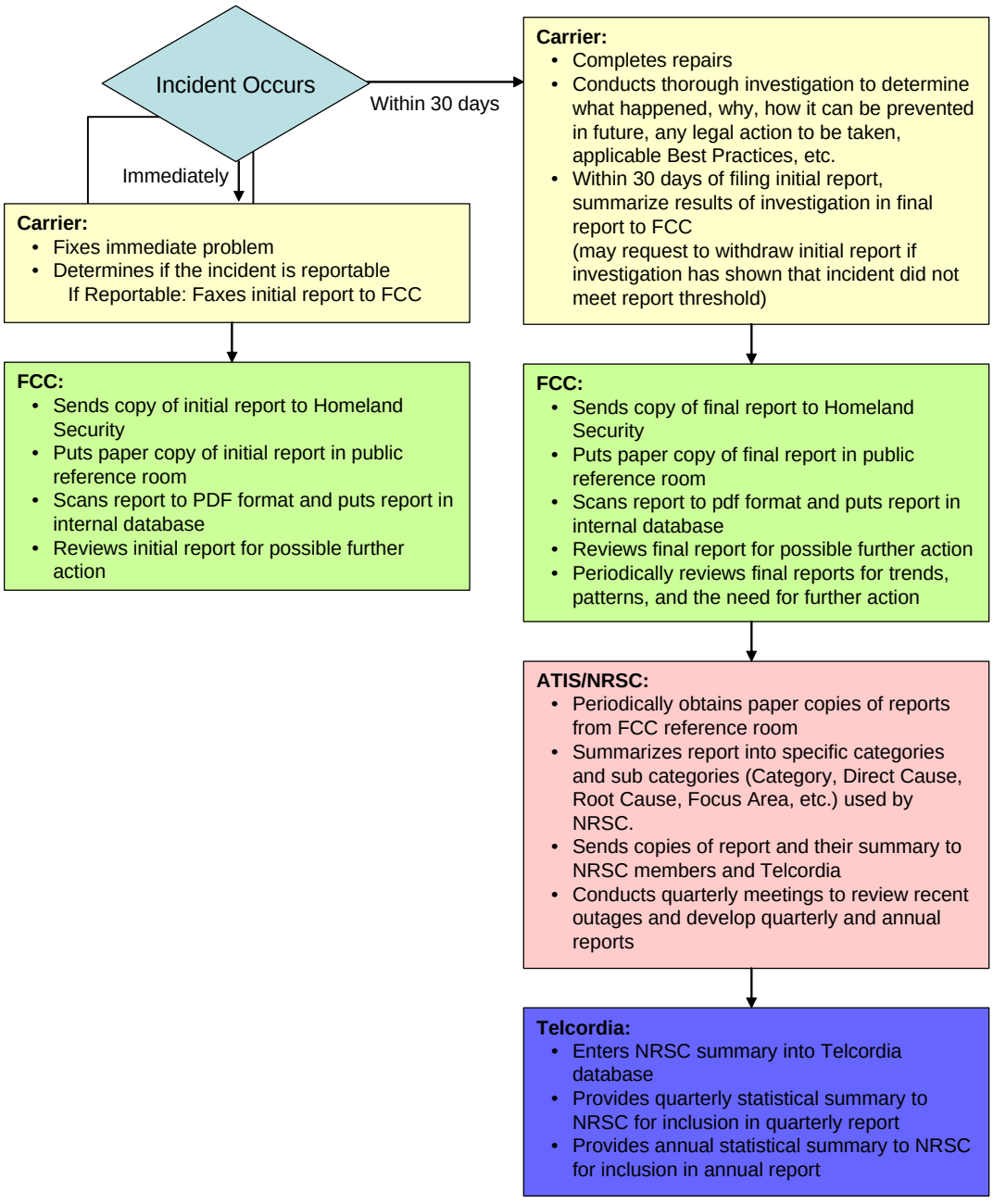
5 Analysis and Findings

5.1 9-1-1/E9-1-1 Outage Analysis

5.1.1 Background

As was mentioned in the methodology section, the outage analysis was performed based on data received from two sources: the FCC and the National Reliability Steering Committee (NRSC). It is useful to understand how these two entities generated the data that was provided to the Focus Group for analysis. The diagram below shows the flow of information from the time an outage takes place to the time it is captured as data in the FCC and NRSC databases. The chart is color coded by the entity taking the action listed in each box (e.g., FCC, carrier, etc.)

Exhibit 5.1.1 A – Outage Reporting Process (as of 9/04) [10]



[10] Since Focus Group 1C's initial review and report on the outage data, the FCC outage reporting process has been changed and the outage reports are no longer publicly available for analysis.

In addition, the Focus Group agreed to use the established NRSC definitions in identifying the direct cause, root cause, and failure category of each outage.

The direct cause is defined as the event, action, or procedure that triggered the incident. While a carrier may identify the direct cause of an incident in any way that it deems appropriate, for its analysis of outages the NRSC has defined and utilizes the direct causes listed in the "Direct Cause Definitions," found in Section 9.2 of this document. It is recommended by the NRSC that for uniformity in reporting these definitions be implemented when determining the direct cause of an outage. [11]

The root cause is defined as the key problem, which once identified and corrected prevents the same or a similar problem from recurring. Typically the root cause can be determined through a thorough reading of the "Background of the Incident". However, it is often necessary to read both the "Background of the Incident" and "Steps Taken to Prevent Recurrence of the Incident" to determine the true root cause. In today's technology, two or more problems may be closely linked and require detailed investigation. However, in any single incident there should be only one root cause. While a carrier may identify the root cause of an incident in any way that it deems appropriate, for its analysis of outages the Network Reliability Steering Committee (NRSC) has defined and utilizes the root cause listed in the "Root Cause Definitions", found in Section 9.2 of this document. It is recommended by the NRSC that for uniformity in reporting these definitions be implemented when determining the root cause of an outage.[12]

In many cases there were NRSC subcategories that were applied to an outage as well. The following diagram shows the hierarchy of this methodology, and highlights some of the key subcategories applied to a large number of outages.

[11] Network Reliability Steering Committee; http://www.atis.org/nrsc/index.asp

[12] Ibid.

Exhibit 5.1.1 B – Hierarchy of outage characterizations

FCC Data – *84 Outages*
The FCC provided outage reports that carriers filed pursuant to C.F.R. § 63.100. The data were for outages that affected 911/E911 between January 2002 and March of 2004.

NRSC Summary Data – *80 Outages*
The NRSC provided summaries of relevant outage data from the same FCC dataset.

NRIC Focus Group 1C – *76 Outages*
Focus Group 1C read through each of the outage reports and summaries, eliminated several outages that were not relevant to 911/E911, and compiled the data for analysis

Direct Cause Category – *76 Outages*

Cable Damage	20
Design Hardware	18
Procedural Service Provider	12
Hardware Failure	7
External Environment	5
Power Failure	5
Internal Environment	3
Design Software	2
Procedural System Vendor	1
Procedural Other Vendor	1
Traffic/System Overload	1
Other/Unknown	1
Design Firmware	0
Insufficient Data	0

Root Cause Category – *76 Outages*

Procedural Service Provider	27
Cable Damage	17
Hardware Failure	9
External Environment	6
Power Failure	5
Internal Environment	3
Procedural System Vendor	3
Procedural Other Vendor	2
Design Hardware	2
Design Software	1
Other/Unknown	1
Design Firmware	0
Traffic/System Overload	0
Operations Support/Strategy	0
Insufficient Data	0

Failure Category – *76 Outages*

Facility	36
CO Power	12
CCS	11
Local Switch	7
DCS	5
Selective Router	3
Other	2

Key Direct Cause Subcategories*

Cable Damage	
➢ Digging error	7
➢ Other	13
Design Hardware	
➢ Insufficient network redundancy/diversity	18
Procedural Service Provider	
➢ Failure to follow standard procedures/documentation	11
➢ Followed procedures/documentation that were incorrect	1
Hardware Failure	
➢ Dual A Link Failure	1
➢ Other	6
External Environment	
➢ Manmade (vehicular accident)	2
➢ Natural (storms, lightning, wind, etc.)	3
Power Failure	
➢ Lack of power redundancy	1
➢ Lack of power diversification	1
➢ Other	3

Key Root Cause Subcategories*

Procedural Service Provider	
➢ Insufficient supervision/control	10
➢ Insufficient training	8
➢ Inaccurate cable locate (dig-up)	5
➢ Documentation/procedures unavailable, unclear, incomplete	4
Cable Damage	
➢ Inadequate/no notification (dig-up)	10
➢ Digging error	3
➢ Other	4
Hardware Failure	
➢ Peripheral Unit Failure	4
➢ Processor Community Failure	1
➢ Other	4
External Environment	
➢ Fire	4
➢ Storm (water, ice)	1
➢ Vandalism/theft	1
Power Failure	
➢ Insufficient response to power alarm	1
➢ Overloaded/undersized power equipment	1
➢ Inadequate/missing power alarm	1
➢ Lack of power redundancy	1
➢ Other	1

Key Failure Subcategories*

Facility	
➢ Cable Dig-Up	24
➢ Cable Electronics	3
➢ Other	6
➢ Aerial Cable Cut	1
➢ Cable Placing/Removing	2
CO Power	
➢ DC Distribution	4
➢ DC Plant	3
➢ Standby Generator	1
➢ Other	4
CCS	
➢ Isolation	9
➢ Link(set)s	1
➢ Other	1
Local Switch	
➢ Translations	4
➢ Software	1
➢ Other	2
DCS	
➢ Hardware	4
➢ Other	1

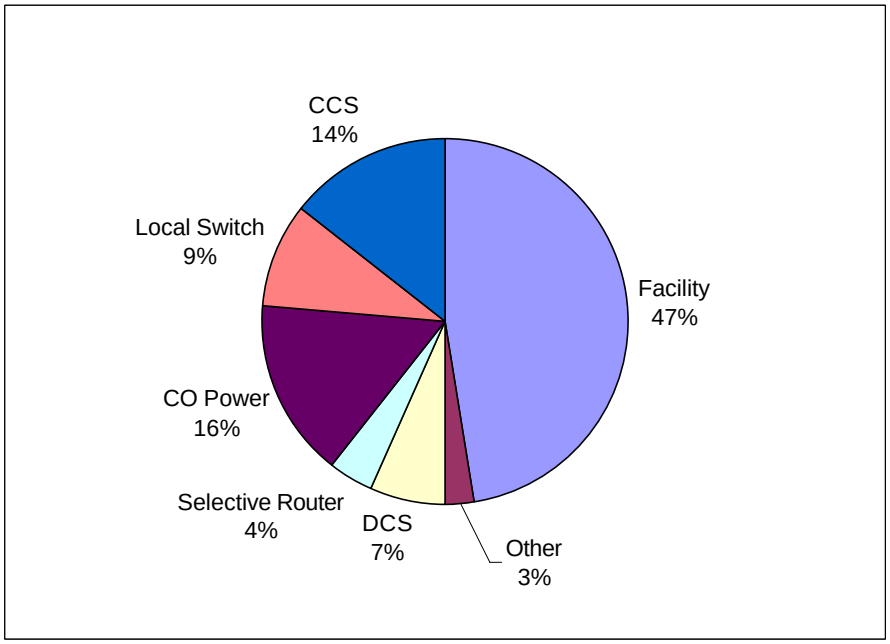
* Only subcategories with five or more outages are expanded in this table, and therefore the subcategory sums do not equal 76.

5.1.2 Analysis

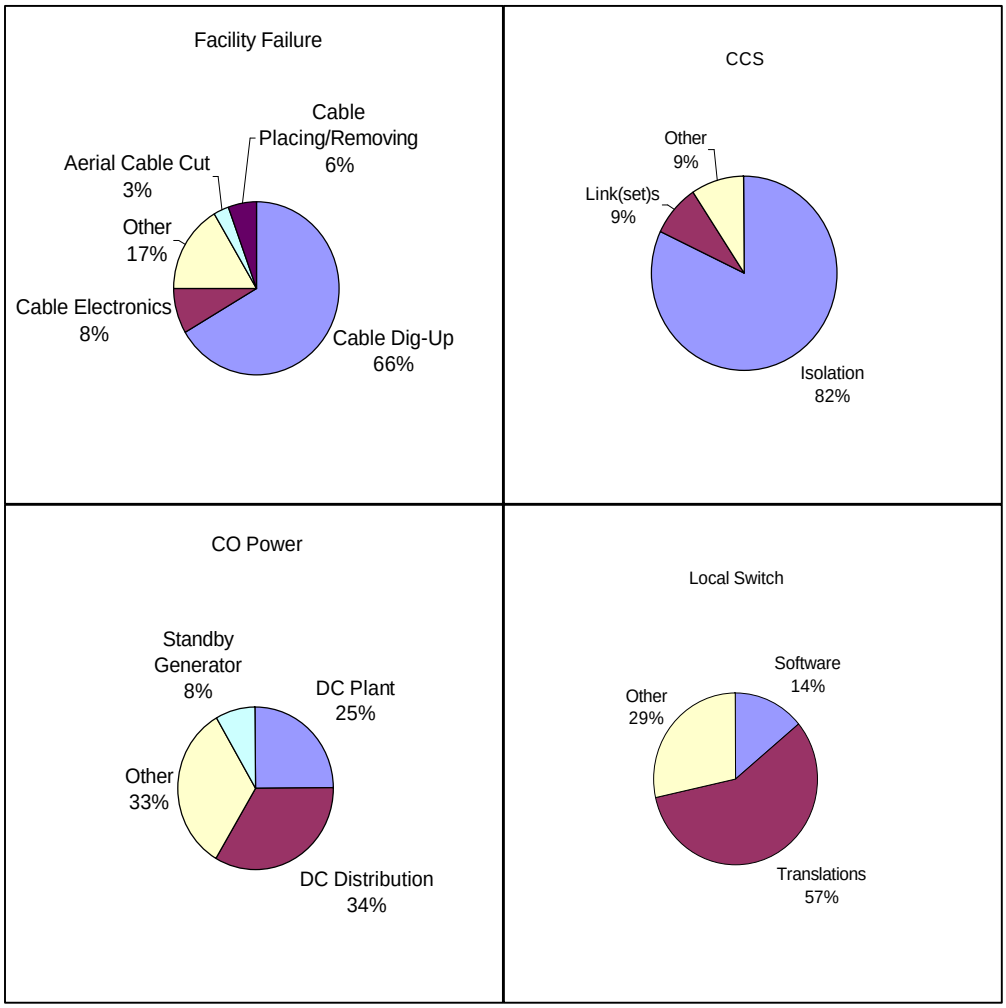
The outage data was analyzed starting with Failure Category, Direct Cause and Root Cause. Further analysis was done by subcategory to identify the key causes

of outages. The absence of diversity was also examined to determine how many outages were potentially affected by a lack of network or equipment diversity on the part of either the carrier or PSAP. Finally, the duration and number of people affected by outages was examined and charted. Below is a graphical representation of the analysis.

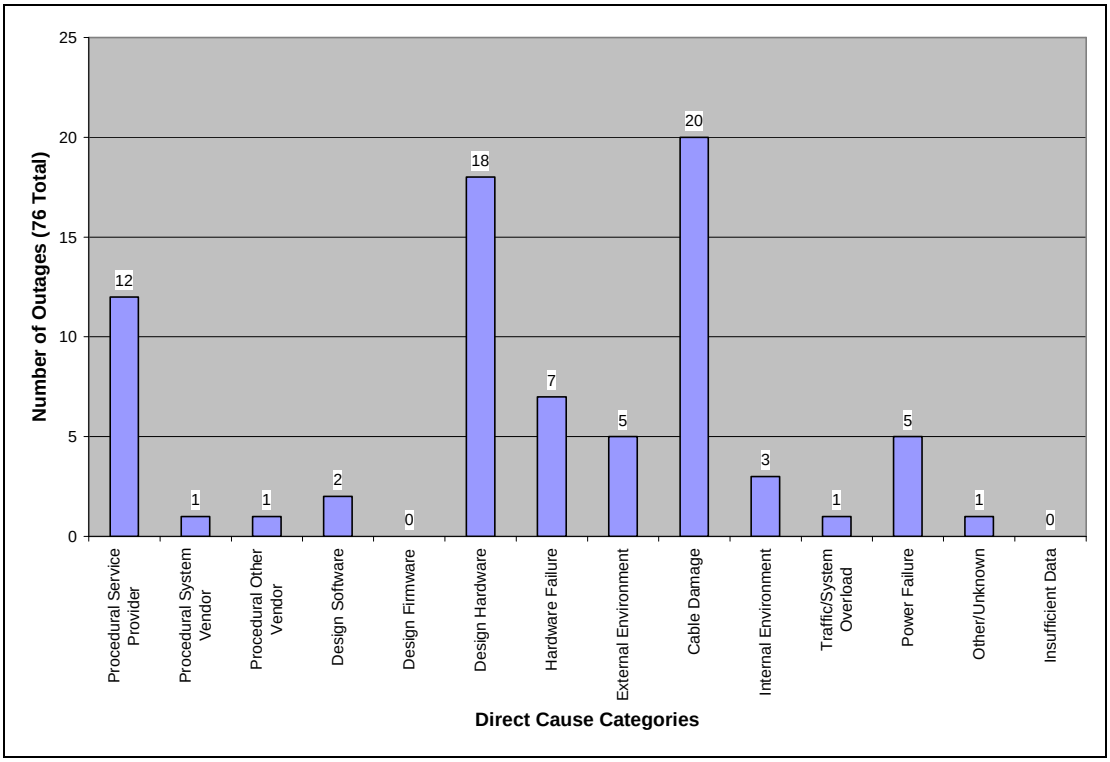
Graph 5A-1: Percentage of outages by failure category



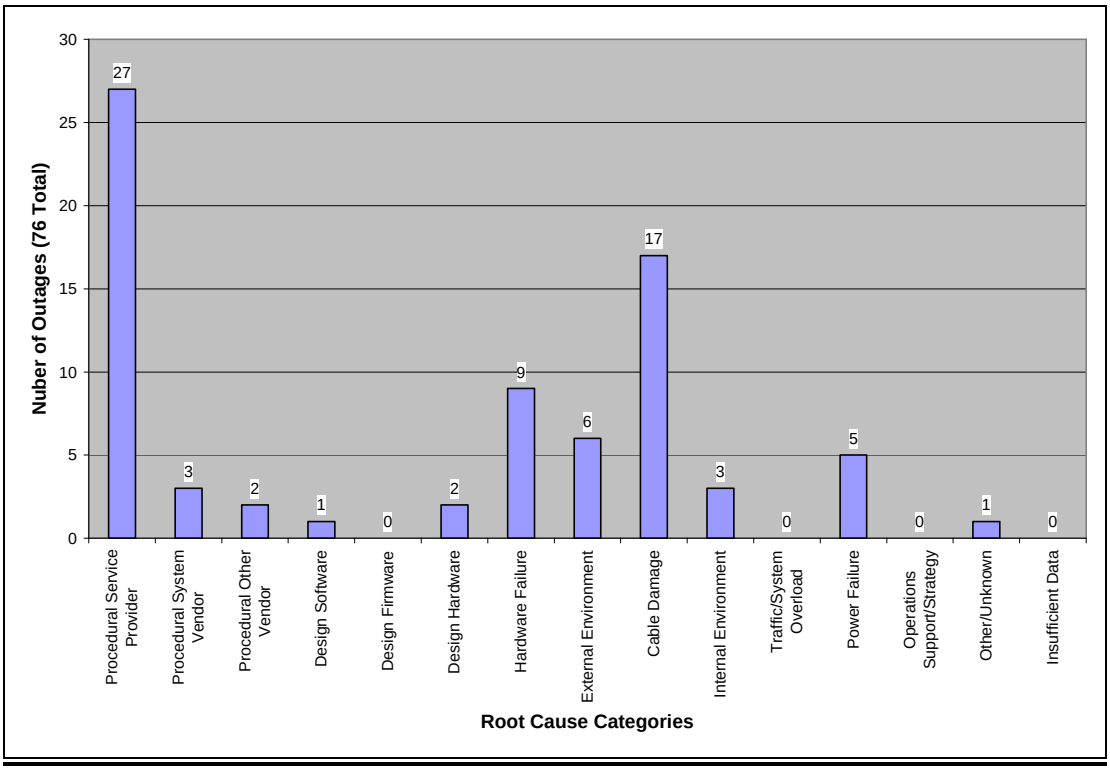
Graph 5A-2: Percentage of outages by failure subcategory



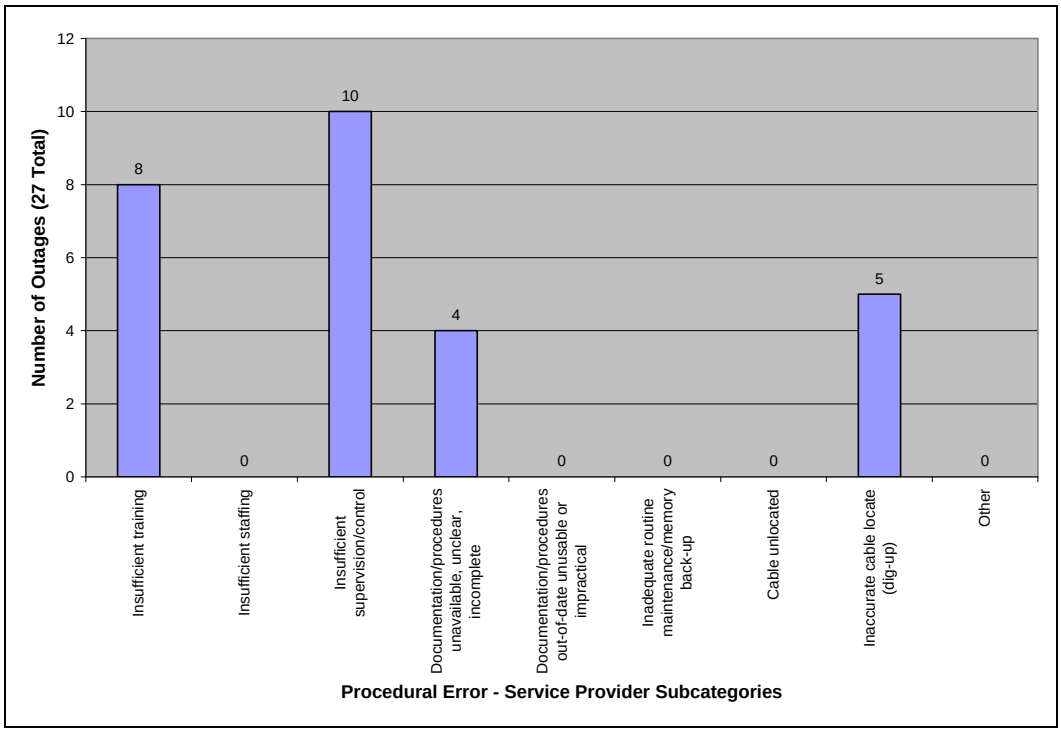
Graph 5B: Number of outages by direct cause category



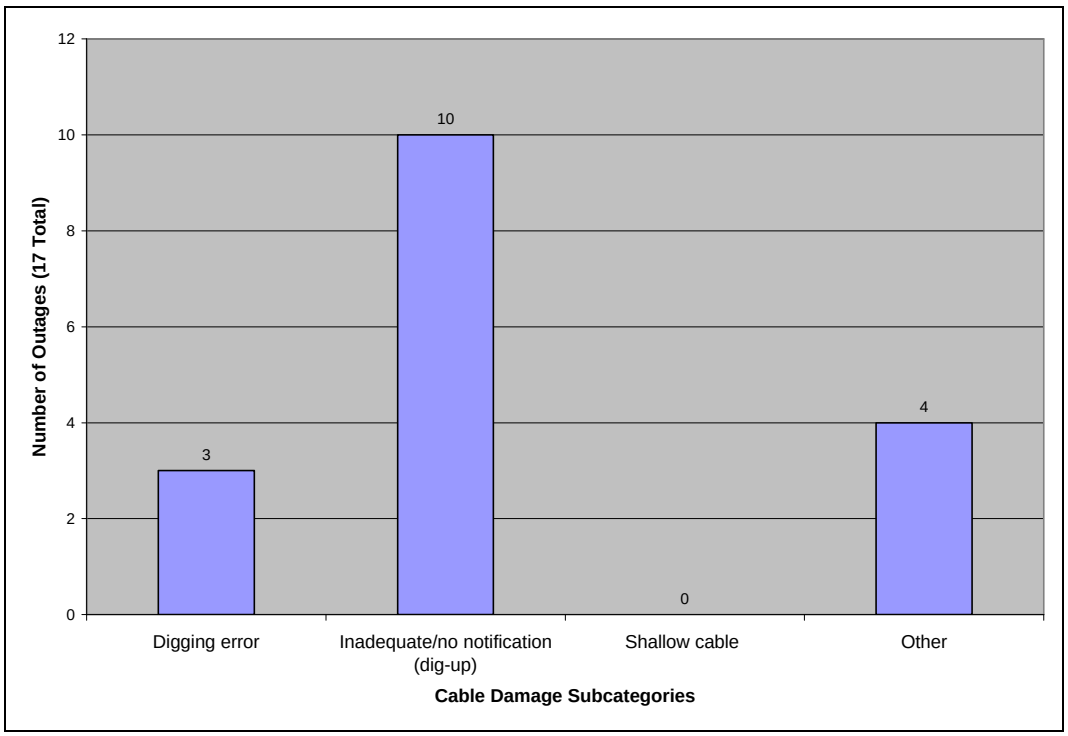
Graph 5C-1: Number of outages by root cause category



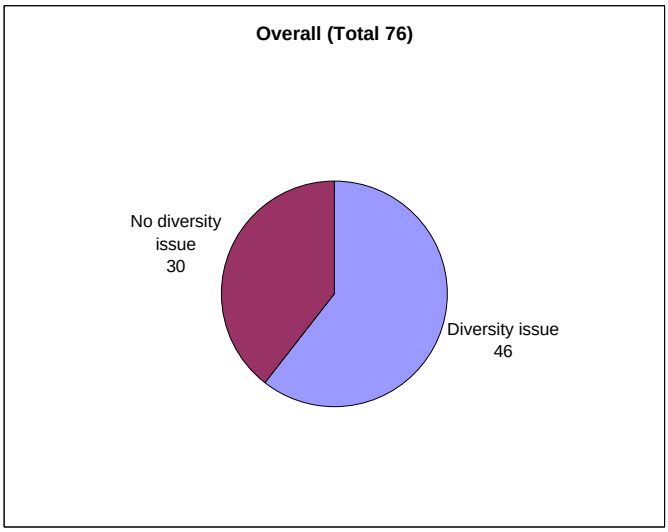
Graph 5C-2: Number of outages by service provider procedural error root cause subcategories



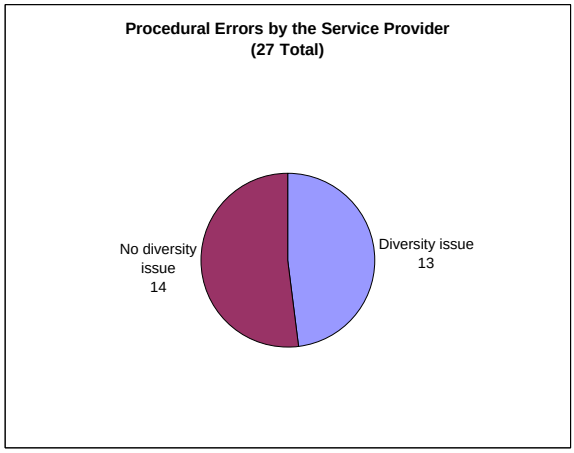
Graph 5C-3: Number of outages by cable damage root cause subcategories

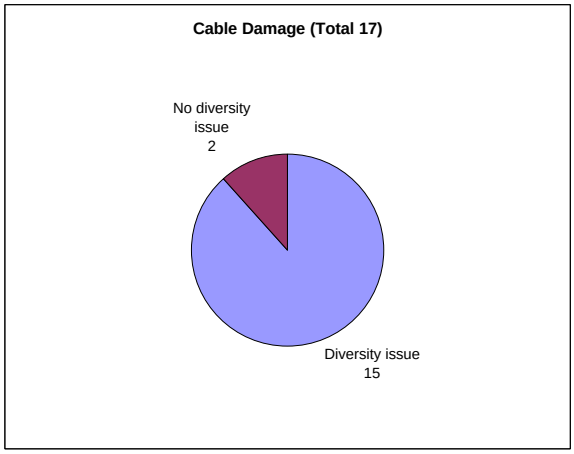


Graph 5D-1: Number of outages that can be linked to lack of diversity

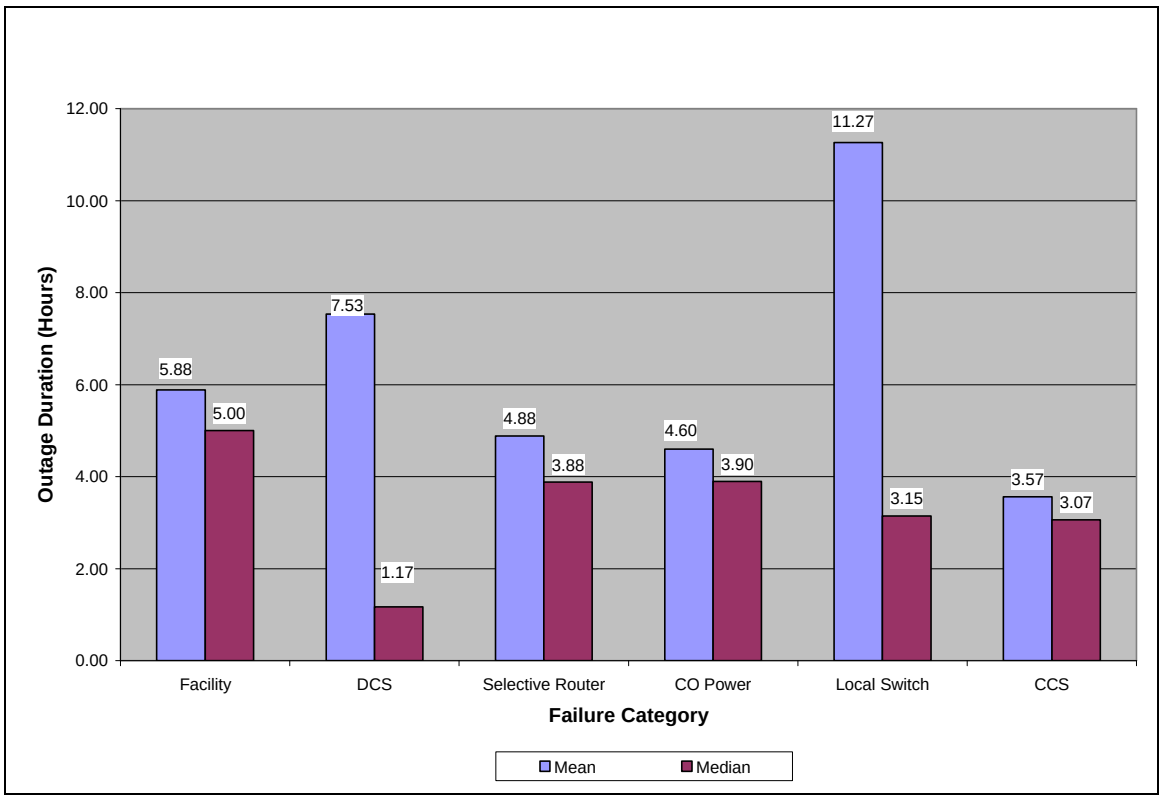


Graph 5D-2: Number of outages that can be linked to lack of diversity by root cause





Graph 5E: Duration of outage by failure category*



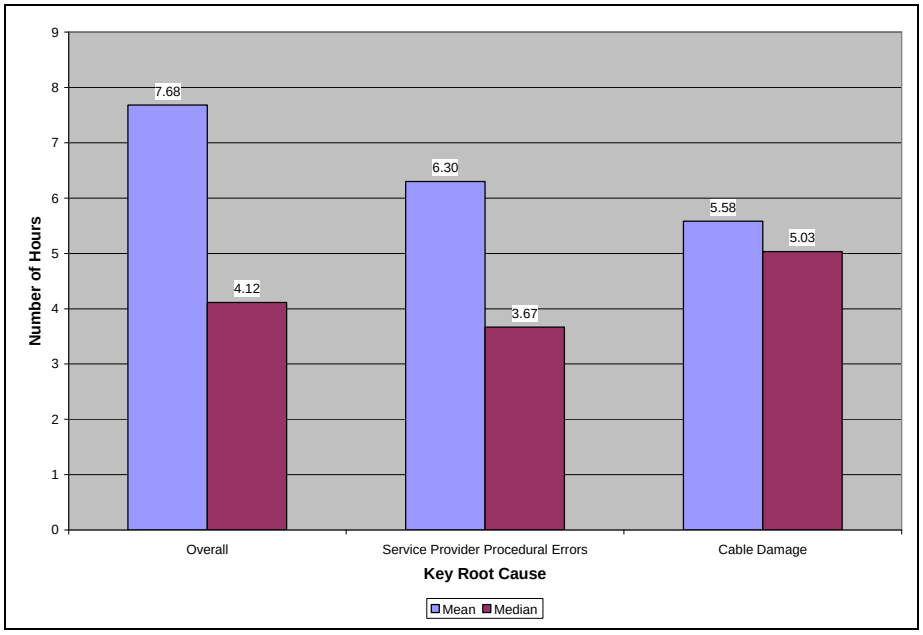
* The "Other" category was removed from this chart. Of the two outages in this category, one of the data points was an outlier (144 hour outage due to severe winter weather).

The disparity between the mean and the median outage durations is notable for DCS and Local Switch categories. Closer investigation of the data shows that outlier data points are responsible for these sharp differences.

Of the five outages categorized as DCS failures, there is a significant gap between the duration of the two longest outages and the other three. The relatively small number of outages compounded by the large gap in the time periods results in a pronounced positive skew to this data.

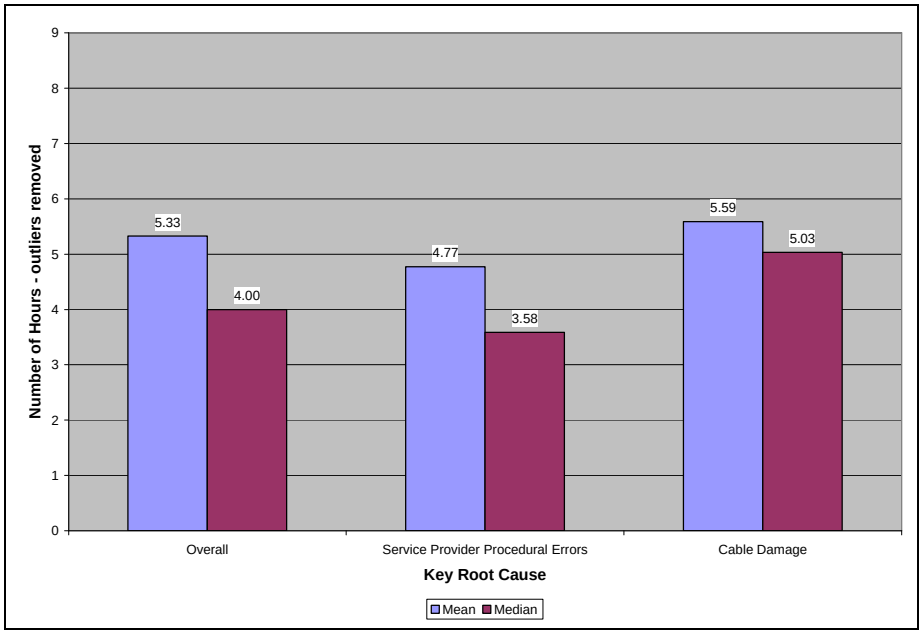
The Local Switch data are skewed by outage 04-013 which is an outlier in duration (46 hours). Removing this outage, which was caused by an improper change to the data on the local switch and did not trigger the notification system, would greatly reduce the gap between the mean and the median for the Local Switch category.

Graph 5F-1: Duration of outage by key root cause categories (all data)

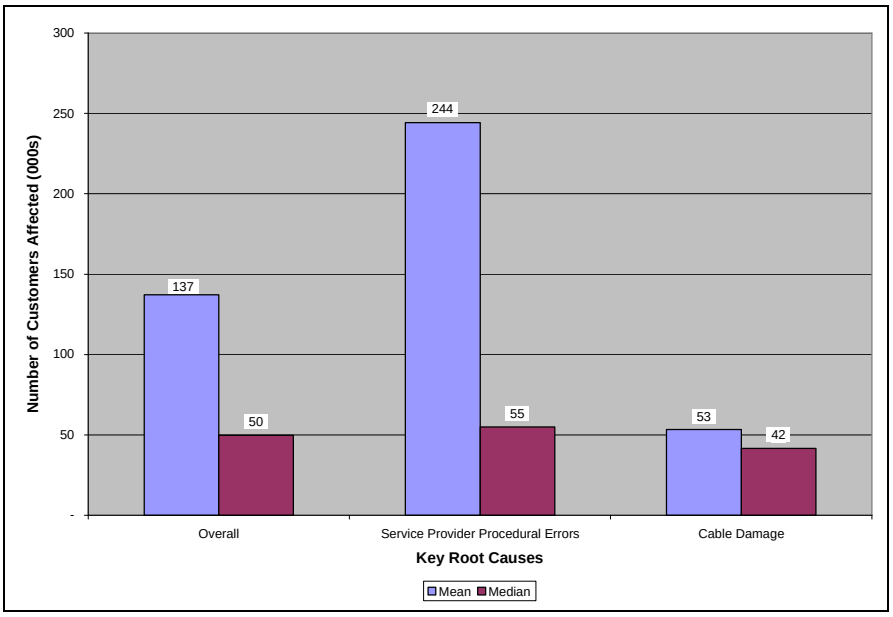


Two specific outlier data points skew the data considerably resulting in higher than expected disparity between the mean and the median of both the "Overall" numbers and the "Service Provider Procedural Errors". Removing outage number 04-013 (46 hours) and outage number 02-135 (144 hours) brings each of these categories closer to expected results, though the Overall data still indicate a skew towards longer outages (see Graph 5F-2).

Graph 5F-2: Duration of outage by key root cause categories (outliers removed)

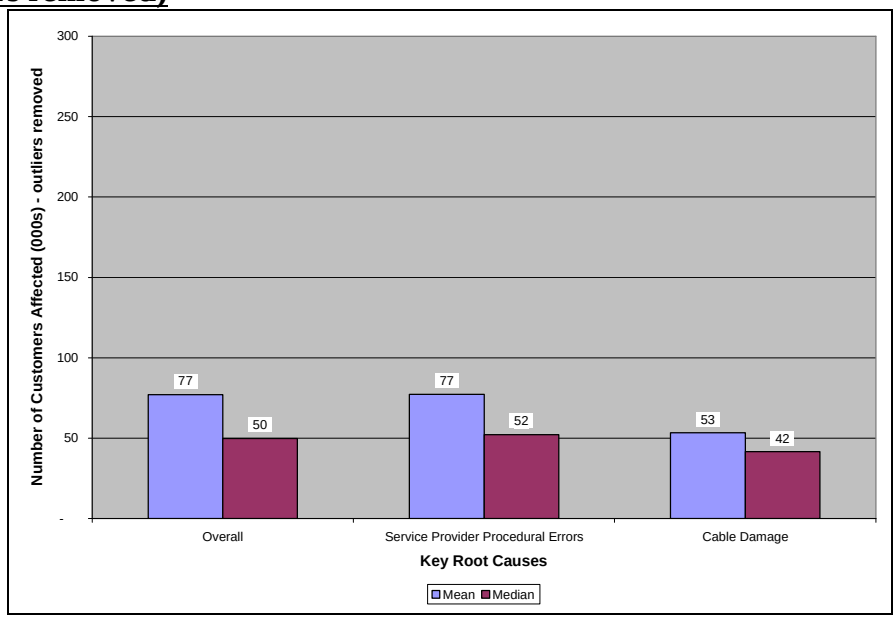


Graph 5G-1: Number of affected customers by key root cause category (all data)

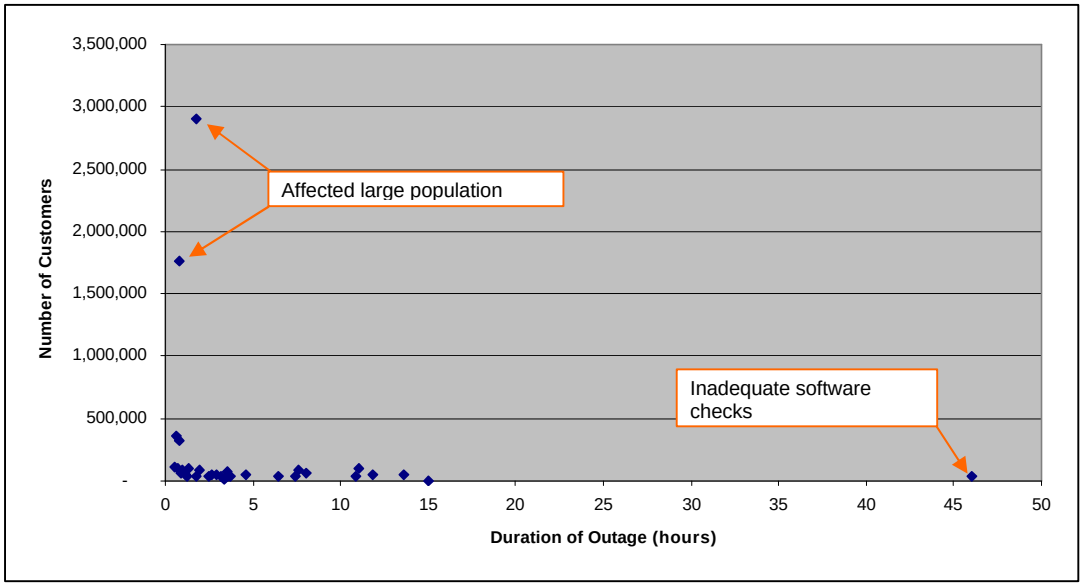


Two specific outlier data points skew the data for "Overall" and "Service Provider Procedural Errors". Included in the data analysis for both of these categories are two outages that affected 2.9 million and 1.76 million customers. Removal of these two outlier data points provides a more realistic view of the mean, which still indicates a positive skew (see Graph 5G-2).

Graph 5G-2: Number of affected customers by key root cause category (outliers removed)



Graph 5H: Outage duration (hours) and number of customers affected



5.1.3 Findings

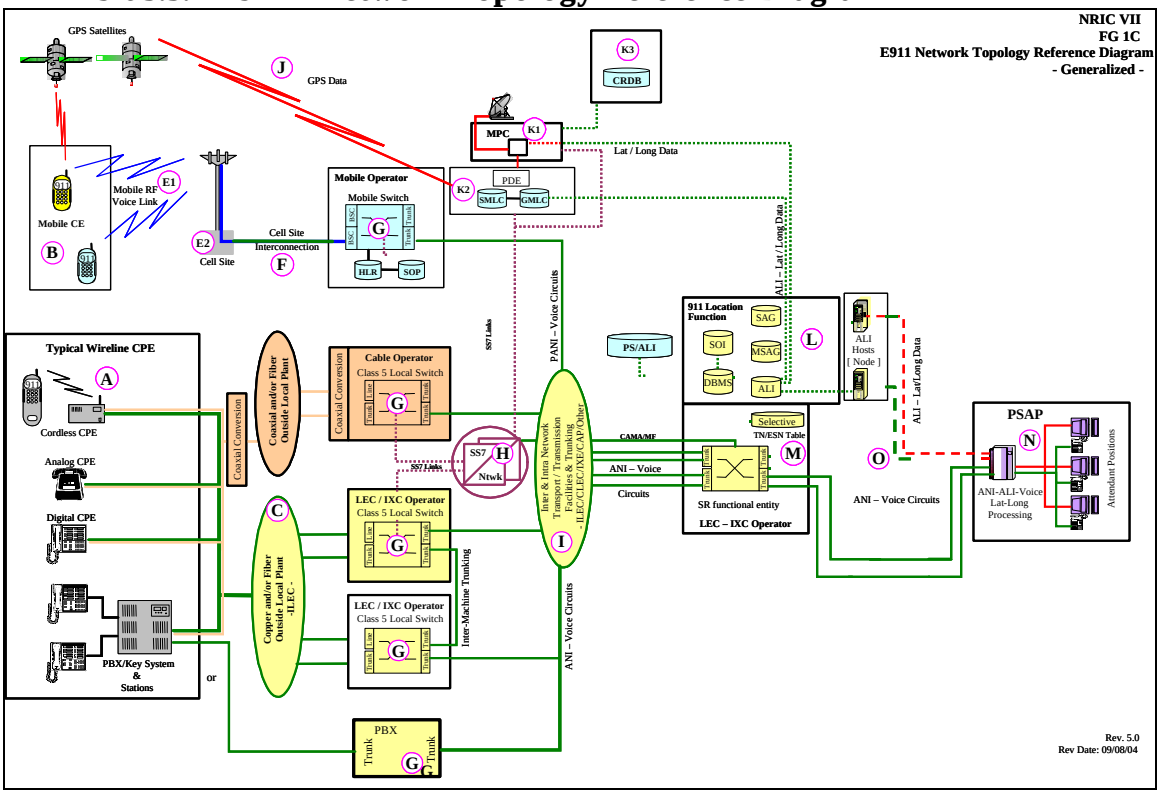
- The total number of outages reported pursuant to 47 C.F.R. § 63.100 from January 1, 2002 through March 31, 2004 that affected 9-1-1/E9-1-1 was 76
- 12% of the outages impacted 9-1-1 service only
- The majority of 9-1-1/E9-1-1 outages (47%) took place within the network facility or plant. Most of those (66%) were due to cable dig ups
- The majority (57%) of 9-1-1/E9-1-1 outages are caused by either cable damage or service provider procedural errors
    - 27 outages (35%) listed a service provider's procedural error as the root cause
    - 17 outages (22%) listed cable damage as the root cause
- In further breaking down these results, the primary causes of service provider procedural errors were:
    - lack of training (29%)
    - lack of supervision (29%)
    - inaccurate cable locate (17%)
    - incomplete procedures (14%)
- In further examination of the cable damage results, the primary cause is the failure to request a locate and other digging errors (76%)

5.2 E9-1-1 Architecture Vulnerabilities

5.2.1 Background

A Reference Diagram was developed to "level-set" the Focus Group when assessing the architecture vulnerabilities. This reference diagram is a graphic illustration of network components and architectures that facilitated analysis by allowing "apples to apples" comparisons when dealing with differing technologies and functionalities. A larger version of the below reference diagram can be found in Section 8.2

Exhibit 5.3.1 – 9-1-1 Network Topology Reference Diagram



5.2.2 Analysis

Vulnerability #1: Facility

Single Points of Failure
In reviewing the outage data, it appears that single points of failure still plague the 9-1-1 network. Best Practices of diversity, redundancy, and adoption of policies of dual network facilities for critical infrastructure are not universally employed. As technologies advance and increase the reliability of networks and network elements it would seem that single failure points could become a design element of the past. However, today, single failure points continue to exist and create problems for 9-1-1 networks.

Unprotected Fiber
Many of the 9-1-1 outages reported in the analysis period from January of 2002 through the first quarter of 2004 demonstrate the vulnerability of unprotected fiber portions of the 9-1-1 network. Cable cuts caused by inaccurate locates of buried fiber by the service provider, or its agents, or no locate of buried fiber requested by contractors contribute to a significant portion of the total outages. The Focus Group noted that the higher concentration of traffic on a single facility that can be achieved by using fiber optic cable for telecommunications transmissions has the unintended effect of impacting a larger segment of the population should an outage occur. Furthermore, buried fiber is also more difficult to field locate than bundles of copper.

There are Best Practices in place to help mitigate outages of this nature, and Focus Group 1C believes increased attention to this critical element should be considered.

Vulnerability #2: Power Elements

Power Sources
Analysis reveals that interruption of power for essential hardware elements (such as DACS) contributes to current outage experiences. These are high capacity concentration points that appear to create opportunities for single points of failure. Environmental situations such as fire, flood, and lightning can all cause the loss of commercial power either at the public safety answering point or in a critical component of the service provider network, such as the Mobile Positioning Center (MPC) or a central office.

It is important to follow Best Practices regarding the maintenance of back-up power sources to ensure that they are operational when needed.

Vulnerability #3: Common Control Signal Isolation

While a number of outages were reported as Common Control Signal (CCS) failures, it would appear the root cause of the failure was related to the supporting network element. There are Best Practices in place addressing diversity that can be specifically applied to address this vulnerability. Examples include:

- Employment of dual network elements deemed to be critical infrastructure
- Auditing of diversity on a regular basis to ensure optimum levels are maintained over time
- Maintaining link diversity

Vulnerability #4: Local Switch/Selective Router

Local Switch

Local switch outages affect the ability to dial 9-1-1 as well as other services. Multiple Best Practices affect the reliability of the end-serving central office, and by extension 9-1-1 reliability. Therefore the implementation of Best Practices that improve office reliability will also improve overall 9-1-1 reliability.

Selective Router

The potential vulnerabilities associated with the 9-1-1 network selective router are similar in nature to those for local switches. Preventative measures such as dual switches, redundant power, and diversity in critical network elements, if deployed, can reduce the number of outages related to selective routers.

All Vulnerabilities: Incorporating Best Practices into Processes & Procedures

Understanding and applying existing NRIC Best Practices may be the best opportunity to diminish the potential vulnerabilities within 9-1-1 networks and reduce related outages. In many of the outages reviewed in the analysis, the problem was not that a Best Practice could not be identified to prevent the outage situation, but that the identified Best Practice was not applied. In many cases the carrier noted multiple Best Practices which, if applied, might have precluded the outage. It is recommended that companies continue incorporating Best Practices aimed at addressing potential vulnerabilities thus minimizing the occurrence and/or impact of an outage.

Best Practices should also be applied by Public Safety entities. NRIC V and VI appropriately provided guidance to Public Safety with regard to Best Practices that fell within the purview of Public Safety's jurisdiction. Education of Public Safety entities on the applicable Best Practices related to network design,

standards, ongoing observance of maintenance, and components within and under the control of the Public Safety entity should be encouraged. Although the Best Practices are typically carrier deployed, there is a clear role for Public Safety to analyze PSAP internal networks and procedure to ensure they are also using redundant or diverse facilities where possible.

Best Practices are typically followed by the carriers, however, deployment of redundant or diverse facilities are based on three factors:

1. The availability of the facilities
2. Up front coordination with the carriers, and
3. Fiscal support for additional facilities

5.2.3 Findings

In summary, through its analysis, Focus Group 1C determined that the most vulnerable areas of the network are:

- Vulnerability #1, Facility– affected by 47% of the 9-1-1 outages
- Vulnerability #2, Power Elements – affected by 16% of the 9-1-1 outages
- Vulnerability #3, Common Control Signal – affected by 14% of the 9-1-1 outages
- Vulnerability #4, Local Switch / Selective Router, affected by 9% & Selective Router – affected by 4% for a total 13% of the 9-1-1 outages

5.3 E9-1-1 Network Failure Notification for Callers

5.3.1 Background

Network design currently provides for audible messaging to callers in certain cases where call delivery cannot be accomplished. These are commonly a busy signal when the called number is unavailable and a fast busy signal when there is congestion or other unavailability of network components. Although these "messages" are generally recognized by telephone users and are clear indicators of call failures (even noted on TTY displays as flashing light call progress indicators), they offer no direction or automatic alternative access to emergency services.

Currently, Public Safety organizations rely heavily on tools such as the Emergency Alert System ("EAS"), mass calling systems, and the media in general, i.e. radio and television, for notifying the public of emergency situations and of E9-1-1 network failures.

5.3.2 Analysis

Network Evaluation

An evaluation of the architectures and capabilities of both the PSTN and the Public Safety network was made by Focus Group 1C. While intertwined, each has its own distinct functionality and responsibility.

PSTN architecture and functionality regarding the E9-1-1 system was examined. As stated in the earlier analysis, outages of the E9-1-1 system can be due to disruptions to the network in general but are most frequently isolated to a particular element or component of the network. After an evaluation of the current network architecture and the physical and functional attributes of the elements within that architecture, the Focus Group determined that there is no current capability within the existing PSTN that allows for notification messages to be inserted, much less delivery of a message which can communicate to the caller the circumstances preventing call completion to the PSAP or offer an alternative access method. If such capabilities were implemented, it would require a collaborative intervention that would re-route the E9-1-1 call to a recording appropriate to the given outage.

The architecture, capabilities and functionality of the E9-1-1 system in general and the PSAPs in particular were examined next. In any circumstance, and independent of the proposed network caller notification, a notification process is generally in place for the network service provider to notify the impacted E9-1-1 jurisdiction or designated PSAP(s) of any outage in the network, so they, in turn, can determine an appropriate course of action. Even though it is the E9-1-1 jurisdiction or impacted PSAP that ultimately determines the appropriate course of action, close cooperation among the affected network service providers, E9-1-1 service providers, and Public Safety Authorities (PSA) is needed so PSA managers can assess the nature and extent of the outage and determine the best way to provide an alternate means to access public safety services and notify impacted customers of the situation.

5.3.3 Findings

E9-1-1 network failure notifications are necessary to inform the public that the system is unavailable, and also to inform the public as to what actions can be taken to ensure access to available public safety services until such time as normal E9-1-1 services can be restored. For any message to be useful from the caller's perspective, the message should provide the caller with instructions on obtaining alternate access to emergency services and, if possible, make allowances for differences in language, (e.g., Spanish, French, etc.). It would, in

effect, need to be a message that replaces the established "dial 9-1-1 in an emergency" with a different set of instructions. This more expansive view of messaging during E9-1-1 network failures, while necessary to evaluate the impact to all parties, must also take precautions against creating additional network capacity issues at a time when it can least afford the additional processing and holding times that might be required.

There is no current network capability which provides for the delivery of messages to individual callers concerning a major failure within the E9-1-1 networks beyond tones indicating the unavailability of the network. At present, the most common indicator to a caller of a call failure is a reorder tone (a fast busy signal). While some failures will initiate a re-route to a recorded message, in general, broadcasting of messages providing the public with alternative access to public safety services currently must be generated outside of the PSTN. Because any given E9-1-1 network failure will be unique, given the many variables such as the area impacted, the capabilities of Public Safety to provide alternate access to emergency services, the extent and duration of the outage, and the demographics of the population served, any notification generated needs to be event specific and must take into consideration both network provider and PSA needs. Critical elements of the notification process are prompt notification to the PSA as outages occur and PSA / network service provider collaboration in planning for and accomplishing an effective response. In general, the Public Safety sector has systems already in place for alerting the public of special circumstances and emergency situations. Currently, the most effective way to inform the calling public of E9-1-1 outages due to network failures is by utilizing these public safety notification systems.

The PSA is perfectly positioned to assume the role of informing the public of alternate methods for accessing Public Safety services. PSAs commonly have the capabilities to deliver messages to the public within their existing emergency notification tools. In particular, the FCC has authorized the use of the Emergency Alert System (EAS) for E9-1-1 outage notification. This capability does not necessarily rely on the PSTN.

EAS has a number of approved uses for notification of extraordinary events impacting the public. One of the uses approved by the Federal Communications Commission is notification of E9-1-1 outages via a radio broadcast. (Section 7.3references a file containing the FCC rules regarding the use of EAS during a 9-1-1 outage situation.) This particular approach has the advantage of not relying on the connectivity to the PSTN by the radio and television stations who will broadcast the message. In addition to a direct message, the EAS alerts the media to outages and in turn, the media does what it does best by turning events into "breaking news" thus widely spreading the information. The message is usually

generated based on Public Safety requirements. Additionally, EAS is tested on a regular basis and therefore there is high confidence that it is reliable and that people know how to use it. Furthermore, alerting the media to a given situation creates additional opportunities for expanding notification via interrupted programming and/or live interviews by leveraging the media's interest in informing the public of the situation and steps the public should be taking. The notification messages are developed cooperatively among involved network service providers and affected PSAs to ensure accurate information is conveyed. Effective notification may involve several different length messages tailored to the time allowed. The audio portion of EAS messages is limited to about 15 seconds, instant message service text or freeway billboard messages must be distilled to a few key words in order to convey meaning on a tiny display or in a short read-time, while a television or radio interview can get 3 or 4 minutes of information to the public.

Commercially available automated dialing systems are another tool to notify the public of emergency or crisis situations. An automated dialing system literally calls all landline phones in an impacted area delivering a message specific to the situation. These automated dialing systems utilize the same information databases used by E9-1-1 and the PSAPs. This allows for a comprehensive and effective notification process for a given geography. Care must be utilized in employing these systems to preclude negative impacts on network capacity such as switch overload, including notifying carriers of the pending broadcast (BP 3202). These are purchased services that require significant implementation and pre-planning, and are not universally available. The cost/benefit evaluation by the PSA determines the availability of this service in a particular jurisdiction.

Service impacting outages should be anticipated and contingencies planned for when deploying and maintaining a reliable and robust E9-1-1 network. It is in the public interest that all parties engaged in providing E9-1-1 services work together to notify the public in the event of an outage. The resources of both the network service providers and the Public Safety sector can be used in concert to limit the impact on the public while building confidence in the situation management capabilities of both.

5.4 Consideration of Redundant E9-1-1 Selective Routers and Alternate PSAPs

5.4.1 Background

In general, the deployment of redundant E9-1-1 Selective Routers and alternate PSAPs are considered to be industry Best Practices. Both are addressed in the NRIC Best Practices as follows:

6-6-0571[13]
Dual Active 911 Tandem Switches - Dual active 911 tandem switch architectures enable circuits from the callers serving end office to be split between two tandem switches. Diverse interoffice transport facilities further enhance the reliability of the dual tandem arrangement. Diversity is also deployed on interoffice transport facilities connecting each 911 tandem to the PSAP serving end office.

6-6-0568[14]
Option 1: Alternate PSAPs from the 911 Tandem Switch - A common method of handling PSAP-to-Tandem transport facility interruptions is to program the 911 tandem switch for alternate route selection. If the 911 caller is unable to complete the call to the PSAP, the tandem switch would automatically complete the call to a pre-programmed directory number or alternate PSAP destination. The alternate PSAP may be either administrative telephones or another jurisdiction's PSAP positions, depending upon the primary PSAP's pre-arranged needs.

Option 2: Alternate PSAPs from the Serving End Office - Another method of handling PSAP-to-Tandem transport facility interruptions is to program the end office for alternate route selection. If the 911 caller is unable to complete the call to the PSAP, the end office may automatically complete the call to a pre-programmed directory number or alternate PSAP destination. The alternate PSAP may be either administrative telephones or another jurisdiction's PSAP positions, depending upon the primary PSAP's pre-arranged needs.

The results of Focus Group 1C's E9-1-1 outage analysis identified NRIC Best Practice 6-6-0568 as a Best Practice that would have addressed the E9-1-1 component of the outage in 25% of the outages reviewed if it had been implemented.

However, Best Practices by their very nature are voluntary and the decision to deploy either redundant selective routers or an alternate PSAP should be made on an individual basis after all relevant factors are considered. The

[13] Focus Group 1C has recommended modifications for NRIC Best Practice 6-6-0571 in Section 8.4 of this report.
[14] Focus Group 1C has recommended modifications for NRIC Best Practice 6-6-0568 in Section 8.4 of this report.

considerations for implementation are situational depending on the jurisdictions and demographics, and those experts performing the evaluation should prioritize the considerations as appropriate for their situation.

5.4.2 Analysis and Findings

While the Charter specifies that redundant E9-1-1 tandems and alternate PSAPs should be considered to avoid a ""fast busy" or a recorded message when one or more non-redundant network elements fail", Focus Group 1C believes that this is just one reason to consider implementing either of these options, and as such has produced a list of factors to be considered in making this decision, regardless of the reason for potential implementation.

The factors and considerations listed below are not necessarily all inclusive, and ultimately it is up to the expert performing the evaluation to identify which factors and/or considerations apply to his/her individual situation, and to assess each of those factors and/or considerations accordingly. Different situations may result in different outcomes, and therefore, it is important that these factors are evaluated for each individual case. For example, while in some cases the deployment of redundant selective routers may increase diversity, in other cases the lack of diverse paths out of a central office may limit the diversity benefits of dual routers.

Factors for Consideration in Providing Redundant Selective Routers

Category	Factor	Considerations
Costs	Cost/Benefit Analysis	Potential Costs • Cost of advance implementation versus deployment during a crisis • Restoration costs (how long will it take and what will it cost if equipment goes down) • Number of selective routers needed to serve area (e.g., possibility of decreasing number of selective routers (and thereby cost) while still increasing diversity) • Cost of default routing circuit requirements caused by switch entities serving multiple agencies (increased cost with dual routers) • Cost of additional PSAP circuits if the existing capacity is duplicated for connections to each SR • Existing number of PSAP circuits can be split between two SRs reducing cost but it will also reduce capacity in the event of a

		failure. Potential Benefits • Likelihood of achievement of increased diversity • Ability to increase resistance to known vulnerabilities and possibly decrease in outages • Increased public trust, especially in the event of a disaster • Ability to focus on other issues during disasters
	Cost / Labor of Maintenance	• Flexibility in switch and day-to-day equipment maintenance • Increased cost of diversified trunking
	Political Cost (of failing to have backup)	• Public trust of government to support them in times of crisis • Personnel time invested in answering questions for authorities, media, public • Image of Public Safety Authorities and local Government
Vulnerabilities	Location	• Vulnerability of outside plant to weather and human access • Public / known place (e.g., sheriff's office) versus unadvertised location
	Signaling (SS7 / MF)	• Diversity on SS7 control links • Delivery of abbreviated dialing calls (e.g., 9-1-1) in the event of SS7 failure • Mated STPs • Redundant SS7 connections between end central offices and STPs • Physical route and carrier system diversity of SS7 data links • Engineering threshold capacity
	Traffic	• Results of traffic studies o Network & equipment o Trunking studies to router o Router to PSAP o Signaling • Blockage • Network design
	Geography and Geological	• Flood plains, sinkholes, susceptibility to earthquakes, tornados, and hurricanes

	Factors	• Proximity to hazardous material sites • Levee stability • Susceptibility to street flooding
	Network Configuration	• PSAP trunking quantities • Configuration of network to the selective router • Likelihood that diversity of engineered network will be minimized over time
	Cause and Number of Outages	• Likelihood that outages could have been alleviated with redundant selective routers • Duration, severity and number of people affected by outages • Risk assessment – probability of having a problem with the selective router
Network Issues	Effects of Consolidation	• Potential decreased capital expenditures and operating expenditures to carriers, PSAPs, etc. • Possible increased vulnerability due to less equipment (e.g., switch, building) or further distance from selective router (i.e., transport mileage)
	Availability of Selective Routing Services	• Cost/feature options available to make the switch a selective router
	Diversity	• Likelihood that diversity will be assured and that selective routers will be deployed in a geographically diverse manner • Ability to engineer diversity (e.g., available alternate routes at acceptable cost) • Ability to attain transport redundancy from end office to selective router • Ability to attain transport redundancy from selective router to PSAP • Reduced chance of removing engineered diversity over time due to facility churn
	Facility Issues	• Availability of facilities across LATA boundaries (while carriers are not prohibited from providing connectivity across LATA boundaries, suitable offices may not be available to house selective routers) • Likelihood of increased cost and

		complexity (e.g., may need to go to long distance carrier for facility)
	Eminence of IP based E9-1-1	• Timing of local conversion to IP-based E9-1-1 network • Design engineering of IP based network (i.e., is engineering standard equal to current level of network redundancy / diversity)
	Alternatives	• Back up router to be deployed if existing router goes down • Ability to reroute to alternative selective router (time, engineering) • Availability of basic 9-1-1 default routing from end serving office to PSAP • Ability to reroute calls to local call box[15] in central office for dispatching • Other options available for improving survivability

Focus Group 1C has enumerated below both the factors in deciding whether an alternate PSAP should be provided, and the items that should be taken into consideration in determining which PSAP should be used as an alternate once the decision to use one has been made.

Factors for Consideration in Providing Alternate PSAPs

Category	Factor	Considerations
Network Vulnerabilities	PSAP System	• Ability to engineer PSAP system to allow reroute within the building
	Traffic	• Traffic patterns to know which PSAPs can act as backups
	Diversity	• Geographic diversity between PSAP and proposed alternate • Network diversity between PSAP and proposed alternate
	Outages	• Duration, severity and number of people affected by outages • Likelihood that people could have reached an alternate PSAP during these

[15] Call box is a device external to the end serving central office to which 9-1-1 calls can be routed. Designated personnel can take the calls at this location and dispatch accordingly via car radios or other means.

		outages
Coordination / Capabilities	Coordination between Jurisdictions	• Relationship between management of both PSAPs • Understanding of protocols of originating PSAP • Ability to share labor without creating problems (e.g., unequal pay between staffs) • Ability to develop guidelines that support labor agreements • Extension of liability protection to alternate PSAP
	Call Handling	• Ability to handle call load • Access to informational resources necessary to process calls (e.g., mapping capabilities for jurisdiction) • Ability to add idle capacity if necessary
	Dispatching	• Ability to dispatch the emergency services of other jurisdiction • Dispatch limits (are they acceptable?) • Radio communications to local responders (are they available and adequate?)
Alternatives	Sites / Messages	• Availability of alternate sites that are not PSAPs (e.g., police precinct, fire station) • Acceptance by public of receiving a "fast busy" instead of a person when equipment fails (as opposed to during times of congestion, when a busy signal is an acceptable indication that the PSAP is, in fact, busy)

5.5 Best Practices for 9-1-1/E9-1-1, Public Safety and Emergency Communications

5.5.1 Background

Initially, Focus Group 1C examined a total of 58 existing NRIC Best Practices that were seen as directly impacting E9-1-1 and Public Safety. The Focus Group then identified one additional Best Practice that met this criterion, bringing the total to 59. The Focus Group conducted a qualitative survey among its member companies to determine how effective these Best Practices are in addressing emergency communications in general, and by extension E9-1-1 networks and Public Safety. Based on the results of this survey, the Focus Group has made

recommendations for additions, deletions and changes to the existing NRIC Best Practices aimed at Emergency Communications.

5.5.2 Analysis

In conducting the analysis, it became evident that each Best Practice fell into one of the following three classifications of effectiveness.

Effective: Focus Group 1C determined that nine of the Best Practices developed to address E9-1-1 and Public Safety were effective in addressing the robustness of emergency communications networks.

For a Best Practice to be considered effective, the Focus Group determined that it met one or more the following criteria:

- Is currently implemented by numerous parties
- Is technically feasible to implement
- Has contributed to:
  - Reduction of 9-1-1 outages
  - Improved emergency response
  - Delivery of critical information to the public or Public Safety
- A more effective Best Practice does not exist

Effective – Needs Modification: Focus Group 1C determined that 43 of the Best Practices developed to address E9-1-1 networks and Public Safety were generally effective in addressing emergency communications, but required some editing or updating to ensure current applicability and accuracy. Planned changes to Best Practices include:

- Standardization of language into Best Practice format
- Clarification of existing language
- Updating of references to include current information
- Inclusion of additional responsible parties
- Elimination of duplication
- Broadening of focus
- Narrowing of focus
- Separation of multiple issues

No Longer Effective – Recommend for Deletion: Focus Group 1C also determined that seven of the Best Practices developed to address E9-1-1 networks and Public Safety are no longer effective. These Best Practices were considered to be no longer applicable and should therefore be deleted. New developments that made the Best Practices obsolete included:

- New network architectures
- Regulatory changes

Section 8.4 of this report contains the Best Practices that were reviewed for effectiveness for Emergency Communications.

5.5.3 Findings

The Focus Group found that the Best Practices for 9-1-1 networks, Public Safety and emergency communications are generally applicable and effective.
Of the 59 Best Practices reviewed by Focus Group 1C, 88% were considered "Effective" or "Moderately Effective" by virtue of their contribution either to reducing 9-1-1 outages, improving emergency response, delivering critical information, or some combination of the three. While considered effective, the application of these Best Practices was recognized, nonetheless, as being situational depending on such factors as demographics, geography, available technology, carrier and PSAP resources, and the availability of infrastructure.

Historically, the Best Practices have had a strong carrier focus. The recent direct participation by Public Safety in the NRIC process led to the acknowledgement that Public Safety plays a significant role and shares responsibility in the collective management of emergency communications systems and networks. Thus, the Focus Group determined that many of the "Effective" Best Practices currently aimed at traditional telecommunications industry players apply to PSAPs. To that end, the Focus Group has suggested wording to extend some of the existing Best Practices to include Public Safety, where relevant. The Focus Group recommends that this inclusion of Public Safety in the Best Practices be continued through future NRICs and industry forums.

Finally, several key procedural issues were identified that the Focus Group considered as it worked to make the 9-1-1 and Public Safety Best Practices even more effective.

- Some of the existing emergency communications Best Practices are long, complex and at times, rather ambiguous. The Focus Group has simplified these and modified them to conform to Best Practice format.

- Several emergency communications Best Practices are duplicative of one another or contain a substantial overlap of issues. The Focus Group has tried to ensure that very similar issues are addressed in one, definitive Best Practice, where this can be accommodated.

- Some of the Best Practices addressing emergency communications are also being reviewed by other Focus Groups. Cross Focus Group coordination is necessary to assure that conflicting changes are not proposed to the Council, while ensuring that the concerns of all parties are addressed. In some cases where the Focus Group agreed with changes recommended to a Best Practice by another Focus Group, Focus Group 1C deferred to the other Focus Group. These Best Practices are included in this report, but are highlighted as being reviewed by multiple Focus Groups.
- When reviewing the Best Practices, the Focus Group found it helpful to refer to the rationale and history behind the Best Practices, when available. The Focus Group worked to include similar data with the updates it recommends for NRIC VII.

The Focus Group determined that the survey would only measure impact to 9-1-1 networks, PSAPs, emergency management, and Public Safety entities. Based on this defined focus, the Focus Group determined that numerous Best Practices listed in its September 2004 report were outside the scope of the intended analysis and were therefore removed from the survey. Also, some additional existing Best Practices were identified as being relevant to the task and were included in the review, bringing the total number of Best Practices reviewed to 59.

The complete list of Best Practices reviewed, along with the recommended modifications and deletions can be found in Section 8.4. Following is a summary of the results:

- 7 of these Best Practices were rated as effective
- 43 of these Best Practices were rated as generally effective, but were deemed to require some degree of modification or updating.
- 9 of these Best Practices were rated as no longer effective and are recommended for deletion
- 2 new Best Practices were identified and are recommended for inclusion in the NRIC Best Practices database

6 Conclusions

9-1-1 has evolved over time and is now considered an essential element of providing telecommunications service. This is demonstrated by the recent FCC requirements for VoIP providers to make 9-1-1 services available to their customers. Customers expect to be able to reach help when they dial 9-1-1, and

with consistent implementation of Best Practices, 9-1-1 outages can be minimized and customer expectations met.

9-1-1/E9-1-1 Outages

Based on its analysis of reportable outages impacting 9-1-1/E9-1-1, Focus Group 1C concludes that telecommunications networks are extremely reliable and that when implemented, Best Practices can go a long way toward reducing the impact of outages on 9-1-1/E9-1-1 service.

The reported causes of most outages are addressed in Best Practices. In 40% of the outages, there was no unique Best Practice that would have prevented the 9-1-1 component of the outage; however, in each of these cases there are Best Practices that address the cause of the overall outage. In another 37% of the outages, the 9-1-1 portion of the outage could have been prevented or mitigated if Best Practices regarding diverse routing or automatic rerouting had been followed.

In general, Focus Group 1C found that previous NRICs have for the most part addressed potential vulnerabilities with Best Practices, and that there were few gaps that needed to be addressed. In the cases where there were gaps, Focus Group 1C has recommended modification to existing Best Practices or new Best Practices to address these gaps. An example is the addition of wording to recommend "testing" of alternate routing plans to address the instances where alternate routing was in place but failed, causing a 9-1-1/E9-1-1 outage.

Finally, even if Best Practices to mitigate 9-1-1/E9-1-1 outages are followed, it is still possible that customers will not be able to place a call to 9-1-1 due to outages elsewhere in the network. This underscores the importance of considering the implementation of Best Practices across all network elements to ensure reliable access to 9-1-1/E9-1-1.

E9-1-1 Architecture Vulnerabilities

Focus Group 1C found that two key vulnerabilities affected 63% of the 9-1-1/E9-1-1 outages. These were in the network facilities and power elements. Focus Group 1C concludes that Service Providers, Network Operators and Public Safety Authorities should focus on addressing known vulnerabilities and anticipating new vulnerabilities in order to strengthen the network, making it more prepared to handle threats. While the initial focus may be on addressing vulnerabilities that have been shown to be affected by outages, other known vulnerabilities should be mitigated before problems occur.

E9-1-1 Network Failure Notification for Callers

There is no current network capability which provides for the delivery of messages to individual callers concerning a major failure within the E9-1-1 network beyond tones indicating the unavailability of the network. Currently, the most effective way to inform the calling public of E9-1-1 outages due to network failures is by utilizing Public Safety notification systems.

Consideration of Redundant E9-1-1 Selective Routers and Alternate PSAPs

Focus Group 1C believes that callers dialing 9-1-1 will continue to call 9-1-1 if they experience a busy signal. While this is an acceptable response when the busy signal indicates that a PSAP is actually busy, valuable time can be wasted if a caller continues to call 9-1-1 hoping to get through when there is an outage. The deployment of redundant selective routers and alternate PSAPs can reduce the impact of network element failures. These options are consistent with other Best Practices that provide for redundancy and/or diversity to mitigate customer impact during outages.

At the same time, it should be noted that the effectiveness of redundant routers and alternate PSAPs in mitigating 9-1-1 outages is dependent upon the location of the failed elements in the network. For instance, 22% of the 9-1-1 outages analyzed were caused by cable damage, which would prohibit a caller from reaching 9-1-1. This cannot be addressed between the end serving office and the customer via network design or redundant selective routers; it can only be addressed by the implementation of Best Practices (e.g., cable locates before digging).

It is therefore imperative to analyze the cause of problems before deploying a solution. Outages are not necessarily prevented by adding more network elements and/or diversity, as this might not mitigate the root cause of the outages.

Effectiveness of Best Practices

Based on its overall analysis, Focus Group 1C concludes that, when employed, Best Practices are generally effective in preventing E9-1-1 outages or mitigating the effect of outages on E9-1-1 services. Even though only three percent of the existing NRIC Best Practices address the role of Public Safety Agencies, it is recommended that the Public Safety Authorities and Network Providers collaborate on the implementation of Best Practices of mutual interest. Focus Group 1C believes 9-1-1 performance can be enhanced through continued cooperation between Public Safety Agencies and Service Providers and Network Operators, and that this should be reflected in future versions of NRIC Best Practices. Additionally, outreach efforts should be continued to inform and educate companies about NRIC Best Practices.

In closing, Focus Group 1C believes that the inclusion of Public Safety in the NRIC process has been beneficial and recommends that participation of Public Safety be continued in future NRICs.

7 Appendix 1—Sources and Documentation

7.1 Scrubbed outage data

See attached file entitled "FG1C_Appendix1_7.1_Scrubbed Outage Data.pdf"

7.2 47 C.F.R. § 63.100: Notification of Service Outage

See the attached file entitled "FG1C_Appendix1_7.2_47cfr63.100.pdf "

7.3 FCC 04-188 New Part 4 of the Commission's Rules Concerning Disruptions to Communications

See attached file entitled "FG1C_Appendix1_7.3_FCC-04-188A1.pdf"

7.4 EAS Rules Document

See the attached file entitled "FG1C_Appendix1_7.4_FCC EAS Rules," which captures Title 47, Chapter 1, Section 11 of the FCC rules regarding EAS.

7.5 Sources

Following are web links to sources referred to in this document:

- 47 C.F.R. § 63.100 - http://a257.g.akamaitech.net/7/257/2422/05dec20031700/edocket.access.gpo.gov/cfr_2003/octqtr/47cfr63.100.htm
- NRIC – www.nric.org
- NRIC Best Practices - http://www.bell-labs.com/cgi-user/krauscher/bestp.pl
- NRSC Direct and Root Cause Definitions - http://www.atis.org/NRSC/Docs/NRSCDefinitions.pdf
- New Part 4 of the Commission's Rules Concerning Disruptions to Communications, FCC 04-188 http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-04-188A1.doc

8 Appendix 2—Focus Group Analyses

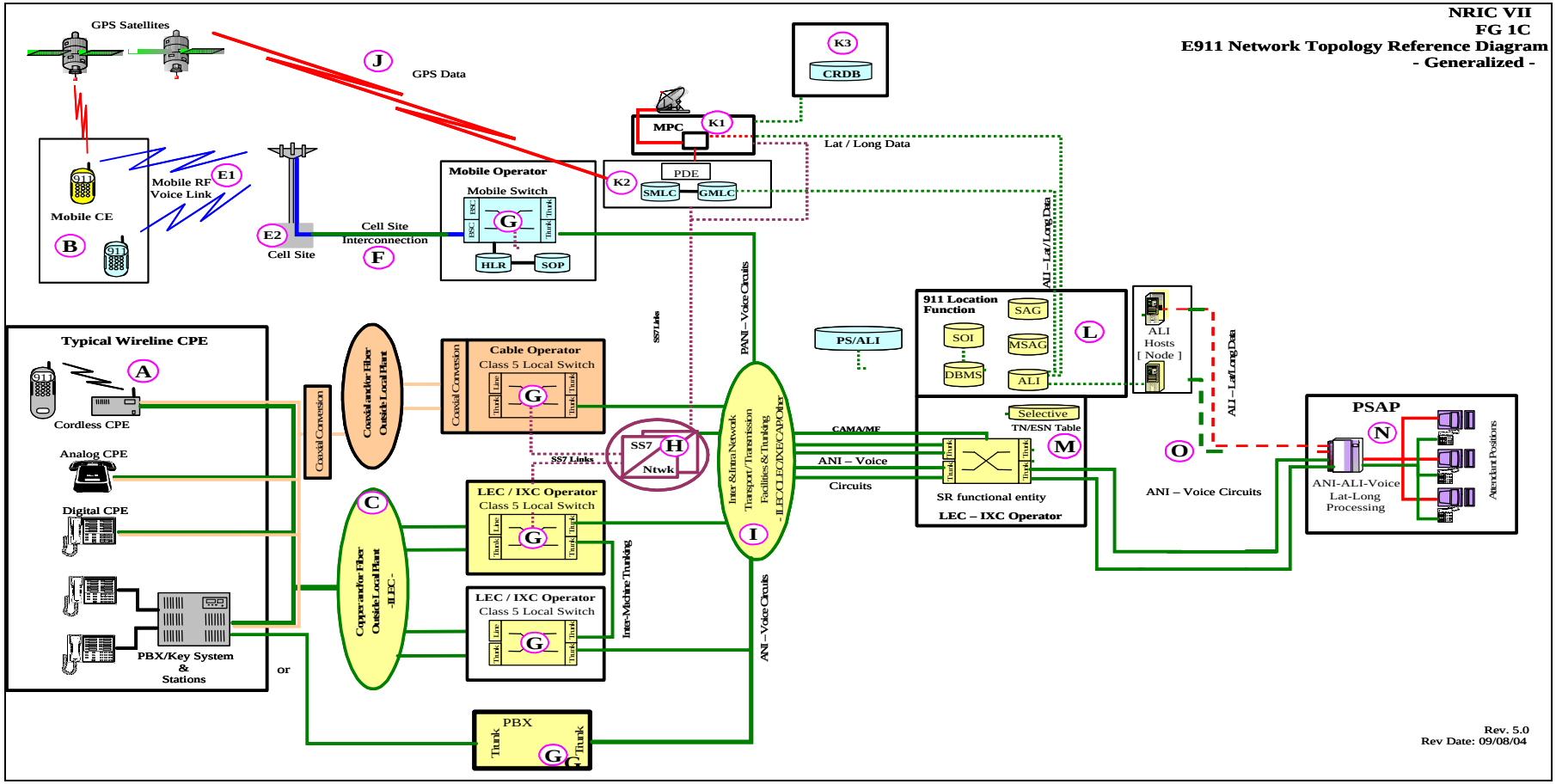
8.1 Network Component Analysis Table

The letters on the left correspond to the reference diagram in Section 8.2.

The question is what message should be delivered to E9-1-1 callers when E9-1-1 is unavailable. It is assumed that the objective is to determine what options, if any, exist to provide the caller a verbal/audible message indicating that 9-1-1 service is unavailable and suggest alternatives to E9-1-1 for contacting Public Safety Services. The primary purpose of this table is the cross-referencing of information relative to what happens when E9-1-1 is dialed within various network failure scenarios and cataloging the notification options generally available. For purposes of this discussion it is assumed that there exists a network failure with no contingency or back-up provisions in place.

	Potential Point of Failure	Potential 9-1-1 dialing results	Potential Network Generated Notification	Public Notification Option
M	Selective Router	Fast Busy Signal	Network generated reorder tone.	Yes, for geography served by SR
O	Selective Router to PSAP	Fast Busy Signal	Network generated reorder tone.	Yes, for geography served by PSAP
N	PSAP	Network Busy Signal, Ring with No Answer, No Ring No Answer - Situation specific	Network generated reorder tone, Ring with No Answer - Situation specific	Assuming PSAP aware…Yes for geography served by PSAP
	Call originators equipment	Situation Specific	None	None
A	Transport from call originator to Central Office	No dial tone, dialing unavailable	None	Yes, for impacted geographic area
C	Remote Central Office Failure	No dialing available. Possible no dial tone.	None	Yes, for impacted geographic area
C	Umbilical from Remote Central Office to Host Central Office	Fast Busy, with routing to a 10 digit number, slow busy	Network generated reorder tone.	Yes, for impacted geographic area
G	Central Office	No dialing available, no dial tone	None	Yes, for impacted geographic area
I	Transport from Central Office to Selective Router	Fast Busy Signal	Network generated reorder tone.	Yes, for geographic area served by Central Office and any remote offices
H	SS7 Network Signaling unavailable	Situation Specific - from no impact to no call initiation after dialing	Switch specific - Network generated reorder tone.	Yes, for impacted geographic area
E2	Cell Site	No service available	No service available or roaming indication	Yes, for impacted geographic area
F	Interconnection facility from Cell Site to Mobile Switching Center	No service available	No service available or roaming indication	Yes, for impacted geographic area
G	Mobile Switching Center	No service available	No service available or roaming indication	Yes, for impacted geographic area
I	Transport from MSC to Selective Router	Fast Busy signal	Network generated reorder tone.	Yes, for impacted geographic area

8.2 Network Topology Reference Diagram



8.3 Network Topology Diagram Reference Point Descriptions

Reference Point	Description	Comment I	Comment II
A	Wireline CPE	Customer Premises Equipment	
B	Wireless CE	Customer Equipment	
C	LEC Operator "Last Mile" Outside Plant	LEC (Incumbent or Competitive Provider) IXC / CAP / Other Transmission Facilities	-
D	Cable Operator Coaxial Outside Plant		
E1	Mobile CE to Cell Site RF Voice Link	Mobile customer equipment transmission to cell site	
E2	Mobile Operator RF Cell Site	Cell site	Reference E2 is not to be confused with the E2 interface utilized between wireless network and 9-1-1 service provider
F	Cell Site to Mobile Switch Backhaul	LEC (Incumbent or Competitive Provider) IXC / CAP / Other Transmission Facilities	
G	Wireline / Cable / Wireless Operator Switches	Class 5 Level Switches, PBX, or equivalent	
H	SS7 Network & Links	Reflects all operator and 3rd party provider STP's and Links	Use of SS7 signaling is optional; traditional methods utilize CAMA signaling
I	Intra & Inter Network Switching Transmission Facilities	LEC (Incumbent or Competitive Provider) IXC / CAP / Other Transmission Facilities	Class 4 Access Tandem
J	GPS Data	GPS data to PDE	Part of AGPS solution
K1	Mobile Positioning Center	Mobile Services Provider Interface	
K2	Position Determining Entity	Mobile Operator Equipment- contains mobile cell site data and calculates subscriber's calling location	
K3	Coordinate Routing Data Base	Database providing routing instructions on wireless call utilizing latitude & longitude translated to routing table for appropriate PSAP based on location data	
L	Wireline Operator E9-1-1 Location Function	Traditional E9-1-1 data processes supporting location information provided to PSAP on wireline 9-1-1 call	
M	9-1-1 Service Provider Selective Router	May or may not be a telephone central office	
N	Public Safety Answering Point - PSAP	Staff, Equipment, and Physical facility which performs PSAP defined responsibilities such as 9-1-1 call taking and public safety response dispatch	
O	PSAP to Operator transmission link	For use only with Public Safety	
SR	Selective Router	Equipment and software providing routing functions in the traditional E9-1-1 network	
SR 2	Selective Router routing instructions	TN / ESN Table or dynamic ALI	

8.4 Best Practices

Following is a complete list of the Best Practices evaluated by Focus Group 1C. Each Best Practice has been assigned a rating of Effective, Effective – Requires Modification, or No Longer Effective – Recommend Deletion. Those Best Practices identified as requiring modification are listed with the recommended new wording for each Best Practice. Those Best Practices recommended for deletion are listed along with the Focus Group's rationale for deletion.

Any Best Practice that has been reviewed by multiple Focus Groups and will be presented in multiple Focus Group reports is highlighted in green. Any changes or deletions recommended to these Best Practices are supported by all Focus Groups involved in the review.

Finally, two new Best Practices addressing gaps identified by Focus Group 1C are recommended for inclusion in the NRIC Best Practices database.

Best Practices rated as Effective (no modifications recommended)

Best Practice Number	Best Practice Wording (no changes)
7-5-0570	Intraoffice 911 Termination to Mobile PSAP - Commonly, the transport facility between the PSAP and the serving end office may not have facility route diversity. To accommodate instances where these facilities are interrupted or it becomes necessary to evacuate the PSAP location, some PSAPs have established mobile PSAP systems that may be connected to phone jacks at the serving end office. The phone jacks, although usually installed inside the end office for security purposes, are typically installed in an accessible location for ease in locating them during an emergency. Some PSAPs have prearranged with the serving LEC to permit a jurisdictional employee having an emergency vehicle (e.g., police car) equipped with radio capability to retain a key to the LECs' end office and to connect to an RJ-11 jack for 911 call interception. Another type of receptacle may be pre-installed in the end office for connection to a mobile PSAP.
7-6-1006	Service Providers, Network Operators and Equipment Suppliers should consider establishing a designated Emergency Operations Center. This center should contain tools for coordination of service restoral including UPS,

	alternate means of communications, maps, and documented procedures to manage business interruptions and/or disasters.
7-6-1007	Service Providers, Network Operators and Equipment Suppliers should consider establishing a geographically diverse back-up Emergency Operations Center.
7-6-1061	Service Providers, Network Operators, and Equipment Suppliers should ensure that Telecommunication Service Priority (TSP) records and data bases are reconciled annually.
7-6-3213	Service Providers, Equipment Suppliers and Public Safety Service and Support providers should work together to establish reliability and performance objectives in the field environment.
7-6-5226	Service Providers, Network Operators and Property Managers should maintain liaison with local law enforcement, fire department and other security and emergency agencies to ensure effective coordination for emergency response and restoration.
7-6-0619	All Service Providers and Public Safety Providers should develop and/or ensure that appropriate pre-plans with fire agencies exist for all equipment locations and provide automatic notification to local fire department.

Best Practices rated as Effective – Requires Modification

Best Practice Number	Recommended Best Practice Wording
7-7-0566	Service Providers and Network Operators should consider placing and maintaining 911 circuits over diverse interoffice transport facilities (e.g., geographically diverse facility routes, automatically invoked standby routing, diverse digital cross-connect system services, self-healing fiber ring topologies, or any combination thereof).
7-7-0567	Service Providers and Network Operators should spread 911 circuits over similar pieces of equipment to avoid single points of failure. They should also mark each plug-in level component and frame termination with a red tag to notify maintenance personnel that the equipment is used for critical, essential services and is to be treated with a high level of care.
7-7-0568	PSAPs and Network Providers should establish a routing plan so that in the case of a lost connection from the selective router to the PSAP, 911 calls are routed to an alternate answering point (e.g., alternate PSAP, appropriate telephone line).
7-7-0569	PSAPs and Network Providers should establish a routing plan so that in the case of a lost connection of dedicated transport facilities from the originating end office to the selective router, 911 calls are routed over alternate transport facilities (e.g., PSTN, wireless).
7-7-0571	Network Operators should consider deploying dual active 911 selective router architectures to enable circuits from the caller's serving end office to be split between two selective routers in order to eliminate single points of failure. Diversity should also be considered on interoffice transport facilities connecting each 911 selective router to the PSAP serving end office.
7-7-0573	Network Operators, Service Providers and Public Safety Authorities, should consider providing local loop diversity to the PSAP including the use of alternate technologies, (e.g., wireless, broadband). PSAPs should consider the availability of diverse local loop connections in the site selection for new PSAP facilities.
7-7-0574	Network Operators and Service Providers should remotely monitor and manage the 911 network components using network management controls, where available, to quickly

	restore 911 service and provide priority repair during network failure events.
7-7-0513	Service Providers and Network Operators should maintain a "24 hours by 7 days" contact list of other providers and operators for service restoration for inter-connected networks. Where appropriate, this information should be shared with Public Safety Service and Support providers.
7-7-0575	Network Operators and Service Providers should deploy Diverse Automatic Location Identification systems used in Public Safety (e.g., Automatic Location Identification and Mobile Positioning Center systems) in a redundant, geographically diverse fashion (i.e. two identical ALI/MPC data base systems with mirrored data located in geographically diverse locations).
7-7-0576	Network Operators and Service Providers should move network access for pre-planned high volume call events away from the 911 selective router.
7-7-0577	Service Providers, Network Operators, and Public Safety Agencies responsible for PSAP operations should jointly and periodically test and verify that critical components (e.g., automatic re-routes, PSAP Make Busy keys) included in contingency plans work as designed.
7-7-0578	Network Operators, Service Providers and Public Safety should actively engage in public education efforts aimed at informing the public of the capabilities and proper use of 911.
7-7-0579	Network Operators, Service Providers, and 911 administrators, and public safety agencies should routinely team to develop, implement, periodically test, evaluate and update as needed plans for 911 disruption contingencies (e.g., share information about network and system security and reliability where appropriate).
7-7-0580	Network Operators and Public Safety Authorities should apply redundancy and diversity (e.g., concepts set forth in Best Practices 6-5-0566, 6-5-0573), where feasible, to other network links considered vital to a community's ability to respond to emergencies. An order for these links would be placed by the Public Safety Authority. Security practices and concepts should be applied to the critical systems supporting Link Redundancy and Diversity.
7-7-0581	Service Providers and Network Operators should include automatic Location Identification (ALI) data for both

	traditional and alternate providers (e.g., Private Switch, CLEC, VoIP) in the ALI systems.
7-7-0582	Public Safety authorities should use 911 as the standard access code for emergency services (e.g., law enforcement, fire, EMS, hazardous materials).
7-7-0655	Network Operators and Service Providers should coordinate hurricane and other disaster restoration work with electrical and other utilities as appropriate.
7-7-0697	Network Operators, Service Providers, and Equipment Suppliers should employ an "Ask Yourself" program as part of core training and daily operations. This initiative is intended to reinforce the responsibility every employee has to ensure flawless network service. (See General Comments for additional details)
7-7-0758	Service Providers should, upon restoration of service in the case of an outage where 911 call completion is affected, make multiple test calls to the affected PSAP(s) to ensure proper completion.
7-7-1011	Service Providers, Network Operators, Equipment Suppliers and Public Safety Authorities should establish alternative methods of communication for critical personnel.
7-7-1037	Service Providers, Network Operators, Equipment Suppliers and Public Safety Authorities should use a disaster recovery support model that provides a clear escalation path to executive levels, both internally and to business partners.
7-7-3201	Service Providers and Public Safety organizations should jointly develop a response plan to notify the public, through the broadcast media, of alternate means of contacting emergency services during a 911 outage.
7-7-3202	The Service Provider and the Public Safety Agency or its agent that utilize Public Safety mass calling systems for emergency notification should have a pre-established procedure to notify all impacted network operators, prior to launching an alert event.
7-7-3205	Service Providers, Network Operators and Public Safety organizations should consider participating in standards bodies and other forums contributing to Emergency Telecommunications Services (ETS).
7-7-3209	CATV service providers, shall where practical, receive signals from local broadcasters via fiber as the primary

	source with automatic fail over to the off-air signal as the secondary source, to support public notification in disasters or emergencies.
7-7-3210	Emergency Operations Centers and PSAPs should consider obtaining connections to provide video (for viewing local weather and news information and monitoring distribution of information over EAS), and utilize that connection to provide diverse access to the Internet and telecommunications.
7-7-3211	Network Operators and Service Providers should develop and maintain operations plans that address network reliability issues. Network Operators and Service Providers should proactively include Public Safety authorities when developing network reliability plans in support of 911 services.
7-7-3212	Network Operators and Service Providers should consider including notification of Public Safety Authorities, as appropriate, in their trouble notification plans.
7-7-5078	Service Providers and Network Operators should receive automated notification upon the loss of alarm data and react accordingly.
7-7-5127	Service Providers, Network Operators, Equipment Suppliers and Public Safety authorities should provide a GETS (Government Emergency Telecommunications Service) card to essential staff critical to disaster recovery efforts and should consider utilizing Wireless Priority Service (WPS) for essential staff. Appropriate training and testing in the use of GETS & WPS should occur on a regular basis (i.e. in conjunction with testing of the corporate disaster recovery plan).
7-7-0512	Service Providers, Network Operators and Property Managers should perform periodic inspections of fire and water stopping where cable ways pass through floors and walls (e.g., sealing compounds).
7-7-0584	Service Providers, Network Operators and Equipment Suppliers and Government representatives [of the National Security Emergency Preparedness (NS/EP) community] should work together to support appropriate industry and international organizations to develop and implement NS/EP standards in packet networks.
7-7-0587	Government, Network Operators and Service Providers of critical services to National Security and Emergency Preparedness (NS/EP) users should avail themselves of the

	Telecommunications Service Priority (TSP) program and support / promote as applicable.
7-7-0599	Network Operators and Service Providers should conduct exercises periodically to test a network's operational readiness through planned drills or simulated exercises. The exercise should be as authentic as practical. Scripts should be prepared in advance and team members should play their roles as realistically as possible.
7-7-0615	Network Operators and Service Providers should test complex configuration changes before and after the change to ensure the appropriate and expected results.
7-7-1009	Service Providers, Network Operators and Equipment Suppliers should regularly conduct exercises that test their Disaster Recovery Plans. Exercise scenarios should include natural and man-made disasters. (e.g., hurricane, flood, nuclear, biological, and chemical)
7-7-1010	Service Providers, Network Operators and Equipment Suppliers should designate personnel responsible for maintaining Business Continuity and Disaster Recovery Plans.
7-7-1023	Service Providers, Network Operators, and Equipment Suppliers should identify essential staff within their organizations that are critical to disaster recovery efforts. Planning should address the availability of these individuals and provide for backup staff.
7-7-1031	Service Providers and Network Operators should consider entering into Mutual Aid agreements with partners best able to assist them in a disaster situation using the templates provided on the NRIC and NCS websites. These efforts could include provisions to share spectrum, fiber facilities, switching, and/or technician resources.
7-7-1033	Network Operators should develop a strategy for employment of emergency mobile assets such as Cellular on Wheels (COW), Cellular Repeater, Switch on Wheels (SOW), Transportable Satellite Terminals (RF equipment), Microwave, Power Generators, HVAC, etc., for emergency use or service augmentation for planned events, (e.g. national special security events (NSSE))
7-7-1058	Service Providers, Network Operators and Equipment Suppliers should work collectively with local, state, and federal governments to develop relationships fostering efficient communications, coordination and support for emergency response and restoration.

7-7-1063	Service Providers and Network Operators should set Initial Address Messages (IAMs) for congestion priority in accordance with applicable ANSI standards. This will ensure government emergency calls (911, GETS) receive proper priority during national emergency situations. Implementation in all networks should be in accordance with ANSI T1.111.
7-7-5204	Service Providers, Network Operators and Property Managers should ensure availability of emergency / backup power (e.g., batteries, generators, fuel cells) to maintain critical communications services during times of commercial power failures, including natural and manmade occurrences (e.g., earthquakes, floods, fires, power brown / black outs, terrorism). The emergency / backup power generators should be located onsite, when appropriate.

Best Practices rated as No Longer Effective – Recommend Deletion

Best Practice Number	Best Practice Wording	Reasons for Recommended Deletion
6-5-0572	Traffic Operator Position System (TOPS) as a 911 Tandem Backup - Operator services tandem switches can also serve as backup and / or overflow for network elements, due to their ubiquitous connectivity throughout the telephone network. In most instances, existing trunking and translations may be used when adding a TOPS to the 911 network. When an interoffice transport facility fails or an all-trunks-busy condition occurs, the backup / overflow route to the operator services tandem is selected. The operator tandem switch recognizes the call as an emergency by translating the 911 dialed digits, and may be preprogrammed to automatically route the call to the serving 911 tandem switch. Further, if the operator tandem switch is unable to access the 911 tandem switch, the call will automatically be "looped around" so that an operator may manually answer the call and manually attempt to reach an emergency services provider.	No longer a Best Practice. Today many TOPS switches are using SS7 so there is no longer a need for this.
6-5-0598	Develop crisis management exercises - Service Providers should, at a minimum, have a communications structure in place for timely notification of affected parties in the event of disasters or emergencies. During the past several years a number of disastrous events have prompted an increased awareness on the part of all members of the telecommunication industry to the critical need to have a	Superseded by NRIC Best Practices: 5239, 1001, 1002, 1004, 1005, 1006 and 0599

	Disaster Preparedness strategy. This strategy should outline a network Service Provider's Disaster Preparedness organization, the roles, responsibilities and training of its members and provide for cooperative interaction among both internal and external organizations. The purpose of this strategy is to provide for the development of emergency plans that protect employees, ensure service continuity and provide for the orderly restoration of critical services in the event of a major network catastrophe.	
6-6-1021	Service Providers, Network Operators, and Equipment Suppliers should provide disaster recovery contact information to the National Coordinating Center (NCC) and update this contact information as changes occur or at the direction of the NCC.	Superseded by Best Practice 8066
6-6-1057	Service Providers, Network Operators, and Equipment Suppliers should ensure deployment of Government Emergency Telecommunications Service (GETS) cards to appropriate Disaster Recovery personnel. Appropriate training and testing should be provided as necessary.	Superseded by NRIC Best Practice 5127
6-6-1059	Service Providers should work with government and other utilities in the development of State Emergency Communications Networks in order to provide a process for key utilities and government emergency responders to communicate during disaster events.	Not a Best Practice. ECN is a network run by States that requires payment to participate.
6-6-1062	Service Providers and Network Operators should establish and maintain an interface with local, state, and federal government agencies to ensure effective support is available upon request as part of disaster recovery.	Superseded by Best Practice 1058

6-6-5093	Service Providers, Network Operators, Equipment Suppliers and Property Managers should establish, implement and test emergency response and crisis management programs to include external first responders and civic authorities in mutual emergency preparedness planning, as appropriate (e.g., on-site visits, access to facilities, mutual familiarity with plans and procedures, single points of contacts). First responders may include Emergency Response Team (ERT), law enforcement, fire department, FEMA, NS/EP, DHS, etc.	Superseded by NRIC Best Practices: 5226, 1058 and 1059
6-5-0585	Service Providers, Equipment Suppliers and representatives of the National Security and Emergency Preparedness (NSEP) community should work together to share information regarding security issues related to packet network convergence with the PSTN, including identification and authentication procedures for emergency calls, and issues related to cyber attacks and malicious intrusion into networks.	Superseded by NRIC Best Practice 8066
6-6-1003	The Business Continuity Plan for Service Providers and Network Operators should address critical business processes (e.g., Call Completion, 911/Emergency Services, Provisioning, Maintenance, etc.), support functions (IT, Sourcing, Logistics, Real Estate, etc.) and key business partners.	Superseded by Best Practices 8132 and 8133

New Best Practices Recommended

Best Practice Number	Best Practice Wording
7-P-1068	Service Providers, Network Operators and Public Safety authorities should continue ongoing deployment of Wireless Priority Service (WPS).
7-P-1069	Service Providers and Network Operators should proactively include Public Safety authorities, electrical and other utilities when developing disaster restoration and prioritization plans.

9 Appendix 3 - Definitions and Acronyms

9.1 NENA Master Glossary of 9-1-1 Terminology[16]

See the attached file entitled " FG1C_Appendix3_9.1_ NENA Master Glossary.PDF"

9.2 NRSC Direct Cause and Root Cause Definitions

The below definitions were taken from the Network Reliability Steering Committee's (NRSC) Outage Reporting Direct and Root Cause Definitions document. NRSC is a committee of ATIS.[17] These definitions were used by Focus Group 1C in identifying the direct cause and root cause categories and sub-categories that could be applied to each of the outages in the outage analysis.

DIRECT CAUSE

Procedural - Service Provider

Failure to follow standard procedures/documentation
Work error by service provider 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 service provider personnel; includes errors in vendor documentation (i.e., faulty or unclear procedures or typographical errors); errors in service provider approved documentation (i.e., inadequate or inaccurate MOPs, in-house technical M&P, local drawings); use of

[16] www.nena.org
[17] www.ATIS.org

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; includes errors in vendor documentation (i.e., faulty or unclear procedures or typographical errors); errors in service provider 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 service provider 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 service provider, or the PCN was waived by the service provider, consider root cause procedural.

Hardware Failure

Random hardware failure not related to design, but due to the inherent unreliability of the system components. Includes failures of dc/dc converters or fuses embedded in switches and transmission equipment, unless the problem was caused by the power plant. 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 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 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 the entry of lightning into the system was caused by bonding and grounding violations, consider root cause procedural or design fault. If water damage was the result of cable pressurization failure, consider root cause procedural.

Man-made (vandalism, accidents)

External man-made conditions that exceed documented (or reasonable) service provider 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.

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.

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.

Temperature

Excessive ambient temperatures, excessive rates of temperature change. 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.

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 service provider / others' activities, consider root cause procedural.

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. 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

System 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.

Power Failure

Instances of outage directly related to failure of the external power system, or failures of service provider back-up power systems. Includes failures associated with commercial power, standby generators, building electrical systems, 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 service provider; 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. This category should be used when multiple procedural causes are reported

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

Documentation/procedures out-of-date unusable or impractical
Documentation / procedures not updated; correction / update available but not incorporated locally. 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.

Cable unlocated

Prior notification was provided by the excavator but the facility owner or locating company failed to establish the presence of a cable which was then eventually damaged.

Inaccurate cable locate

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

Other

Procedural - System Vendor

Insufficient training

Training not available from vendor; training not available from service provider; 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. This category should be used when multiple procedural causes are reported

Documentation/procedures unavailable, unclear, incomplete

Documentation or procedures (vendor or service provider) 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 service provider; 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. This category should be used when multiple procedural causes are reported

Documentation/procedures unavailable, incomplete
Documentation or procedures (vendor or service provider) 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/redundancy/diversity
System design with unnecessary aggregation of components or features; or system deployment with single-point-of-failure configurations.

Insufficient network redundancy/diversity
Network design with unnecessary aggregation of systems or network deployment (e.g., CCS network, self-healing rings) with single-point-of-failure configurations.

Other

Hardware Failure

Processor community failure

Memory unit failure

Peripheral unit failure

Other

External Environment (for limited use when applicable root causes actionable by service provider or vendor cannot be identified)

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 service provider plant, includes 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.)

Shallow cable

The cable was at too shallow a depth, (notification was adequate, locate 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, 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.

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).

Dirt, 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 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.

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.

Other

Power Failure (does not include failures of dc / dc converters or fuses embedded in switches and transmission equipment, which should be reported as a hardware failure, unless the problem was caused by the power plant.)

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.)

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.)

Lack of routine maintenance/testing

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

Overloaded/undersized power equipment

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

Lack of power diversification

Failure to diversify equipment among redundant power system components, including ac rectifiers / chargers, battery power plant, dc distribution facilities, etc.

Lack of power redundancy

Failure directly associated with insufficient redundancy of 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 had emergency operating procedures and contingency plans been available; outage was prolonged because of lack of site-specific information including equipment engineering data, portable engine hook-up hardware / procedures, load shedding plans, etc.

Extended Commercial Power Failure

System failure due to commercial power failure that extends beyond the design back-up capabilities at the location and beyond reasonable contingency planning assumptions.

Other

Operations Support/Strategy

Insufficient surveillance capability

System failure that could have been avoided / minimized had remote operations 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 had remote operations 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 had better communication and / or process control been in place between / among operations organizations.

Ineffective alarm threshold/display

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

Impractical trouble-correlation among operations systems

System failure that could have been avoided / minimized had output of disparate operations systems been better integrated / intelligible - unreasonable output language / naming convention differences among operations systems.

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.