# Appendix A

C

## Appendix A - NRC Issue Statement

**Issue Title:** Switching (Focus on Software)
**Author:** Mick McCarthy , Sprint

**Problem Statement/Issues to be Addressed**
As the switching environment has transitioned from electromechanical to a stored program control environment, the role of software in switching system reliability has become increasingly critical. Additionally, software inside switching machines is becoming more distributed, adding to the complexity of interoperability and synchronization.

Unlike hardware, software redundancy does not help software reliability since unknown bugs will appear in mated copies of the same software. Furthermore, software coded in low level languages for performance reasons lack the modularity of newer software architectures which provide a degree of compartmentalism that potentially lessens interoperability problems.

In addition to software architecture design, the team should consider other areas of analysis based on study of specific outage data. These may include, but should not be limited to such areas as software upgrades, hardware, procedural error (operator & supplier), technician expertise, testing, alarming, etc.

**Areas of Concern & Problem Quantification**

1. A Bellcore study of 346 switching outage events over a 9 month period during 1991 indicated 47% of all outages were the result of software design and/or software release installation and maintenance activities. These areas should be examined in greater depth.

2. Other specific areas of concern including the following:

   A. Effective software change management control is essential. In particular, corrective software changes (i.e., patches) must be designed with the highest software quality and tested thoroughly prior to implementation. Furthermore, forward and backward propagation of corrective software changes (i.e., patches) must be accomplished without service impact. Consider best practices in this area of software change management.

   B. Regression testing and integration testing in the switching system node and between networks are important areas to analyze. While integration testing is intended to ensure that software operates as designed, recent outages resulting from increasingly complex new software releases suggest that the extent and/or quality of testing may not be sufficient.

   C. With ever increasing dependencies on complex partitioned software and numerous distributed interlinked processors, it is critical that internal software and hardware be sufficiently robust to detect errors or mismatches, and take appropriate action before these errors or anomalies become significant.

   D. In the area of software architecture, consider whether current and emerging switching software architectures pose risks that can be mitigated or eliminated, and consider best practices in this area. Furthermore, to the degree that unique system supplier software implementations result in reliability risks, consider whether standards are complete, adequate, and timely.

**Description of Proposed Work**
Although early analysis would indicate software is a major contributor to switching outages, rigorous collection and analysis of all available data should be undertaken to confirm or dispute this assumption. The team working this issue should consider the following total quality process to quantify switching system vulnerability, identify major reliability issues and propose problem solutions.



C

1. Collect appropriate data from all available industry sources to determine and/or confirm areas of greatest criticality and risk, and with the greatest potential for switching system reliability improvement. Data should be collected on both the front end processors and the peripheral processors.

2. Perform sufficient analysis of the data to determine the root cause(s) of the problem(s), e.g., software release installation procedures. Sub-analysis should include:
   - Design shortcomings
   - Alarms
   - Alarm response
   - Procedures
   - Training
   - Documentation
   - Testing
   - Customer Education (Public service agencies, users, etc.)

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

4. Determine industry "Best Practices" for dealing with the root cause analysis findings and share this information with industry participants as soon as possible. Also consider cost/benefit tradeoffs of these "Best Practices."

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

6. Consider the following tactics/ideas offered by the Steering Team as potential means to address the findings of the root cause analysis. These represent ideas from the Steering Team which we want to share. They may be accepted or rejected by the switching systems focus team.

   A. Quality partnerships could be developed between system suppliers and users, and also among system suppliers. Targets could be established for the reduction of software errors. The procedures that are necessary to achieve these levels could be rigorously implemented by system suppliers in writing and testing software, among system suppliers for interface testing, and by users in integration testing and deployment.

   B. System suppliers could replace switch software with modular code that permits rapid, safe and reliable application development. Much of this effort is already encompassed in the move to Intelligent Network Architectures with Service Creation Environments. However, the transition must be carefully planned to prevent the introduction of new problems as the program is enacted.

   C. Consider ways for more rapid standards negotiation and development to minimize standards differences in the early phases of implementation.

   D. Software developers must expand the toolbox of tools (e.g., diagnostics, debug capabilities, etc.) provided to users. Too often, complex software systems are developed and sold with less than adequate automatic, as well as external manually exercisable diagnostic capabilities. These capabilities must be considered mission critical in that they are the last line of defense and present the opportunity to forewarn of more serious consequences.

**Existing Work Efforts**
Various switch suppliers and/or switch operators have been individually pursuing solutions to the above issues, including:

- development of plans to re-architect existing software to make it more modular.
- more thorough up-front testing of software prior to deployment.
- interconnection of testbeds and/or interconnection testing (e.g., NOF Internetwork Interoperability Test Plan – IITP Committee).
- testing operating system software using user provided applications software and data.

**Team Leader**
Will Smith - U S WEST

C

# Appendix B

Appendix B - Switching System Focus Area Data Request

## NRC Switching System Focus Area
## Service Provider Outage Data Request

### Instructions

**1. Purpose**

The purpose of this request for outage data is to collect outage information on switching systems from the service providers' perspective.

**2. Scope**

The scope of this request covers service providers' general switching system population data as well as specific data on individual outage events. The switching systems include end-office switches, tandem switches, toll switches, cellular switches, packet switches, and Service Control Points (SCPs).

Form 1 should be used to provide the population data for each type of switching system. This form should be completed only once for each service provider. Form 2 should be used to provide data on each outage event that satisfies any of the following conditions:

1. Switch-related outages reported to the FCC between April 1992 and September 1992, under the FCC's reporting requirement set forth in FCC Docket 91-273.

2. Total or partial outages[1] longer than 10 minutes on all types of switches due to all causes during the third quarter of 1992 (3Q92).

3. Total or partial outages of any duration on tandem switches, toll switches, and packet switches due to all causes during the first, second, and third quarter of 1992 (1Q92), 2Q92, 3Q92).

4. Total or partial outages of any duration on all types of switches caused by scheduled events[2] or retrofits during the first, second, and third quarter of 1992 (1Q92, 2Q92, and 3Q92).

**3. Description of Form 2**

Form 2 is similar to the existing Service Failure Analysis Report (SFAR) that is being used by some Bell Operating Companies to report and analyze switching system outages. Complete data for an outage event will be most advantageous. However, for the purpose of analyzing the root cause of an outage, Form 2 contains only a subset of the standard SFAR and has been expanded to include additional information regarding the outage. Each service provider should fill out one form for each outage event that satisfies the conditions mentioned in Section 2. The following contains a detailed description of the fields in the form.

- Field 1 - Report Number: A report number unique to the case assigned by the service provider.

---

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

[2] Scheduled events include all scheduled or planned manual initializations that result in outages, restarts, phases, etc. This includes activities such as: software/firmware change, patch application, memory allocation, feature activation , office data change, etc. Scheduled initialization that is used to clear an earlier trouble is not included in this definition. See Attachment A for additional information.



C

- Field 2 - System ID/CLLI Code: A unique system identifier or the 11-digit CLLI code for the entity.
- Field 3 - FCC-Reportable: Check the "Yes" box if the outage event meets the reporting requirement set forth in FCC Docket 91-273 for major service disruption. Otherwise, check the "No" box.
- Field 4 - Reporting Center Name: The name or identification of the reporting center (if available).
- Field 5 - Company Name: The name of the company issuing the report.
- Field 6 - Originator's Name: The name of the person originating the report (if available).
- Field 7 - Originator's Phone Number: The originator's telephone number (if available).
- Field 8 - System Location: the city and the state where the entity is located.
- Field 9 - Date of Incident: The date when the outage occurred.
- Field 10 - Time of Incident: The time (24-hour clock) when the outage occurred.
- Field 11 - System Name: The name of the system as given by the vendor.
- Field 12 - System Type: The type of the system whether it is a host end-office switch, a remote switch off a host, a packet switch, a tandem switch, a toll switch, a cellular switch or a Service Control Point (SCP).
- Field 13 - System Cutover Date: The date when the system was cutover to the service provider (if available).
- Field 14 - Software Generic/Version: The generic software program installed at the time of the outage.
- Field 15 - Software Load Date: The date when the generic software identified in Field 14 was loaded into the system (if available).
- Field 16 - Latest Patch: The most recent software patch or overwrite installed and activated in the system prior to the outage (if available).
- Field 17 - Equipped Terminations: The total number of equipped lines and trunks in the system.
- Field 18 - Total Outage Duration: The cumulative downtime of the system during a total outage.
- Field 19 - Partial Outage Duration: The cumulative downtime of the system during a partial outage.
- Field 20 - Terminations Affected: The number of lines and trunks affected by the outage.
- Field 21 - No. of Trouble Reports: The number of customer trouble reports received as a result of the outage (if available).
- Field 22 - Level of Assistance: The organization that provided technical assistance to recover the system (e.g., SCC, ESAC, vendor, etc.).
- Field 23 - Services Affected: The type of services affected by the outage (check all the applicable boxes or write in additional services affected).
- Field 24 - Description of Service Failure: A general description of the incident including a chronological discussion of events: (a) leading to the failure, (b) during recovery activities, and (c) in response to any

residual service effects following initial recovery. Specify all manual or system-initiated recovery actions.

- Field 25 - Causes of Failure: A detailed description of the causes of the outage. Use the categories in Fields 26 and 27 to assign a cause code.
- Field 26 - Classification of Major Causes: Use the categories provided to assign the code for the major cause. See Attachment A for a detailed description of the categories.
- Field 27 - Contributing Sub-Causes: Use the categories provided to assign the code of the sub-cause. See Attachment B for a detailed description of the categories.
- Field 28 - SFAC Recommendations: A description of the Service Failure Analysis Committee (SFAC) recommendations and plans for corrective or preventive actions (including time table, plans, or commitments) to: (a) prevent future occurrences, (b) lessen the impact of future occurrences, (c) speed recovery in future occurrences, or (d) improve the performance of the system.
- Field 29 - Specific information for "Scheduled Event" or "Retrofit" Outages: Answer the specific question for outages in the categories of "H: Scheduled Event" and "R: Retrofit" identified in Field 26 above.

**4. When and Where to Send the Response**

All the responses should be returned by November 9, 1992 to:

J. D. Healy
Bellcore
331 Newman Springs Road, Room 2X-227
Red Bank, NJ 07701
Telephone: 908-758-3065
Fax: 908-758-4344

Questions relating to this request can be directed to J. D. Healy.

**5. Future Plan**

It is likely that the industry would want to collect this type of outage information from service providers on a going-forward basis. So, if this type of data is not routinely collected today, we suggest that your company establish a data collection process to collect outage information so that it will be available for future use in NRC network monitoring and reliability analyses.

NRC Switching System Focus Area
Form 1 - Switching System Population Data Request - Service Provider

| System Name | Total number of systems in service within U.S. at the end of | | | |
|---|---|---|---|---|
| | 4Q91 | 1Q92 | 2Q92 | 3Q92 |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |



C

NRC Switching System Focus Area
Switching System Outage Data Request — Service Provider

| 1. Report Number | 2. System ID/CLLI Code | 3. FCC-Reportable<br>__Yes __No | 4. Reporting Center Name |
|---|---|---|---|
| 5. Company Name | 6. Originator's Name | 7. Originator's Telephone #<br>(  )  - | 8. System City & State |
| 9. Date of Incident<br>/  / | 10. Time of Incident (24hr clock)<br>:  : | 11. System Name | 12.SystemType:Host__ Remote__Tandem__Toll__ SCP__PacketSwitch__ Cellular Switch__ |
| 13. System Cutover Date<br>/  / | 14. Software Generic/Version | 15. Software Load Date<br>/  / | 16. Latest Patch/Overwrite |
| 17. Equipped Terminations<br>Lines: _____<br>Trunks: ___ | 18. Total Outage Duration<br>_____:_____:_____<br>HR MIN SEC | 19. Partial Outage Duration<br>_____:_____:_____<br>HR MIN SEC | 20. Terminations affected<br>Lines: _____<br>Trunks:_____ |
| 21. Durations of Restoration Actions (hh:mm:ss)<br>Detection: _Travel:_____<br>Repair: _____ | | 22. Level of Assistance<br>__ CO/SCC __ESAC __Vendor<br>__Other (Specify:_____) | |

**23. Services Affected** (Check all applicable boxes):
__a. Intra LATA Switch-to-Switch Call __b. Toll Calls to IEC __c. Intra-Switch (local) Calls __d. 800 Calls
__e. CLASS Calls __f. Alternate Billing Services
__g. Operator Assisted Service __h. Cellular Calls
__i. All Available Services __j. Not Service-Affecting
__k. Others (specify: _____ )

**24. Description of Service Failure**: Describe in detail the incident including a chronological description of events: (a) leading to the outage; (b) during recovery activities; (c) in response to any remaining service effects following initial recovery. Specify all recovery actions initiated on or by the system. (Add attachments if necessary.)

**25. Causes of Failure:** Describe the cause of the outage. Refer to the categories below and on the attached guidelines for outage classification.

**26. Classification of Major Causes:** Use the categories below to describe the outage cause (check appropriate box):



C

| | | | |
|---|---|---|---|
| __ A. Procedural—Telco | __ E. Design—Firmware | __I. Lightning Related | __ M. Remote facilities/Umbilical isolation |
| __ B. Procedural—System Vendor | __ F. Design—Hardware | __J. Traffic Overload | __ R. Successful Retrofit† |
| __ C. Procedural—Other Vendor | __ G. Hardware Failure | __K. Environmental | __ N. Unknown/Other (Specify: _____) |
| __ D. Design—Software | __ H. Scheduled Event† | __ L. Power Failure | |

**27. Contributing Sub-causes:** Check the appropriate box for the sub-cause that contributed to or prolonged the outage.

| | | |
|---|---|---|
| __a. Work Error – Operational | __j. Retrofit | __u. SS7 Unit |
| __b. Work Error – Data Entry | __k. Hardware Growth | __v. Clock Unit |
| __c. Work Error – Hardware | __l. Software Administration | __w. Database Error – Dynamic |
| __d. Documentation Error | __m. Firmware Administration | __x. Database Error – Static |
| __e. Fix Available – Not applied | __q. Central Control Unit | __y. Data Synchronization |
| __f. Recovery Action – Escalated | __r. Switching Fabric Unit | __z. Routine Exercise |
| __g. Defective Patch | __s. Peripheral Control Unit | |
| __i. Insufficient Data | __t. Line/Trunk Unit | |

† See next page for additional information regarding the outage.

**28. Service Failure Analysis Committee (SFAC) Recommendations:** State the Committee recommendations and plans for corrective or preventive actions, including time table, any plans, commitments, or recommendations to: (a) prevent future occurrences; (b) lessen the impact of future occurrences; (c) speed recovery in future occurrences; or (d) otherwise improve the performance of the system. (Add attachments if necessary.)

**29. Specific information for outages in the "H: Scheduled Event" and "R:Retrofit" categories:**
Answer the following questions for outages in the categories of "H: Scheduled Event" and "R: Retrofit" identified in Item 26 above.

- Why was the event undertaken?
  _a. New Customer (growth) _b. Change in engineering rules (growth) _c. Change in regulatory rules (i.e., equal access)
  _d. Implement new features _e. Stay within vendor support "window"
  f. Correct an error (specify:_____)
  g. Other (specify:_____)
- Was there an alternative to re-initializing the switch?
  _No _Yes (specify: _____ )
- When was the last time this switch was re-initialized for retrofit or scheduled event?
  Date: ___ Time: ___ Reason:_____
- Was this retrofit or scheduled event coordinated with retrofits/scheduled events in other switches?
  _No _Yes (how many switches were involved? ____)
- Identify practices, procedures, and strategies in use in **Item 28** above to minimize the number of scheduled outages and retrofits.



C

## NRC Switching System Focus Area
## Switching System Supplier Outage Data Request

### Instructions

### 1. Purpose

The purpose of this request for outage data is to collect outage information on switching systems from the switching system suppliers' perspective.

### 2. Scope

The scope of this request covers switching system suppliers' general switching system population data, specific data on individual outage events, as well as suppliers' plans to reduce the conditions that involve planned system re-initialization. The switching systems include end-office switches, tandem switches, toll switches, cellular switches, packet switches, and Service Control Points (SCPs).

Form 1 should be used to provide the population data for each type of switching system. This form should be completed only once for each service provider. Form 2 should be used to provide data on each outage event that satisfies any of the following conditions:

1. Total or partial outages[1] longer than 10 minutes on all types of switches due to all causes during the third quarter of 1992 (3Q92).

2. Total outages of any duration on all types of systems due to all causes during the third quarter of 1992 (3Q92).

3. Total or partial outages of any duration on all types of systems caused by scheduled events[2] or retrofits during the first, second, and third quarter of 1992 (1Q92, 2Q92, and 3Q92).

Form 3 contains additional questions related to the supplier's software architecture in addressing activities that involve planned system re-initializations. These questions should be answered for the current and prior two general software releases for each of the supplier's products.

### 3. Description of Form 2

Form 2 is similar to the existing Service Failure Analysis Report (SFAR) that is being used by some Bell Operating Companies to report and analyze switching system outages. Complete data for an outage event will be most advantageous. However, for the purpose of analyzing the root cause of an outage, Form 2 contains only a subset of the standard SFAR and has been expanded to include additional information regarding the outage. Each switching system supplier should fill out one form for each outage event that satisfies the conditions mentioned in Section 2. The following contains a detailed description of the fields in the form.

- Field 1 - Report Number: A report number unique to the case assigned by the service provider.

---

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

[2] Scheduled events include all scheduled or planned manual initializations that result in outages, restarts, phases, etc. This includes activities such as: software/firmware change, patch application, memory allocation, feature activation , office data change, etc. Scheduled initialization that is used to clear an earlier trouble is not included in this definition. See Attachment A for additional information.

- Field 2 - Supplier Name: The name of the switching system supplier issuing the report.
- Field 3 - Date of Incident: The date when the outage occurred.
- Field 4 - Time of Incident: The time (24-hour clock) when the outage occurred.
- Field 5 - System Name: The name of the system as given by the supplier.
- Field 6 - System Type: The type of the system whether it is a host end-office switch, a remote switch off a host, a packet switch, a tandem switch, a toll switch, a cellular switch or a Service Control Point (SCP).
- Field 7 - System ID/CLLI Code: A unique system identifier or the 11-digit CLLI code for the system.
- Field 8 - System Location: the city and the state where the entity is located.
- Field 9 - System Cutover Date: The date when the system was cutover to the service provider (if available).
- Field 10 - Software Generic/Version: The generic software program installed at the time of the outage.
- Field 11 - Software Load Date: The date when the generic software identified in Field 14 was loaded into the system (if available).
- Field 12 - Latest Patch: The most recent software patch or overwrite installed and activated in the system prior to the outage (if available).
- Field 13 - Equipped Terminations: The total number of equipped lines and trunks in the system.
- Field 14 - Total Outage Duration: The cumulative downtime of the system during a total outage.
- Field 15 - Partial Outage Duration: The cumulative downtime of the system during a partial outage.
- Field 16 - Terminations Affected: The number of lines and trunks affected by the outage.
- Field 17 - Description of Root Causes: A general description of the root causes of the outage. Use the categories in Fields 18 and 19 to assign a cause code.
- Field 18 - Classification of Major Causes: Use the categories provided to assign the code for the major cause. See Attachment A for a detailed description of the categories.
- Field 19 - Contributing Sub-Causes: Use the categories provided to assign the code of the sub-cause. See Attachment B for a detailed description of the categories.
- Field 20 - Fix Status: Check the appropriate box to indicate the availability of the fix.
- Field 21 - Recommendations/Best Practices: State the supplier's recommended best practices or plans for corrective or preventive actions (including time table, plans, or commitments) to: (a) prevent future occurrences, (b) lessen the impact of future occurrences, (c) speed recovery in future occurrences, or (d) improve the performance of the system.
- Field 22 - Specific information for "Design-Software" Outages: For outages identified as "D: Design - Software" in Field 18 above, check the appropriate box to indicate the generic software life cycle during which the outage occurred.

- Field 23 - Specific information for "Scheduled Event" or "Retrofit" Outages: Answer the specific question for outages in the categories of "H: Scheduled Event" and "R: Retrofit" identified in Field 18 above.



C

**4. When and Where to Send the Response**

All the responses should be returned by November 9, 1992 to:

J. D. Healy
Bellcore
331 Newman Springs Road, Room 2X-227
Red Bank, NJ 07701
Telephone: 908-758-3065
Fax: 908-758-4344

Questions relating to this request can be directed to J. D. Healy.

**5. Future Plan**

It is likely that the industry would want to collect this type of outage information from service providers on a going-forward basis. So, if this type of data is not routinely collected today, we suggest that your company establish a data collection process to collect outage information so that is will be available for future use in NRC network monitoring and reliability analyses.



C

NRC Switching System Focus Area
Form 1 - Switching System Population Data Request - Supplier

| System Name | Total number of systems in service within U.S. at the end of | | | |
|---|---|---|---|---|
| | 4Q91 | 1Q92 | 2Q92 | 3Q92 |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |



C

NRC Switching System Focus Area
Switching System Outage Data Request — System Supplier

| 1. Report Number | 2. Supplier Name | 3. Date of Incident / / | 4. Time of Incident (24hr clock) : : |
|---|---|---|---|
| 5. System Name | 6. System Type: qHost qRemote qTandem qToll qSCP qPacket Switch qCellular Switch | 7. System ID/CLLI Code | 8. System City & State |
| 9. System Cutover Date / / | 10. Software Generic/Version | 11. Software Load Date / / | 12. Latest Patch/Overwrite |
| 13. Equipped Terminations Lines: _____ Trunks _ | 14. Total Outage Duration _____:_____:_____ HR MIN SEC | 15. Partial Outage Duration _____:_____:_____ HR MIN SEC | 16.Terminations affected Lines: _____ Trunks: _____ |

**17. Description of Root Causes:** Describe the root cause of the outage and assign an outage cause code using the categories below and on the attached guidelines for outage classification. (Add attachments if necessary)

**18. Outage Cause Classification:** Use the categories below to describe the cause of the outage (check appropriate box):

__ A. Procedural—Telco
__ B. Procedural—System Vendor
__ C. Procedural—Other Vendor
__ D. Design—Software†
__ E. Design—Firmware
__ F. Design—Hardware
__ G. Hardware Failure
__ H. Scheduled Event†
__I. Lightning Related
__J. Traffic Overload
__K. Environmental
__ L. Power Failure
__ M. Remote facilities/Umbilical isolation
__ R. Successful Retrofit†
__ N. Unknown/Other (Specify below _____)

**19. Contributing Sub-causes:** Check an appropriate box for the sub-cause that contributed to or prolonged the outage.

__a. Work Error – Operational
__b. Work Error – Data Entry
__c. Work Error – Hardware
__d. Documentation Error
__e. Fix Available – Not applied
__f. Recovery Action – Escalated
__g. Defective Patch
__i. Insufficient Data
__j. Retrofit
__k. Hardware Growth
__l. Software Administration
__m. Firmware Administration
__q. Central Control Unit
__r. Switching Fabric Unit
__s. Peripheral Control Unit
__t. Line/Trunk Unit
__u. SS7 Unit
__v. Clock Unit
__w. Database Error – Dynamic
__x. Database Error – Static
__y. Data Synchronization
__z. Routine Exercise

**20. Fix Status:** __a. Fix not developed __b. Fix developed, not in the field __c. Fix available in the field



C

| 21. **Recommendations/Best Practices:** State the supplier's recommended best practices or plans for corrective or preventive actions, including time table, plans, commitments, or recommendations to: (a) prevent future occurrences; (b) lessen the impact of future occurrences; (c) speed recovery in future occurrences; or (d) otherwise improve the performance of the system. (Add attachments if necessary.) |
|---|
| |
| |
| |

† See the next page for additional information regarding the outage.



C

**22. Specific information for outages in the "D: Design – Software" category:** Check the appropriate box or boxes for outages in the category of "D:Design – Software" identified in Item 18 above.

__1. Customer Requirements: The outage was caused by errors, inconsistency, incompleteness, or ambiguity in customer requirements.
__2a. Industry Requirements/Standards for Single Nodes: The outage was caused by errors, inconsistency, incompleteness, or ambiguity in industry requirements/standards (e.g., Bellcore requirements, CCITT Recommendations, etc.) related to single nodes.
__2b. Industry Requirements/Standards for Networks: The outage was caused by errors, inconsistency, incompleteness, or ambiguity in industry requirements/standards (e.g., Bellcore requirements, CCITT Recommendations, etc.) related to networks.
__3. Vendor Specifications: The outage was caused by errors, inconsistency, incompleteness, or ambiguity in the vendor's product specifications.
__4a. Design – Feature: The outage was caused by errors or insufficiency in the design for features.
__4b. Design – Fault Tolerance: The outage was caused or prolonged by errors or insufficiency in the design for software fault tolerance.
__5. Coding: The outage was caused by programming errors or misinterpretation of design in the coding phase.
__6. Testing: The outage was caused by insufficient coverage of unit, integration, or system testing.
__7. Field Implementation: The outage occurred during the software generic application process.
__8. Field Support: The outage occurred during software updates or data changes (e.g., patches, parameters changes for feature activations, etc.) for field support.

**23. Specific information for outages in the "H: Scheduled Event" and "R:Retrofit" categories:** Answer the following questions for outages in the categories of "H: Scheduled Event" and "R: Retrofit" identified in Item 18 above.

- Why was the event undertaken?
  __a. New Customer (growth) __b. Change in engineering rules (growth) __c. Change in regulatory rules (i.e., equal access) __d. Implement new features __e. Stay within vendor support "window" __f. Correct an error (specify: _ )
  __g. Other (specify: _ )
- Was there an alternative to re-initializing the switch?
  __No __Yes (specify: _ )
- When was the last time this switch was re-initialized for retrofit or scheduled event?
  Date: ___ Time: ___ Reason:
  _____
- Was this retrofit or scheduled event coordinated with retrofits/scheduled events in other switches?
  __No __Yes (how many switches were involved? ____)
- Identify practices, procedures, and strategies in use in **Item 21** above to minimize the number of scheduled outages and retrofits.

NRC Switching System Focus Area
Form 3 - Additional Information Request - Supplier

A. For each switching product, please answer the following questions for each supported current and two prior general software releases (generics):

1) What is the date when the release was generally available to your customers?

2) What is the number of patches to the general release in the field that involved system re-initialization to become effective?

3) For each patch identified in (2) above, please answer the following:

a) What did the patch do?

b) Was there an alternative to re-initialization in order to activate the patch? (If yes, specify the alternative and why the alternative was not implemented.)

B. General software architecture questions:

1) What is the likelihood and projected implementation date for the following features:

a) Automated outage reporting by the system in a standard format that contains information such as the identification of the system, date/time/duration of the outage, number of terminations (lines/trunks/circuits/channels) affected by the outage, location of the failure in the system, causes of the failure, etc.

b) Reduction in conditions requiring system re-initialization

c) Reduction in the length of system re-initialization time to a maximum of 30 seconds for scheduled events

2) Do you currently have design objectives or requirements for minimizing outage duration during planned initialization? If yes, what are the objectives for systems with:

a) less than 20,000 terminations

b) between 20,000 and 50,000 terminations

c) more than 50,000 terminations

d) a rich set of features

3) What are the barriers to improve the design objectives stated in (2) above?

4) Do you envision more coordinated software generic updates (or retrofits) in the future?

## Attachment A

### Classifications of Major Causes of Outages

This attachment contains definitions of the major classifications of outage causes. These classifications are intended for use in service failure analysis to obtain consistent measurements of outage performance. The standard major classifications are:

A. **Procedural - Telephone Company**

The primary cause of the outage was a procedural error on the part of telephone company personnel. This classification includes cases where telephone company forces either deviated from published or accepted procedures or where a human error was made even though the correct procedure was being used. (Example: removing a circuit pack form an in-service unit after proper preparation of the off-line unit for circuit pack replacement; or entry of improper translations.) Also included in this classification would be cases where failure to respond to an incident in accordance with BCC practices resulted in a prolonged outage.

**NOTE:** This classification does *not* include errors or procedural flaws in documentation published by the vendor and used by telephone company personnel.

B. **Procedural - System Vendor**

The primary cause of the outage was a procedural error on the part of the vendor:

- An error or improper deviation from published or accepted procedures by vendor personnel. Examples might be an error on the part of vendor installation forces or an improper action instructed by vendor technical support personnel. Deviation from an approved Method of Procedure belongs in this classification.

- A documentation error in an official publication from the vendor (e.g., faulty or unclear procedure or typographical error) that was followed by telephone company employees.

C. **Procedural - Other Vendor**

The primary cause of the outage was procedural error on the part of an organization other than the telephone company or system vendor, for example, an independent installation organization or building contractor.

D. **Design - Software**

The primary cause of the outage was faulty or ineffective software design. This category includes outages caused by faulty patches or software overwrites provided by the vendor.

**NOTE:** Generally, the telephone company is permitted three weeks to install a patch from the date that patch is released. However, if a vendor has a patch that must be installed on a special emergency basis, the vendor is normally required to notify the telephone company. The telephone company and the vendor would agree upon a special commitment date for installation of the emergency patch in all applicable systems. That special commitment would supersede the normal three-week interval for such rare emergency cases.

**Exception:** If lack of a critical patch that has been available for three weeks causes an outage incident, the

incident is categorized as "Procedural - Telephone Company." However, an outage caused by a critical patch that is delayed beyond the three-week period because of a temporary patch that cannot be removed without serious impact on customer service, is categorized as "Procedural - Vendor". Similarly, outages that are the result of failure to remove an obsolete patch would be assigned to the appropriate procedural category.

E. **Design - Firmware**

Firmware design problems that result in system outages are included in this category. If the installation of a Product Change Notice has been delayed beyond the expected application date (similar to Product Change Notices in Item F below), the outage is attributed to the appropriate procedural classification above.

F. **Design - Hardware**

The primary cause of the outage was a design deficiency or error in the system hardware. Outages caused by hardware design deficiencies are classified as "Design - Hardware" *unless*:

- A Class A Product Change Notice (PCN) was inappropriately delayed by the vendor or telephone company or
- The PCN was waived by the telephone company.

If the installation of the PCN has been waived or delayed beyond the expected application date, the outage is attributed to the appropriate procedural classification above (A or B).

G. **Hardware Failure**

The primary cause of the outage was random hardware failure not related to design, but due to the inherent unreliability of the system components. If hardware failures cause loss of duplicated critical system units resulting in a system outage, the SFAC would normally consider whether procedural errors were also involved.

If response to a simplex failure of a critical system component is deferred before failure of the mate unit, the outage is assigned to the appropriate procedural category normally "Procedural - Telephone Company." If poor or questionable trouble isolation procedures were employed resulting in the introduction of multiple troubles, the appropriate procedural classification is normally assigned.

H. **Scheduled Event**

All scheduled or planned manual initializations that result in outages, restarts, phases, etc., are recorded in this category. The system should be running normally both before and after the initialization. This includes activities such as: parameter loads, software/firmware changes (patch/overwrite application, feature activation, office data change, PROM change-out, etc.), hardware growth, other OA&M activities, etc.

**NOTE:** This category does not include outages caused by scheduled software generic update (or retrofit) which are charged to a stand-alone category as "R: Retrofit." In addition, this category does not include scheduled initialization to clear an earlier trouble. Under such circumstance, the outage should be charged to the initial cause of the trouble.

I. **Lightning-Related**

The primary cause of the outage was lightning or external high voltage transients (such as those caused by high voltage commercial power faults) introduced into the system. If the entry of lightning into the system is caused by bonding and grounding *violations*, the outage is assigned to the appropriate procedural

category above (A or B).

J. **Traffic Overload**

The primary cause of the outage was true system overload from high traffic or load conditions that exceeded the engineered capacity of the system. This classification is used when unexpected traffic that is the result of extraordinary weather, emergency, disaster, transmission facility failure, or similar external conditions causes overload.

**Exceptions:** Outages are *not* classified as "Traffic Overload" if the outage event is instigated by a serious system trouble or by inability of the system to cope with traffic. Examples include:

- **Outages resulting from system trouble:** This classification is *not* used when outages create overload as a result of regenerative attempts and "pent-up demand that result from serious system trouble. Sometimes a system recovery action during high traffic periods precipitates an overload following what would otherwise have been a rapid recovery. Such traffic overload may prolong the outage or even prevent the recovery. In such cases, the outage is attributed to the cause of the initial failure, regardless of the duration of extended downtime as a result of traffic overload.

- **Inadequate System Capacity Engineering:** If traffic overload is caused by inadequate engineering, the outage is assigned to the appropriate procedural category above. If the telephone company engineering organization was in error (that is, the telephone company did not properly apply the engineering rules and guidelines published by the vendor), the outage is classified as "Procedural - Telephone Company." If the engineering rules and guidelines provided by the vendor were deficient or erroneous, the outage is classed as "Procedural - Vendor."

- **Inadequate Network Management:** If external conditions were improperly handled by the telephone company (e.g., radio call in contest with no "choke" network or inadequate network management in place before/during the event), the outage is classified as "Procedural - Telephone Company."

- **System Design Deficiencies:** If the outage is caused by the inability of the system to respond properly to high-traffic conditions (shed load or implement appropriate network management controls) as a result of system design deficiencies, the outage is assigned to the appropriate design category.

In summary, the "Traffic Overload" classification is limited to true cases when unexpected, extraordinary actual traffic load exceeds the engineered capacity of a properly designed and engineered system.

**NOTE:** It is recommended that the committee determine the degree and duration of service degradation that results from an overload condition (regardless of what caused o precipitated the overload condition). A number of judgment factors and considerations are involved in this determination. The primary factors that might be considered by the committee are:

- The number of calls handled by the system during the period of degraded service.

- Dial tone delay measurements (system data if the system data are considered reliable; manual data if they are not).

- Other traffic or operational measurement data if such data are considered reliable.

- Outcome of test calls placed.

- Network Management information.

- Analysis of system output and indicators.

- Analysis of known causes/conditions.
- Customer reaction/perspective - Customer Trouble Reports and other measurements.
- Effects on operator services (if the system is capable of supporting Operator Services Systems).
- Impact of BCC feature software development.

K. **Environmental**

This classification includes instances of system outages caused by environmental conditions that exceed limitations documented in the vendor's technical specifications. Examples are:

- Entry of water into the system (e.g., roof leaks, air conditioning leakage, water system ruptures, flooding, etc.).
- Excessive ambient temperatures (e.g., air-handling system failures causing temperatures that exceed short term limitations of the system), excessive rate of temperature change, and humidity that exceeds specified limits.
- Corrosive contamination that enters the system from the surrounding environment.
- Fire.

If the incident arises from poorly designed hardware, the "Design - Hardware" classification would be used if the environmental factors were not excessive in the committee's opinion.

L. **Power Failure**

This classification includes instances of outage directly related to failure of the external power system, DC or AC. Because all offices in the BCC environment are protected by battery systems (and, typically, by standby generator backup) use of this classification is normally rare. This classification includes procedural errors or any other problem related to the *external* power plant equipment and systems that interrupt essential power to the system equipment.

This classification does *not* include failure of converters and inverters internal to the system. All network switching elements employ internal converters and/or inverters considered integral to the system itself. Failure of an integral converter or inverter that interrupts power to critical equipment, resulting in system outage, is assigned to the appropriate category for the system (normally one of Items A, B, E, F, G, or I).

M. **Remote Facilities/Umbilical Isolations**

This classification includes any switching system outage caused by loss of facilities between the remote and host switching system. In the event the remote switch does not have "stand-alone" capabilities, outages are reported as partial system outages of the host system.

When the loss of facilities is caused by activities external tot he host or remote switch (such as a cable dig-up) the outage is charged to the appropriate procedural category ("Procedural - Telephone Company" or "Procedural - Other Vendor").

In the event an outage is caused by duplex hardware faults within the host/remote or by system software design, the outage is charged to the appropriate category.

R. **Retrofit**

This classification includes switching system outages caused by an initialization during a successful software upgrade or retrofit process. The switching system should be running normally both before and after the retrofit process. In the event a failure occurred during the retrofit process, the outage should be charged to the appropriate procedure, hardware or software category.

N. **Unknown/Other**

If the committee cannot determine a cause of the outage, or the cause does not match any of the classifications above, the outage is classified as "Unknown/Other." Every effort is normally made to avoid use of this classification because corrective and preventive efforts are very difficult if the cause is unknown. Avoidance of the use of this classification requires rapid and thorough investigation by the SFAC before data are lost or "tainted" and before memories fade.

Even when the cause cannot be proven, when actions that can be deduced from the evidence are denied, and when data necessary to substantiate the cause are incomplete, it is usually still possible to determine the probable cause with a degree of confidence. In such cases, the most probable and appropriate classification is normally assigned to enhance subsequent "downstream" analysis efforts. This "Unknown/Other" category is considered absolutely the *last resort* for the committee.

## Attachment B

## Classifications of Sub-Causes of Outages

This attachment contains definitions of the sub-causes that either contributed to or prolonged the outage. These classifications are intended for use in service failure analysis to obtain consistent measurements of outage performance. The standard sub-cause classifications are:

a. **Work Error - Operational:** Documentation (e.g., Method of Procedure [MOP], Input Manual, Recent Change Manual) was correct, but not followed; skipped a step; operated a wrong key; typing error; labeling error; etc.

b. **Work Error - Data Entry:** Incorrect input (e.g., parameter, translation, overwrite, recent change); new load database built incorrectly; etc.

c. **Work Error - Hardware:** Removed wrong circuit pack; worked at wrong location (e.g., Unit 0 instead of Unit 1); removed wrong fuse; etc.

d. **Documentation Error:** Information provided was incorrect (e.g., Input Manual, Telco or vendor Method of Procedure, patch application instruction, etc.)

e. **Fix Available/Not Applied:** Did not apply available software or hardware fixes (e.g., Patch, Product Change Notice, Broadcast Warning, etc.)

f. **Recovery Action Escalated:** Action taken exceeded prescribed recovery methodology; less severe recovery action was available, but not applied.

g. **Defective Patch:** A patch that was ineffective in correcting the original trouble or impacts other service.

h. **Reserved:** This category is reserved for future use.

i. **Insufficient Data:** Outage description contains insufficient data to determine the sub-cause.

j. **Retrofit:** Successful generic software upgrade or application.

k. **Hardware Growth:** Addition of hardware equipment (circuit packs, frames, etc.) requiring initialization activities.

l. **Software Administration:** Software administration activities (e.g., patch activation, memory allocation, feature activation, parameter change, etc.) requiring initialization activities.

m. **Firmware Administration:** Firmware administration activities (e.g., PROM change-out, etc.) requiring initialization activities.

n. **Reserved:** This category is reserved for future use.

o. **Reserved:** This category is reserved for future use.

p. **Reserved:** This category is reserved for future use.



C

q. **Central Control Unit:** Failures in the central control unit (CCU), e.g., central processing unit (CPU), input/output controller (IOC), Administrative Module (AM), Coordination Processor (CP), memory device (random access memory, disk drive, tape drive), cabling, power converter, etc.

r. **Switching Fabric Unit:** Failures in the switching fabric unit (SFU), e.g., Communication Module (CM), Time Multiplex Switch (TMS), Switching Networks (SN), Message Buffer (MB), Line Group Concentrator (LGC), interface between CCU and peripheral control unit, etc.

s. **Peripheral Control Unit:** Failures in the peripheral control unit (PCU), e.g., Digital Trunk Controller (DTC), Line/Trunk Controller (LTC), Switching Module (SM), Line Trunk Group (LTG), Digital Line Unit (DLU), Line Concentration Module (LCM), miscellaneous frames (ringing and tone plant, Remote Office Test Line (ROTL), test trunk frame, recorded announcement frame), etc.

t. **Line/Trunk Unit:** Failures in the line/trunk unit (LTU) - non-controller, e.g., line card, trunk card, grid, etc.

u. **SS7 Unit:** Failures in the SS7 unit, e.g., Link Peripheral Processor (LPP), Common Channel Signaling Network Control (CCSN), Communications Network Interface (CNI), etc.

v. **Clock Unit:** Failures in the clock unit, e.g., slippage, loss of sync, etc.

w. **Database Error - Dynamic:** Corruption of or error in dynamic data, e.g., operational measurements, call progression registers, etc. (Corruption is defined as database information in Unit ) and Unit 1 which has been mutilated and is not correctable by the system.)

x. **Database Error - Static:** Corruption of or error in static data, e.g., operating system data, generic data, parameters, etc.

y. **Data Synchronization:** Mismatch of static and/or dynamic data in Unit 0 and Unit 1 not correctable by the system.

z. **Routine Exercise:** Initialization required due to routine exercise (REX) activities, e.g., the REX test does not detect a fatal fault condition or introduces a fatal fault condition which requires a system or manual initialization.

# Appendix C

C

## Appendix C - Network Reliability Industry Initiatives Matrix

Network Reliability Industry Initiatives
Focus Area: Switching System

| Topic | Industry Group | Doc. No. Issue No. Standards No. | Version No. and Date | Title | Brief Description |
|---|---|---|---|---|---|
| Network Reliability Performance Objectives | Bellcore | TR-TSY-000179 | II, 7/89 | Software Quality Program Generic Requirements (SQPR) | Requirements for telecomm software development process |
| | Bellcore | TR-TSY-000282 | II, 86 | System Reliability and Quality Acceptance Criteria | Software acceptance criteria for system testing, FOA, andgeneral availability |
| | Bellcore | TR-NWT-000284 | I2, 10/90 | Reliability and Quality Switching Systems Requirements Generic Requirements (RQSSGR) | Reliability objectives for system design and architecturesmanufactu ring and production and in-service support |
| | Bellcore | SR-TSY-000385 | II,6/86 | Bell Communications Research Reliability Manual | |
| | Bellcore | TR-TSY-000512 | I3, 2/90 | Reliability Section 12 of the LSSGR | Switching system reliability objective defined |

| Topic | Industry Group | Doc. No. Issue No. Standards No. | Version No. and Date | Title | Brief Description |
|---|---|---|---|---|---|
| Network Reliability Performance Objectives | Bellcore | SR-NWT-000821 | 13,12/90 | Field Reliability Performance Study Handbook | Generic guidelines for conducting field performance studies |
| | Bellcore | TR-TSY-000929 | 11,6/90 | Reliability and Quality Measurements for Telecommunications Systems (RQMS) | Bellcore's view of generic requirements regarding supplier measurements |
| | Bellcore | TR-TSY-000929 | 11,R1,5/92 | Reliability & Quality Measurements for Telecommunications Systems (RQMS) | Bellcore's view of generic requirements regarding supplier measurements |
| | Bellcore | TR-TSY-000929 | 11,S1, 3/91 | Reliability & Quality Measurements for Telecommunications Systems (RQMS) RQMS Performance Report | Bellcore's view of generic requirements regarding supplier measurements |
| | Bellcore | SR-TSY-000963 | 11, 89 | Network Switching Element Outage Performance Monitoring | Outage reporting process and service failure analysis |
| | Bellcore | TR-NWT-001047 | 11, 3/91 | ISDN Switching System Reliability Objectives for Basic Rate Access | ISDN switch system reliability objectives |
| | Bellcore | TR-NWT-001047 | 11,S1, 7/91 | ISDN Switching System Reliability Objectives Supplement for Primary Rate Access | ISDN switch system reliability objectives |

| Topic<br><br>Network Reliability Performance Objectives | Industry Group | Doc. No. Issue No. Standards No. | Version No. and Date | Title | Brief Description |
|---|---|---|---|---|---|
| | Bellcore | TR-NWT-001047 | II,SI, 7/91 | ISDN Switching System Reliability Objectives Supplement for Primary Rate Access | ISDN switch system reliability objectives |
| | Bellcore | TR-NWT-001213 | II, 92 | Objectives for the Maintenance User Interface of Switching Systems and Transport Systems | Switching and transport system design goals for the maintenanceuser interface |
| | ANSI | T1A1.2/93-015 | 2/93 | Draft Proposed Technical Report onNetwork Survivability Performance,Project T1Q1/90-004R2 | Survivability as a function of architecture |
| | Comm T1 | T1.202 | 88 | Internetwork Operations | Guidelines for network mangement under disaster conditions |
| | FCC | CC Docket 87-313 | 87 | ARMIS Reports | |
| | FCC | CC Docket 91-273 | 91 | Major Service Disruptions Reports | Notifications requirements for network service disruptions |

| Topic<br><br>Network Architecture and Design | Industry Group | Doc. No.<br>Issue No.<br>Standards No. | Version No. and Date | Title | Brief Description |
|---|---|---|---|---|---|
| | Bellcore | TR-EOP-000063 | 13,3/88 | Network Equipment - Building Systems (NEBS) GenericEquipment Requirements | |
| | Bellcore | TR-NWT-000078 | 13,12/91 | Generic Physical Design Requirements for Telecommunications Products and Equipment | Bellcore's view of minimum generic physical design requirements for telecommunication products |
| | Bellcore | TR-TSY-000282 | 11, 86 | System Reliability and Quality Acceptance Criteria | Software acceptance criteria for system testing, FOA, and general availability |
| | Bellcore | TR-NWT-000332 | 14,9/92 | Reliability Prediction Procedure for Electronic Equipment | Contains the recommended parts count, laboratory and fieldtracking methods for predicting and measuring hardware reliability |
| | Bellcore | TR-TSY-000357 | 11,12/87 | Generic Requirements for Assuring the Reliability of Components Used in Telecommunication Equipment | Defines practices for equipment suppliers to ensure satisfactory component reliability |

| Topic<br><br>Network Architecture and Design | Industry Group | Doc. No.<br>Issue No.<br>Standards No. | Version No. and Date | Title | Brief Description |
|---|---|---|---|---|---|
| | Bellcore | SR-TSY-000385 | 11,6/86 | Bell Communications Research Reliability Manual | A tutorial on reliability concepts and methods |
| | Bellcore | TR-NWT-000870 | 11,2/91 | Electrostatic Discharge Control in the Manufacture of Telecommunications Equipment and Components | Bellcore's minimum generic requirements for controlling electrostatic dischange during manufacture |
| | Bellcore | TR-NWT-000930 | 11,12/90 | Generic Requirements for Hybrid Microcircuits Used in Telecommunications Equipment | Bellcore's minimum generic physical design and reliability assurance requirements |
| | Bellcore | TR-NWT-001213 | 11, 92 | Objectives for the Maintenance User Interface of Switching Systems and Transport Systems | Switching and transport system design goals for the maintenance user interface |
| | Comm T1 | T1.110 | 92 | System 7 | General Information |
| | Comm T1 | T1.117 | 91 | Digital Hierarchy | Optical Interface Specifications (Short Reach) |
| | Comm T1 | T1.205 | 88 | Representation of Places for Information Interchange | |

| Topic<br><br>Network Architecture and Design | Industry Group | Doc. No.<br>Issue No.<br>Standards No. | Version No. and Date | Title | Brief Description |
|---|---|---|---|---|---|
| | Comm T1 | T1.209 | 89 | Principles of Functions, Architectures, and Protocols for Interfaces Between Operations Systems and Network Elements | Analog Voicegrade Switched Access Using Loop Reverse Battery Signaling |
| | Comm T1 | T1.405 | 89 | Interface Between Carriers and Customer Installations | Survivability as a function of architecture |
| | ANSI | T1A1.2/93-015 | 2/93 | Draft Proposed Technical Report onNetwork Survivability Performance, Project T1Q1/90-004R2 | Congestion in SS7 networks |
| | ANSI | T1S1 | | | Survivable architectures |
| | CCITT | Study Group II | | | Survivable architectures |
| | CCITT | Study Group XVIII | | | |

| Topic<br><br>Network Interconnection and Interoperability | Industry Group | Doc. No. Issue No. Standards No. | Version No. and Date | Title | Brief Description |
|---|---|---|---|---|---|
| | Bellcore | TR-NWT-000394 | I4, 12/92 | Switching System Requirements for Interexchange Carrier Interconnection Using the Integrated Services Digital NetworkUser Part (ISDNUP) | |
| | Comm T1 | T1.111 | 92 | Signaling System 7 | Message Transfer Part |
| | Comm T1 | T1.112 | 92 | Signaling System 7 | Signaling Connection Control Part |
| | Comm T1 | T1.113 | 92 | Signaling System 7 | ISDN User Part |
| | Comm T1 | T1.114 | 92 | Signaling System 7 | Transaction Capability Application Part |
| | Comm T1 | T1.117 | 91 | Digital Hierarchy | Optical Interface Specifications (Short Reach) |
| | Comm T1 | T1.118 | 92 | Signaling System 7 | Intermediate Signaling Network Identification |
| | Comm T1 | T1.201 | 87 | Information Interchange | Structure for the Identification of Location Entities for the North American Telecommunications System |

| Topic<br><br>Network Interconnection and Interoperability | Industry Group | Doc. No.<br>Issue No.<br>Standards No. | Version No. and Date | Title | Brief Description |
|---|---|---|---|---|---|
| | | | | | |
| | Comm T1 | T1.204 | 92 | Operations, Administration, Maintenance and Provisioning | Lower Layer Protocols for Interfaces Between Operations Systems and Network Elements |
| | Comm T1 | T1.204a | 92 | See Above | See Above |
| | Comm T1 | T1.204b | 92 | Operations, Administration, Maintenance and Provisioning | Lower Layer Protocols for Interfaces Between Operations Systems and Network Elements |
| | Comm T1 | T1.205 | 88 | Representation of Places for Information Interchange | |
| | Comm T1 | T1.210 | 89 | Principles of Functions, Architectures, and Protocols for Interfaces Between Operations Systems and Network Elements | |

| Topic | Industry Group | Doc. No. Issue No. Standards No. | Version No. and Date | Title | Brief Description |
|---|---|---|---|---|---|
| Network Interconnection and Interoperability | Comm T1 | T1.211 | 89 | Information Interchange | Representation of National Security Emergency Preparedness-Telecommunications Service Priority |
| | Comm T1 | T1.213 | 90 | Coded Identification of Equipment Entities of the North American Telecommunications System for the Purpose of Information Exchange | |
| | Comm T1 | T1.405 | 89 | Interface Between Carriers and Customer Installations | Analog Voicegrade Switched Access Using Loop Reverse Battery Signaling |
| | Comm T1 | T1 Committee Technical Report #5 | 6/90 | Carrier to Customer Installation Interface Connector Wiring Configuration Catalog | |

| Topic | Industry Group | Doc. No. Issue No. Standards No. | Version No. and Date | Title | Brief Description |
|---|---|---|---|---|---|
| Network Management | Comm T1 | T1.115 | 90 | Signaling System 7 | Monitoring and Measurements for Signaling System 7 Networks |
| | Comm T1 | T1.202 | 88 | Internetwork Operations | Guidelines for Network Management of the Public Switched Networks Under Disaster Conditions |
| | Comm T1 | T1.210 | 89 | Principles of Functions, Architectures, and Protocols for Interfaces Between Operations Systems and Network Elements | |

| Topic | Industry Group | Doc. No. Issue No. Standards No. | Version No. and Date | Title | Brief Description |
|---|---|---|---|---|---|
| Restoration and Recovery | Bellcore | TR-TSY-000732 | I1,3/90 | Backup and Recovery | |
| | Comm T1 | T1.115 | 90 | Signaling System 7 | Monitoring and Measurements for Signaling System 7 Networks |
| | Comm T1 | T1.202 | 88 | Internetwork Operations | Guidelines for Network Management of the Public Switched Networks Under Disaster Conditions |
| | ANSI | T1S1 | | | Congestion in SS7 networks |
| | CCITT | Study Group IV | | | Restoration studies |

| Topic | Industry Group | Doc. No. Issue No. Standards No. | Version No. and Date | Title | Brief Description |
|---|---|---|---|---|---|
| Operations, Administration, Maintenance | Bellcore | TR-TSY-000509 | I2, 7/87 | Maintenance Section 9 of the LSSGR | |
| | Bellcore | TR-TSY-000509 | I2, R1, 12/88 | Maintenance Section 9 of the LSSGR | |
| | Bellcore | TR-TSY-000541 | I2, 87 | Measurements and Administration Section 8.6 of the LSSGR | Retrofit requirements and patch processes |
| | Bellcore | TR-TSY-000929 | I1,6/90 | Reliability and Quality Measurements for Telecommunications Systems (RQMS) | |
| | Bellcore | TR-TSY-000929 | I1,R1,5/92 | Reliability & Quality Measurements for Telecommunications Systems (RQMS) | |
| | Bellcore | TR-TSY-000929 | I1,S1, 3/91 | Reliability & Quality Measurements for Telecommunications Systems (RQMS) RQMS Performance Report | |
| | Bellcore | TR-NWT-001148 | I1, 2/91 | OSSGR Section 9: Maintenance | |

| Topic | Industry Group | Doc. No. Issue No. Standards No. | Version No. and Date | Title | Brief Description |
|---|---|---|---|---|---|
| Operations, Administration, Maintenance | Bellcore | TR-NWT-001213 | 11, 92 | Objectives for the Maintenance User Interface of Switching Systems and Transport Systems | Switching and transport system design goals for the maintenance user interface |
| | Comm T1 | T1.116 | 90 | Signaling System 7 | Operations, Maintenance and Administrative Part |
| | Comm T1 | T1.201 | 87 | Information Interchange | Guidelines for Network Management of the Public Switched Networks Under Disaster Conditions |
| | Comm T1 | T1.204b | 92 | Operations, Administration, Maintenance and Provisioning (Supplement) | Lower Layer Protocols for Interfaces Between Operations Systems and Network Elements |
| | Comm T1 | T1.205 | 88 | Representation of Places for Information Interchange | |
| | Comm T1 | T1.210 | 89 | Principles of Functions, Architectures, and Protocols for Interfaces Between Operations Systems and Network Elements | |

| Topic | Industry Group | Doc. No. Issue No. Standards No. | Version No. and Date | Title | Brief Description |
|---|---|---|---|---|---|
| Operations, Administration, Maintenance | Comm T1 | T1.211 | 89 | Information Interchange | Representation of National Security Emergency Preparedness-Telecommunication Service Priority |
| | Comm T1 | T1.213 | 90 | Coded Identification of Equipment Entities of the North American Telecommunications System for the Purpose of Information Interchange | |
| | Comm T1 | T1 Committee Technical Report #12 | 9/91 | Application Guidelines for Use of the DS1 Extended Superframe Format Data Link | |

| Topic | Industry Group | Doc. No. Issue No. Standards No. | Version No. and Date | Title | Brief Description |
|---|---|---|---|---|---|
| Human Factors Design | Bellcore | TR-TSY-000439 | 12, 1/88 | OTGR User System Interface. Section 10.1 | |
| | Bellcore | TR-NWT-001213 | 11, 92 | Objectives for the Maintenance User Interface of Switching Systems and Transport Systems | Switching and Transport System Design Goals for the Maintenance User Interface |
| | Comm T1 | T1.203 | 88 | Operation, Administration, Maintenance and Provisioning | Human-Machine Language |
| | Comm T1 | T1 Committee Technical Report #5 | 6/90 | Carrier to Customer Installation Interface Connector Wiring Configuration Catalog | |

| Topic | Industry Group | Doc. No. Issue No. Standards No. | Version No. and Date | Title | Brief Description |
|---|---|---|---|---|---|
| Survivability Analysis Models and Tools | Bellcore | SR-TSY-001130 | 11,5/89 | Reliability and System Architecture Testing | |
| | Bellcore | SR-TSY-001171 | 11,1/89 | Methods and Procedures for System Reliability Analysis | |
| | Bellcore | SR-TSY-001547 | 11, 1/90 | The Analysis & Use of Software Reliability & Quality Data | |
| | Bellcore | SR-NWT-002419 | 11,12/92 | Software Architecture Review Checklists | Bellcore's View of SAR Methodology and Checklists |
| | RAM | Proceedings of the Annual Reliability and Maintainability Symposium | pp. 320-327, 83 | Hardware/Software FMECA | Failure Modes and Effects Analysis Procedures |
| | RAM | Proceedings of the Annual Reliability and Maintainability Symposium | pp. 274-279, 92 | Assuring Software Safety | |

| Topic | Industry Group | Doc. No. Issue No. Standards No. | Version No. and Date | Title | Brief Description |
|---|---|---|---|---|---|
| Network Security | Bellcore | TR-TSY-000736 | 11,3/90 | Data Base Integrity and Security FSD 45-01-0900 | |
| | Comm T1 | T1.211 | 89 | Information Interchange | Representation of National Security Emergency Preparedness-Telecommunications Service Priority |
| | Comm T1 | T1.405 | 89 | Interface Between Carriers and Customer Installations | Analog Voicegrade Switched Access Using Loop Reverse Battery Signaling |

| Topic | Industry Group | Doc. No. Issue No. Standards No. | Version No. and Date | Title | Brief Description |
|---|---|---|---|---|---|
| Regulations | FCC | CC Docket 87-31 | 8/92 | Modifications to Service Quality/Infrastructure Reporting | This docket expanded the Quarterly Service reporting requirements to include date and time of switch down times |

| | | | | |
|---|---|---|---|---|
| Congress | H.R. 4789 | 4/92 | Telephone Network Reliability Improvement Act of 1992 | This bill would have required the FCC to establish and enforce network reliability standards (failed to pass in 92) |
| Congress | S.237 | 1/93 | National Network Security Board Act of 1993 | Bill to create NS board to investigate and make recommendations regarding network security and reliability |
| Congress | S.238 | 1/93 | Telecommunications Network Security and Reporting Act of 1993 | Bill to require FCC to report to Congress network security and reliability matters |