Appendix 1

D

Fault Fix History (Prior to Release)

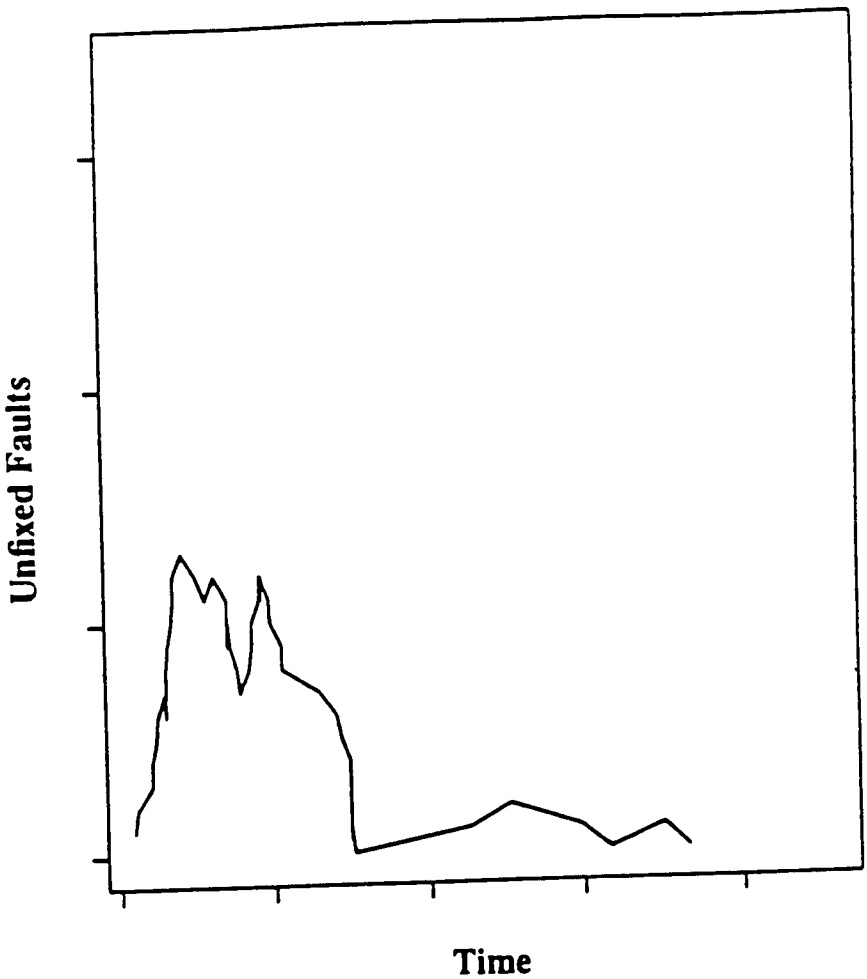


Figure 29

D

Network Reliability Council
Issue Statement

Issue Title: Reliability of Digital Cross-Connect Systems (DCS)

Author: Frank Ianna
AT&T - NSD

Problem Statement/Issues to be Addressed

Digital Cross-Connect Systems (DCS) are a principal transmission element within telecommunications networks. DCS are software-based, microprocessor-controlled systems that serve as a junction point at which traffic (e.g., switched or dedicated DS1s) passing through a central office is groomed (i.e., routed onto or off of the appropriate digital facility towards its destination). DCS essentially automate the function of the old patch panel used to manually connect circuits.

Since large volumes of traffic on digital facilities are routed through DCSs, and since DCSs play an increasingly important role in service restoration in the event of cable cuts, facility electronics failures, central office failures or other threats to service continuity, it is important to assure the overall reliability of DCS.

Areas of Concern & Problem Quantification

Little in the literature suggests any general reliability problems with DCS. However, when a problem does occur, the consequences have the potential of being significant because of the large volumes of traffic passing through DCS. Thus, it is prudent to examine the DCS area to determine if there are any potential weaknesses before a significant service disrupting problem occurs. Specifically, the areas of concern include the following:

- Are the hardware features employed by DCS effective in protecting its internal operations, and minimizing the impact on service of an internal or external failure?
- Are the software diagnostic and self-healing features employed by DCS effective in monitoring the status of every component in its system, testing itself without interrupting service, and capable of rapid reconfiguration without service disruption?
- Are the network operations, administration, maintenance and provisioning (OAM&P) features effective in setting up and testing customer circuits, provisioning and maintaining the terminating digital facilities and in maintaining the cross-connect system itself?
- Do the system growth and retrofit methods and procedures contribute to service disruptions?
- Are the automatic and manual tools adequate for detecting and repairing software problems (e.g., generic program bugs, database corruptions, transient registers in incorrect states, etc.)?
- Are there adequate software change control processes for corrective software changes (i.e. patches) to the current software load? Do these processes assure propagation of these corrective software changes to appropriate existing and new software loads (forward and backward propagation)? Are there adequate mechanisms for timely and high quality delivery and implementation of these corrective software changes?

D

D

team.

A. Data should be collected on each of the areas of concern identified previously. Since there are well over 20 manufacturers of DCS with numerous models to serve various needs, a threshold issue to be addressed is the type of DCS to be included in the work program. It is recommended that this threshold be based upon the capacity of the DCS and its estimated market share. Initial attention should be focused on those DCS models having high capacity and high utilization.

B. In analyzing the data associated with DCS in-service performance, it should be determined if any patterns exist of hardware, software, or OAM&P problems that could result in service disruptions.

C. The team should consider systems engineering analyses of network architectures, self healing capabilities, system monitoring system recovery, alarming and testing capabilities. If problems are identified, recommendations for correction should be developed.

D. The team should also consider evaluating the people processes used for controlling DCS changes and installation activity that could potentially disrupt service and recommend the best industry procedures.

E. The team should consider the porting of appropriate processes and tools used in switching for managing generic software and database changes in the digital cross-connect systems.

F. The team should also identify any issues associated with DCS and the introduction of SONET into telecommunications networks and prioritize for potential future study.

Confidential Information

Arrangements must be established to protect confidential and proprietary information and to insure that any such information is included in reports only on an aggregate/or masked basis.

Existing Work Efforts

We are currently unaware of any industry-wide efforts directed at all of the above concerns.

Focus Group Additions

— Are the network reliability requirements and/or objectives complete and sufficient to require/assure DCS system defensiveness.

— IEEE DCS Workshops can be used to address some of these concerns.

- Are the methods of procedures utilized by communications technicians effective in controlling DCS changes and installation activity that could potentially disrupt service?
- Are alarms available and effectively monitored to assure that minor troubles do not escalate?
- Are survivable network architecture guidelines available and are they implemented for appropriate services?
- How will the introduction of SONET into telecommunications networks impact the overall reliability of DCS?

Description of Proposed Work

The team working this issue should consider the following total quality process to quantify the vulnerability of networks using DCSs, identify major DCS reliability issues and propose problem solutions.

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 network & DCS reliability improvement.
2. Perform sufficient analysis of the data to determine the root cause(s) of the problem(s). 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 (e.g., the best methods to prevent and deal with the effects of DCS failures) 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 DCS focus

Appendix 2

D

D

DCS FOCUS GROUP QUESTIONNAIRES

Please help us with a survey on performance of Digital Cross-connect Systems (DCSs). We are attempting to understand what has gone and could go wrong with these important network elements, so that we can give recommendations to improve network reliability.

This package includes a one-page questionnaire and a four-page questionnaire.

Questionnaire No. 1 requests some general information about yourself and the population of DCSs on which you are reporting. Please fill out and return only one copy of that Questionnaire.

Please fill out a copy of the four-page questionnaire (Questionnaire No. 2) for every major outage or incident since June 1, 1991, affecting one of the DCSs on which you are assigned to be surveyed. For the purposes of this survey, the term *outage* refers to a loss of the transport function on the affected channels, while the term *incident* refers to a loss of the reconfigurability function, alarm visibility, or the ability to communicate with the main processor of the DCS. An outage or incident is considered to be *major* for this survey if it affects ten or more DS1s, or one DS3 channel. Please use one copy of Questionnaire No. 2 for each such failure, and fill it out as completely as possible.

We truly value your cooperation in this effort. Thank you.

D

DCS Focus Group - Questionnaire No. 2
Information on Individual Outages and Incidents

Section 1. General information.

- Name of LEC or IEC:_____
- Location of failure (city, state, office):_____
- Environment (staffed, unstaffed):_____
- Failure date:_____
- Starting time (hour:minute, AM or PM)_____
- Duration of outage or incident (minutes):_____
- Equipment vendor/model:_____
- Software release:_____
- Did the responding craft have formal training on the affected DCS?

  ☐ Yes ☐ No

- Who responded to the outage or incident?

  ☐ Central Group (Tier 1)
  ☐ Support Group (Tier 2)
  ☐Vendor ☐Local craft only

- Did the responsible craft have duties other than DCS maintenance and operations?

  ☐ Yes ☐ No

- Was the DCS connected to Operations Support Systems (OSSs)

  ☐ OPS/INE ☐ NMA ☐ ITS

  ☐ Other(specify system and software release: _____)

  ☐ None

- Language used in Craft Interface

  ☐ PDS ☐ TL1 ☐ Menu-Driven ☐ Other_____

D

DCS Focus Group - Questionnaire No. 1
General Information

Information on person filling out this form:

Name:_____ Date:_____

Title:_____

Telephone number:_____

Company:_____

Address:_____

_____

DESCRIPTION OF DCS POPULATION ON WHICH YOU ARE REPORTING

Use the table below to describe the DCSs on which you are reporting. For rows labeled DCS 1/1, DCS 1/0, etc., indicate the number of systems on which you are reporting. For the indented rows below each such entry, indicate the aggregate number of DS1 and DS3 terminations on each kind of DCS.

	Total Numbers	
	Staffed*	Unstaffed*
DCS 1/1		
No. of DS1s		
DCS 1/0		
No. of DS1s		
DCS 3/3		
No. of DS3s		
DCS 3/1		
No. of DS1s		
No. of DS3s		
DCS 3/1/0		
No. of DS1s		
No. of DS3s		

Send this form to: John Healy. Bellcore. 331 Newman Springs Road. Room NVC 2X227. Red Bank. NJ 07701-7040. telephone 908-758-3065. fax 908-758-4344

* *Staffed* refers to offices staffed on a regular basis. e.g.. 8AM-5PM. Monday-Friday.

D

Section 3. Cause(s) of failure.

If more than one cause contributed, check all applicable causes.

- ☐ Hardware failure
- ☐ Firmware failure
- ☐ Software failure
- ☐ Procedural error of telephone company (failure to follow documented instructions)
- ☐ Documentation unavailable or out of date
- ☐ Error in vendor documentation
- ☐ Error by vendor personnel (including personnel from DCS vendor and other vendors in telephone company office)
- ☐ Act of God (including lightning and natural disasters)
- ☐ Scheduled event (including scheduled loads of configuration maps or generic software, and any other scheduled craft activity that results in loss of service or function)
- ☐ Environmental (including contamination, leaks, building temperature, etc.)
- ☐ Operations support system failure (specify system and release:_____)
- ☐ Other (including power failure and failure of connecting equipment)

Describe how the failure occurred. (Example: while re-writing the configuration map on one memory unit, the other memory unit hardware failed.)

_____

_____

_____

_____

D

Section 2. **Breadth and depth of failure.**

- Number of affected working channels and interfaces (fill in table)

KIND OF CHANNEL	NUMBER OF AFFECTED WORKING CHANNELS	NUMBER OF WORKING CHANNELS
DS1		
DS3/STS1/OC1		
STS3/OC3		
OC12		
OC24 or higher speed		

(Note that the number of affected channels, not boards, should be entered in the table. For example, if seven DS1 interface boards are affected, and each board interfaces eight working DS1 channels, then $7 \times 8 = 56$ should be entered above.)

- Impact on affected channels (check all that apply)
  - ☐ Complete loss of service (no transmission on affected channels)
  - ☐ Loss of reconfigurability function
  - ☐ Loss of alarm visibility
  - ☐ Loss of protection switching function
  - ☐ Loss of ability to communicate with processor
  - ☐ Other (describe):

  _____

  _____

- What was the first indication of trouble? (Check all that apply.)
  - ☐ Local alarm
  - ☐ Remote (OSS) alarms
  - ☐ Customer complaint
  - ☐ Routine maintenance
  - ☐ Other (describe):_____

D

Appendix 3

D

Section 4. Trouble resolution, observations, and recommendations for preventing recurrences.

Trouble resolution (Check all that apply.)

- ☐ Trouble was resolved by local craft.
- ☐ Trouble was resolved by local craft with vendor assistance.
- ☐ Trouble was resolved by local craft with assistance of Tier 2 Technical Support (RTAC, ESAC, etc.)

Was there any delay due to dispatch of field forces?

☐Yes ☐No

Describe how the trouble was resolved.

_____

_____

_____

_____

Provide any suggestions you may have for avoiding similar problems in the future. These may include suggestions for DCS features, features in connecting systems including Operations Support Systems, documentation changes, increased or different training, or any other relevant area.

_____

_____

_____

_____

D

Digital Cross-Connects
Network Applications Subgroup
Recommendations

1. Executive Summary

Digital cross-connect reliability requirements were studied from an applications perspective. The application considered in this analysis are high availability services, high capacity services, centralized controller restoration and multiple ring interconnect. A generic question of "how big is too big?" was also studied. Best practices and recommendations are presented based on these findings.

- Cross-connect reliability requirements are sufficient to meet existing service demands.
- Evolving services and technologies will require review of the allocation of theoretical downtime between hardware, software and specific network elements.
- Each carrier should look at "how big is too big" from a cost, reliability application, and procedural perspective.
- Redundant controllers and OS links are an important part of high availability command and control of cross-connects.

2. Introduction

The evolution of the network and increasing demands for reliability/survivability suggest a reexamination of digital cross-connect (DCS) reliability requirements is necessary to ensure consistency with the evolving network.

2.1 Evolving Services are changing Cross-connect Requirements

Digital Cross-Connect Systems are deployed in the network to provide benefits of equipment consolidation (e.g., multiplexers and channel banks for DCS 3/1 and DCS 1/0, respectively), facility grooming, bandwidth management, and centralized operations. Special services, such as business non-switched service, are the predominant traffic carried on DCSs. For these DCS applications, service outage is defined as an interruption in existing cross-connections. Therefore, an out-of-service condition of the administrative controller or communication port of the DCS was not measured as a "service interruption". The reliability of a DCS was focused primarily on the termination ports.

With the introduction of new services carried through DCSs, such as video dial-tone, customer control, real time surveillance, and network restoration, DCS suddenly are in a different network application arena. Although DCSs continue providing the "basic" functions in the network, service evolution has definitely redefined their functionality. Under new service offerings, the availability to access and interrogate DCSs becomes a critical factor in meeting the customers' needs. The DCS service evolution has impacted not only the functions but also the architecture of the systems. The issue of DCS reliability will need to be carefully reexamined in order to meet the new challenge and definition of DCS service.

An examination of cross-connect requirements from the perspective of customer services is used to provide both quantitative and

D

D

Fully Diverse Service

Section	Outage (min/yr) (hardware only)	Availability
TM	0.25	99.9999525
Each Branch	3.1	99.9994106
Diverse Path	0.00001827	99.99999999653
End-to-End	**0.50001815**	**99.9999049**

This represents the sum of 2 TMs and the diverse path.

The largest contribution to the theoretical downtime is the two terminal multiplexers (these could be add/drop) that appear at the customer premise. Therefore, in the fully-diverse application, the duality of the path protects the user from DCS outages, while the near-end equipment is the major contributor to equipment risk.

3.4 Centralized Facility Restoration

3.4.1 How does the application drive reliability requirements?

3.4.1.1 Description of the application The restoration of failed circuits using a DCS to reroute traffic is an important current and future DCS application. The current method of restoration is centralized, where alarms are sent to a central location, the failure is analyzed, and reconfiguration commands are sent back to the DCS for implementation. This form of restoration has benefits compared to other forms of restoration currently available such as diverse fiber routing or SONET rings, depending on the network topology, complexity, and size.

The centralized DCS restoration typically takes two forms, either using pre-determined plans, or using the existing network topology and spare capacity at the time of the failure to dynamically determine re-routes. The pre-determined plans make use of a DCS feature of "pre-stored alternate maps", where many possible alternate configurations are pre-stored in the DCS and the central system sends a single command to invoke a particular configuration. However, for the purposes of the reliability analysis below, we will not make any distinction between these two methods.

3.4.1.2 Assumptions

1. The restoration is typically invoked in response to a major failure, such as a fiber cut or a node failure. We assume a mean-time-to-repair for these events of 8 hours (or 500 minutes), i.e. service is restored in 500 minutes.
2. The current centralized restoration systems perform the restoration in 5 minutes.
3. The typical circuit that is part of the restorable network goes through 10 DCS ports on the service path.
4. The network topology is such that 10 DCSs are involved in the restoration of a circuit. To simplify the analysis, we assume that if any of the 10 DCSs are unavailable for alarming or reconfiguration, the restoration does not proceed and it takes the full 500 minutes to restore the service. This is a conservative assumption because there may be multiple alternate paths that can be used by the central OS to route around the failure, even if a DCS in the primary path does not respond.
5. A typical major failure will involve 100 circuits (typically DS3s today).
6. The number of major failure events per year per circuit that invoke restoration is 0.1 failures per circuit per year. Obviously this varies with the length of the circuit and other factors such as the construction activity.
7. The total number of major failure events per year in the US that should invoke restoration is 200. This is

qualitative assessments of current practices.

From a complete list of DCS applications, four specific network applications were studied in detail. These applications are: multiple ring interconnect, high capacity services, high availability services, and centralized controller restoration.

3. Discussion and Analysis

3.1 Interconnected ring service analysis

Multiple interconnected ring services are represented by **Figure 1**. The fundamental requirement of the cross-connect in this application is connectivity of differing types of circuits from varying parts of the network.

This application does require the DCS to be of sufficient size to allow seamless connection of traffic between rings. The effect of larger system size on DCS requirements is discussed later in **Section 3.7.**

3.2 High Capacity Services

This application does require the DCS to be of sufficient size for the provisioning, monitoring and control of higher capacity services. Service offering into the gigabit range are now offered in some areas. The effect of larger system size on DCS requirements is discussed in **Section 3.7**.

3.3 High Availability Services

Most high availability services can be modeled by the 50-mile HRC [Hypothetical Reference Circuit (TR-418)] shown in **Figure 2**. The total downtime allocation for this HRC model is 21 minutes per year (99.996%). The hardware allocation is 3.0 minutes per year. Let's compare this with tariffed services.

Model	Downtime Allocation (min/yr)	Availability
50-mile S-HRC	3	(1) 99.9994296%
Tariffed Service	0.4	(2) 99.9999239%

(1) allocation for hardware causes only.
(2) allocation for all causes.

The 3 minute allocation in the 50-mile HRC is for hardware failures *only*. Software and media failures are excluded.

Where these services are tariffed, the requirement is based on any outage greater than two seconds in a month requires credit back to the end customer. The tariff is also applied *regardless* of the root cause of the outage - fiber, hardware or software.

However, the protected service is not just based on a linear model as shown in **Figure 3**. The model should consider the fully diverse architecture of the service. Typically, no regenerators are used in this application, and therefore, comparison to the 50-mile HRC is appropriate.

With this model, the end-to-end availability of the service based on HRC downtime allocations can be calculated by using HRC network element requirements in the high availability service model. This calculation is based on the combination of availabilities for the diverse path given by the formula A1+A2-A1A2, where A1 is the availability of one path and A2 the availability of the other path. The remaining availability is the product of the Terminal Multiplexer (TM) allocation. Finally the TM and diverse path availabilities can be combined to predict the theoretical availability of the service shown in **Figure 3**.

D

on one circuit pack), this can be lumped into the factor p. Therefore, the expected circuit outage time per event is 5 min. + p x 500 min. This relative analysis then requires that the contribution from the second term is much smaller than the first term. If we quantify much smaller as 10%, then the requirement is that

$$500 \times p < .1 \times 5 \text{ or } p < 0.001$$

This means that the restoration network should be available 99.9%, but since there are 10 DCS involved in the restoration, this implies that each DCS should be available 99.99% which translates to a controller unavailability of less than 50 min./year.

3.4.1.8 Absolute Analysis The total downtime per circuit due to controller availability is

$$0.1 \text{ events/year} \times 500 \text{ min./event} \times p, \text{ or } p \times 50 \text{ min./yr.}$$

Typically where tariffed, these services require availability in the range of 99.95% to 99.99%. If we propose a high availability service (discussed in Section 3.3) with a tariffed availability of 99.9999% or 0.5 minutes per year, then the contribution to the circuit unavailability due to the controller availability should be small. If as above, we define small as 10%, then

$$p \times 50 \text{ min./yr.} < 0.1 \times 0.5 \text{ min./yr. or } p < 0.001$$

This translates to a per DCS availability of 99.99% or 50 minutes/year controller unavailability.

3.4.1.9 Frequency of Major Event As discussed above in the assumptions, it seems likely that there are less than 200 major failures in the US per year that require restoration. If there should not be unrestorable outages more than once every 5 years, then the restoration system should be available 99.9%, which again translates to a DCS controller availability of 99.99% or unavailability of 50 minutes per year.

3.4.2 Performance

If the restoration needs to be performed in 5 minutes for 100 circuits, then 1 second per configuration command at a DCS may not be adequate. The worst case has 200 commands at a DCS (disconnect followed by connect for each circuit), which takes a significant fraction of 5 minutes. However, the restoration topology may need to be investigated in more detail before changing any requirements. Possibly the DCS should have a new disconnect/connect command for restoration purposes or maybe the time per command should be reduced somewhat to meet the overall service requirement.

3.4.3 DCS Requirements

To summarize the above requirements

1. DCS port requirements of 0.2 minutes per year end-to-end are acceptable.
2. DCS controller availability requirements of 50 minutes per year seem acceptable. There is certainly no evidence that the controller availability needs to be more stringent than existing requirements of 14 minutes per year.
3. Performance requirements of 1 second per cross-connect may need to be tightened to meet the 5 minute goal for the restoration.

3.4.4 Future Directions

DCS restoration may be enhanced in three ways in the future.

1. Centralized restoration may be improved to achieve restoration times around 30 seconds.
2. Distributed restoration will become available, with response times that are possibly around 2 seconds.

D

clearly related to the size of all of the networks, e.g. the number of route-miles and the construction density along each route. Major failures are rare, and it seems unlikely that there are more than a few hundred such incidents in the US per year. (Note: this assertion is consistent with the finding of the Fiber Cable Focus Group).

3.4.1.3 Analysis This section will determine the impact on DCS requirements in the following four areas:

1. Per-circuit outage time
2. Total system outage
3. Controller unavailability
4. Performance

3.4.1.4 Per-circuit Outage Time The additional circuit downtime per year due to having the DCS in the circuit, if it was not there already, is in the neighborhood of 2 minutes per year, based on 0.2 min./year end-to-end port requirements on DCS ports (for DS3 and higher rates) and assuming 10 ports involved in the circuit. The downtime due to a major failure is 0.1 events/year x 500 minutes per event or 50 minutes per year if there was no restoration, so the additional contribution to having a DCS in the circuit is negligible compared to the outage that would occur because there was no restoration.

3.4.1.5 Total System Outage The requirements on total system outage are small enough (0.02 min./year) that there is no additional impact in having a DCS in the circuit. However, field experience may show that this number is significantly higher. (This assumption should be reviewed in light of the present findings.)

3.4.1.6 Controller Availability There are three possible methods of analyzing controller availability requirements.

1. The first and simplest analysis is to calculate the controller unavailability under the condition that the relative additional expected downtime due to controller failures is small compared to the downtime that is expected, even if restoration occurs successfully.
2. The second analysis is to estimate the absolute circuit unavailability due to controller unavailability during restoration and require that it be smaller than the level required by some particular service.
3. The third analysis is to determine the frequency that the loss of controller will lead to an FCC reportable event or other major customer impact.

3.4.1.7 Relative Analysis We assume that restoration is unavailable for a fraction p due to controller unavailability, unavailability for a fraction q due to OS-link unavailability, and unavailable for a fraction r due to OS unavailability. The expected circuit outage time per event is

$$(1-p-q-r) \times 5 \text{ min.} + (p+q+r) \times 500 \text{ min.}$$

which is approximately equal to

$$5 \text{ min.} + (p+q+r) \times 500 \text{ min.}$$

since p+q+r is assumed small. The contribution due to OS unavailability is unrelated to any DCS requirements, but the contribution due to the OS links can be related to some DCS requirements. For example, if the DCS has two communications ports and the DCS can receive commands from both ports, then the contribution due to OS link failure can be made very small if the network provider constructs fully diverse OS links. If the DCS has a single point of failure (e.g. both links are

D

The loss of the control system results in the inability to control or reconfigure the system but generally does not affect service provided by existing cross-connections.

3.7.2 Software

The software in a DCS consists of two components: the operating system and the office database. The size of the operating system depends on the features provided in the software load. Therefore, the probability of a software bug in the operating program of a large DCS should not be any greater than in a smaller DCS (although the large system may have more opportunities for problems due to greater interaction of the hardware and software modules). However, the office database is directly related to the DCS size. Therefore, the larger DCS is likely to experience a greater number of database errors resulting from provisioning errors.

A major concern with the larger DCS is the reduced speed of processing changes, updates, reboots, and daily backups. For example, a reboot of the control processor following a software or hardware failure in the active processor generally includes downloading the database to all the distributed peripheral control units. For a large system, this can take up to one-half hour since each peripheral control unit is updated sequentially. The longer the update period, the greater the potential for an outage since protection switching may be denied during portions of the update process.

Another factor which may affect the reliability of the network (or availability of the DCS control subsystem) is the daily backup of the office database from disk to tape. This process can take up to an hour in a large system during which time the control subsystem is unavailable for most administrative functions. Protection switching and alarm reporting is generally provided by most DCSs during this backup process. The daily backup activity actually has a far greater impact on the availability of the control system than the probability of either hardware or software failure.

3.7.3 Risk of a Large Scale Outage

Assuming that the traffic concentration in the network has been reasonably distributed, the answer to the question "how big is too big" largely depends on the relative risk of a large scale outage. At present, W-DCSs can handle 250 DS3s with future versions capable of handling 1000 or more DS3s. B-DCSs are currently capable of over 2000 DS3s. It should be noted that regardless of whether all or part of the traffic passes through one DCS, all of the traffic remains at risk if it passes through a single Central Office (CO). From a probability standpoint, the question that arises is whether the likelihood of having a complete CO outage is significant compared to a complete DCS outage. Causes of an entire CO outage include fire, flood, loss of CO power, etc., while a complete DCS failure requires multiple failures or a possible procedural error (e.g., accidental reconfiguration of the matrix).

In a typical telephone network, if the probability of a complete DCS network element failing (i.e., double failure or procedural error) is greater than that of an entire CO outage, a distributed DCS architecture adds little to the reliability of the network. On the other hand, when the risk of an entire CO outage is greater than that of a complete DCS network element failing, justification can be made for a distributed DCS architecture.

There are several topics which need to be considered by each carrier when considering whether one large or two small machine implementation is appropriate.

1. **Office floor space limitations.** Two machines of any type are somewhat larger than a single machine given the

D

3. DCSs will be integrated in SONET rings.

The second and third analyses above on controller availability are unaffected by the improvement in restoration speeds. The first analysis, the relative analysis, is affected and it leads to correspondingly more stringent DCS requirements. However, it is not obvious that the relative analysis is the most meaningful in these cases, and care should be taken in deciding whether there is a need to tighten the controller availability requirements.

Obviously, there will need to be an improvement in performance. Restoration in 30 seconds implies reconfiguration speeds an order of magnitude faster and restoration in 2 seconds may require an improvement of two orders of magnitude. Clearly, a much better understanding of these restoration scenarios and application to telecommunications networks is needed before proposing any major (and possibly costly) changes to DCS reconfiguration performance.

3.5 Processor/OS Link Requirements

Figure 4 shows representative OS-DCS implementations commonplace in the network today.

In both cases, there is a single link to the OS port on the DCS. With the advent of customer controlled reconfiguration, and the increasing importance of network survivability, the availability of these links may no longer be sufficient. Alarms reported are reported via telemetry or over the OS link.

The telemetry (contact closures) provided by the cross-connect does not provide the detailed reporting messages that can be used to remotely identify and correct equipment or network problems. The telemetry can be used for local office alarming.

Simplex dial-up or dedicated links are subject to network reliability and often, simplex modems or control interfaces. The X.25 interface is preferred from a reliability perspective because of its ability to dynamically reroute messages to their destinations.

In many real-time systems, it is not uncommon for designs to be I/O bound in the communications or mass storage interface. With increasing real-time processing requirements on digital cross-connects, these bounds will be more apparent. Hence, special consideration should be given to redundancy of I/O links.

3.6 DCS Allocations with and without integrated optics

The allocation of availability in the integrated optics case is done on a per office, rather than a per network element basis represented by Figure 5. It has been proposed that the reliability requirements of the DCS with or without SONET integrated optics be identical (0.1 min./yr.), but is still under review.

3.7 How Large is Too Large?

The major (or primary) benefits of increasing DCS size include: decreased cost per port, reduced floor space and power, reduced cable congestion, and simplified administration and maintenance. In examining the tradeoffs, issues pertaining to hardware and software reliability and the risk of a large scale outage are addressed below.

3.7.1 Hardware

- For systems with redundant port modules, the estimated downtime on a per port basis is not affected by the DCS size.
- The probability of a total system outage affecting all ports is generally not affected by the DCS size due to the modular structure of the matrix.
- The probability for the loss of the control subsystem is independent of office size.

D

practice for high controller demand applications may require an alternate OS link to the DCS.

- Cross-connect times may have to be improved for restoration applications. A single disconnect/connect command may be required.

NRC DCS Network Applications Subgroup

John Adler	Alcatel
Joe Cheng	Bellcore
Bruce Cortez	AT&T
Fred Ellefson	Alcatel
Fred Hawley	Bellcore
Ken Manke	Bell Atlantic

D

elimination of common equipment and DSX appearances.

2. **Physical proximity risk.** If more than a single machine were used, there are risk elements that can affect both machines (fire, flood, power outages etc.) Placing both machines in the same physical location, i.e., back-to-back is less reliable than two machines in separate offices.

3. **Aversion to tie lines.** A multiple machine architecture requires tie-lines. How difficult or expensive is it to maintain these lines?

4. **Probability of a double failure.** All cross-connect matrices have some form of redundancy to prevent total outages due to single failures. The statistical probability of a double failure is very small. However, if/when it does occur it could fail some or all of the cross-connect paths.

5. **Impact of a total failure.** The real impact of losing an entire DCS is driven by the number of lines affected, customers using those lines and the type of service provided.

6. **Network Architecture.** If there were a DCS outage, what is the impact on surrounding facilities? How are SS7 links distributed?

7. **Equipment Cost.** The cost of purchase, installation, maintenance, and upgrades of two independent machines would be higher than a single machine.

8. **OAM&P Costs.** The on-going cost of OAM&P for multiple machines would be higher than a single machine.

4. Findings and Recommendations

SONET High Availability Service Application

- Existing cross-connect reliability requirements are sufficient.
- The majority of the theoretical cause of hardware failure is the customer premise terminal.

SONET Multiple Ring Interconnnect Application

- Existing cross-connect reliability requirements are sufficient.

SONET Centralized Restoration Application

- Existing cross-connect controller availability requirements are sufficient.
- Existing DCS port availability requirements are sufficient.

SONET High Capacity Services

- Existing cross-connect reliability requirements are sufficient.

Other Findings

- Cross-connect and ADM reliability requirements will require further study with the advent of integrated SONET.
- Allocation of software and hardware failure rates in the network model needs further study with the advent of integrated optics.
- New services such as customer control, distributed restoration and switched high capacity services place more importance on OS-NE communications and controller availability.
- OS link design is a critical element in the control function of the DCS. Best

D

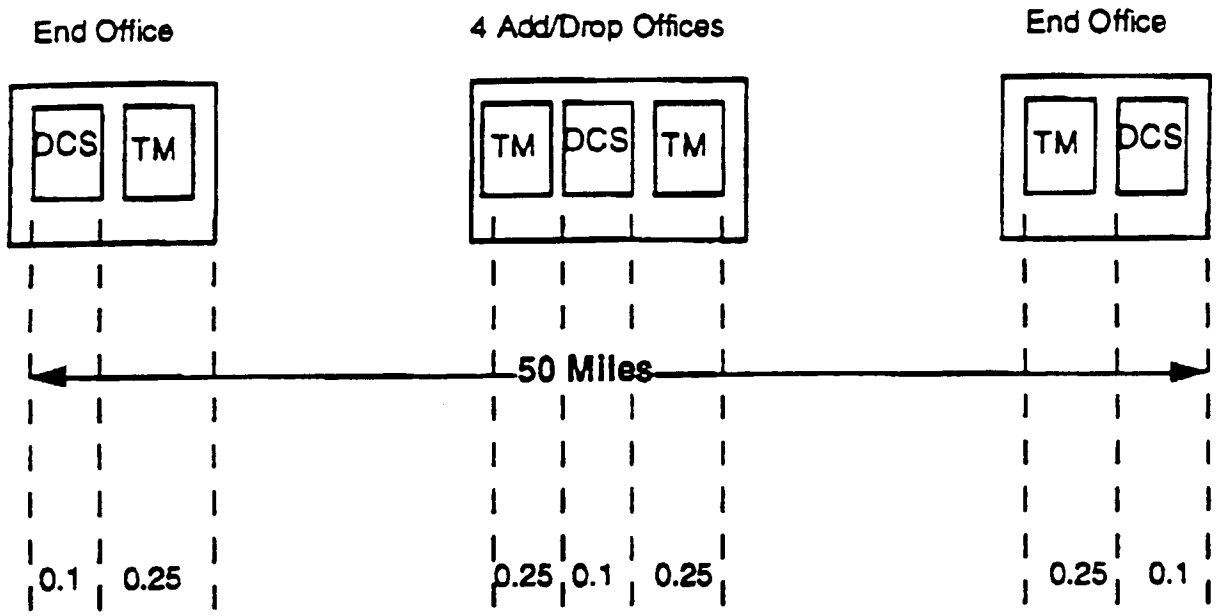
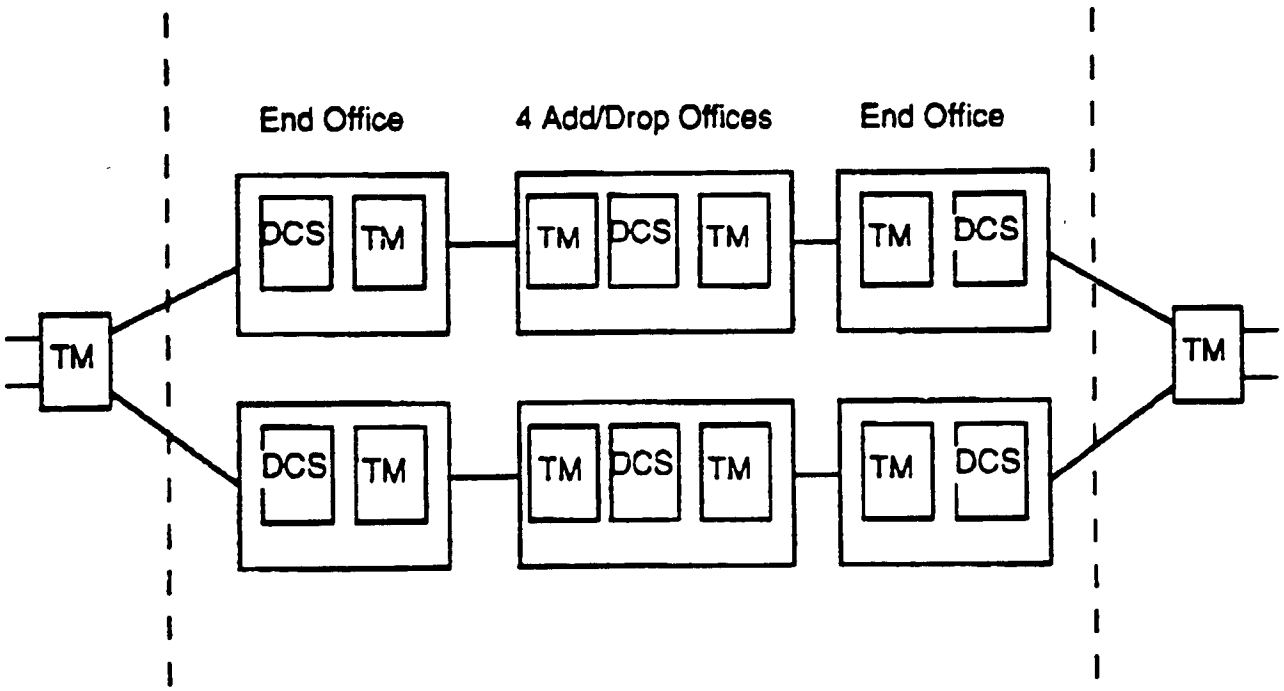


Figure 2 . SONET HRC Model (TR-418) - 50 Miles



Min./yr. Outage 0.25 3.1 per branch 0.25

Figure 3. High Availability Service Model

D

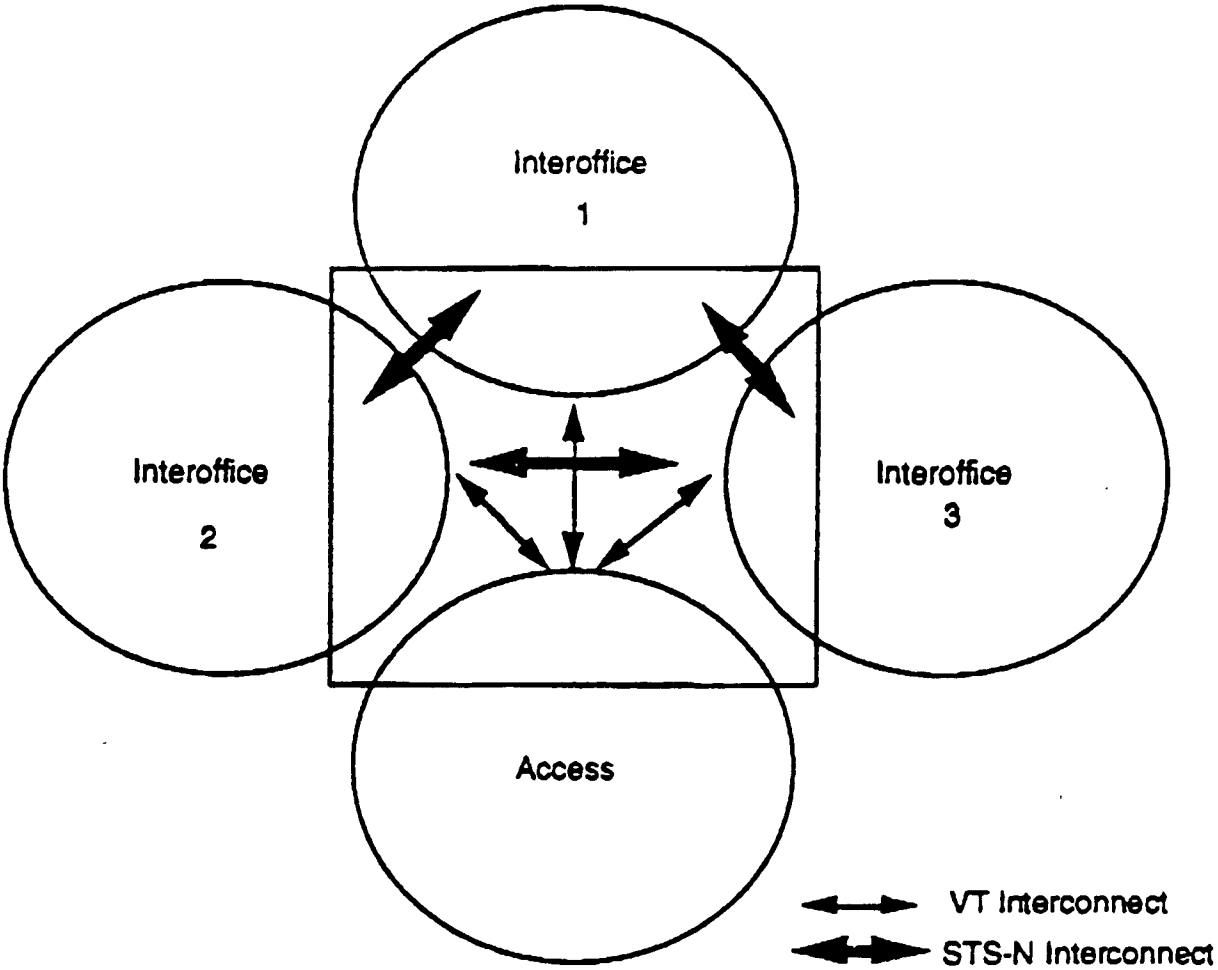


Figure 1. Multiple Ring Interconnect Application

D

Appendix 4

D

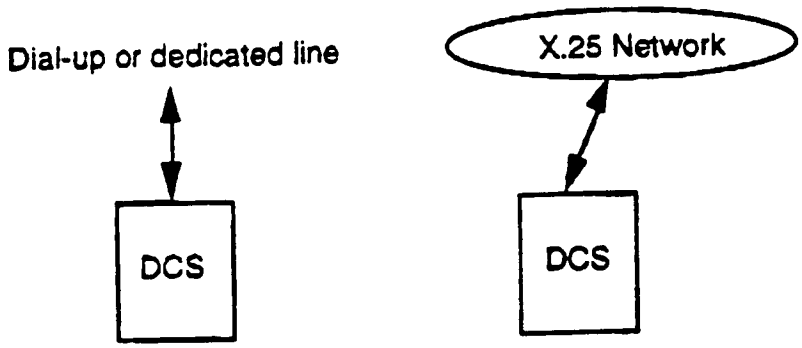


Figure 4. Common OS Link Designs

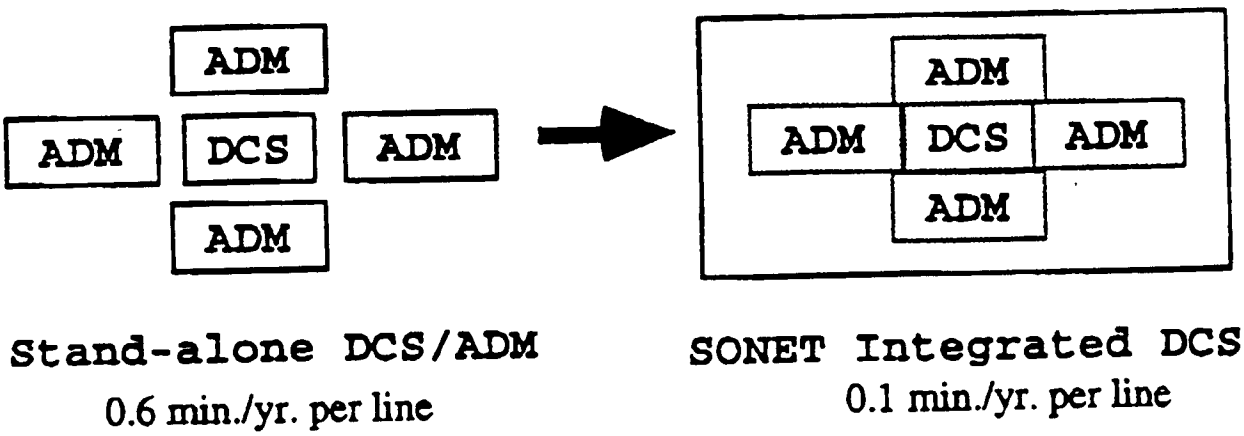


Figure 5. Effects of SONET Integration on Requirements

D

Network Reliability Industry Initiatives

Focus Area: Digital Cross Connect System

Topic	Industry Group	Doc. No. Issue No. Standards No.	Version No. and Date	Title	Brief Description
Network Reliability Performance Objectives	Bellcore	TR-NWT-000170	I2, 1/93	Digital Cross-Connect System Generic Requirements and Objectives	Generic requirements for digital cross connect systems
	Bellcore	TR-TSY-000179	I1, 7/89	Software Quality Program Generic Requirements (SQPR)	Requirements for telecomm software development process
	Bellcore	SR-NWT-000821	I3,12/90	Field Reliability Performance Study Handbook	Generic guidelines for conducting field performance studies
	Bellcore	TR-TSY-000929	I1,6/90	Reliability and Quality Measurements for Telecommunications Systems (RQMS)	Bellcore's view of generic requirements regarding supplier measurements
	Bellcore	TR-TSY-000929	I1,R1,5/92	Reliability & Quality Measurements for Telecommunications Systems (RQMS)	Bellcore's view of generic requirements regarding supplier measurements
	Bellcore	TR-TSY-000929	I1,S1, 3/91	Reliability & Quality Measurements for Telecommunications Systems (RQMS) RQMS Performance Report	Bellcore's view of generic requirements regarding supplier measurements

D

Network Reliability Industry Initiatives

Focus Area: Digital Cross Connect System

Topic	Industry Group	Doc. No. Issue No. Standards No.	Version No. and Date	Title	Brief Description
Network Architecture and Design	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-NWT-000332	14,9/92	Reliability Prediction Procedure for Electronic Equipment	Contains the recommended parts count, laboratory and field tracking 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
	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 Component	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

Network Reliability Industry Initiatives

Focus Area: Digital Cross Connect System

Topic	Industry Group	Doc. No. Issue No. Standards No.	Version No. and Date	Title	Brief Description
Network Reliability Performance Objectives	Bellcore	SR-TSY-001136	11, 1/89	Handbook for Digital Cross-Connect System Quality & Reliability Analyses	
	ANSI	T1A1.2/93-015	2/93	Draft Proposed Technical Report on Network Survivability Performance, Project T1Q1/90-004R2	Survivability as a function of architecture
	IEEE	Trans on Reliability	Vol 40, 10/91	Using Distributed Topology Update and Preplanned Configurations to Achieve Trunk Network Survivability	

Network Reliability Industry Initiatives

Focus Area: Digital Cross Connect System

Topic	Industry Group	Doc. No. Issue No. Standards No.	Version No. and Date	Title	Brief Description
Network Architecture and Design	ANSI	T1A1.2/93-015	2/93	Draft Proposed Technical Report on Network Survivability Performance, Project T1Q1/90-004R2	Survivability as a function of architecture
	ANSI	T1S1			Congestion in SS7 networks
	IEEE	Trans on Reliability	Vol 40, 10/91	Using Distributed Topology Update and Preplanned Configurations to Achieve Trunk Network Survivability	
	CCITT	Study Group II			Survivable architectures
	CCITT	Study Group XVIII			Survivable architectures

Network Reliability Industry Initiatives

Focus Area: Digital Cross Connect System

Topic	Industry Group	Doc. No. Issue No. Standards No.	Version No. and Date	Title	Brief Description
Network Architecture and Design	Bellcore	SR-TSY-001171	I1,1/89	Methods and Procedures for System Reliability Analysis	Outlines the general methods and procedures Bellcore uses to predict hardware reliability
	Bellcore	SR-NWT-002419	I1,12/92	Software Architecture Review Checklists	Bellcore's view of SAR methodology and checklists
		Telephony	10/90	Getting to the source of network disasters	
	Comm T1	T1.101	87	Digital Networks	Synchronization Interface Standards for Digital Networks
	Comm T1	T1.102	87	Digital Hierarchy	Electrical Interfaces
	Comm T1	T1.104	91	Exchange-Interexchange Carrier Interfaces	Individual Channel Signaling Protocols
	Comm T1	T1.105	91	Digital Hierarchy	Optical Interface Rates and Formats Specifications
	Comm T1	T1.105a	91	See Above	See Above
	Comm T1	T1.106	88	Digital Hierarchy	Optical Interface Specifications: Single-Mode
	Comm T1	T1.107	88	Digital Hierarchy	Formats Specifications
	Comm T1	T1.107a	90	See Above	See Above

Network Reliability Industry Initiatives

Focus Area: Digital Cross Connect System

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
	ANSI	T1S1			Congestion in SS7 networks

Network Reliability Industry Initiatives

Focus Area: Digital Cross Connect System

Topic	Industry Group	Doc. No. Issue No. Standards No.	Version No. and Date	Title	Brief Description
Network Interconnection and Interoperability					

Network Reliability Industry Initiatives

Focus Area: Digital Cross Connect System

Topic	Industry Group	Doc. No. Issue No. Standards No.	Version No. and Date	Title	Brief Description
Operations, Administration, Maintenance	Comm T1	T1.104	91	Exchange-Interexchange Carrier Interfaces	Individual Channel Signaling Protocols
	Comm T1	T1.105	91	Digital Hierarchy	Optical Interface Rates and Formats Specifications
	Comm T1	T1.116	90	Signaling System 7	Operations, Maintenance and Administrative Part

Network Reliability Industry Initiatives

Focus Area: Digital Cross Connect System

Topic	Industry Group	Doc. No. Issue No. Standards No.	Version No. and Date	Title	Brief Description
Restoration and Recovery	Bellcore	FA-NWT-001353	11, 12/92	Restoration of DCS Mesh Networks with Distributed Control: Equipment Framework Generic Criteria	Early view of distributed control in mesh networks
	IEEE	Trans on Reliability	Vol 40, 10/91	Using Distributed Topology Update and Preplanned Configurations to Achieve Trunk Network Survivability	
	Comm T1	T1.115	90	Signaling System 7	Monitoring and Measurements for Signaling System 7 Networks
	CCITT	Study Group IV			Restoration studies
	CCITT	Study Group XV			Restoration requirements for DCS

Network Reliability Industry Initiatives

Focus Area: Digital Cross Connect System

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	I1,5/89	Reliability and System Architecture Testing	
	Bellcore	SR-TSY-001171	I1,1/89	Methods and Procedures for System Reliability Analysis	
	Bellcore	SR-TSY-001547	I1, 1/90	The Analysis & Use of Software Reliability & Quality Data	
	Bellcore	SR-NWT-002419	I1,12/92	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	

Network Reliability Industry Initiatives

Focus Area: Digital Cross Connect System

Topic	Industry Group	Doc. No. Issue No. Standards No.	Version No. and Date	Title	Brief Description
Human Factors Design					

Network Reliability Industry Initiatives

Focus Area: Digital Cross Connect System

Topic	Industry Group	Doc. No. Issue No. Standards No.	Version No. and Date	Title	Brief Description
Regulations	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

Network Reliability Industry Initiatives

Focus Area: Digital Cross Connect System

Topic	Industry Group	Doc. No. Issue No. Standards No.	Version No. and Date	Title	Brief Description
Network Security	Bellcore	SR-NWT-002374	I1, 10/92	Special Report on Digital Cross-Connect System Software Security Features	

Network Reliability Industry Initiatives

Focus Area: Digital Cross Connect System

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
	ANSI	T1S1			Congestion in SS7 networks

Network Reliability Industry Initiatives

Focus Area: Digital Cross Connect System

Topic	Industry Group	Doc. No. Issue No. Standards No.	Version No. and Date	Title	Brief Description
Operations, Administration, Maintenance	Comm T1	T1.104	91	Exchange-Interexchange Carrier Interfaces	Individual Channel Signaling Protocols
	Comm T1	T1.105	91	Digital Hierarchy	Optical Interface Rates and Formats Specifications
	Comm T1	T1.116	90	Signaling System 7	Operations, Maintenance and Administrative Part

Network Reliability Industry Initiatives

Focus Area: Digital Cross Connect System

Topic	Industry Group	Doc. No. Issue No. Standards No.	Version No. and Date	Title	Brief Description
Restoration and Recovery	Bellcore	FA-NWT-001353	I1, 12/92	Restoration of DCS Mesh Networks with Distributed Control: Equipment Framework Generic Criteria	Early view of distributed control in mesh networks
	IEEE	Trans on Reliability	Vol 40, 10/91	Using Distributed Topology Update and Preplanned Configurations to Achieve Trunk Network Survivability	
	Comm T1	T1.115	90	Signaling System 7	Monitoring and Measurements for Signaling System 7 Networks
	CCITT	Study Group IV			Restoration studies
	CCITT	Study Group XV			Restoration requirements for DCS

Network Reliability Industry Initiatives

Focus Area: Digital Cross Connect System

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	I1,5/89	Reliability and System Architecture Testing	
	Bellcore	SR-TSY-001171	I1,1/89	Methods and Procedures for System Reliability Analysis	
	Bellcore	SR-TSY-001547	I1, 1/90	The Analysis & Use of Software Reliability & Quality Data	
	Bellcore	SR-NWT-002419	I1,12/92	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	

Network Reliability Industry Initiatives

Focus Area: Digital Cross Connect System

Topic	Industry Group	Doc. No. Issue No. Standards No.	Version No. and Date	Title	Brief Description
Human Factors Design					

Network Reliability Industry Initiatives

Focus Area: Digital Cross Connect System

Topic	Industry Group	Doc. No. Issue No. Standards No.	Version No. and Date	Title	Brief Description
Regulations	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

Network Reliability Industry Initiatives

Focus Area: Digital Cross Connect System

Topic	Industry Group	Doc. No. Issue No. Standards No.	Version No. and Date	Title	Brief Description
Network Security	Bellcore	SR-NWT-002374	I1, 10/92	Special Report on Digital Cross-Connect System Software Security Features	