DIGITAL CROSS-CONNECT SYSTEMS

Louis J. Scerbo
Executive Director - SONET/Transport Analysis
Bellcore
445 South Street, MRE 2K378
Morristown, NJ 07960
(201) 829-3200

1. Executive Summary

Digital Cross-Connect Systems (DCS) are increasingly a standard part of many telecommunications service providers networks. High reliability in the DCS must be assured today due to the large and growing volume of traffic on digital facilities which are routed through the DCS and the vital role the DCS plays in recovering from network failures. Although little in the literature suggests any major reliability problems with the DCS, recent outages have demonstrated that when problems occur, the consequences are significant. For this reason the Network Reliability Council (NRC), through their subtending Network Reliability Steering Team (NO REST), chartered a DCS Reliability Focus Team to quantify the vulnerability of networks using DCSs, identify major DCS reliability issues and propose problem solutions. The DCS Focus Team, which consists of subject matter experts from the telecommunications and user community, have conducted a unique data collection and analysis activity to address these issues. The results of the analysis describe the Current Situation. **DCSs are very reliable network elements with Mean Time Between Outages of greater than 12 years. When they fail nearly half of the outages are resolved in less than one hour, however, 8% of the outages last for six hours or more. These systems are in the vast majority of cases staffed by trained craft and are effectively locally and remotely alarmed; however, they are very complex systems which require an up-to-date high level of expertise for most trouble resolution. In addition, DCS outages are correlated with activity and this activity is known to be increasing with new applications.** Because of the historical "plug-in" nature of the transmission business and the ever increasing sophistication of the DCSs, a paradigm shift is required for all involved if we are going to make significant improvements in the reliability.

Root Cause Analysis of the outages identified four broad categories for improvement; Procedures, Active Hardware, Passive Connecting Hardware and Software. It is recommended that Procedural Errors which accounted for 30-40% of the outages be counteracted by having service providers implement OAM&P practices patterned after those for switching equipment and having equipment suppliers treat Documentation and Training as a product with proactive user involvement. Active Hardware failures and their impact, which accounted for 20-30% of the outages, should be countered by increased inspection and surveillance of critical components of the DCS (matrix cards, bridging cards, sync cards, controllers, and disk drives), having sufficient spares of these critical components readily available to minimize downtime and going forward implementations with more robust matrix, disk drive and controller architectures. The team recommended that the only tried and true countermeasure to minimize Passive Connecting Hardware failures, which surprisingly accounted for 15% of the in-service outages, is to systematically inspect all

D

visible passive hardware during installation, during turnup, and periodically in service off peak hours. Software alone or in combination with hardware and/or procedural errors account for 10-25% of the outages reported and for the large majority of failures where there was no loss in service, however there was a loss of protection switching, access, or visibility into the DCS. To address this condition the team recommends to the equipment suppliers a rigorous software development process patterned after switching with particular attention being paid to enhanced software self-defensiveness.

The DCS Focus Team recommends the use of FCC outage reports per Docket 91-273 as the standard metric by which national DCS improvements will be tracked. They also recommend that service providers and equipment suppliers continue to collect actual field performance data and perform joint root cause analysis of all DCS outages to help prioritize their actions to be taken.

If these recommendations are appropriately applied to each of the individual equipment suppliers and service providers' current situations, the team would expect a significant reduction in the already low level of DCS related outages.

2. Background

Digital Cross-Connect Systems (DCS) are increasingly a standard part of many telecommunications service providers network transmission facilities. High reliability in the DCS must be assured today due to the large volumes of traffic on digital facilities which are routed through the DCS, and the vital role the DCS plays as a service restoration vehicle during cable cuts, facility electronics failures, central office failures, or other threats to service continuity. DCSs are also being planned and deployed for new service offerings such as flexible High Capacity Services (DS1, DS3, OC-N, etc.), High Available Services (automatic path diversity) and as a gateway for Multiple Ring Interconnections. These new applications put even higher demand on DCS reliability especially on the availability to access and communicate with the DCS to meet customer needs.

2.1 System Overview

The DCS is a software based, microprocessor controlled system that can switch, reorganize, and redistribute standard digital signals to and from interoffice facilities, distribution facilities, and terminating network elements within a central office in a nonblocking manner. These tasks are accomplished locally or remotely according to an electronically alterable memory map. Additionally, the DCS has test access, maintenance, and performance monitoring features.

Figure 1 represents a generic DCS model. The model consists of seven modules as described below. Those modules which have the greatest impact on performance and/or system downtime are chosen by designers for redundancy. The redundancies are provided either with dual circuitry or component protection switching.

- *Digital Interface* - Provides extraction and insertion of signaling information, conversion to internal clock rates, and some diagnostic functions such as: path connection, identification and verification, data path parity checks, filtering out incoming timing variations.
- *Switching Matrix* - Provides channelization of a signal for cross-connectability to and from any termination. These elements provide the transmission path through the DCS and are designed to be nonblocking.
- *Clock Synchronizer* - Provides an internal clock source that conforms to Stratum 3 or better clock requirements. This module usually interfaces two DS1 timing signals, one as the primary source and the other as the secondary source.

D

- *Main Processor or Controller* - Provides the ability to control the cross connection for any signal including test access, houses the primary and secondary data storage media, provides physical interfaces to the craft and other operations systems, gathers performance monitoring data, schedules system diagnostics, and compiles system reports.
- *Power Converter* - Converts -48Vdc to Internal dc voltages required by the DCS.
- *Alarm Interface* - Provides alarm messages, locally or remotely by monitoring alarm points in the system.
- *Terminal Interface* - Provides data link for local or remote administrative terminals.

2.1.1 Cross Connect System Types

There are different types of cross-connect systems, differentiated by feature and functions, including the digital level at which cross-connects are made.

- DCS 1/0 - Narrowband DCS, which crossconnects at the DS0 (64 Kb/s) level and interfaces the network at the DS0 and/or DS1 (1.544 Kb/s) levels.
- DCS 1/1 - Electronic DSX, which cross-connects and interfaces the network at the DS1 level.
- DCS 3/1 - Wideband DCS, which cross-connects at the DS1 level and interfaces the network at the DS1 and/or DS3 (44.736 Mb/s) levels.
- DCS 3/1/0 - which cross-connects at the DS0 level and interfaces the network at the DS0, DS1 and DS3 levels.
- DCS 3/3 - Broadband DCS, which cross-connects and interfaces the network at the DS3 level.
- SONET DCS - Synchronous Optical Network (SONET) is the transport platform for future technologies and services. SONET DCS will have SONET interfaces (OC-N, Optical Carrier - level N and STS-N Synchronous Transport Signal - level N) to support SONET-to-SONET as well as SONET-to-asynchronous cross-connections.

2.2 DCS as National Reliability Focus Area

Although little in the literature suggests any major reliability problems with DCS, recent outages have demonstrated that when problems occur, the consequences are significant because of the large volumes of traffic - often involving vital services - traversing the DCS. Furthermore, those recent outages have impacted the general public's perception of network reliability. For these reasons, the Network Reliability Council (NRC) endorsed the recommendation of its subtending Network Reliability Steering Team ("NO REST") to formulate an Issue Statement concerning "Reliability of Digital Cross-Connect Systems (DCS)", and to establish a Focus Team to "quantify the vulnerability of networks using DCSs, identify major DCS reliability issues, and propose problem solutions." Appendix 1 contains a copy of the Issue Statement.

3. DCS Focus Team

The DCS Focus Team consisted of subject matter experts of local and interexchange service providers, DCS equipment suppliers, and the user community:

Louis Scerbo	Bellcore, Focus Team Leader
Frank Ianna	AT&T-NSD, Focus Team Champion
Allen Adams	DSC
Steve Clark	Ad Hoc
H. L. Crim	BellSouth
Frank Denniston	New York Telephone
Robert Fitzgerald	Sprint
Bill Jones	AT&T-NS

D

Ken Lewis	Alcatel
Eva Low	Pacific Bell
Mike Nawrocki	Bell Atlantic
Rob Pullen	Tellabs
Phil Rubin	AT&T-NS
Carlos Santiago	ICA
Sid Shelton	Bellcore
Pete Shelus	AT&T-NSD

In addition, the team members received significant support from other members in their corporations. Figure 2 is a listing of only those supporting staff who made significant contributions.

3.1 Focus Team Structure

The Team organized its efforts into six sub-groups. (Figure 3) An Assess the Risk sub-group was formed to facilitate the data collection and analysis needed to understand the current situation. In parallel, five other sub-groups were established to acquire and share knowledge and industry practices in the areas of network applications and architecture, hardware reliability, software reliability, operations, training and documentation. Each sub-group established a work plan, and results were shared with the full team at regularly scheduled meetings.

The DCS Focus Team established as its theme: **Improve network reliability by reducing the likelihood and resulting service impact of DCS-related outages.** The basis for national improvement would be the measured reduction of FCC reportable DCS-related outages. The baseline for improvement will be the period April 6, 1992 through April 5, 1993, the first year of FCC reporting. The basis for individual corporate improvement would be the continuous reduction of one recommended in-service measure, total downtime/DCS/yr. This measure incorporates frequency, duration, and size of outage in a normalized form, can be easily baselined against the data collected for this effort, and should be easy to track on an ongoing basis (See Section 4.3.4 for definition and details).

4. Data Collection and Analysis Process

In order to understand the current situation and its attendant risks, the Assess the Risk subgroup developed two questionnaires to solicit information from the industry to answer the questions:

1. What is the existing level of risk?
2. Where are the DCS Systems most vulnerable?
3. What are the root causes of the field problems?
4. Are there any industry practices which have been shown to work?
5. Is there any correlation with fewer, shorter outages and assigned staff, training and documentation?
6. Did the alarm and operations systems help in the detection and resolution of problems?

4.1 Questionnaire Description

Questionnaire #1 requested general information about the responding company and the population of DCS being reported on. See Appendix 2.1 for a copy of this questionnaire.

Questionnaire #2 requested details on every major DCS-related failure since June 1, 1991. A failure was considered major if it affected at least one DS3 port or 10 or more DS1 ports. See Appendix 2.2 for a copy of this questionnaire.

The questionnaire used the following definitions:

Incident refers to the loss of reconfigurability function, alarm visibility, protection switching function, or the ability to communicate with the main processor, i.e., the event did not affect existing cross-connect traffic, but there was loss of protection, access to, or visibility into the DCS.

Outage refers to a complete loss of the transport function on the affected channels; i.e.,

D

the event was service affecting. For the purposes of the analysis, any event which resulted in the complete loss of transport of at least one DS3 port or 10 or more DS1 ports is considered an outage. Thus, in the analysis, the total number of failures is the total number of outages plus the total number of incidents.

Three members volunteered to trial the draft questionnaires within their companies, and the trial results were incorporated into the final version. Although this effort delayed the delivery of the questionnaires for about a month, it was invaluable in getting meaningful data.

4.2 Questionnaire Responses

In accordance with the procedures endorsed by the Network Reliability Council, Bellcore distributed the questionnaires and assembled the responses into aggregated form. The questionnaires were sent to 19 companies considered to be major "users" of DCSs; namely, all the major local and interexchange carriers, several alternate access providers (AAP), and several end user customers. The questionnaire was also sent to four DCS equipment suppliers. It was recognized that requesting information from both the equipment suppliers and the service providers/users could potentially result in duplicates. However, it was felt that distinguishing characteristics such as date and time of the event would enable Bellcore to identify these duplicates and we wanted the broadest coverage possible.

Responses were received from 13 "users" (i.e., carriers, AAPs, end users), and all four equipment suppliers, for a 73.9% response rate.

Bellcore compiled the questionnaire responses into a computer database which facilitated the subsequent production of various analytical reports and charts. Bellcore worked with the Assess the Risk subgroup to determine breakouts of the data. A variety of tools such as Pareto diagrams, pie charts, and graphs were used to analyze the data and determine the major root cause categories of DCS failures.

4.2.1 Users' Data

The 13 users reported a total of 2598 DCSs (Figure 4) terminating 588,897 DS1 ports and 552,060 DS3 ports. If each DS3 port is counted as 28 equivalent DS1 ports, these DCSs terminated 16,046,577 equivalent DS1 ports. 81% of these systems (or 95% of the equivalent DS1s) were reported as staffed (Figure 5). A total of 381 failure reports were received from the users.

4.2.2 Suppliers' Data

The suppliers reported a total of 3364 DCSs terminating 1,070,190 DS1 ports and 621,286 DS3 ports, or 18,466,198 equivalent DS1 ports. A total of 368 failure reports were received from the suppliers.

4.2.3 Combined Data

Since the user respondents represented the large majority of equipment in the United States, the user totals for equipment (2598 DCSs) were used as a basis for normalization in the analysis.

Out of the 749 total failure reports, a combined set of 629 "unique" failure reports from user and supplier respondents was created. Failure reports were deleted for either of the following reasons.

1. Supplier and user each reported the same failure.
2. Supplier reported failures from a user who did not respond to the survey.

It should be noted that this set of failure reports still contained 53 potential duplicate reports. These reports agreed with respect to user, city, and date, but did not necessarily agree in any other respects (e.g. duration, cause). Therefore, this report's estimates of downtime and failure rate could be approximately 10-20% lower if all potential duplicates were removed.

D

An analysis of the earliest reported failure for each user and each supplier indicated that the majority of users and suppliers did not start reporting on the requested June 1, 1991 date. Seven users and two suppliers reported the first failure after July 1, 1991. The reports indicate that all respondents were reporting consistently from March 1992 through July 1992 inclusive. A calculation weighting each respondent's length of survey participation by its DCS population estimates that the failure reports represent an average study length of 1.1 years.

4.3 General Findings

Of the 629 failure reports, 231 (37%) were reported as outages where the affected channels had a complete loss of service, and 398 (63%) were reported as incidents where there was no loss of service; however, there was a significant loss of protection, access or visibility into the DCS.

4.3.1 Mean Time Between Outages (MTBO)

Figure 6 displays the month-by-month variation in the total number of failures and outages reported. As mentioned previously, the most consistent reporting for users and suppliers was from March '92 to July '92. The average reporting rate during this period is 17 outages/month. Therefore, the Mean Time Between Outages can be calculated as follows:

$$\textit{Mean Time Between Outage} = \frac{1}{\#\ \textit{Outage/yr/DCS}} = \frac{1}{\left[\frac{17\times 12}{2598}\right]} > 12\textit{yrs}.$$

Given the conservative definition for outage (10 DS1's or 1 DS3) from a network reliability perspective and an MTBO of greater than 12 years, we have confirmed the assumption and general consensus that DCSs are very reliable network elements.

4.3.2 Outage Duration

Figure 7 presents the entire distribution of outage durations. The median duration (data mid-point) is 1.3 hours. This is due to the fact that 46% of all outages have a duration less than one hour and another 18% fall between one and two hours. However, the mean is much higher than the median due to the fact that the data is heavily skewed by the presence of some very long outages (8% greater than 6 hours; 1% greater than a day). If we were now to divide the outage population by size into small, medium, and large as defined as follows:

Outage Size		Equivalent DS1s		
		1/0	3/1	3/3
Small	<5% of Capacity	<34	<359	<672
Medium	5%-20% of Capacity	34-133	359-1433	672-2688
Large	>20% of Capacity	>134	>1433	>2688

we would determine that the mean outage duration for each size category to be 2.8 hours (small), 4.5 hours (medium), and 2.1 hours (large). These results raise two concerns. First, that many significant sized outages last for longer than 6 hours and the mean (2.8 hrs) outage duration is significantly longer than the assumed two hour repair time, which are built into all DCS reliability and availability requirements and modeling.

4.3.3 Outage Size

Of major concern to national network reliability are very large outages. There were 23 outages reported (10%) that affected more than 500 equivalent DS1s. Figure 8 is a plot of that data. These 500 DS1s could represent 500 data customers using an individual DS1 channel (1.54 MB/sec) or 12,000 voice customers using an individual DS0 channel (64 KB/sec). In addition, 6 of these outages were reported as total system outages. If we were to attempt to anticipate the number of FCC reportable DCS events that would affect greater than 30,000 customers for longer than 30 minutes from the data given in Figure 8 and by assuming that each DS1 represents 24 voice customers, we would obtain 14 events that qualify. Considering the multiplicity of unknowns, the best we can say is that these 14 outages would have had a high probability of qualifying if FCC DCS reporting were in effect when they occurred. This approximate one per month rate from a population of 2598

D

DCSs is comparable to the 3 to 4 per month FCC reports for electronic switches, which have a population of approximately 10,000 switches. It would appear that the FCC reportable DCS-related outages will provide an acceptable metric for measuring national DCS related performance.

4.3.4 Total Downtime/DCS/Yr

If we now take the product of the duration of each outage and the number of equivalent DS1s affected and sum over all outages during a year and divide by the number of DCSs from which the data is being collected; we come up with a very interesting and useful in-service metric, **Total Downtime/DCS/Yr in Equivalent DS1 Hours.**

If we do this for all the outages reported in this survey we can baseline our combined data as:

Total Downtime/DCS/Yr = 68 Equivalent DS1 Hours

Figure 9 vividly depicts how the 68 Equivalent DS1 Hours are distributed among small, medium, and large outages. It is interesting to note that 66% of the total downtime is from large outages. **This metric, which combines outage frequency, size, and duration in somewhat of a normalized form, is recommended at a minimum to all equipment suppliers and service providers to more closely, yet simply track improvements** in DCS related outages. It is recognized that this metric is somewhat biased against large DCSs, however it is felt to be appropriate given the significant impact large DCSs could have on network reliability.

4.3.5 First Indication of Trouble

The first indication of trouble in 70% of the failures reported were local and/or remote alarms. Figure 10 also shows that about 10% of the failures are detected while performing routine maintenance, and 10% are first reported by the customer.

4.3.6 Who Resolves the Problem?

In 88% of the cases the local craft requires tier 2 (centralized support group) and/or vendor support to resolve the trouble (Figure 11). Upon further analysis (Figure 12) one can determine that the local craft does handle 27% of the outages alone (predominantly a change out of circuit packs). However they handle only 3% of the incidents, which are more subtle and have to do with the controller and/or software. These results can easily be explained by the complexity of the system, the current state of trouble shooting documentation and training, standard operating procedures in some large service providers which automatically trigger tier 2 support, and by the simple fact that the local craft in many companies have additional duties other than the DCSs. These factors may practically have a negative impact on the duration of the outages and incidents.

4.3.7 Failures Correlate with Activity

Figures 13 and 14 clearly show how failures correlate with activity. They show that the vast majority of failures occur from Monday to Friday from 8 AM to 6 PM. In addition, there are peaks in the early hours of the morning when routine maintenance and upgrade procedures are performed and at 12 Noon and 4 PM when craft errors are typically higher.

4.3.8 Current Situation

If we combine all the general findings together we can get a compact description of the Current Situation. **DCSs are very reliable network elements with Mean Time Between Outages of greater than 12 years. When they fail nearly half of the outages are resolved in less than one hour, however, 8% of the outages last for six hours or more. These systems are in the vast majority of cases staffed by trained craft and are effectively locally and remotely alarmed; however, they are very complex systems which require tier 2 and/or supplier support for most trouble resolution.**

D

In addition, DCS failures are correlated with activity and this activity is known to be increasing with new applications. A general conclusion which can be drawn from these facts is that there is a **real and growing need for DCS system self defensiveness.**

5. Root Cause Analysis

If we again return to the data reported we can obtain some insight as to the root cause of the problems. In this case, it is most advantageous to look at the failures in two distinct groupings, outages (loss of service) and incidents (no loss of service, however loss of protection, visibility and control). If we were to do a Pareto analysis on **outages** (loss of service, Figure 15) we would determine that Procedural Errors are the single most **reported** cause of outages (30-40%), followed by Active Hardware (20-30%), Passive Connecting Hardware (15%), and Software (10-25%). If we were to further subdivide the **incidents** into the subcategories identified in the questionnaire; loss of reconfigurability, alarm visibility, protection switching, and communication with processor; and do a Pareto analysis of each of these subcategories (Figure 16, 17, 18, 19) we would determine that Software and Active Hardware together account for greater than 80% of the reports and procedural errors (5-10%) and passive connecting hardware (5%) are minor reported causes. The exact percentage for each of the reported causes are somewhat interesting and important, however not as important as the general conclusion that you must address all four reported causes if you wish to have impact on 90-95% of the problems.

5.1 Procedural Errors

Procedural errors account for 30-40% of the reported outages. Further analysis of the written comments provided in the questionnaires, indicate that the root causes of these procedural errors stem from routine maintenance activities, provisioning activities, mistakes being made while doing upgrades (installation and growth), and tape backups. Figure 20 is a plot of this data for all procedural caused outages. If we were to further subdivide the procedural caused outages using the same size categories introduced in Section 4.3.2, we would find that provisioning errors are the root cause of 50% of all small procedural caused outages and they do not contribute to any other size category (Figure 21); that maintenance activities and upgrades cause 45% of all small procedural caused outages, 100% of all medium procedural caused outages (Figure 22) and 75% of all large procedural caused outages (Figure 23); and that tape backups are the root cause of 25% of the large procedural caused outages. Figure 24, which is a replot of Figure 15 taking into account the impact of each outage, vividly displays that procedural errors alone or in combination with software account for 76% of the equivalent DS1 outage downtime. These results are consistent with the experiential feelings of the subgroup.

The questionnaire's narrative section also provided us a means to access the "reasons" for the outages from those most closely involved. That input can be summarized as follows.

5.1.1 Lack of Awareness

- of the critical role DCSs play in support of service provider networks on the part of the local and remote operators and management. Because of the historical "plug-in" nature of the transmission business and the ever increasing sophistication of the DCSs, a paradigm shift is required for all involved to improve reliability.

5.1.2 Lack of Centralized Support Organization

- with good relationships with the equipment suppliers. In many companies, field technicians are required to work on a wide variety of equipment and technology and may not have the opportunity to "stay current" on all

D

of them. This implies that for these companies no one appears to have the responsibility for collecting and tracking in-service DCS metrics.

5.1.3 Lack of Sufficient Documentation and Training

- especially for remote or centralized OAM&P. The current situation indicates that DCS documentation and training is, in many cases, poorly organized, not timely, and not user friendly. These facts coupled with the ever increasing DCS complexity must be jointly addressed by equipment suppliers and service providers.

5.1.4 Lack of Detailed Methods and Operating Procedures (MOP)

- for DCS installation, upgrades, growth, local and remote provisioning, maintenance, and troubleshooting. Many of the customer reported outages were found to be caused by improperly performed maintenance procedures (i.e., loop back to a wrong facility, improperly executed tape backup, etc.). Clearly, the major deficiency is in the MOPs to do trouble shooting from remote locations.

5.1.5 Lack of Sufficient System Self Defensiveness

- which is usually expressed as a software deficiency. In general, there needs to be more consideration given to the craft interaction with the DCS system and the potential impact on reliability. This issue is discussed in detail in Section 6.3.2.2.

5.2 Active Hardware

Hardware alone or in combination with software accounts for 20-30% (Figure 15) of all outages. Figure 24 further indicates that 11% of the reported equivalent DS1 outage down time is due to hardware only. This hardware allocation equates to 7.5 hours per year per DCS (11% of 68 equivalent DS1 Hrs/year/DCS) or 0.07 minutes per year per equivalent DS1 port.

5.2.1 DS1 Hardware Outages

A detailed analysis of the 41 DS1 hardware outages reported was performed. For each hardware outage, the product of the "number of DS1s affected" times "outage duration in minutes" was determined and its contribution to the total DS1 outage time was evaluated. Three significant observations were made.

- The results show that the 41 outages represent 3,009,570 DS1 outage minutes. Nine out of these 41 outages represent "total system outages" where all traffic on the DCS was lost. These total system outages represent 30% of the total DS1 outage minutes.
- A single hard disk failure combined with a procedural error (no current back-up tape) accounted for 1,171,800 DS1 outage minutes. This outage corresponds to 39% of the total DS1 outage minutes.
- Other significant contributors to DS1 downtime included:

  5 Matrix/bridge card failures
  3 Unit controller failures
  2 Hard disk failures
  6 Clock/sync card failures
  1 Fuse and switch to failed side

The duration of these hardware caused outages ranged from 10 hours to 2.5 days.

DS1 Downtime Estimate

Based on the total number of DS1 outage minutes and the total number of DS1 ports in the study, the average downtime per DS1 port is given as:

$$\frac{3{,}009{,}570 \text{ DS1 outage minutes}}{588{,}897 \text{ DS1 ports}} = 5.1 \text{ minutes/yr/DS1 port}$$

This downtime estimate represents 41 outages of 10 or more DS1 ports. The Bellcore hardware requirement for all DS1 ports is 5.0 minutes per year per DS1 port.

In addition, we can conclude that matrix/bridge card, unit controller, disk drive, and sync card failures are the major root causes for DS1 port hardware failures.

D

5.2.2 DS3 Hardware Outages

Of the 231 reported outages, 41 outages were caused by hardware that affected one or more DS3 ports (7.7% of the total equivalent DS1 downtime). These DS3 hardware outages correspond to 29.218 DS3 outage minutes. Based on a total population of 552.060 DS3 ports in the study (Figure 5), the average downtime per DS3 port is given as:

$$\frac{29.218 \text{ outage minutes}}{552.060 \text{ DS3 ports}} = 0.053 \text{ minutes/yr/DS3 port}$$

This downtime estimate meets the present Bellcore hardware requirement of 0.06 minutes per year per DS3 port.

5.2.3 Total System Outages

Since the DS1 outage data discussed in Section 5.2.1 did not include all total system outages resulting in the loss of DS3 ports as in the case of a DCS 3/3, a second look at total system outages for all types of DCSs was made.

Of the 29 total system outages reported for all causes of failure and all types of DCSs, 12 were caused by hardware failures (41%).

Root Cause Analysis

A root cause analysis on these 12 hardware outages and their average duration provided the following data:

- Matrix controller (6 hrs.)
- Matrix/bridge card (2.2 hrs.)
- Fuse and switch to failed side (12 hrs.)
- Hard disk failure (19.6 hrs.)
- Sync card failure (1.4 hrs.)
- Lightning (2 hrs.)

Once again, matrix/bridge cards, controller, disk drive and sync card failures have a significant impact on total system downtime as well.

Total System Downtime Estimate

For all 29 outages, the Total System Downtime due to all causes can be calculated as 2.4 minutes per year per DCS. For hardware only, the Total System Downtime is 1.3 minutes per year per DCS.

This hardware estimate significantly exceeds the present Bellcore hardware requirements of 0.003 minutes per year per DCS for total system downtime.

5.2.4 Comparison with Hardware Requirements

The following table compares the average hardware downtime estimates derived from the outage data with the present Bellcore hardware requirements.

Downtime Parameter	Bellcore Requirement	Survey Data
DS1 Port	5.0 minutes/year	5.1 minutes/year
DS3 Port	0.06 minutes/year	0.053 minutes/year
Total System	0.003 minutes/year	1.3 minutes/year

Note that the Bellcore requirement for DS1 Downtime includes all outages that affect the DS1 port, while the survey data includes only outages that affect 10 or more DS1 ports.

One conclusion that can be made from this table is that the current DCSs are not meeting the Bellcore requirement for Total System Downtime. A significant factor contributing to this downtime estimate are hardware failures combined with software or procedural errors which often result in long outages.

5.2.5 Downtime of Control and Reconfiguration

Downtime for control and reconfiguration was calculated based on the data that 35% of the failures are associated with a loss of reconfiguration or communications with the processor (Figure 25) and the mean duration for an incident is 8.6 hours.

Therefore the average downtime is:

$$.35 \times (629 \text{ failures}/2598 \text{ DCS}) \times (8.6 \text{ hrs/incident}) \times (60 \text{ min/hr}) = 44 \text{ minutes/year/DCS}$$

Downtime, due to hardware, of control and reconfiguration is approximately 50% of the total (Figure 16). Therefore, the calculated downtime, due to hardware, of control and

D

reconfiguration of 22 minutes/year/DCS can be compared to the Bellcore requirement of 7 minutes/year/DCS. This raises additional concerns with regards to the reliability of the in service disk drives and controllers.

5.3 Software

Software alone or in combination with hardware and/or procedural errors account for 10-25% of the outages reported (Figure 15) and 35-65% of the incidents reported (Figures 16, 17, 18, 19). Further analysis of the written comments in the questionnaire indicates that there were three dominant scenarios reported.

a. Improper commands and/or data bases were entered into the machine and this led to an outage.

b. A hardware failure occurred and service was lost because the software did not recognize the failure and switch service to protection.

c. Insufficiently tested software was loaded into the system and failed in the real operating environment.

An examination of the DCS failure data in conjunction with the current software process (Figure 26) allows us to understand the root cause of the failures and tie each to the specific phase of the software process where it is introduced. The following section summarizes the root causes and areas for improvement in each of the different software phases.

5.3.1 Definition Phase

There are two general areas for improvement in the definition phase that have been identified. A key contributor to failures that were classified as procedural is that insufficient consideration was given to craft interactions with the system and potential impact on reliability. In addition, in some cases there was inadequate understanding of customer (service provider) requirements by the equipment supplier.

5.3.2 Development Phase

The key areas for improvement in the development phase is that insufficient design consideration has been given to fault management capabilities, including diagnostics, fault isolation, and fault tolerance. Comparative studies of switching systems development done by the subgroup members shows that these capabilities are a large fraction of the overall software design. In contrast, DCSs have not evolved with a similar sensitivity to fault management, although this situation is improving.

5.3.3 Verification Phase

The major area for improvement in the verification phase is that there is inadequate testing in the service provider environment where the product is eventually used. Except for the first office application site, there may be little or no service provider environment testing before general availability of the product.

5.4 Passive Connecting Hardware

We were quite surprised to find out that single point failures in the passive connecting hardware accounted for 15% of the in-service outages reported (Figure 15). Further analysis indicates that the root causes of these outages were:

a. DSX to DCS interbay cabling (troubles with coax connectors).

b. DS1 and DS3 terminating connectors becoming loose after installation.

c. physical failures in the Port shelf backplane.

d. untimely failures of DS3 signal splitters, input/output transformers, and line build out (LBO) networks which are not duplicated.

These failures are particularly difficult to diagnose since one assumes that once these passive connections are working they always will be working.

6. Countermeasures and 'best practices'

Listed below are countermeasures and "best practices" for each of the significant causes of DCS outages. **The definition of "best practices" as used in the network reliability focus area Technical Papers is as follows: "Best practices" are those countermeasures (but not the only countermeasures) which go furthest in eliminating the root cause(s) of outages. None of the practices are construed to be mandatory; however, a very small number of countermeasures that are deemed by the Focus Team, and concurred by the Network Reliability Steering Team (NO REST), to be especially effective countermeasures will be designated as "recommended".**

Service providers and suppliers are strongly encouraged to study and assess the applicability of all countermeasures for implementation in their companies and products, respectively. It is understood that all countermeasures, including those designated as "recommended", may not be applied universally. Each recommendation, which could be of considerably different importance for any individual current situation, should be prioritized by cost and impact in putting together an action plan for improvement.

Also discussed are the current and emerging DCS applications employed by carriers, AAPs, and end users; and the implications of those applications on DCS architectures and engineering designs, as well as reliability requirements.

Operations, Administration, Maintenance and Provisioning (OAM&P); Documentation and Training; as well as the Software Self Defensiveness recommendations are offered as countermeasures and best practices for Procedural Errors. The Software and Hardware recommendations map directly to the root causes.

6.1 OAM&P

The DCS represents a major paradigm shift for "transmission systems" in terms of how they should be operated and maintained. **In many ways the DCS transcends the traditional boundary between switch and transmission and, in fact, the DCS lends itself more to the methods and techniques of switch operations and maintenance than traditional transmission systems.** Utilizing switching systems principles and learning, the focus team recommends eight areas for improvement in DCS operations.

6.1.1 Operational Philosophy and System Administration

There is a critical need for a broad based educational system for all field and management personnel involved in operation and support of cross-connect systems. Data from the questionnaires as well as studies by subgroup members indicates that failures occur when maintenance personnel unfamiliar with the system attempt to repair troubles. This may have been successful in other hardware based transmission equipment but will lead to large scale outages in a software intensive DCS environment. **We recommend a DCS Awareness Program patterned after Pacific Bell's and AT&T's efforts as an industry "best practice."** Both programs have shown to drastically reduce procedural errors. A successful program is one that educates both field and management on the new technology, its benefits and pitfalls, and the magnitude of traffic carried. The program must concentrate on training, procedures, and a detailed process to be used in resolving issues.

Past methods of troubleshooting relied on cause and effect hardware replacement techniques, e.g., "does the problem go away when I replace this circuit pack." There are simply too many negative impacts using this style of troubleshooting and procedures must be ingrained into the technical and maintenance forces if improvements are going to be realized.

D

A new philosophy is required to address the maintenance and administration needs of DCSs. **It is recommended that service providers should adopt and closely emulate the maintenance, administration, and support operations structures of the switching environment for the DCSs.** This new philosophy would include centralized administration, surveillance and support. The DCS should be monitored and controlled in as few places as possible to increase consistency of operations and overall management. If the DCS is used as a service restoration platform, central control is essential.

Another recommendation is that service providers and equipment suppliers collaborate on formal root cause analysis of network events to identify both equipment and procedural deficiencies. The result of these post mortems should be published by the equipment suppliers to inform and to be used by both as a preventive measure. Methods, like "flashes", must be established to ensure rapid dissemination of critical outage prevention information found in these investigations.

6.1.2 DCS Installation, Upgrade, Growth, and Maintenance Activities

Providing for a high quality installation or upgrade activity not only reduces customer exposure but is less expensive as well. **A best practice from Sprint and NYNEX is to establish a multi-discipline Core Team, including the supplier; to plan, test, and evaluate all major change activities.** This team's role will be to oversee all network element and final system testing. Final system tests should be conducted in a lab environment that as closely as possible emulates the real operational environment.

All upgrades or growth procedures must be fully validated in the lab environment prior to first application in the field. Each user must work with their supplier to develop these procedures and customize them to their application. Emergency backout processes must be included and each step in the process should be timed to enable the installation team to identify when something has gone awry. Some benefit can also be obtained by including copies of printouts for each step to verify that the system is responding as expected. A good practice is to have members from all installation teams practice the procedure and all emergency actions in the lab environment prior to field work commencing.

Each service provider must establish standardized parameters and office settings for each hardware and software option in the DCS and a system to verify compliance. This will allow for more predictable system operation and quicker troubleshooting.

Prior to deployment of any new upgrade, all new procedures and commands must be fully validated in the lab environment for accuracy and completeness.

Because of the potential for service impact in many repair activities, the industry needs to more thoroughly prepare for the work and do a better job of reviewing procedures prior to work commencing. One method becoming more prevalent is to establish a "Change Management" group to act as a customer advocate, enforce the requirement for proper Methods of Procedures (MOP) for each maintenance action, and manage network activity as well.

6.1.3 Provisioning Activities

Provisioning of cross-connects can be performed manually by on-site technicians or remotely by other terminal technicians or a centralized provisioning group. **There must be a method to ensure that the transmission facility database and DCS database are fully synchronized.** If the databases are not in sync, an outage is likely to happen. A method to download/upload this information via a DCS management system is desirable.

Procedures must be in place to allow for manual provisioning in the event of system failure. These methods should provide the ability to manually enter the information into

D

the system once it is restored.

Provisioning activities have the potential to negatively affect traffic if procedures are not closely followed. It is recommended to **restrict the provisioning technicians from all commands except those that are needed for their work. Avoid any "global" command that may have the potential for significant impact.**

Security issues have also come to the forefront recently. This includes the issuance of passwords, establishing privileges, and preventing unauthorized access. Some DCS machines allocate command privileges based on a matrix, e.g., several levels of commands exist and a user assigned to a given level can execute any command on that and any lower level. Other DCS systems associate a set of privileges with a given password. From a security standpoint, the latter is much more restrictive. Companies must also initiate and strictly follow procedures to routinely review passwords in each machine or system and delete those that are no longer necessary. The Industry must quickly migrate to more sophisticated technology for modem access to DCS machines. As a minimum, they should be employing security modems that call a user back at a telephone number associated with their password.

One practical pervasive issue that must be dealt with is how to minimize facility level alarms at the monitoring center during provisioning activities. The volume of alarms create a potential for alarm saturation and makes it very difficult to differentiate between a "real" alarm and those caused by other activities. A common practice is to simply inhibit these alarms or set their thresholds so high they do not report. The danger here is that there must be a fail-safe measure to turn these alarms back on when the facility is carrying traffic.

6.1.4 OS and Management Systems

Most cross-connect systems use some type of Operations Support or Management system. Primary uses of these include alarm collection and correlation, centralized provisioning and administration of transmission facilities, gathering of transmission performance monitoring information, and remote control of the DCS. Central collection and display of alarm and messaging information is enhanced by employing graphical representation of network status by severity levels and using a multi-windowing environment. Embedded filtering and message patterning capabilities are also highly useful. There must also be a method to synchronize or audit alarm conditions between the OS and DCS to ensure that no messages have been lost. Finally, **there must be sufficient processor and communication transport capability to simultaneously process messages from a major network event and remotely control the DCS.** Service providers must also work closely with their equipment suppliers to further develop multi-tasking capabilities of the DCS.

When the DCS is used as a service restoration tool for network survivability, requirements for the OS and management system are more strict and additional features are required. In most other applications, only one communication link is established to the cross-connect from the management system. **In the service restoration application, it is crucial that communication links to the DCS are highly reliable and fully redundant, with automatic switch over in the event of link failure.** Obviously, the supporting OS system must be capable of supporting redundant links. The monitoring center must have full visibility of link status at all times, with visual and audible notification if links are out of service. The DCS controller must be extremely reliable and give priority to restoration over other internal processing functions. Fully redundant controllers may be required. The status of traffic re-routed based on manually or automatically executed alternate route traffic maps should be graphically displayed on the management system screen.

D

A silent failure is one in which a critical system or component ceases functioning without any indication until that particular feature or functionality is required. If this is a communication transport facility, DCS controller, or some function of the DCS itself; the result could be serious if the system is needed for emergency traffic protection. Therefore, **efforts should be made to eliminate the possibility of having a silent failure on any DCS system component, including the OS or Management System, cross-connect, or communications links.**

6.1.5 Support Organization

In many cases the DCS system is maintained by transmission maintenance personnel who are generally unprepared for the complexity of the system. This is not to say that transmission maintenance groups are not capable of maintaining the DCS, simply that they do not have the skills required based on past training or current DCS training. A parallel issue is that, with the exception of provisioning, most responses to DCS are demand in nature and require considerable in-depth knowledge. Most field technicians are required to work on a wide variety of equipment and may not have the opportunity to stay current on all of them. This can be especially dangerous on a DCS system, without the proper system defensiveness controls being in place.

As the complexity of network elements grow, and the diversity of equipment that field forces are called upon to maintain increases, a centralized technical support organization is recommended. It is very clear from the questionnaire responses that many service providers have implemented this best practice. They support field forces in day to day trouble resolution and usually are involved in trouble management with the equipment supplier. If organized centrally, and located with the monitoring facility, the support group will be able to gather information more effectively and observe equipment behavior directly. This is an example of how DCS organizations can emulate existing switching operations structures.

The central support organization should have involvement in all troubles associated with the DCS system and be the control point for complex trouble resolution activities. If the organization is not staffed for seven days a week twenty four hours a day, on call engineers must have immediate access to the DCS through portable terminals. They should also control all equipment supplier access to the DCS system. If the situation is unusual, or involves traffic loss, the vendor technical support organization should be contacted and, if possible, be involved in the root cause analysis process.

Additional duties of a technical support organization include participation in test and acceptance activities for new software and/or hardware applications, test and approval of all procedures used on the DCS, and approval of product change notices.

One of the support organization's principal roles should be to collect data on all DCS system events and track them through an on going record keeping system such as a database. This will enable them to quickly identify trends in performance and recognize similarities in equipment events and anomalies. An accurate system of data collection will also assist the organization when working with the equipment supplier to resolve troubles. The performance and event information collected should be shared regularly with the equipment supplier. Any significant traffic impacting events should be reported to the supplier immediately.

The support organization should also be involved in the analysis of all DCS related events to identify the root cause. Results of these analyses should be shared with all affected groups including field forces, application or design engineering, and the equipment supplier.

D

6.1.6 Vendor Quality Management

Any discussion of performance in the operational environment must include the role of the equipment supplier. **The service provider and the equipment supplier should partner in order to maximize their mutual success.** There is no substitute for cooperation in areas such as feature clarification and identification and customer focused integrated testing early in the development process.

As the system is deployed, these channels of communication must continue. The service provider must give the supplier feedback on equipment performance in ways such as formal report cards, (using operational measurements described in this paper), and trouble report reviews. The team must agree on formal processes to use for change notices, maintenance releases, and trouble resolution and escalation. The equipment supplier must also provide immediate notification to the service provider of potentially service affecting issues found in other networks. It goes without saying that all of these interactions should take place with proper care being taken to protect proprietary information.

Service providers, equipment suppliers and the rest of the DCS community must work together to establish acceptable thresholds of equipment performance in the field environment. Many published documents refer to objectives and requirements but, these apply only to the laboratory or evaluation environment.

6.1.7 Operations Measurements

In order to evaluate and track system performance and to identify trends, data needs to be gathered in several key areas. Examples are given here for consideration by service providers. One distinction that should be made in gathering this data (and used in database records for sorting later) is whether the machine caused the trouble or whether it was caused by the craft - machine interface. A third category would be those situations where system defensiveness allowed or didn't prevent a performance deviation. The reason for these distinctions is to put the emphasis on the root cause for the fault: Machine; Craft interaction; Lack of system defensiveness.

Performance of the DCS can be measured in many ways. **The group recommends Total Downtime/DCS/Yr in equivalent DS1 Hours (See Section 4.3.4 for details) as one of those measures.** Additionally, analysis of each event and its cause provides good insight into the system and its performance, especially if the percentage of "No Trouble Found" events is high. A similar analysis of circuit pack repair statistics can give clues as to the effectiveness of current troubleshooting and maintenance practices. A high "No Trouble Found" rate here could point to a need for enhanced maintenance practices or could point to a need for better system diagnoses processes. A global analysis of alarms by function and type can also prove fruitful to identify trends in performance.

6.1.8 Disaster Recovery

Effective disaster plans must be developed in advance, constantly updated, and occasionally exercised. Service providers must evaluate their networks and brainstorm those events that could occur and come up with measures to either prevent, control, mitigate or recover from them.

One of the major contributors to large DCS outages has been mismanagement of the cross-connect database storage media. DCS systems typically utilize a tape based storage system. **We recommend that each company review the level of provisioning activity in their DCS equipment and devise a schedule of system backups that will minimize the amount of data base information lost if any one tape should become corrupted or otherwise unusable.** In addition, consideration should be given to storing one of those tapes off premises for protection against physical site disasters. All tapes should be prominently marked with the office

D

name, DCS identifier, date of last backup, and name of technician that did the backup. Color coding of tapes is very useful if a routine is based on days or weeks of the month. Database backup procedures should be established by each company versus reliance on book methods, to take into effect any differences in DCS application, and OS or management system and to ensure conformity across the network.

Surveillance and management systems will play an important role in disaster recovery since they should be the first indication of a problem. Several major DCS outages have resulted from relatively minor activities getting out of control because those monitoring and working the problem did not recognize escalating conditions. There is no question that system defensiveness should prevent these conditions, however DCS systems are still in their infancy and time is required to develop more elaborate measures. Continuous improvement in the DCS system defensiveness will substantially decrease the failures caused by human error and system anomalies. Each user must work with the supplier to constantly improve these features. In any event, processes must be in place for the monitoring facility to immediately notify site personnel of any unusual or unexpected alarms or conditions. Maintenance organizations must review procedures for a specific work activity, monitor the work closely, and be able to immediately identify a situation going awry.

Each company should develop maintenance routines to defend against silent failure of systems, interconnecting communication transport links, or DCS components. These procedures could include occasional manual access to each DCS, review of activity reports, and "health check" messaging between the management system and the DCS. This is especially crucial in systems designed for service restoration.

6.2 Documentation and Training

The following documentation and training best practices are offered as a countermeasure to procedural errors and some software related problems. They are offered as a result of the subgroup's analysis of existing documentation and training and several quality improvement team efforts between equipment suppliers and service providers. The list is not meant to be all inclusive, nor are these countermeasures and best practices offered as a guarantee against future DCS related outages. However, we do recommend that they be incorporated into the product documentation and training practices utilized by each equipment supplier.

6.2.1 Product Documentation

Product documentation associated with any DCS system, new or old, is an important element of that system, and should be treated as a product unto itself. **It is essential that the proper amount of resources be devoted to ensure that the documentation is produced in a complete, easy-to-use, and timely manner, and is made accessible to the entire customer base.** Without a complete, easy-to-use set of documentation, learning to operate and maintain a system becomes a process of trial and error.

6.2.2 Documentation Development Process

The development of the documentation is an inherently difficult task from the perspective of "user friendliness". The producer of the document must meet the criteria of the expert and the novice - no small task. A poorly managed documentation development process will almost always result in a product that will not effectively meet the needs of the customer base for which it is intended.

In compiling a complete set of documentation, the amount of instructional material may be extensive. It may not make sense to try to package all of the material under one heading, or even in one binder. A logical segmentation (e.g., along the user segments-remote provisioning, maintenance, etc.) or

D

grouping of material should be offered.

Customer input is essential! Documentation should be developed with a clear understanding of customer needs. The customer, as well as the person developing the documentation, should have hands-on-experience with the equipment to ensure that all facets of operations and maintenance will be accounted for (both from a service provider and an equipment supplier point of view).

In order to maintain the proper quality level throughout the development of the documentation, a series of quality metrics should be first developed. If errors or problems found within the material being developed reach a certain threshold, the process should be stopped and all of the completed work should be thoroughly reviewed.

Once the documentation is developed, **it should again be thoroughly tested with the customer before being made generally available.** Customer satisfaction should be assured through a series of acceptance tests and sign-off reviews.

6.2.3 Distribution Channels/Timeliness of Availability

Once a set of documentation is produced, the task of making it available to a large, diverse group of customers is enormous. **The use of electronic media to maintain the documentation manuscripts and to access customer distribution information is essential.** As new customers originate, they must be added to the distribution database. This database must be kept up-to-date, and changes must be made expeditiously.

Since product changes are constantly being introduced, the documentation must be constantly revised to reflect these changes. Bulletin-like updates should be sent out to reflect small, periodic changes. These changes must also be reflected in the master set of documentation and, when appropriate, a complete update of the documentation or a section of the documentation should be made available.

To keep track of the numerous changes to both the product and the corresponding documentation, a change control data base is recommended. This will help to detail what information is contained in each of the documentation updates or releases, and when the information was made available. It will also help in preparing errata sheets which should be sent out with documentation updates. If at all possible, it would be highly desirable for service providers to have on line access to the equipment supplier's data base which contains the most up-to-date information.

6.2.4 OAM&P Documentation

Many of the DCS outages identified in this study, and a large percentage of those first reported by the customer, can be related back to improperly followed routine operations and maintenance procedures. This clearly identifies the need for a well-organized and comprehensive operations and maintenance manual as a standard document for all digital cross-connect systems.

The DCS operations and maintenance manual should give an overview of the system and identify procedures for daily operation. It should contain detailed routine maintenance procedures, diagnostics, and procedures for replacing components.

There also should be information devoted to acceptance testing, which is to be done after a new installation or addition of new bays. **An acceptance testing checkoff sheet should be developed and utilized during each new installation or addition.**

A comprehensive troubleshooting set of flowcharts (state diagrams) should be included in any set of documentation to guide all levels (both Tier 1-Novice and Tier 2-Expert) of maintenance support. These flowcharts should include detailed descriptions of each diagnostic, the probable cause of each failure, and the corrective steps to fix the problem.

D

6.2.5 *Human Factors Considerations*

As important as the human factors considerations are to the development of any DCS product, they are as equally important in the development of the DCS documentation material. To facilitate the ease-of-use of the documentation, tables of contents, indexes, cross-references, and checkoff boxes to indicate the completion of each step in procedure should be utilized.

As product updates are released along with documentation revisions, errata sheets should be used to highlight where changes have been made.

Each section of the documentation should be self-contained, including clearly identified steps detailing inputs, responses, and estimated completion times. It should also give a brief explanation of the purpose of each section, provide warning statements when critical procedures (i.e., those that could potentially disrupt the system) are about to be started, and identify back-out procedures or system recovery procedures.

Another key human factors consideration should be the use of consistent documentation style across sections, volumes, and product lines. A routine maintenance checklist should be developed that lists the routine activities and recommended intervals. Copies should be made of this checklist and used on a regular basis.

Quick reference job aids should also be developed (preferably on laminated sheets) containing tables listing all DCS messages, error codes, autonomous messages, unit and cable numbering information, fuse charts, figures identifying circuit pack locations, test mode loopbacks, and performance monitoring information.

6.2.6 *Product Training*

Product training should complement product documentation. In and of itself, documentation material may not be enough to meet customer needs. Due to the complex nature of most DCS equipment, hands-on training courses are required. Training courses, as well as documentation, should cover all areas associated with product operations, maintenance, and general support.

6.2.7 *Training Development Process*

The same as with the documentation development process, a poorly managed training development process will almost always result in a product that will not effectively meet the needs of the customer base for which it was intended.

Training should be developed with a clear understanding of customer needs. Customer input is essential. The customer, as well as the person developing the training courses, should have hands-on experience with the equipment to ensure that all facets of operations and maintenance will be accounted for (both from an end user and a vendor point of view).

In order to maintain a proper quality level throughout the development of the training courses, a series of quality metrics should be first developed. If errors or problems found within the material being developed reach a certain threshold, the process should be stopped and all of the completed work should be thoroughly reviewed.

Once the training course is developed, it should again be thoroughly tested with the customer before being made generally available. Customer satisfaction should be assured through a series of acceptance tests and sign-off reviews.

6.2.8 *Organization/Timeliness of Availability*

Training must keep up with the numerous changes to both the product and its documentation material. They need to be developed concurrently with the product changes, and distributed to the field within the timeframe that the product will be available.

D

The material presented in the training courses must be taught by qualified and experienced instructors. The courses should have as much hands-on involvement with the equipment as possible.

In addition, to help train technicians on some of the more sophisticated Intelligent Network Elements (INEs), equipment suppliers may want to look into developing internship programs where service providers send their technicians to work in suppliers' laboratories or factories for a period of time to gain more knowledge of the equipment.

6.2.9 OAM&P Training

Once again, many of the DCS outages identified in this study can be related back to improperly followed routine operations and maintenance procedures. This clearly identifies the need for well-organized and comprehensive set of operations and maintenance training courses for digital cross-connect systems.

Training courses should be developed for operations, maintenance, and provisioning personnel and supervisors. They should be designed to enable the student to operate and maintain the DCS equipment. These courses should allow the student to interpret messages, provision equipment, establish cross-connections, and clear troubles using system documentation.

Advance courses should be developed for personnel responsible for the technical support of DCSs, including operations supervisors, maintenance engineers, operational support personnel, and communications technicians. These courses should be designed for individuals responsible for the highest level of technical support. All aspects of operations and maintenance should be covered, from normal day-to-day activities to advanced trouble analysis.

6.2.10 Training for Remote OAM&P

Training should not only cover local central office OAM&P needs, but should cover all phases of remote or centralized OAM&P.

More emphasis needs to be placed on the deployment of DCS systems in a network providing centralized control of the network, through centralized provisioning and centralized maintenance. The ability to make cross-connections electronically from a remote location eliminates the problem of coordinating several craft at different locations to restore a service outage. A centralized DCS controller allows fast restoration with little or no manual intervention.

6.2.11 Methods of Procedure (MOPs)

A key component of the MOPs being developed for DCS equipment is the DCS Awareness Program. This program is an internally initiated program developed by individual service providers with support from DCS equipment suppliers. Its intent is to identify practical information and checklists to assist field personnel to maintain and administer DCS equipment. It looks at areas dealing with the central office environment, security, equipment inventorying, housekeeping, technical readiness, and emergency preparedness.

Positive reinforcement of procedures should be stressed at all times. The use of signs designating various work areas, labels on equipment and cabling, properly identified inventory storage areas, log sheets for work performed, and procedures to be followed in case of emergencies is posted. **In addition, certification programs should be started to ensure that technicians have been properly trained to perform critical tasks.**

6.2.12 Training Criteria for DCS

DCS systems are becoming increasingly more and more complex, and are beginning to resemble switching systems. However, in the switching environment, the amount of training material offered and the frequency at which it is made available is clearly much greater than what is available for DCS training. **Therefore, the level of DCS training**

D

should be significantly increased to parallel the level of training associated with switching.

Because of the similarities between modern day DCS systems and switching systems, it would be desirable for DCS technicians to have familiarity with switches or a switching background in addition to transmission based training and background. This would facilitate the usage of well developed switching and operations procedures.

6.3 Software

6.3.1 Software Countermeasures

After understanding the root cause of software related failures and determining which phase of the software process each belonged to, the following countermeasures for each phase were determined.

6.3.1.1 Improve Definition Process The first countermeasure to improve the definition process is to solicit service provider feedback on requirements early in the process. The other countermeasure is to define system defensiveness features. This is addressed as a recommendation in the next section.

6.3.1.2 Improve Development Process Three main countermeasures to improve the development process are:

— Failure mode and effects analysis

— Early testing of the product by the verification test group.

— Plan for preliminary releases for service provider testing.

These are all discussed in the next section as recommendations.

6.3.1.3 Improve Verification Process The major countermeasure is to perform testing in the customer environment. This includes:

— Develop joint test plan with service providers

— Test service providers specific scenarios

— Encourage establishment of appropriate service providers environments for testing

— Test in service provider (or simulated service provider) environment

These are discussed in more detail in the next section as the recommendation on testing in the customer environment.

6.3.1.4 Continually Improve Software Process As was noted above, the DCS equipment suppliers need to continually monitor and improve their own software process to meet the increasing reliability needs of service providers and their end customers. There are four aspects to continually improving the software.

1. **Establish and use metrics to identify key areas of focus, and measure progress in improving quality and reliability before and after general availability (this is described further as a recommendation in the following section).**
2. **Solicit and use customer feedback.**
3. **Perform detailed Root Cause Analysis for reported software faults and procedural errors.**
4. **Based on these, use a total quality management approach to identify, plan, and implement improvements in the entire software process.**

The feedback from the customer is important to understand how the system functions while it is used day-to-day. It is especially important that efforts are made to get complete data on failures and outages.

As failures and outages are reported a root cause analysis is typically done. Frequently this involves seeking to answer two questions:

- What problem in the process or this particular implementation allowed the problem to occur?

D

- Why did the Quality Assurance portions of the process (e.g., reviews, inspections, testing) not prevent this problem from getting to the field?

It is sometimes necessary to ask the questions repeatedly to get to actionable root causes. Further data may need to be collected to validate suspected root causes. It may also be necessary to accumulate these answers to look for general process trends.

Metrics will be needed to assess improvement in quality and reliability. Metrics may also be used to help select the most effective actions to counteract the process problems identified by the root cause analysis. The recommendation on use of these metrics is described in more detail in the next section.

Based on the data obtained in other steps, specific process countermeasures should be identified. A plan should be put in place to implement these countermeasures. This plan should be traced and the improvement measured using the established metrics.

6.3.2 Software Recommendations

To assist the DCS vendors in implementing the countermeasures described above, the following recommendations have been identified from across the industry.

1. **Software Reliability Metrics**
2. **System Defensiveness,**
3. **Failure Modes and Effects Analysis,**
4. **Early Product Integration and Test and Early Service Provider Testing**
5. **Testing In Service Provider Environment.**

More details and references for each of these recommendations are given in the sections below.

6.3.2.1 Software Reliability Metrics
Software is a relatively new discipline where the reliability methodology is not well defined, particularly predictions of software reliability. Yet, without detailed measuring of software systems and without thorough analysis of these measurements, maintaining the quality of software and increasing its reliability is simply not possible. Given this need, there are a number of factors that contribute to the difficulty of performing measurement of software reliability. This includes the difficulty of performing predictions, having complete data available and the need to reflect the customer perception of reliability, not simply a theoretical model.

As with any form of data analysis, there has to be a choice of which metrics to select. The ones chosen here are particularly related to software development and are defined as part of the Bellcore TR-TSY-000929 requirements. Three measurements are selected and described below:

1. **Fault Density**

   This plot provides monthly data of the cumulative number of software faults as a function of time, divided by the lines of code for each release. **Comparison of the cumulative fault density of new and changed lines of code in different software releases of an equivalent age provides an understanding of their relative software quality** (that is, whether the software quality of releases is improving or not as normalized by the size of the release). An example of this plot for two different releases is in Figure 27.

2. **Fault Fix History**

   These two plots provide weekly data of the cumulative number of faults being uncovered (Figure 28) and of unfixed faults (Figure 29), beginning with the verification phase for a given release. **This metric helps in providing an understanding of whether a release is ready for deployment and provides insight into the effectiveness of the fault detection and removal process.** Of particular interest in such a plot is the rate at which faults are being

D

discovered, since this can be examined as evidence of whether a present software release is ready for widespread field deployment.

3. **Actual Software Faults and Prediction**

   This metric provides monthly data of the cumulative number of software faults for a release by the cumulative field operation-months starting from the General Availability of the release. **This measurement helps to provide a prediction of the quality of the software for a given release, based on prior fault discovery.** The prediction (using the Kaplan - Meier median) provides an indication of what can be expected in terms of future experience with a release. Since this plot will eventually include multiple software releases, it will also provide an indication of the software quality based upon comparison with earlier releases. An example of this plot is in Figure 30.

Use of Metrics by Service Provider. Although the equipment vendor is the primary user of these metrics to understand and improve the quality of their software process, the metrics can be shared with the service provider also. This can give the service provider confidence in the integrity of the release process, an expectation of the field performance through the predictive metrics, and can foster trust and teamwork between the two organizations. The recommendation on testing in the service provider environment below describes partnering between the service provider and equipment supplier in more detail.

6.3.2.2 System Defensiveness The goal of providing system defensiveness features in the software is to prevent failure, service outage, or accidental loss of cross-connect information by either an internal system process or an external source.

Software is the primary interface for the majority of interactions with the DCS system. This interaction can either be remotely through an Operations Support System or locally through a Craft Interface Terminal. In either case, a system of commands, messages and responses is used and the commands that can be entered can affect service on all or part of the system. Defensiveness may be improved by applying an increased sensitivity towards human factors engineering in the definition phase of the software development process. **Recent work (including Bellcore Special Report SR-NWT-002374) has focused on the system defending itself against any loss of service resulting from inadvertent or accidental use of a service affecting command.**

Below are a few items that have been determined as areas where improvements have been shown to be beneficial to the industry. Most of these apply to the craft interface.

- **Increased security on commands with system-wide impact**

  This capability restricts access to powerful commands to experienced users, and only users with a sufficiently high security level (as assigned by a system administrator) will have access to service-affecting commands.

- **Media Validation**

  This is the capability to ensure that the correct tape or disk with the correct software release and database is to be loaded into the system. If there is any discrepancy, then the software should deny the operation and inform the user that the operation has been halted due to a media mismatch.

- **Prevent problems from null database scenarios**

  A particularly powerful command within a DCS system is the capability to create and subsequently load a null database into a live system, thereby disconnecting

D

service on the entire system. Such commands require careful implementation and administration to eliminate potential service-affecting events. It may be necessary in some cases to eliminate these commands in production systems.

- **Restrictions on Range Commands**

  While increasing the security system for users is a major improvement, a related item that should be considered is that of restricting the scope that even experienced users can address. For example, many software commands have an "ALL" option, meaning that the command can be executed on the entire system. Consideration should be given to particularly powerful commands being restricted to a subset of the system (that is, a module or sub-module).

- **Command Verification Warning Messages**

  Command Verification messages are issued to alert users to the fact the the command they are about to issue has service-affecting implications. This warning message contains precise information as to the implications of the command and provides the user with one last check to verify that this is indeed the command that was intended to be executed.

- **Corruption of storage device**

  Further improvement in system prevention, tolerance and recovery from corruption of information in the storage devices.

- **System reaction to unconnected/not working output devices**

  The system should gracefully handle situations where output is delayed or backed up due to problems with the output devices.

- **Security against viruses or intentional intrusion**

  Although there are no documented failures where the DCS software is contaminated with a virus, or where an illegal user gains access to a DCS, these are problems with software systems in general. With widespread communications networks and the ability to remotely download software, these items must be addressed to prevent any future problems.

6.3.2.3 Failure Modes and Effects Analysis
Failure Modes and Effects Analysis (FMEA), sometimes referred to as FMECA (the "C" is for Criticality), is a systematic procedure for identifying the modes of failures and evaluating their consequences. Its purpose is to identify and manage critical failure modes so as to mitigate the effects of failures on the operation of a system. **FMEAs are used extensively in the Department of Defense (see MIL-STD-1629 "Procedures for Performing a Failure Mode, Effects and Criticality Analysis") as an effective technique for revealing design deficiencies and potential hazards.**

A FMEA is generally performed on the basis of limited design information during the early stages of design and is periodically updated to reflect changes in design and improved knowledge of the system. The basic questions that are answered by the analyst in performing a FMEA are:

1. How can each component or subsystem fail? (What is the failure mode?)
2. What cause might produce each failure? (What is the failure mechanism?)
3. What are the effects of each failure if it does occur?

Once a FMEA is completed, it can assist the analyst in:

- Identifying critical system components whose reliability warrants special attention
- Selecting early in design, various design alternatives with high reliability, such as robust, fail-safe human interfaces

D

- Ensuring that all possible failure modes, and their effects on operational success of the system, have been taken into account
- Identifying potential failures and the magnitude of their effects on the system
- Providing a basis for qualitative reliability and availability analyses
- Identifying areas where protective structures should be used to minimize the impact of failures on the systems performance (e.g. redundancy and failure detection and recovery systems)
- Designing maintainability aspects into the system by establishing failure detection logic, test points, and test procedures

Fault insertion testing is a technique used to validate the design and implementation and to demonstrate the system's defensiveness to failures.

Rigorous adherence to this process can assure that a robust, highly reliable system is designed, developed, and delivered to a service provider environment.

6.3.2.4 Early Product Integration and Test Within the development phase of the process, the product is developed in a step-wise fashion, where increasing functionality is delivered in a prescribed sequence of planned loads. Critical features, e.g. those that are traffic related, are developed earlier in the cycle. These loads, which must contain mature features with no traffic-related problems, can be given to the service provider in a controlled fashion for early testing. Note that this testing should not be done with live traffic, but rather should occur in a simulated environment as described in the next recommendation.

The advantages of early product integration and test are:

- The internal development test team can be involved as early as feasible
- Problems are found as early as possible in the development cycle and can be corrected earlier with less impact on the schedule. This avoids a big-bang approach where everything is developed, then everything is tested, then the product is shipped.

The advantages of providing preliminary software loads to the service provider are:

1. Allows for comprehensive office-dependent testing
2. Allows for early correction of any service provider or office related issues before general availability of the release.
3. Gives the service provider the ability to affect the product operation in the current release and to affect requirements in future releases.
4. Gives the service provider confidence in the functionality of the product.

6.3.2.5 Testing In Service Provider Environment When the service provider finds critical failures in the field after deployment of new software or hardware, it indicates that the supplier did insufficient testing or did not fully understand the service provider's application. To mitigate the probability of these difficulties, **the service provider and supplier should team up to understand what each wants or is providing, decide where there may be conflicts in need and capability, and to fully explore the service provider environment.** Through this process, each partner will gain a more in-depth understanding of the requirements and capabilities. It is important that this partnership be established well before general availability of the software and/or hardware.

Although testing should not be done with live traffic, it is important to validate the DCS system as it will operate in the field environment. To achieve this, it must be tested as an integrated system. This includes the DCS, any Operations System or management system, and the interlinking communications network. The best method to utilize is a lab

D

setting that as closely as possible replicates the real operational environment. This setting could be on the service provider's or equipment supplier's location or both; or at a designated integrated testing lab (i.e., Bellcore, etc.) Since the real operational environment is rich with transitive transport link failures, significant delay characteristics, and burst messaging conditions, these must be kept in mind during test and development efforts.

When writing the test plan for this integrated testing effort, the operational environment must be studied and the service provider's expectations for features and functionality reviewed. Input from several major users is recommended to obtain a variety of ideas and areas of investigation. Field operations and technical support personnel from the service provider should be included in the test plan development process as they have direct knowledge of the environment to be emulated. In this way, the testing effort can be made more thorough.

Any testing that is accomplished should use the "Devil's Advocate" approach. Efforts should be made to stress the system to its limits and beyond. This will characterize the system's performance at the edge of the operating envelope and possibly uncover properties that are not desirable. To further validate equipment operation, craft personnel should perform all maintenance and troubleshooting procedures to find any discrepancies or unusual characteristics. One specific area that needs to be tested in detail is the software upgrade procedure. This is critical because of the potential for disrupting live traffic when a new software release is placed on a DCS in the field.

Any failures or anomalies that do occur during this effort should be thoroughly investigated. Internal system diagnostics should be used to determine whether they are sufficient for the field or whether they should be enhanced.

6.4 Hardware

6.4.1 Matrix, Controller and Disk Drive Failures

As mentioned earlier, the matrix cards, bridging cards, sync cards, controller circuit packs, and disk drive failures in combination with procedural errors are the major cause of large and long duration outages. Several straightforward countermeasures were identified which can help to eliminate these type of failures in the future.

a. Recommendation to all equipment suppliers that they **critically review the level of inspection and surveillance on critical DCS components** (i.e. matrix cards, bridging cards, sync cards, disk drives, and controllers) and **do aggressive root cause analyses of all field failures.**

b. Recommendation to all service providers to have **sufficient spares of critical DCS components readily available to minimize downtime.** (i.e, matrix cards, bridging cards, controller cards, etc.)

c. **Deploy systems on a going forward basis with redundant disk drives with common data or a new technology** which radically improves in-service reliability and/or reduces downtime in the event of an outage.

d. Recommendation to equipment suppliers that they provide **improved documentation on memory backup procedures and methods to recover from total system outages.**

6.4.2 Controller Failures

Controller failures are the root cause of most non-service effecting DCS failures. As mentioned previously, this failure typically results in no loss of traffic, however, it does result in a loss of reconfigurability, protection switching, alarm visibility, and/or communication with other parts of the system. Although this condition is less severe than a

D

loss of service, in the very near future some new services will consider this condition as an outage. The only way to deal with this uncertainty today is some sort of redundant or duplex controller architecture.

a. **In general "best practices" from the existing DCS designs indicate redundant controllers while "best practices" from the switch world would indicate full duplex, synchronized controllers.**

b. Of course, there is a cost/benefit tradeoff that has to be made here. However, at a minimum, the service provider should **insist on the equipment supplier providing them hard data to prove that their simplex or redundant controller design meets their in service network reliability criteria.**

6.4.3 Passive Connecting Hardware Failures

The only tried and true countermeasure to minimize these problems is to **systematically inspect** the interbay cabling, terminating connectors, port shelf backplane, signal splitters and other visible passive hardware **during installation, during turn up, and periodically in service during off peak hours.** Several "best practices" which can help in knowing what to look for are included in the references.

6.4.4 In-Service Reliability Requirements

Bellcore's and/or the equipment supplier's existing hardware reliability requirements are not suitable as a metric for measuring in-service reliability performance (but are appropriate for assessing the hardware design). We recommend that:

a. **a new set of hardware metrics for in-service reliability measurement and tracking be developed** (an effort is underway at Bellcore to create a straw proposal for industry review),

b. a means for accomplishing **an in-depth root cause investigation of every total system failure be established,** and

c. **rapid, complete, and accurate reporting of outages to equipment suppliers by service providers.**

If all three recommendations are followed, Bellcore in cooperation with the DCS industry will be successful at generating meaningful in-service reliability requirements.

6.5 Network Applications

Digital Cross-Connect System (DCS) reliability requirements were studied from an applications perspective. The applications considered in this analysis are High Capacity Services (DS1, DS3, OC-N, etc.), High Availability Services (automatic path diversity), Gateway Service for Multiple Ring Interconnects, and Centralized Controller Restoration Services for facility or switch failures. The generic questions of what is the impact of a new technology such as SONET and "how big is too big?" have been studied. Appendix 3 provides the complete detail of these analyses. What will be presented next are the key learnings from those analyses.

6.5.1

Existing DCS reliability and availability requirements are theoretically sufficient to meet existing service demands for high availability, high capacity, multiple ring interconnects, and centralized controller restoration applications. These calculations may have to be revisited when data from in-service metrics are available.

6.5.2

SONET integration into the DCS will require a reallocation of software and hardware (integrated optics) failure rates in network models, which may affect real deployment plans.

6.5.3

Most envisioned new services place more importance on OS-NE communications,

D

controller availability, and reduced cross-connect times - best practices would indicate that redundant controllers, redundant OS-NE links, and high powered connect/disconnect commands will be required.

6.5.4

Each service provider should look at "how big is too big?" from a cost, reliability, and procedural perspective before making a decision for a specific application. **One size DCS does not fit all applications optimally.**

7. Measuring Improvements

The DCS Focus Team recommends the use of FCC outage reports per Docket 91-273 as the standard metric by which national DCS improvement will be tracked. The baseline period will be April 6, 1992 through April 5, 1993. As of March 1, 1993, there have been two FCC reports due to DCS outages.

It is also recommended that service providers and equipment suppliers continue to collect and perform joint root cause analysis of the DCS outage data. It is highly desirable to have the data collection template designed to facilitate "true" root cause analysis, i.e., what happened as well as why it happened. Collection of quantitative data such as those contained in Bellcore TR 929 and the recommended metric of Total Downtime/DCS/Yr in Equivalent DS1 Hours will also be useful for assessing actual field performance over time.

8. Path Forward

The DCS Reliability Focus Team supports the proposal that the Exchange Carriers Standards Association (ECSA) assemble and perform macro-analysis of the FCC outage reports on behalf of the industry. ECSA will also interface with the appropriate standards groups whenever DCS-related technical changes are deemed appropriate by the industry participants. If required, ECSA may also request that the Focus Team or its equivalent be reconstituted.

It is expected that several Bellcore DCS requirements and in-service metrics will be updated as a result of this effort. In addition, there are numerous other industrial initiatives on Network Reliability. A partial listing of those ongoing initiatives which will impact on DCS Reliability are given in Appendix 4.

It is also expected that the NRC members will use the above data and metrics as a means of benchmarking their individual current situation; and if improvements are needed they will look to the assemblage of countermeasures and do a cost/benefit analysis on each item to prioritize their action plan. As a getting started scenario the team would recommend a DCS Awareness Program and a significant emphasis on the improvement of documentation and training material. This should not require any more than a modest investment in funding.

Finally, the DCS Reliability Focus Team is honored to be part of the NRC Industry Symposium. It is also glad to announce that the IEEE DCS Workshop, which will be held on 6/14-17/93 in Banff, Canada, has an entire session focused on DCS Network Reliability and many of the focus team members are presentors. This is an attempt to spread the message and keep the momentum of the team effort.

9. Conclusion

This paper presents the results of a unique data collection and telecommunications industry team effort focused on DCS Reliability. It has confirmed that DCSs are very reliable network elements, however, when they fail nearly half of the outages are resolved in less than one hour, however, 8% of the outages last for six hours or more. The root causes for the failures have been identified as well as countermeasures and recommendations of best practices, which should significantly improve the current situation. The team goes on to recommend a voluntary DCS Awareness Program as a means to initiate these recommendations and

D

the FCC outage reports per Docket 91-273 as the standard metric by which national DCS Reliability can be tracked. In addition, they recommend that service providers and their suppliers proactively share all outage data, collaborate on root cause analyses, and measure their in-service DCS performance using a comprehensive and detailed metric, such as Total Downtime/DCS/year. The momentum of the effort will be carried on by the DCS industry through the issuance of several new Bellcore requirements, the NRC Industry Symposium and IEEE DCS Workshops, and the macro analysis of the FCC outage reports by the ECSA.

10. Acknowledgements

The author wishes to acknowledge the significant contribution of the Subgroup Team Leaders and the text editors, who provided the majority of the document.

Assess the Risk and Data Presentation
Eva Low, Team Leader
Louis Scerbo, Editor

OAM&P
Frank Denniston, Team Leader
Bencilla Jenkins &
Robert Fitzgerald, Editors

Documentation and Training
Rob Pullen, Team Leader
Rob Pullen &
George Stanek, Editors

Software
Phil Rubin, Team Leader
Bruce Cortez, Editor

Hardware
Sid Shelton, Team Leader
Fred Hawley &
Joe Cheng, Editors

Network Applications
Ken Lewis, Team Leader
John Adler, Editor

The DCS Focus Team gratefully acknowledges the contributions and assistance of the following companies and associations who provided data and shared technical expertise. Those contributions were invaluable to the Focus Team's study effort and the preparation of this paper.

Ad Hoc	MCI
Alcatel	New York Clearing House
Ameritech	NYNEX
AT&T	Pacific Bell
Bell Atlantic	Pitney-Bowes
Bellcore	SNET
BellSouth	Southwestern Bell
DSC	Sprint
GTE	Stentor
ICA	Tellabs

Finally, the Focus Team wishes to extend a special thank you to Messrs. John Healy, Joe Cheng, Fred Hawley, and Jay Bennett of Bellcore who conducted the all important data collection and analysis effort and to Mary Basiaga who was responsible for production and distribution of this document.

11. References

Following is a partial listing of technical references related to a number of the countermeasures proposed in this paper.

References/Best Practices

1. TR-NWT-000170, Digital Cross-Connect System Generic Requirements and Objectives, Issue 2, January 1993
2. TA-NWT-000233, Wideband and Broadband Digital Cross-Connect Systems Generic Criteria, Issue 4, November 1992
3. TR-TSY-000233, Wideband and Broadband Digital Cross-Connect Systems Generic Requirements and Objectives, Issue 2, September 1989
4. TA-NWT-000253, SONET Transport Systems: Common Generic Criteria, Issue 2, December 1991
5. TA-NWT-000253, SONET Transport Systems: Common Generic Criteria for Operations Communications Routing and LAN Support, Issue 7, September 1992
6. SR-TSV-002387, SONET Network and Operations Plan: Features, Functions, and Support, Issue 1, August 1992
7. TR-NWT-000499, Transport Systems Generic Requirements (TSGR): Common Requirements, Issue 4, November 1992; plus Revision 1, April 1992
8. TR-TSY-000191, Alarm Indication Signal Requirements and Objectives, Issue 1, May 1986
9. TA-NPL-000436, Digital Synchronization Network Plan, Issue 1, November 1986
10. SR-NWT-002224, SONET Synchronization Planning Guidelines, Issue 1, February 1992
11. TA-NWT-001244, Synchronized Clocks: Common Generic Criteria, Issue 1, September 1991
12. TR-TSY-000828, Operations Technology Generic Requirements (OTGR): Generic Operations Interfaces - OSI Communications Architecture, Issue 1, November 1988, plus Revision 1 March 1991
13. TR-NWT-000472, Operations Technology Generic Requirements (OTGR): Memory Administration, Issue 3, October 1991, plus Supplement 1, July 1992
14. TR-TSY-000474, Operations Technology Generic Requirements (OTGR): Network Maintenance: Network Element, Issue 3, November 1989, plus Revision 2, July 1991; Bulletin No 1, November 1991, and TA-NWT-000474, Issue 1, December 1991
15. TR-TSY-000820, OTGR: Network Maintenance: Transport Surveillance - Generic Digital Transmission Surveillance, Issue 1, June 1990
16. TR-EOP-000063, Network Equipment - Building System (NEBS), Generic Equipment Requirements, Issue 4, July 1991
17. TR-NWT-000332, Reliability Prediction Procedure for Electronic Equipment, Issue 4, September 1992
18. TA-NWT-000418, Generic Reliability Assurance Requirements for Fiber Optic Transport Systems, Issue 3, November 1991

D

19. TR-NWT-000468, Reliability Assurance Practices for Optoelectronic Devices and Interoffice Applications , Issue 1, December 1991

20. TR-NWT-001089, Electromagnetic Compatibility and Electrical Safety Generic Criteria for Network Telecommunications Equipment, Issue 1, October 1991

21. TR-NWT-000078, Generic Physical Design Requirements for Telecommunications Products and Equipment, Issue 3, December 1991

22. TR-TSY-000454, Supplier Documentation for Network Elements, Issue 1, July 1988, plus TA-OPT-000454, Issue 2 May 1991, and TA-OPT-000454, Issue 3, July 1992

23. TR-OPT-000839, Supplier-Provided Training Generic Requirements, Issue 3, December 1991

24. TA-NWT-001339, Generic Reliability Requirements for Digital Cross-Connect Systems, Issue 1 (to be issued)

25. SR-NWT-002419, Software Architecture Review Checklists, Issue 1, December 1992

26. TA-NWT-000929, Objectives for Reliability and Quality Measurements for Telecommunications Systems (RQMS)

27. SR-TSY-001130, Reliability and System Architecture Testing (RSAT), Issue 1, May 1989

28. SR-TSY-001171, Methods and Procedures for System Reliability Analysis, Issue 1, January 1989

29. SR-NWT-002374, Digital Cross-Connect Systems Software Security Features, Issue 1, October 1992

30. SR-TSY-000357, Component Reliability Assurance Requirements for Telecommunications Equipment, Issue 1, December 1987

31. TR-TSY-000411, Manufacturing Program Analysis for Quality and Reliability Issue 1, August 1987

32. TA-TSY-000281, Digital Cross-Connect System Requirements and Objectives for the Digital Multipoint Bridging Feature, Issue 2, June 1986

33. TA-TSY-000280, Digital Cross-Connect System Requirements and Objectives for the Sub-Rate Data Cross-Connect Feature, Issue 2, May 1986

34. TA-TSY-000189, Generic Requirements for Subrate Multiplexer, Issue 1, April 1986

35. TA-TSY-000192, Digital Data System (DDS) Multipoint Junction Unit (MJU) Requirements, Issue 2, April 1986

36. TA-TSY-000077, Digital Channel Bank - Requirements for Dataport Channel Unit Functions, Issue 3, April 1986

37. TR-TSY-000179, Software Quality Program Generic Requirements (SQPR), Issue 1, July 1989

38. SR-TSY-001136, Handbook for Digital Cross-Connect System Quality & Reliability Analysis, Issue 1, January 1989

D

39. TM-NWT-021234, Digital Cross-Connect Systems and CCS Network Survivability, June 30, 1992

40. TA-NWT-001353, Restoration of DCS Mesh Networks with Distributed Control: Equipment Framework Generic Criteria, Issue 1, December 1992

41. Proceedings of the Annual Reliability and Maintainability Symposium, Hardware/Software FMECA, pp. 320-327, 83

42. Proceedings of the Annual Reliability and Maintainability Symposium, Assuring Software Safety, PP. 274-279, 92

43. Telephony, Getting to the Source of Network Disasters, 10/90

44. Bellcore Digest, The Evolution of Digital Cross-Connect Systems Analysis, July 1990

45. ANSI, Draft Proposed Technical Report on Network Survivability Performance, February, 1993

46. CCITT Study Group II & XVIII, Survivable Architectures

47. National Security Telecommunications Advisory Committee, NSIE DCS Security Checklist MDYS

48. DCS Awareness and Site Evaluation Checklist, Pacific Bell, Contact: Eva Low (510-823-2910)

49. AT&T DCS Awareness Program, AT&T-NSD, Contact: Paul Wolfmeyer (908-234-6320)

50. TR-NWT-001217, Generic Requirements for Separable Electrical Connectors Used in Telecommunications Hardware, 9/92

51. Sprint DCS Generic Upgrade Procedure, Sprint, Contact: Robert Fitzgerald (913-967-2220)

52. New York Telephone Upgrade Procedure, New York Telephone, Contact: Bencilla Jenkins (212-285-2854)

53. Pacific Bell Installation Job Acceptance Handbook, Pacific Bell, Contact: Eva Low (510-823-2910)

54. Pacific Bell Inspector/Observer Handbook, Pacific Bell, Contact: Eva Low (510-823-2910)

55. Pacific Bell Guidelines for Prevention of Transport Maintenance Work Errors, Pacific Bell, Contact: Eva Low (510-823-2910)

56. Pacific Bell Guidelines for Vendor Installation Activities Pacific Bell, Contact: Eva Low (510-823-2910)

57. TR-NWT-001275, Central Office Environment Installation/Removal Generic Requirements, February 1993

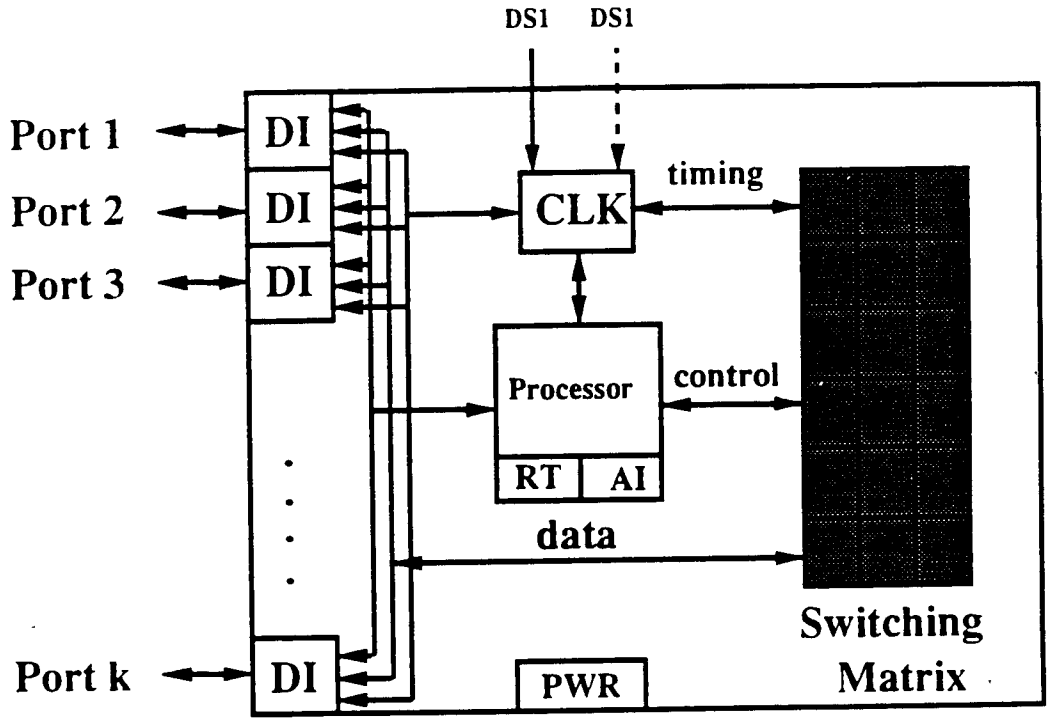
58. SR-TSV-002168, SONET Network Operations Plan, Issue 2, December 1992

D

12. Figures

D

D



DI - Digital Interface
CLK - Clock
RT - Remote Terminal Interface
AI - Alarm Interface
PWR - Power Converter

Figure 1

A Generic DCS Model

D

Focus Area: Digital Cross Connect Systems

Leader: Louis (Lou) J. Scerbo, Bellcore

Champion: Frank Ianna, AT&T-NSD

Supporting Staff:

John Adler, Alcatel
P.J. Aduskevicz, AT&T-NSD
Jay Bennett, Bellcore
Joe Cheng, Bellcore
Bruce Cortez, AT&T-NS
Steve Deschaine, DSC
Fred Ellefson, Alcatel
Fred Hawley, Bellcore
John Healy, Bellcore
Sam Hon, Bellcore
Bencilla Jenkins, NY Telephone
Donnie Jones, Pitney-Bowes
Ming Lai, Bellcore
George Stanek, AT&T-NSD

Figure 2

LJS 2 03/17/93

DCS Reliability Subgroups

1. Assess the Risk and Data Presentation - Eva Low (C), Frank Denniston, Robert Fitzgerald, Bill Jones, Mike Nawrocki, Lou Scerbo, Sid Shelton
2. Hardware Reliability - (Design and Process) - Sid Shelton (C), Fred Hawley, Lou Scerbo, Joe Cheng
3. Software Reliability (Design and Process) - Phil Rubin (C), Bruce Cortez, Bill Jones, Eva Low, Ken Lewis, Sam Hon, Ming Lai, Robert Fitzgerald
4. Network Applications - Ken Lewis (C), John Adler, Joe Cheng, Ken Menke, Bruce Cortez, Fred Ellefson, Fred Hawley, Duane Kobagashi
5. Operations (OAM&P) - Frank Denniston (C), H. L. Crim, Robert Fitzgerald, Bencilla Jenkins, Eva Low, Don Jones
6. Training and Documentation - Rob Pullen (C), Eva Low, Mike Nawrocki, Don Jones, Pete Shelus, George Stanek, Joe Cheng

Figure 3

LJS 3 03/17/93

Distribution of DCSs by User Company

Total DCSs = 2598

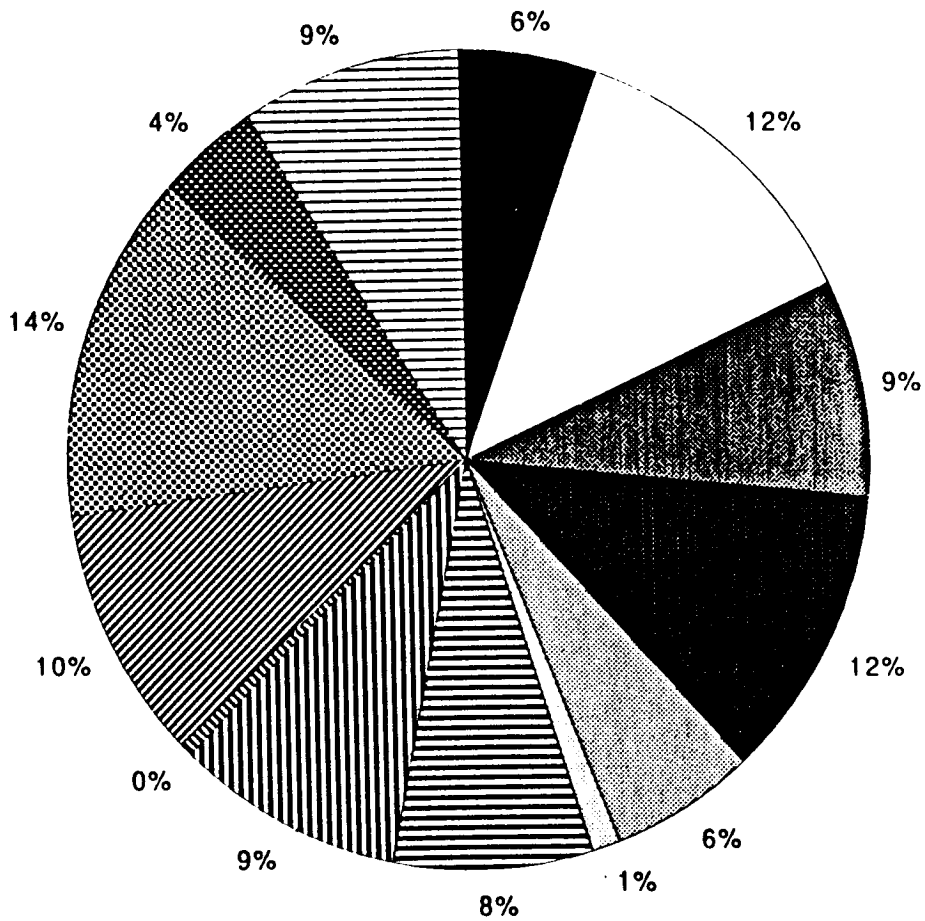


Figure 4

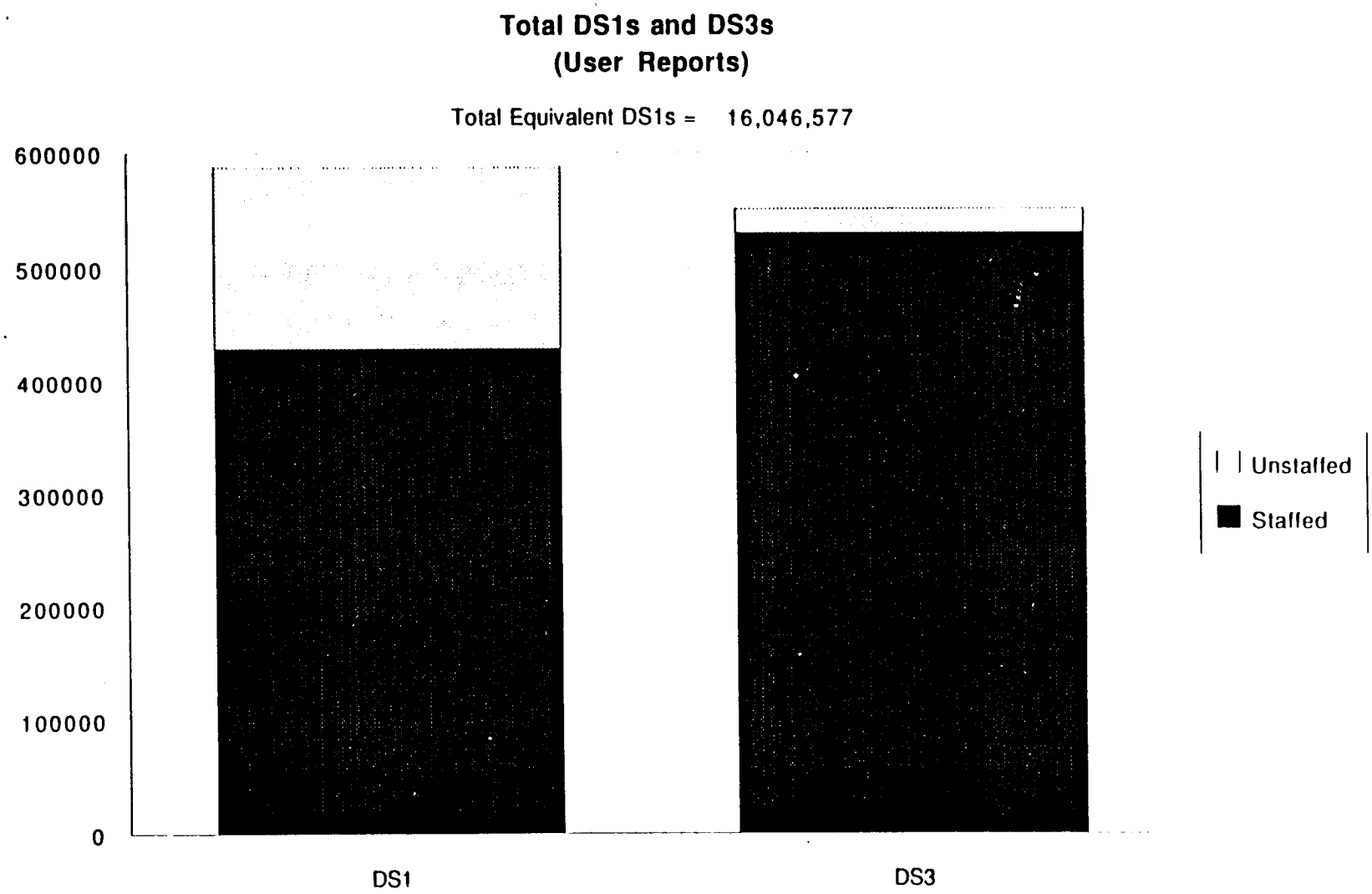

Total DS1s and DS3s
(User Reports)
Total Equivalent DS1s = 16,046,577
600000
500000
400000
300000
200000
100000
0
DS1
DS3
Unstaffed
Staffed

Figure 5

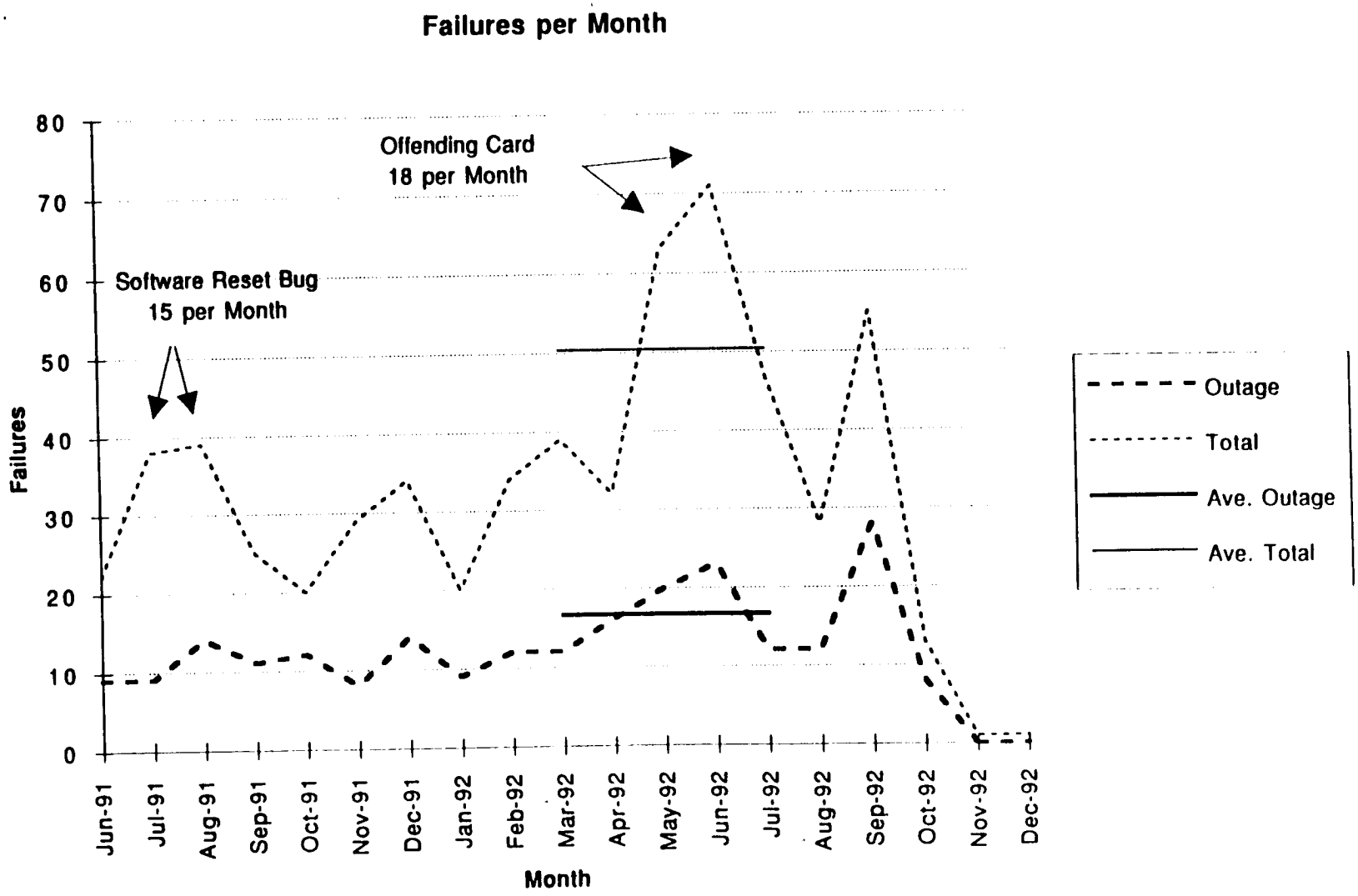

Failures per Month
Offending Card
18 per Month
Software Reset Bug
15 per Month
Failures
80
70
60
50
40
30
20
10
0
Jun-91
Jul-91
Aug-91
Sep-91
Oct-91
Nov-91
Dec-91
Jan-92
Feb-92
Mar-92
Apr-92
May-92
Jun-92
Jul-92
Aug-92
Sep-92
Oct-92
Nov-92
Dec-92
Month
Outage
Total
Ave. Outage
Ave. Total

Figure 6

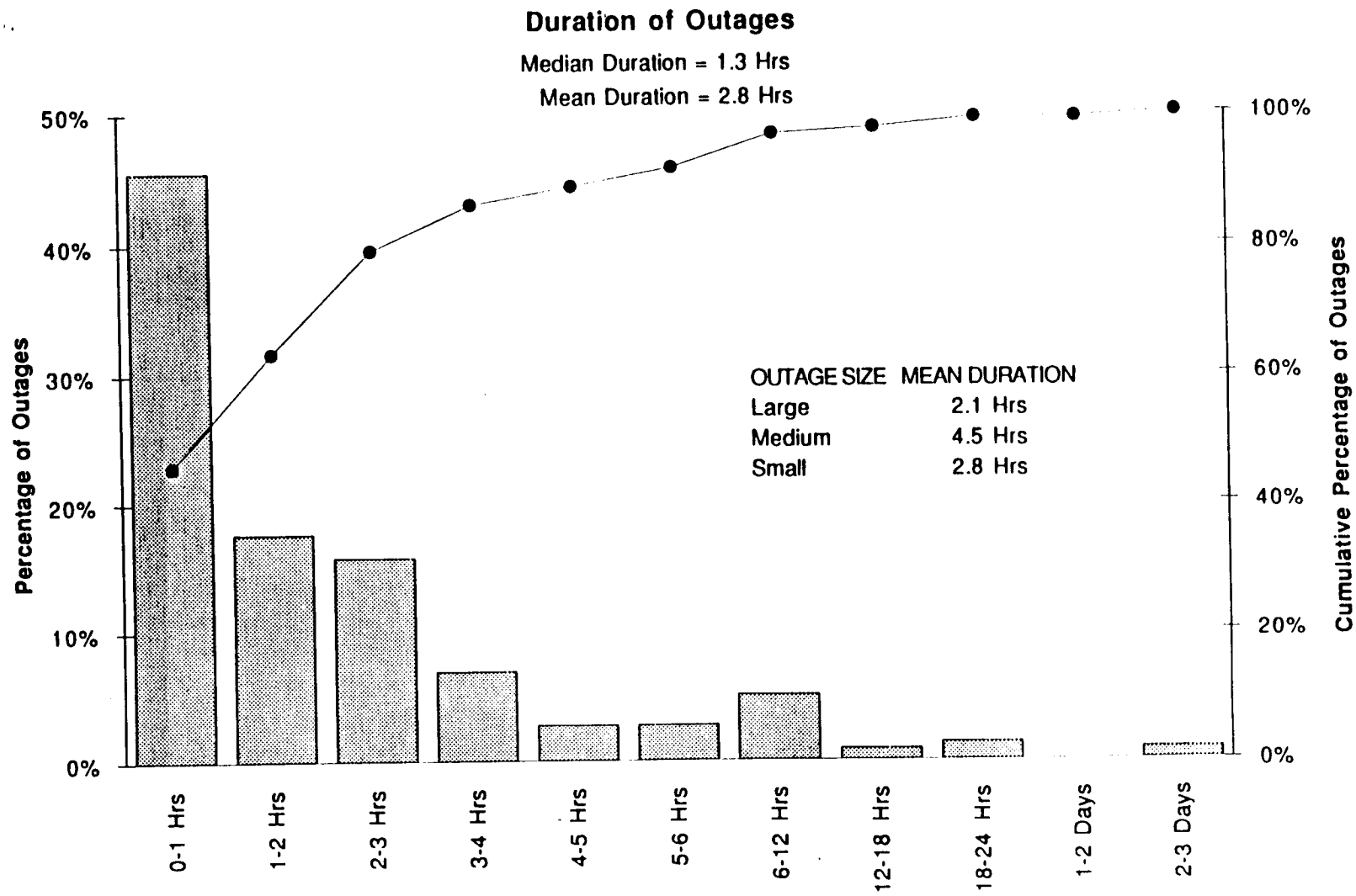

Duration of Outages
Median Duration = 1.3 Hrs
Mean Duration = 2.8 Hrs
Percentage of Outages
50%
40%
30%
20%
10%
0%
Cumulative Percentage of Outages
100%
80%
60%
40%
20%
0%
OUTAGE SIZE MEAN DURATION
Large 2.1 Hrs
Medium 4.5 Hrs
Small 2.8 Hrs
0-1 Hrs
1-2 Hrs
2-3 Hrs
3-4 Hrs
4-5 Hrs
5-6 Hrs
6-12 Hrs
12-18 Hrs
18-24 Hrs
1-2 Days
2-3 Days

Figure 7

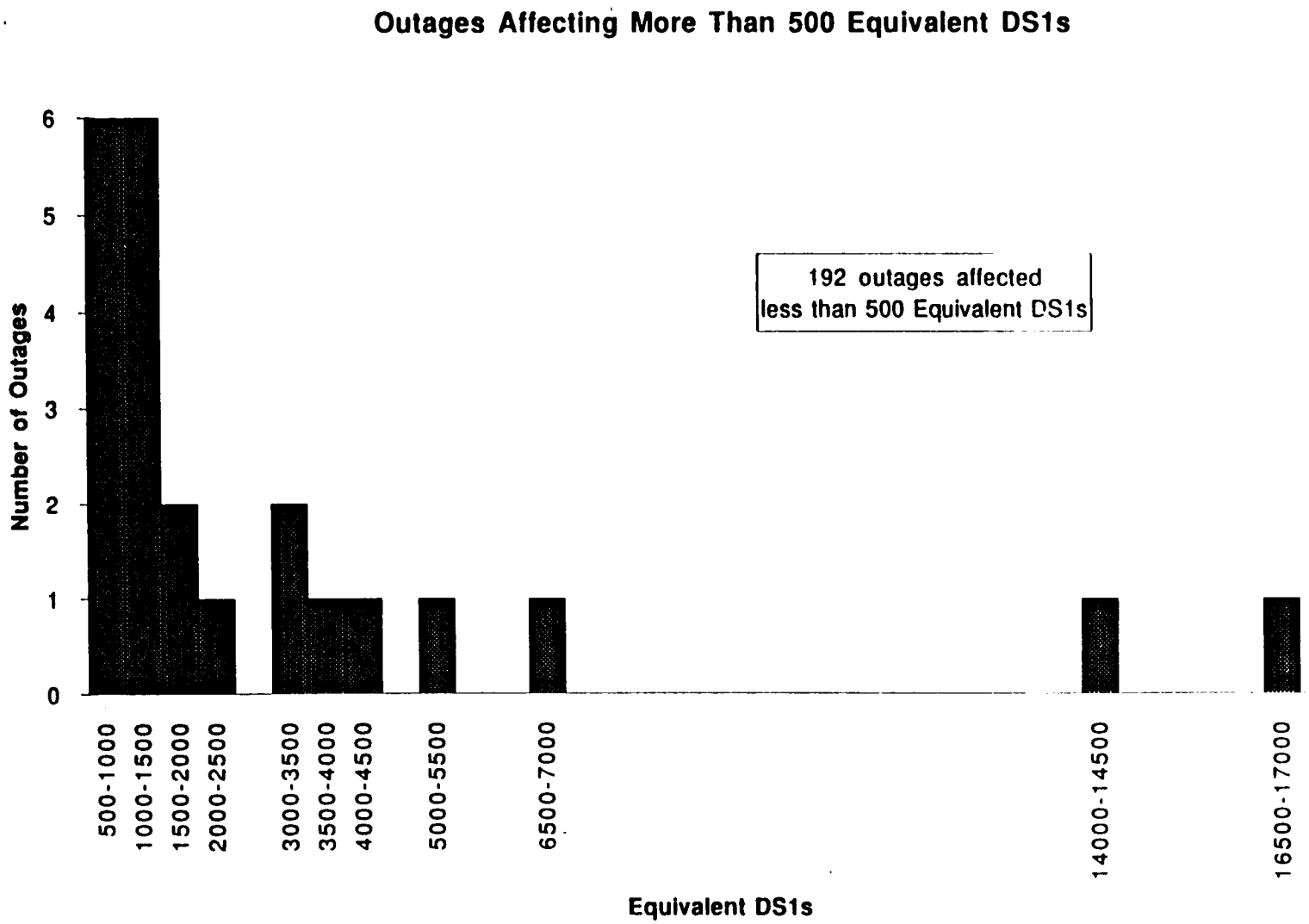

Outages Affecting More Than 500 Equivalent DS1s
Number of Outages
0
1
2
3
4
5
6
192 outages affected
less than 500 Equivalent DS1s
500-1000
1000-1500
1500-2000
2000-2500
3000-3500
3500-4000
4000-4500
5000-5500
6500-7000
14000-14500
16500-17000
Equivalent DS1s

Figure 8

Equivalent DS1 Downtime by Outage Size

DS1 Downtime (DS1 Hours/DCS) = 68

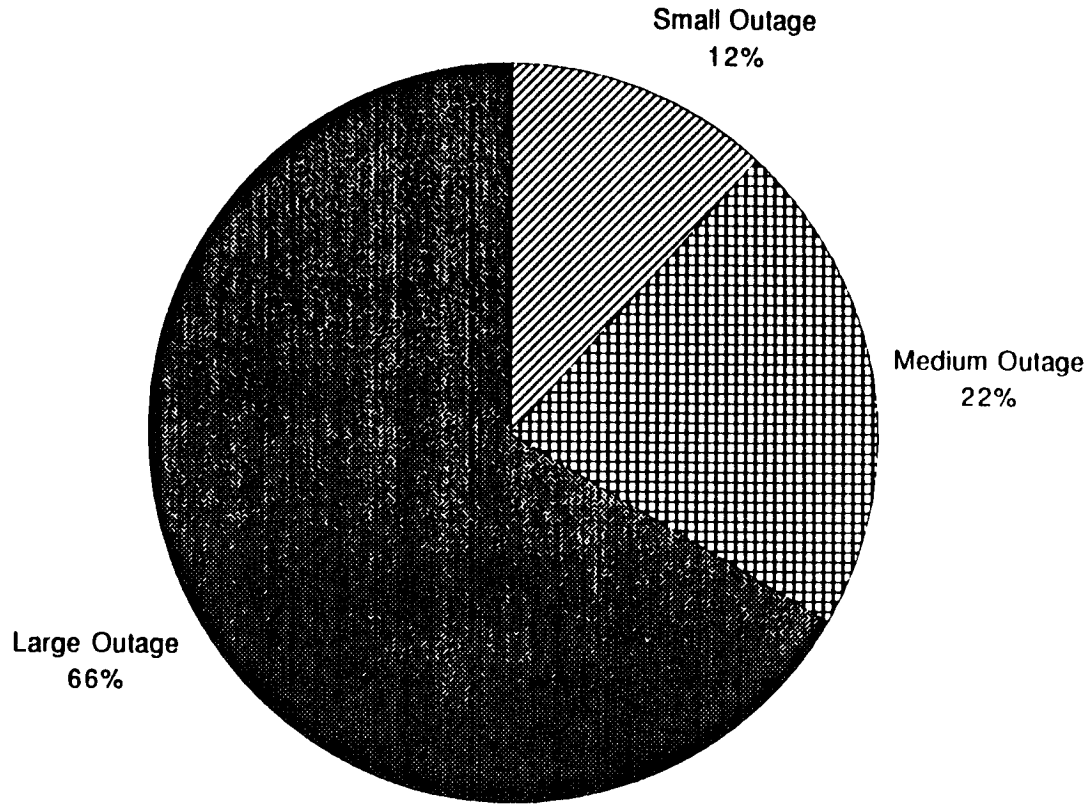


Figure 9

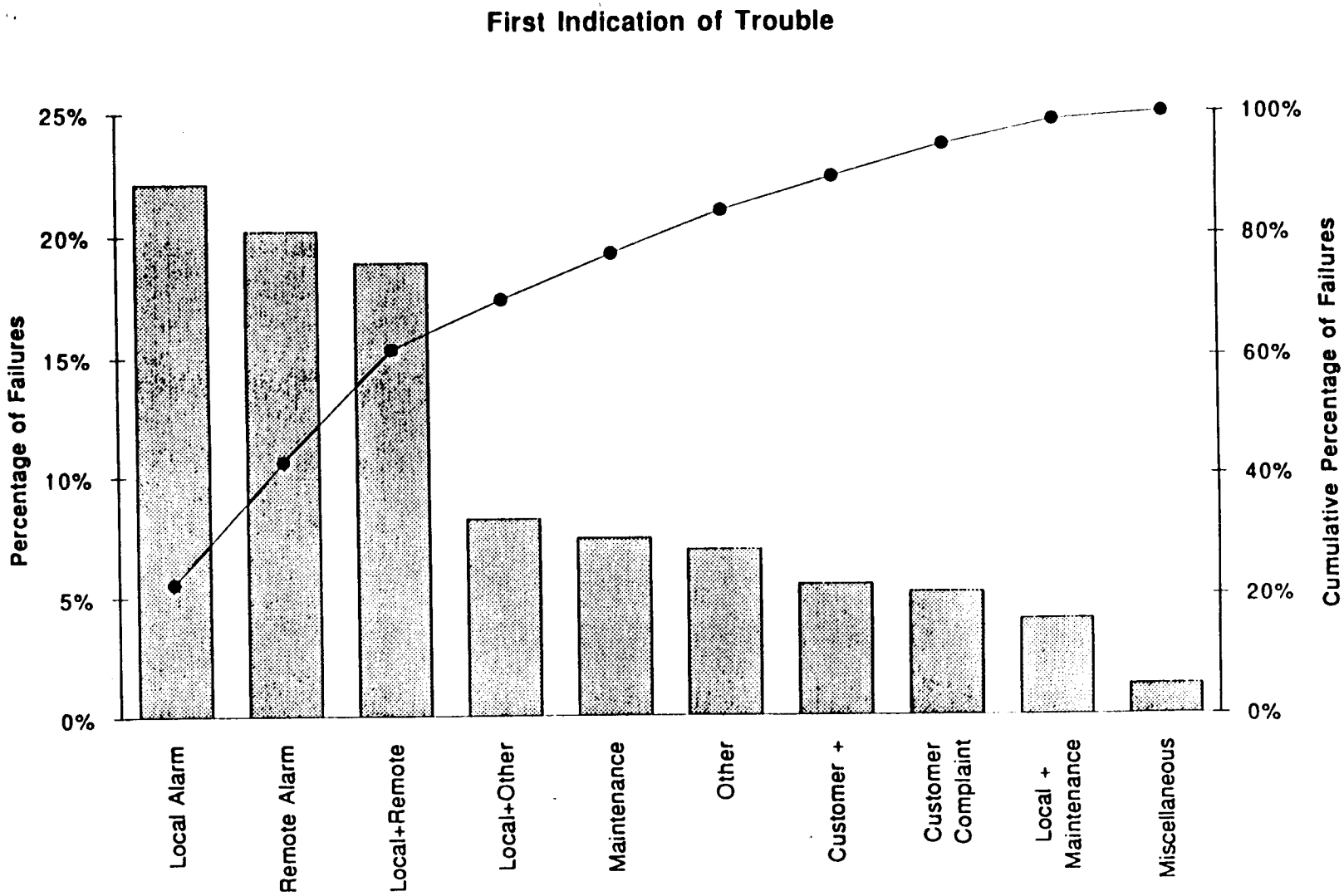

First Indication of Trouble
Percentage of Failures
25%
20%
15%
10%
5%
0%
Cumulative Percentage of Failures
100%
80%
60%
40%
20%
0%
Local Alarm
Remote Alarm
Local+Remote
Local+Other
Maintenance
Other
Customer +
Customer Complaint
Local + Maintenance
Miscellaneous

Figure 10

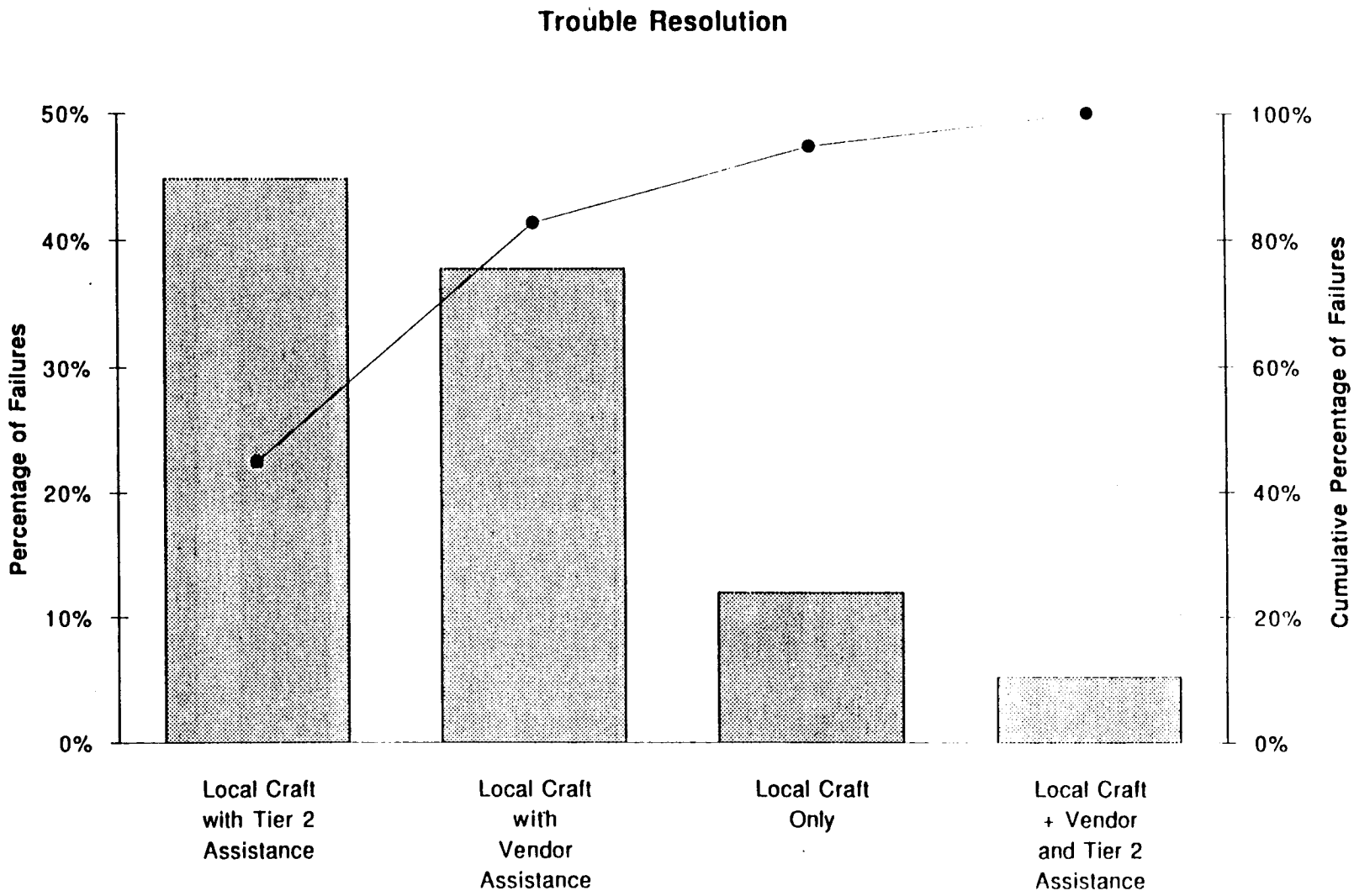

Trouble Resolution
50%
40%
30%
20%
10%
0%
Percentage of Failures
100%
80%
60%
40%
20%
0%
Cumulative Percentage of Failures
Local Craft with Tier 2 Assistance
Local Craft with Vendor Assistance
Local Craft Only
Local Craft + Vendor and Tier 2 Assistance

Figure 11

Trouble Resolution by Service Impact

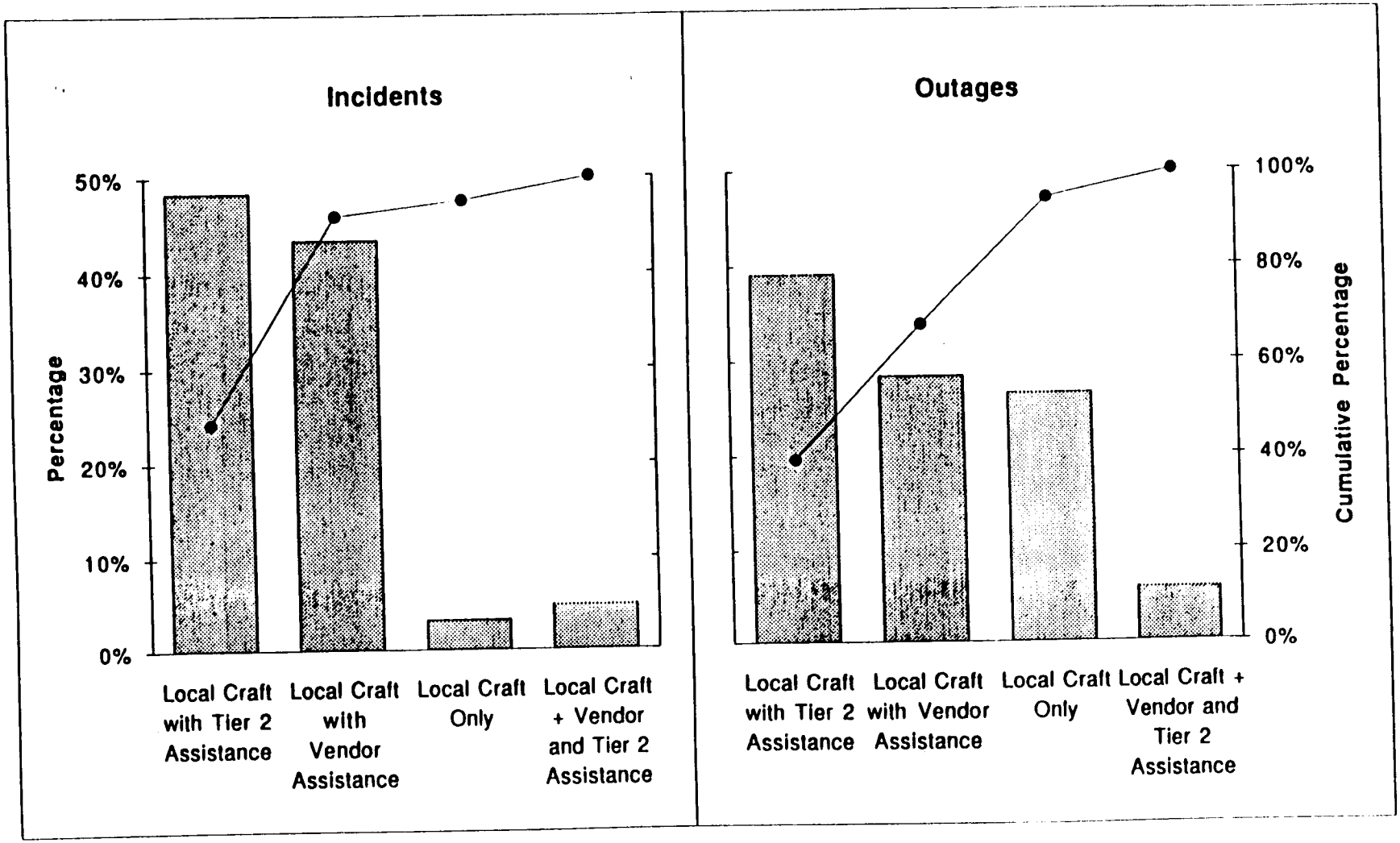


Figure 12

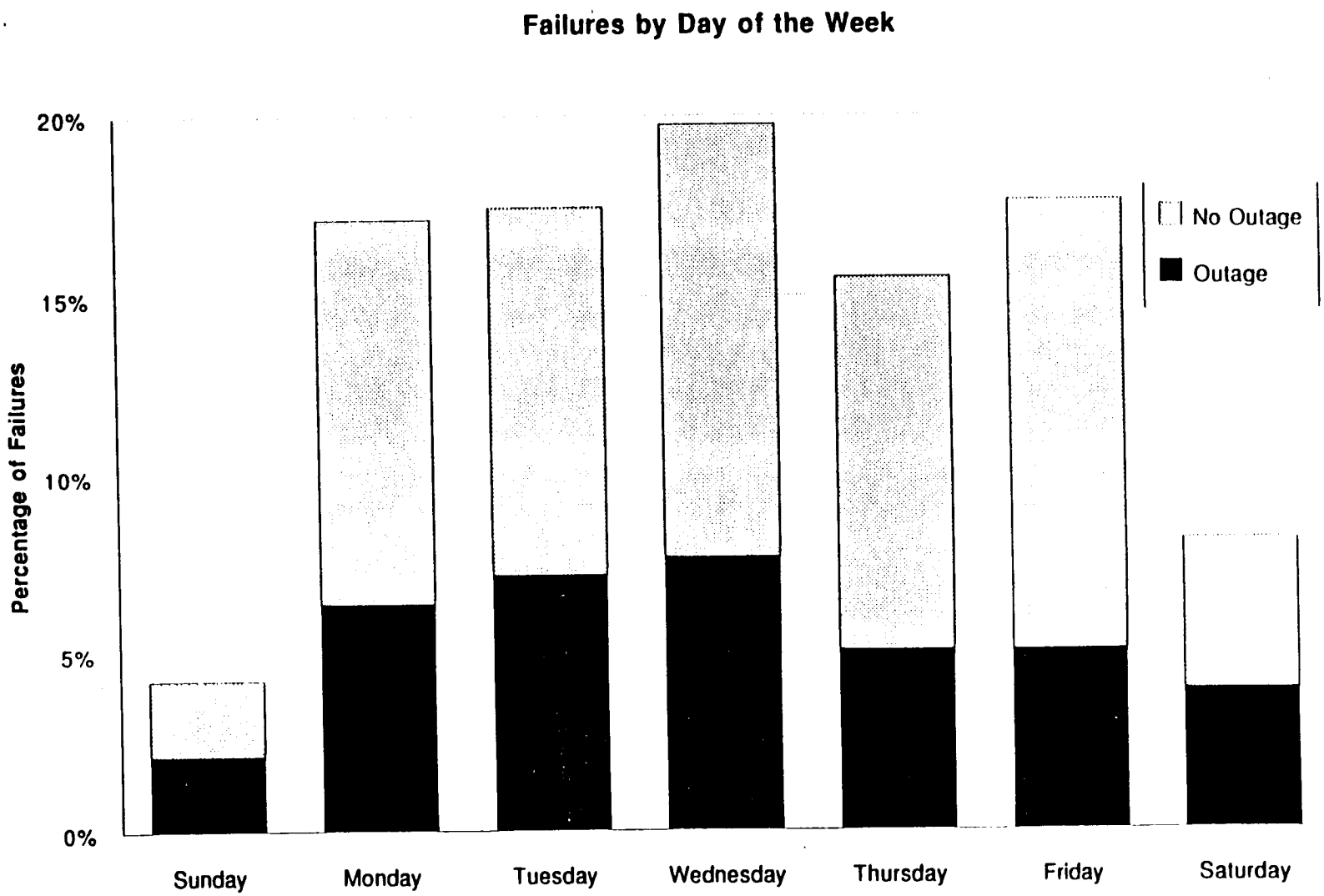

Failures by Day of the Week
20%
15%
10%
5%
0%
Percentage of Failures
Sunday
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday
No Outage
Outage

Figure 13

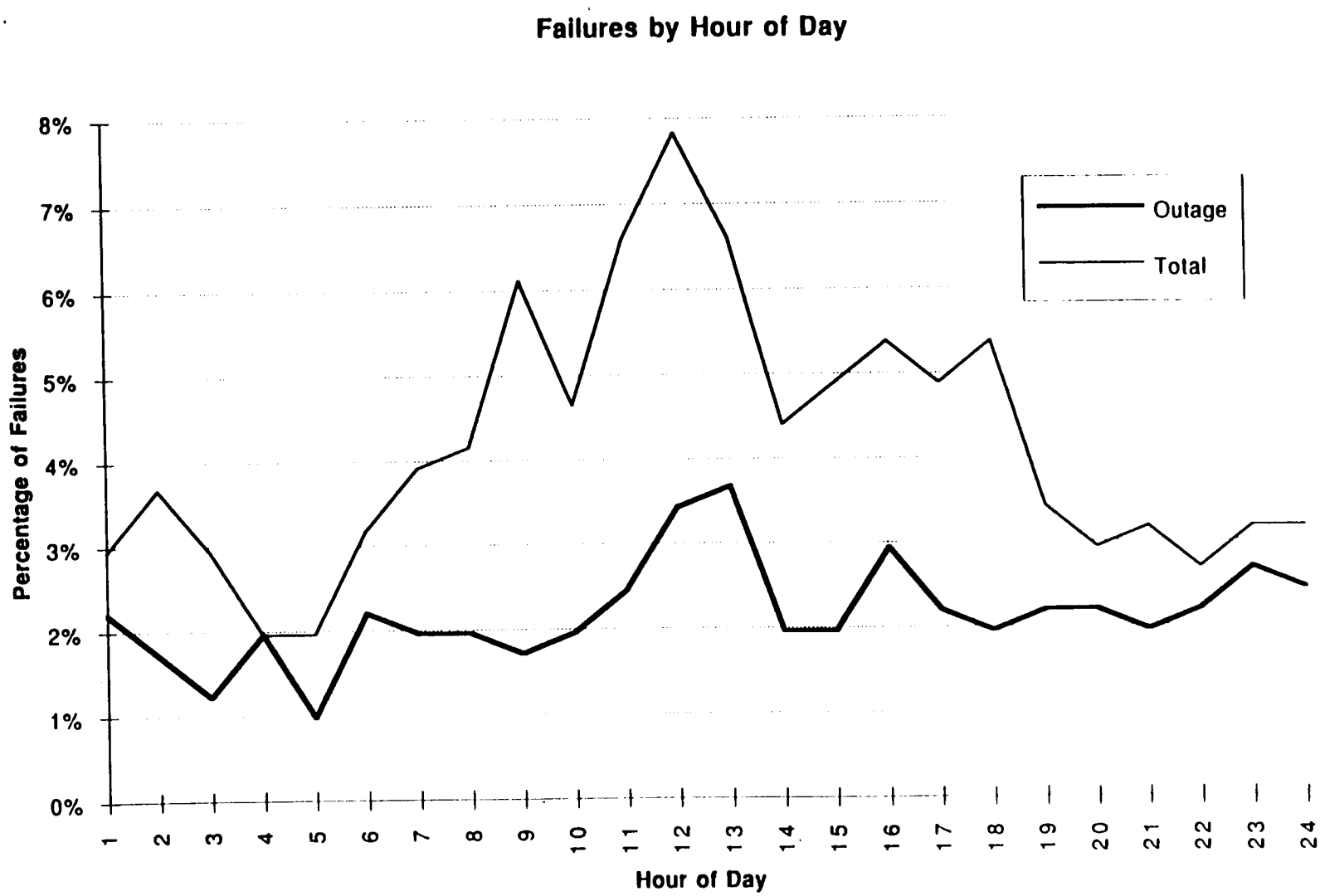

Failures by Hour of Day
Percentage of Failures
8%
7%
6%
5%
4%
3%
2%
1%
0%
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
Hour of Day
Outage
Total

Figure 14

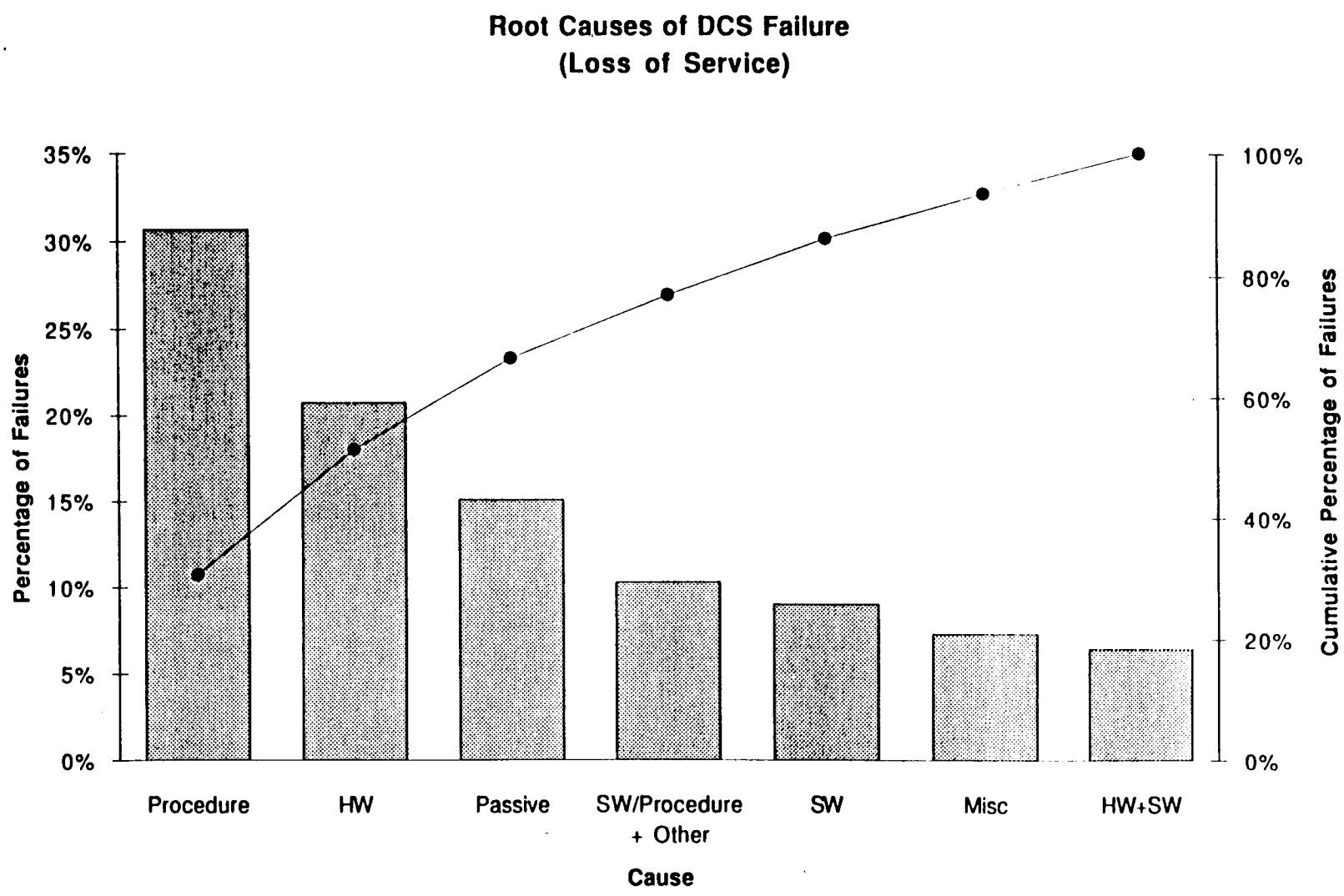

Root Causes of DCS Failure
(Loss of Service)
35%
30%
25%
20%
15%
10%
5%
0%
Percentage of Failures
100%
80%
60%
40%
20%
0%
Cumulative Percentage of Failures
Procedure
HW
Passive
SW/Procedure
+ Other
SW
Misc
HW+SW
Cause

Figure 15

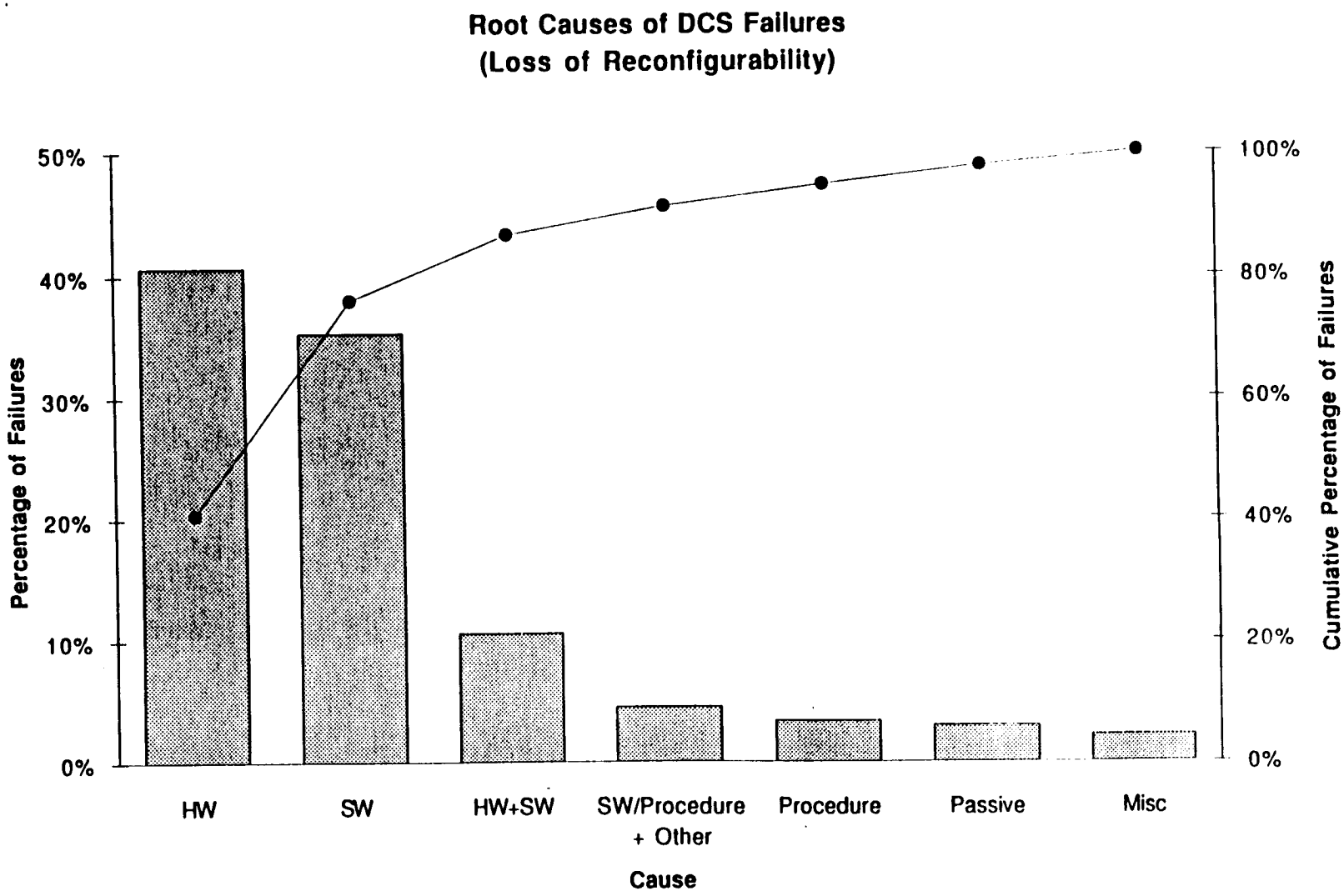

Root Causes of DCS Failures
(Loss of Reconfigurability)
50%
40%
30%
20%
10%
0%
Percentage of Failures
100%
80%
60%
40%
20%
0%
Cumulative Percentage of Failures
HW
SW
HW+SW
SW/Procedure + Other
Procedure
Passive
Misc
Cause

Figure 16

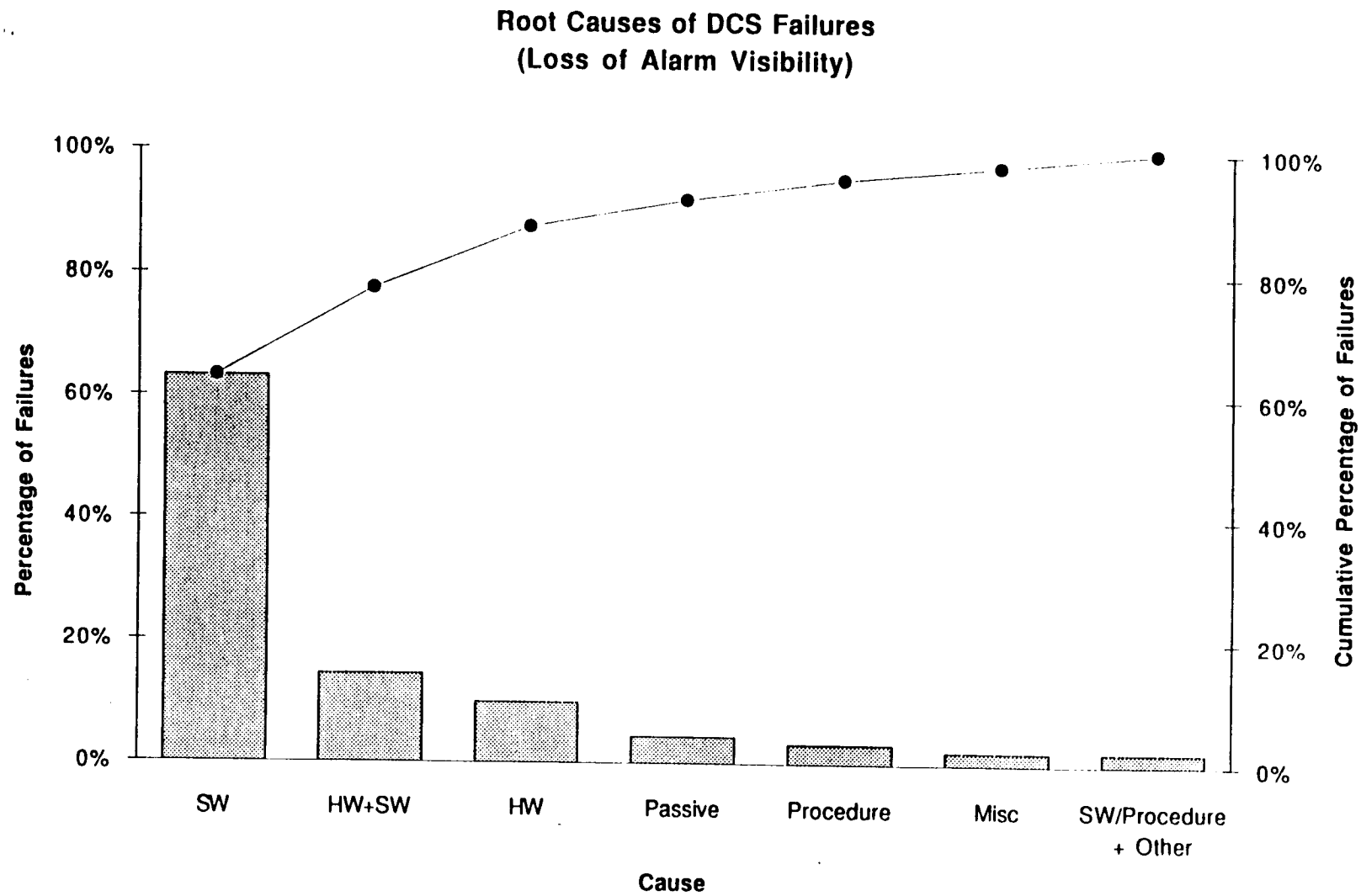

Root Causes of DCS Failures
(Loss of Alarm Visibility)
100%
80%
60%
40%
20%
0%
Percentage of Failures
Cumulative Percentage of Failures
SW
HW+SW
HW
Passive
Procedure
Misc
SW/Procedure
+ Other
Cause

Figure 17

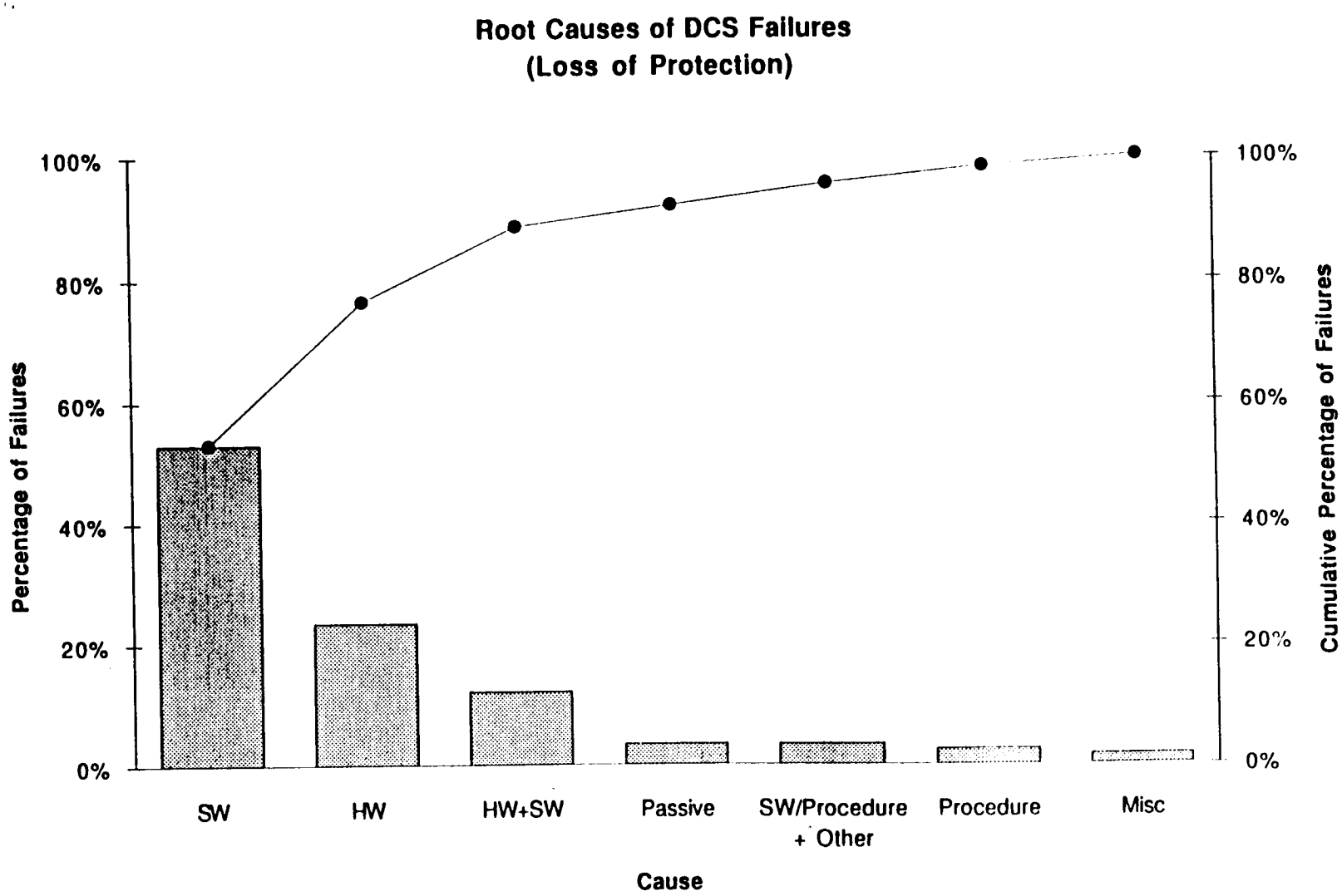

Root Causes of DCS Failures
(Loss of Protection)
100%
80%
60%
40%
20%
0%
Percentage of Failures
100%
80%
60%
40%
20%
0%
Cumulative Percentage of Failures
SW
HW
HW+SW
Passive
SW/Procedure + Other
Procedure
Misc
Cause

Figure 18

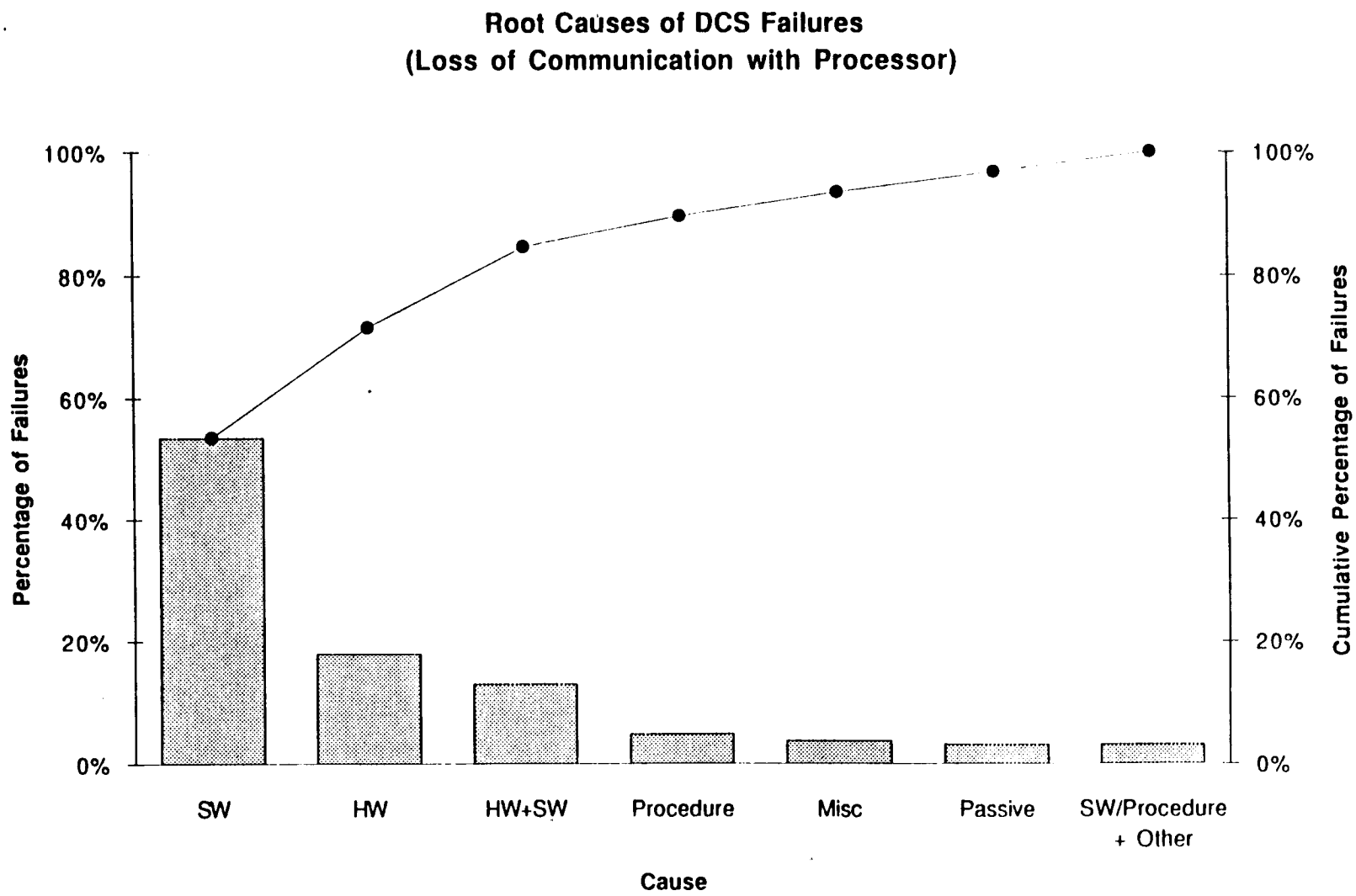

Root Causes of DCS Failures
(Loss of Communication with Processor)
100%
80%
60%
40%
20%
0%
Percentage of Failures
Cumulative Percentage of Failures
SW
HW
HW+SW
Procedure
Misc
Passive
SW/Procedure
+ Other
Cause

Figure 19

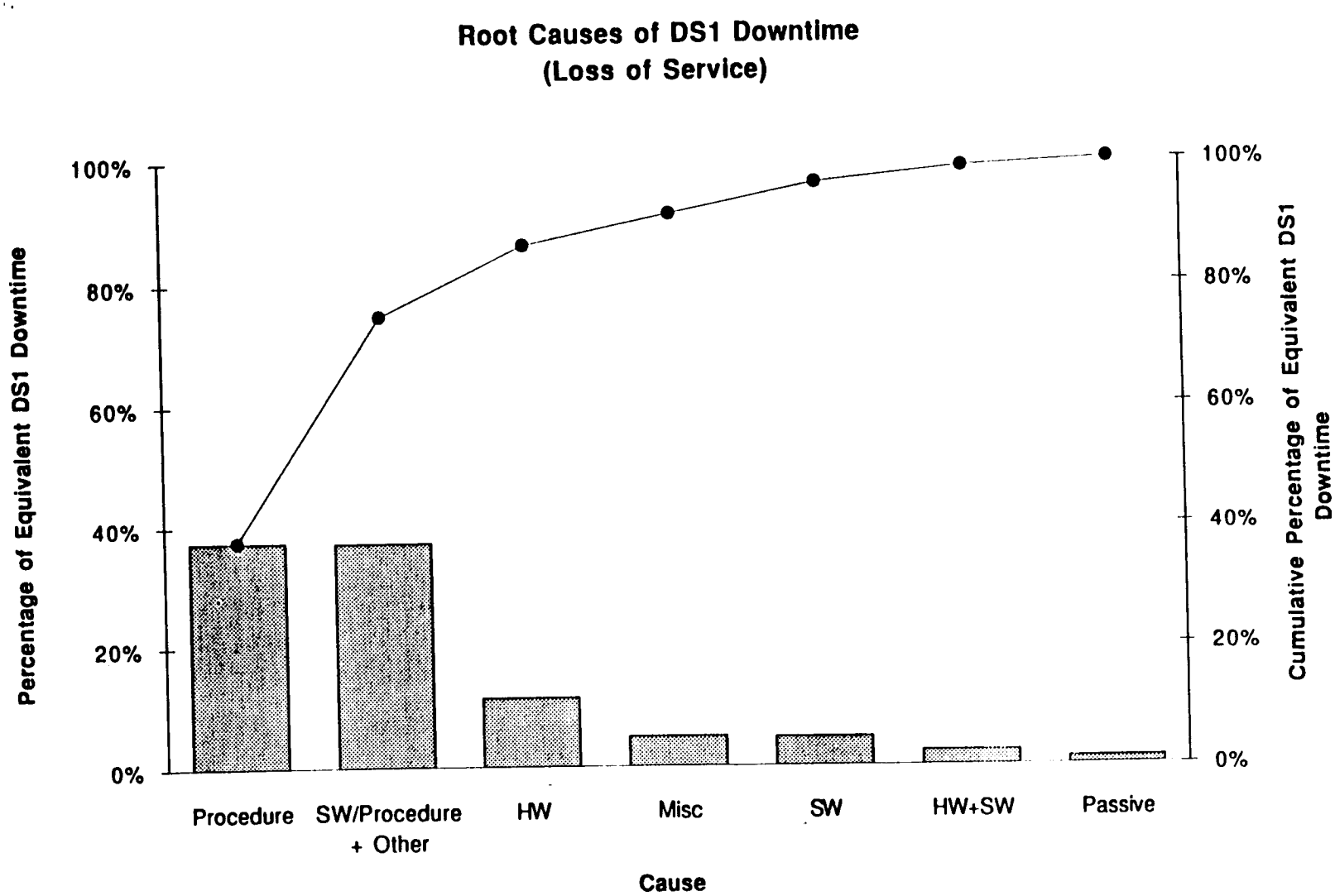

Root Causes of DS1 Downtime
(Loss of Service)
Percentage of Equivalent DS1 Downtime
100%
80%
60%
40%
20%
0%
Cumulative Percentage of Equivalent DS1 Downtime
100%
80%
60%
40%
20%
0%
Procedure
SW/Procedure + Other
HW
Misc
SW
HW+SW
Passive
Cause

Figure 20

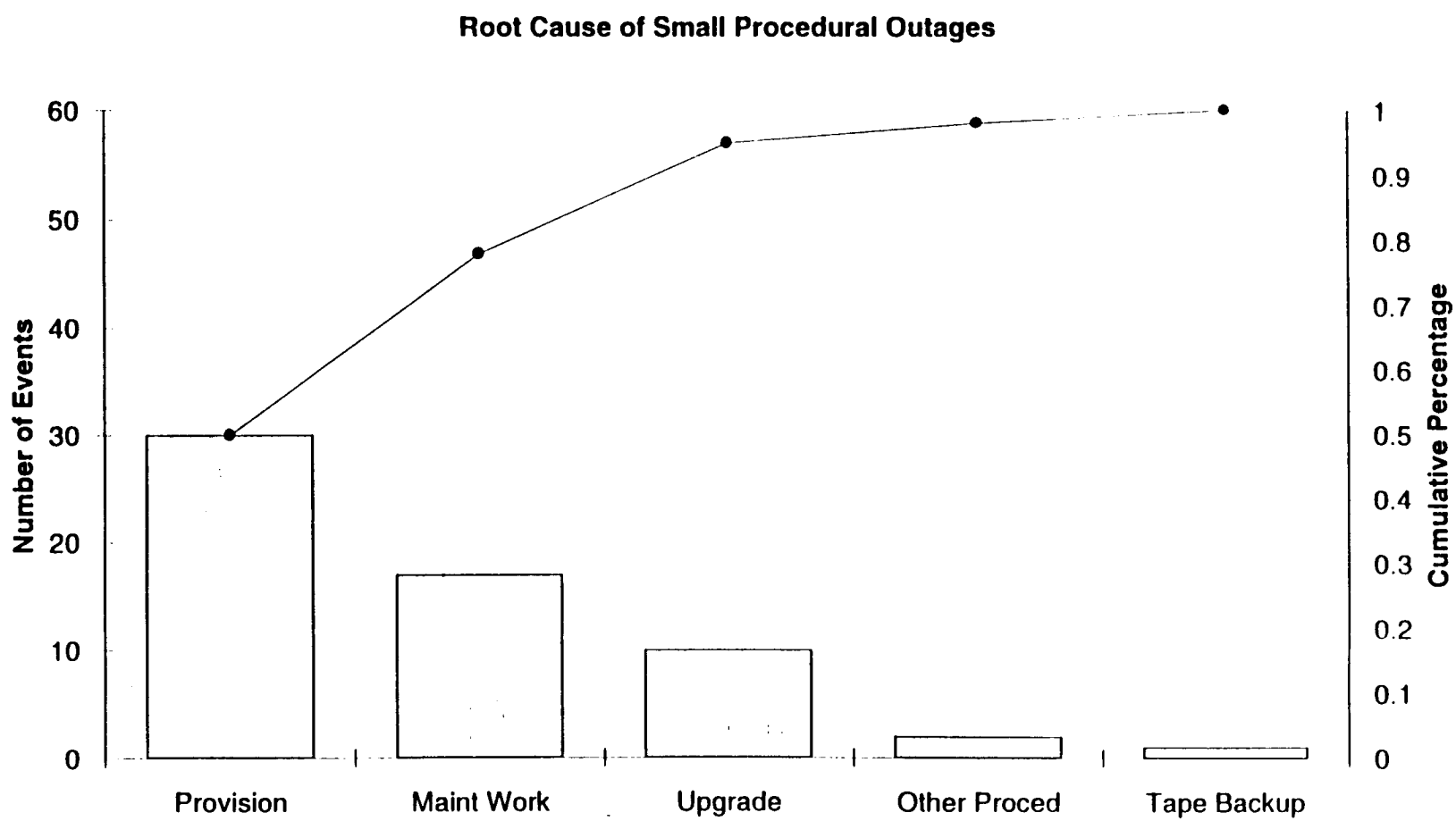

Root Cause of Small Procedural Outages
Number of Events
60
50
40
30
20
10
0
Cumulative Percentage
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
Provision
Maint Work
Upgrade
Other Proced
Tape Backup

Figure 21

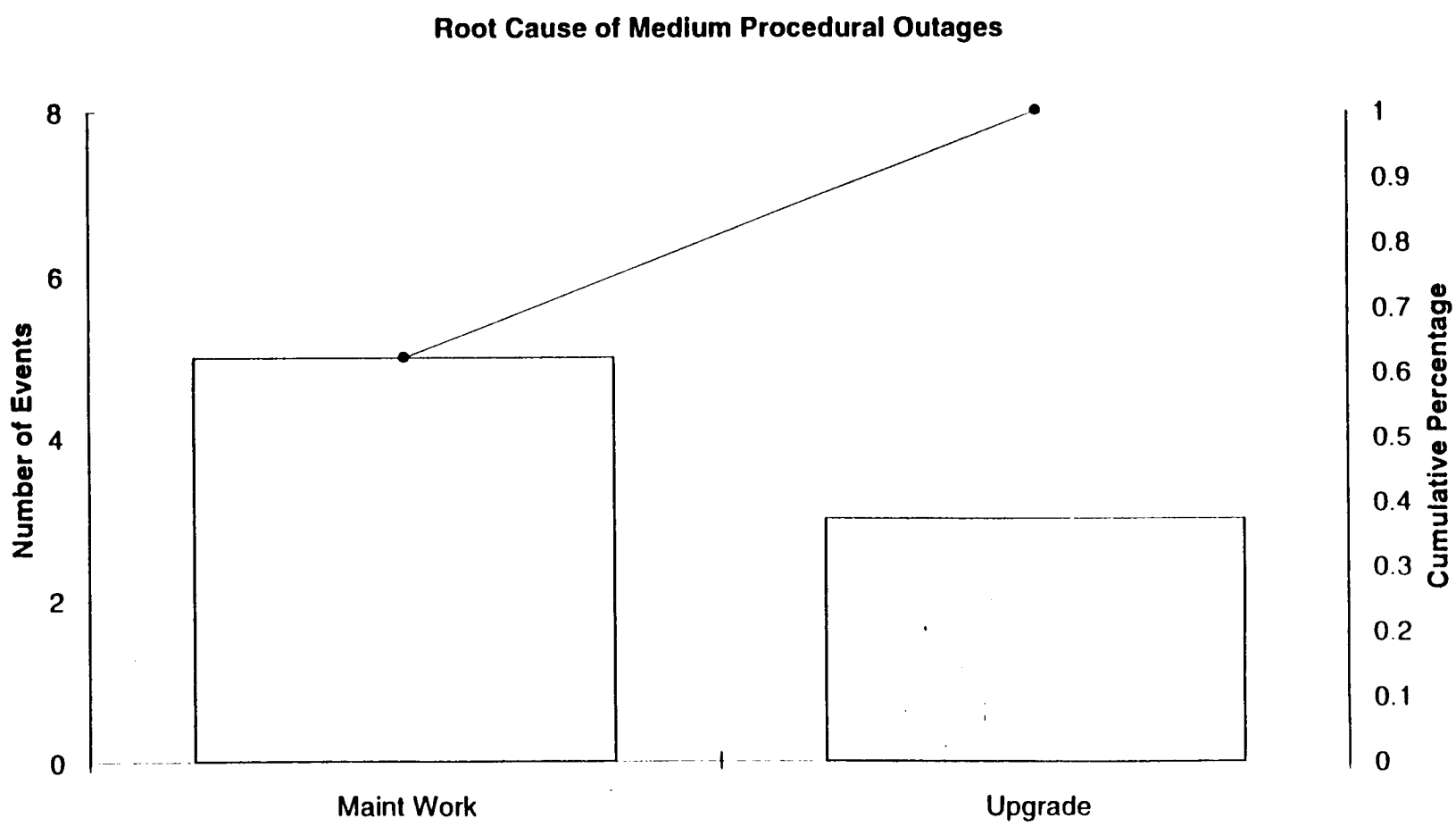

Root Cause of Medium Procedural Outages
Number of Events
8
6
4
2
0
Cumulative Percentage
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
Maint Work
Upgrade

Figure 22

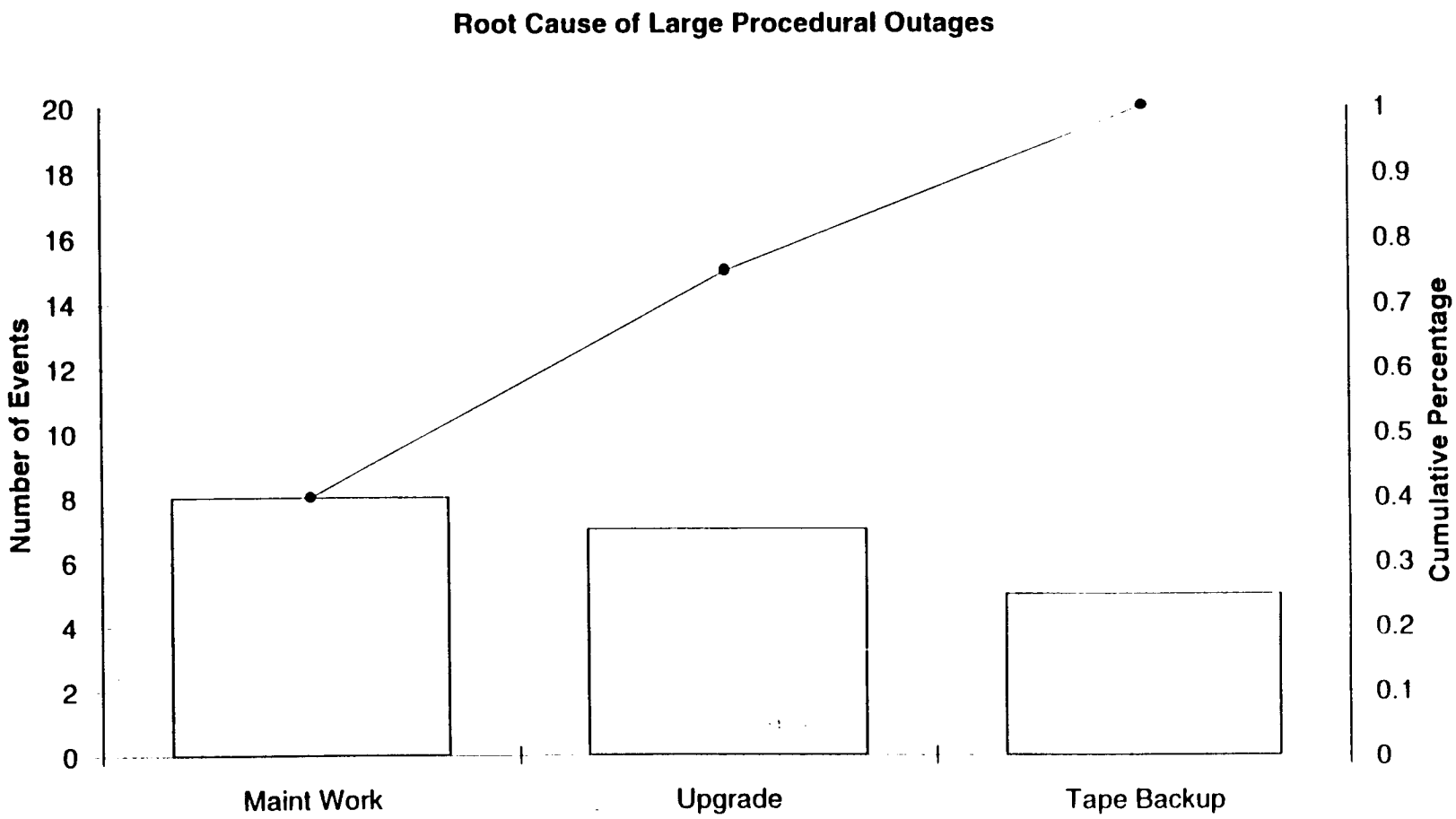

Root Cause of Large Procedural Outages
Number of Events
20
18
16
14
12
10
8
6
4
2
0
Cumulative Percentage
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
Maint Work
Upgrade
Tape Backup

Figure 23

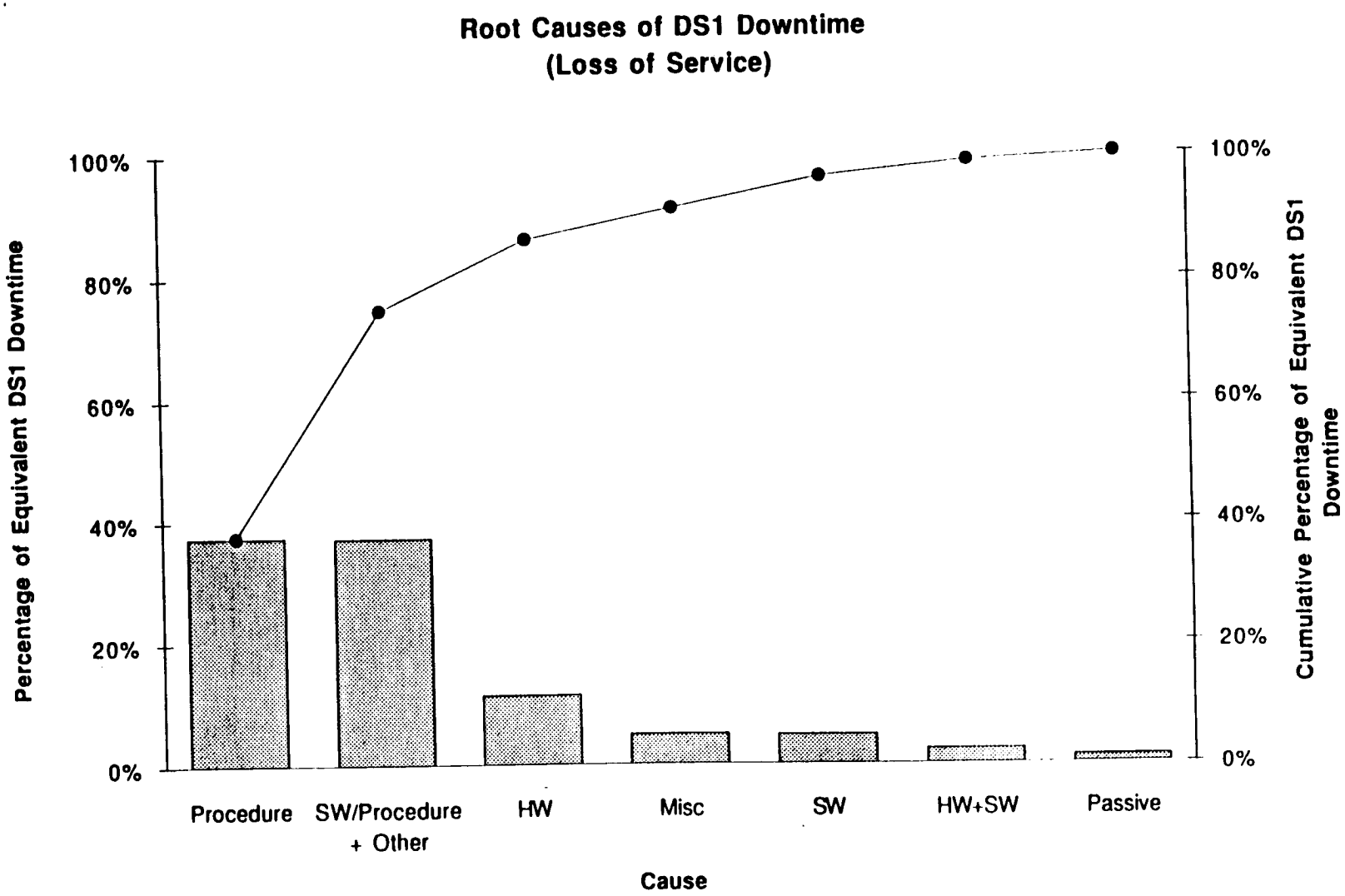

Root Causes of DS1 Downtime
(Loss of Service)
Percentage of Equivalent DS1 Downtime
100%
80%
60%
40%
20%
0%
Cumulative Percentage of Equivalent DS1 Downtime
100%
80%
60%
40%
20%
0%
Procedure
SW/Procedure + Other
HW
Misc
SW
HW+SW
Passive
Cause

Figure 24

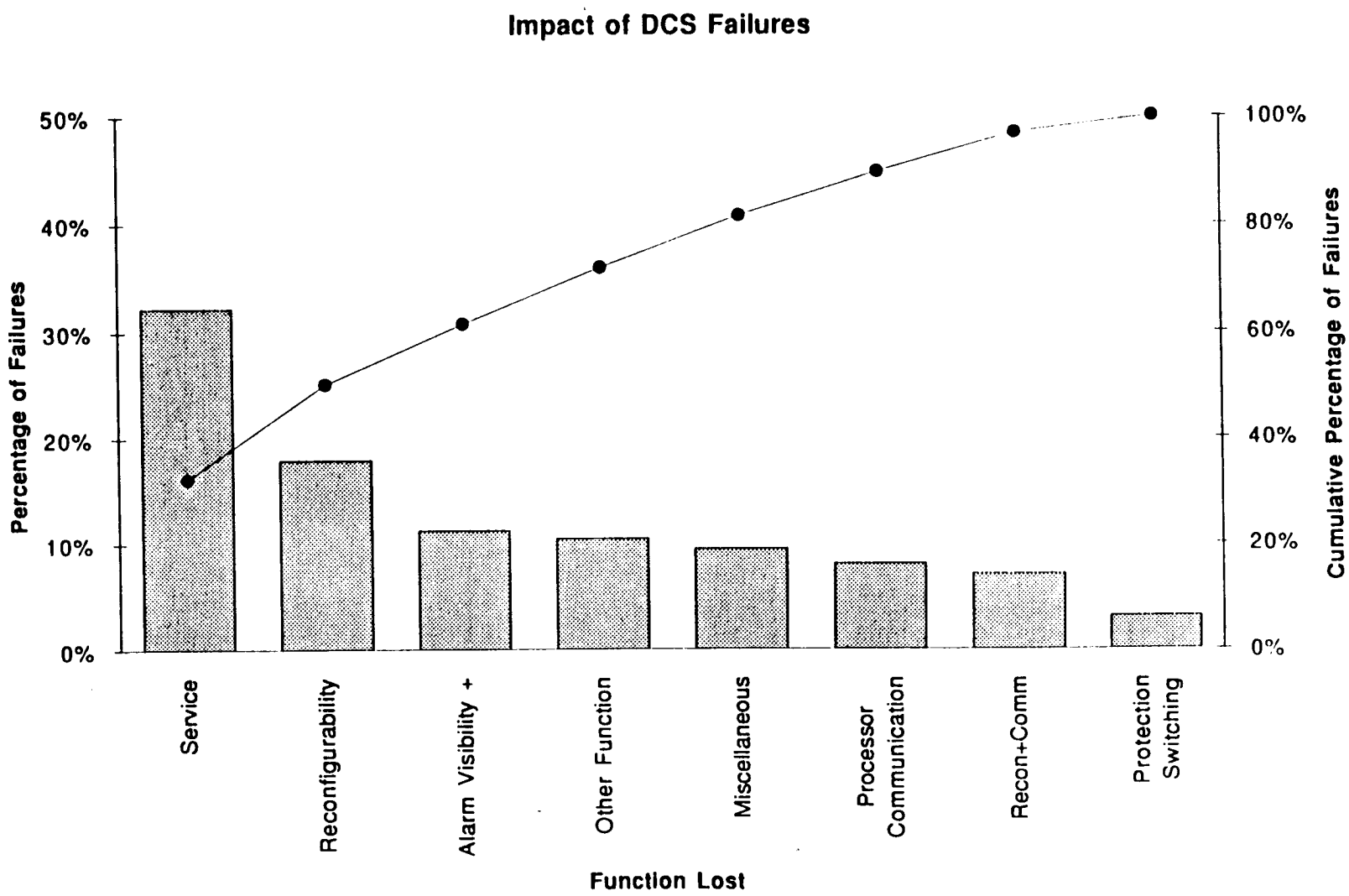

Impact of DCS Failures
Percentage of Failures
50%
40%
30%
20%
10%
0%
Cumulative Percentage of Failures
100%
80%
60%
40%
20%
0%
Service
Reconfigurability
Alarm Visibility +
Other Function
Miscellaneous
Processor Communication
Recon+Comm
Protection Switching
Function Lost

Figure 25

Current Situation - Software Process

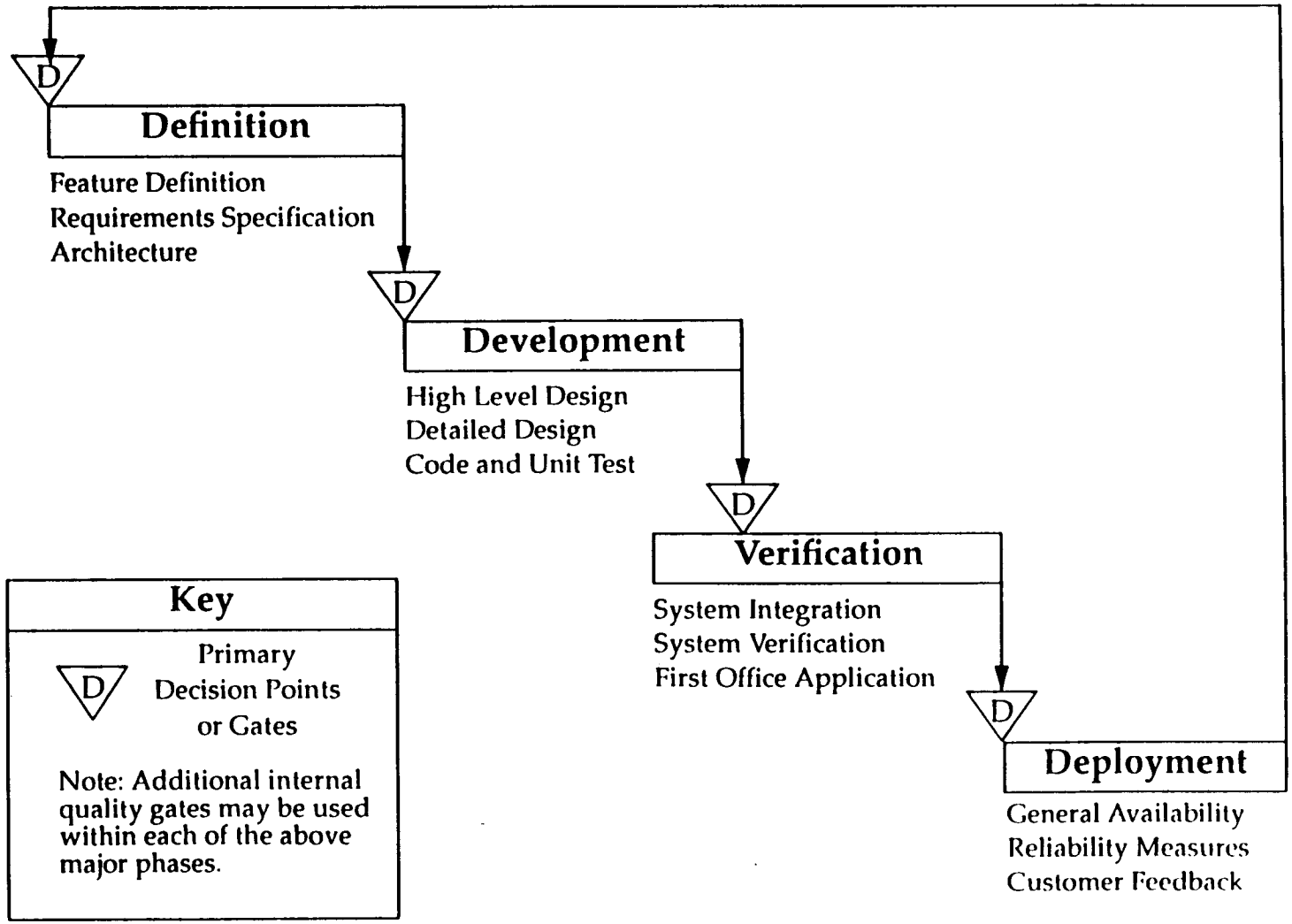


Figure 26

Fault Fix History (Prior to Release)

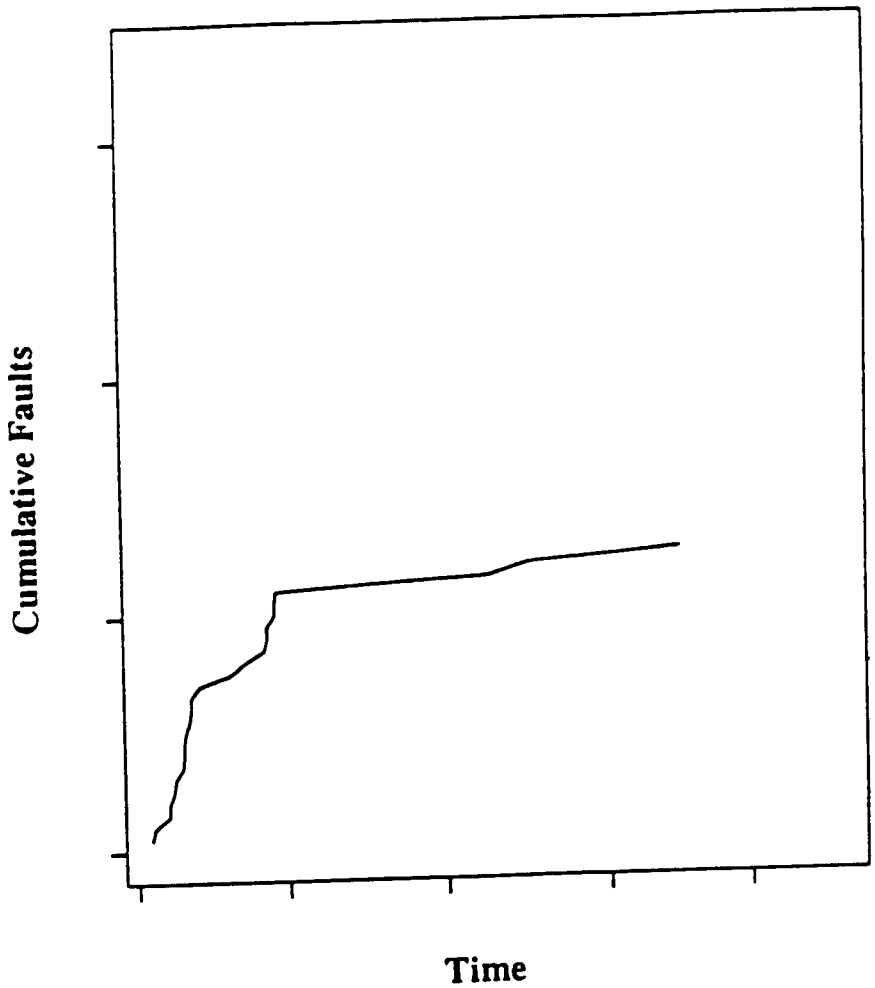


Figure 28

D

Fault Density Vs Time (Prior to Release)

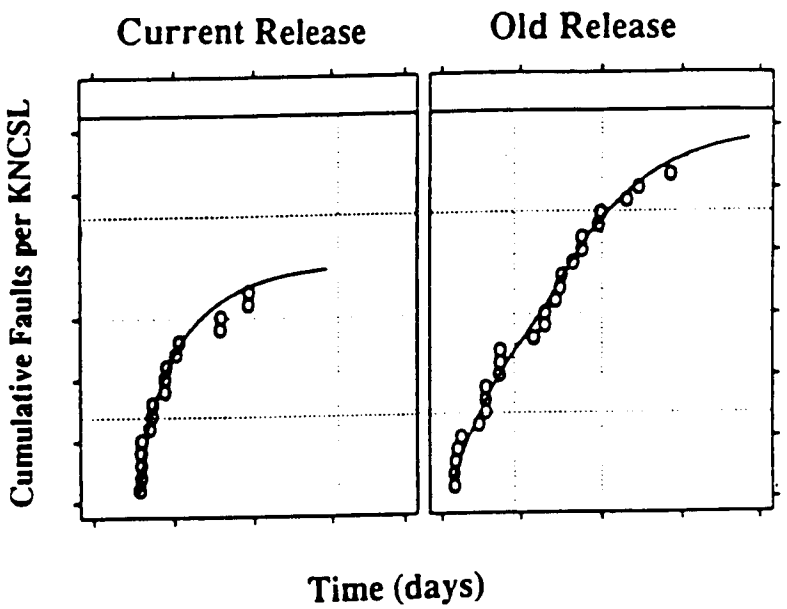


Figure 27

D

Field Performance

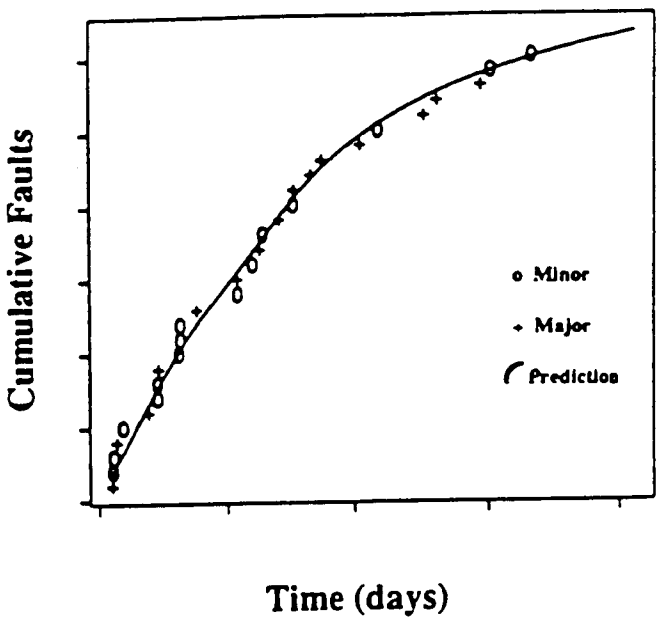


Figure 30

D