NRSC Bulletin No. 2008-1
Digital Cross-Connect Systems
July 2008

***Background**:*

During the March 2006 quarterly public meeting, the FCC requested, and the NRSC agreed to, a special study in response to analysis by the FCC that suggested that the number of outages due to Digital Cross-Connect Systems (DCS) that were being reported by providers were outside of control parameters.

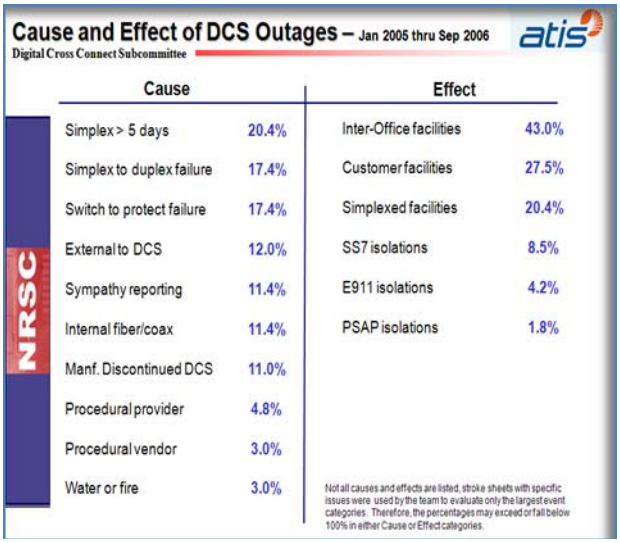
The participating team members included five service providers and three equipment vendors. The study gave particular attention to the potential impact on network reliability and the causes of DCS failures, and how this impact could be minimized using architectural and/or operational procedures. The team also reviewed existing Best Practices that apply to DCS network elements, DCS deployment, and DCS operational procedures.

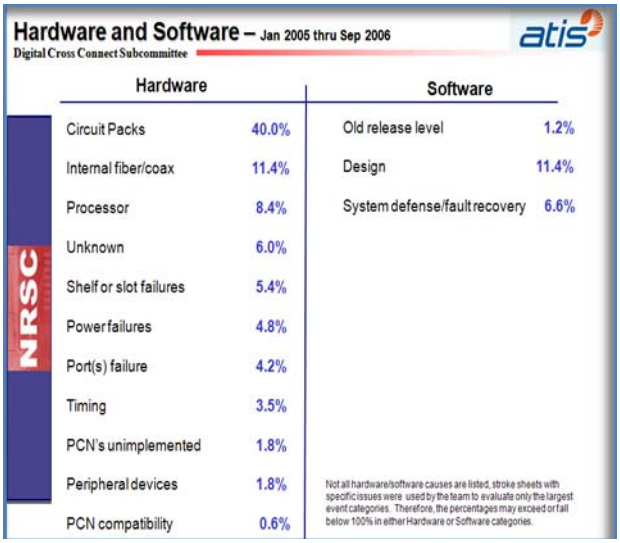
Findings and Guidance of the Special Study:

- Estimated that FCC notifications directly related to DCS caused events during study period of 21 months equated to ~ 4% or less of all FCC reportable events reported by participating team members.
- Approximately 1% of the events evaluated in the 21 months of the study period resulted in a total DCS system failure (.03% or less of total reports).
- 93% reduction in FCC reported events attributed to DCS in 2006 month over month as compared to 2005 data.
- Single circuit pack fall out is leading cause of FCC reported events and contributes highly to the overall quantity of reported events.
- Equipment vendors have insufficient data from providers to assist in analyzing packs that resulted in an FCC outage.
- A moderate percentage of overall total resulted in an SS7 isolation, PSAP isolation, and/or E911 isolation. These events are mostly preventable based on existing Best Practices and provider policies.
- 58% of DCS events occurred in urban areas with greater than 10K Telephone Numbers. This would be expected since DCS systems are more likely to be installed in an urban area.
- Failures of one DCS optical level card can impact up to 48 DS3's which is indicative of the engineered capacity of these systems. Potential that a single port failure may result in a reportable event.
- Unknown are the number of near misses or "saves" that occur each day where equipment operates as designed and no impact is seen. This prevents an accurate picture of overall operation of a DCS system. Only events resulting in network outages were studied.

In addition, the DCS team produced cause and effect and a breakdown of studied outages by hardware and software events.

Table 1 – NRSC DCS Team Findings





Lessons Learned

- Vendor default alarming should be reviewed and upgraded as appropriate by providers to maximize alarming opportunities.
- As outlined by existing Best Practices, periodic review of SS7 link and E911 diversity should be conducted and discrepancies corrected whenever possible and feasible. In most cases where multiple offices were isolated due to SS7 links and E911 facilities riding or being groomed through same DCS, diversity alternatives were available.
- An excellent partnership between provider and vendor with an "all hands on deck" whatever it takes approach to restoration makes the difference.
- Remote access for support personnel should not be restricted to options that require PSTN. Alternatives such as corporate networks, IP, X.25, etc. should be explored as part of restoration preplanning.
- As outlined by an existing Best Practice, awareness training on critical systems is crucial in assisting employees in making proper decisions at the onset of work activities and prioritization.

Recommendations:

<u>TL-9000 Standard Outage Template (SOTS)</u>

Providers are encouraged to evaluate the SOTS process, which is designed to report standard outage information to vendors following an event, and the level to which they feel they can support and implement this process. This data can then be used to improve Network Reliability and produce vendor to provider scorecards.

> **Best Practice 7-7-0583**, Network Operators, Service Providers and Equipment Suppliers should adopt an industry uniform method of reporting and tracking significant service outages (e.g., TL-9000 standard outage template).

Best Practice 7-7-0422, Failure Data Collection and Review: Network Operators should collect failure-related data and perform cause analysis, impact and criticality analysis and failure trending. Network Operators and Equipment Suppliers should work together to jointly perform this analysis, and meet periodically with the specific agenda of sharing the failure and outage information to develop corrective measures.

Critical Infrastructure Diversity

Best Practice 7-6-0761, Network Operators and Service Providers should conduct periodic verification of the office synchronization plan and the diversity of timing links, power feeds and alarms.

Best Practice 7-6-5250, Network Operators should consider intra-office diversity of all critical resources during restoration, and address losses of diversity following restoration.

Best Practice 7-7-0532, **Diversity Audit:** Network Operators should periodically audit the physical and logical diversity called for by network design and take appropriate measures as needed.

Best Practice 7-7-0549, Network Operators should develop an engineering design for critical network elements and inter-office facilities that addresses diversity, and utilize management systems to provision, track and maintain that inter-office and intra-office diversity.

Best Practice 7-7-0594, **Maintaining SS7 Link Diversity:** Network Operators and Service Providers should follow industry guidelines for validating SS7 link diversity. SS7 link diversification validation should be performed at a minimum of twice a year, and at least one of those validations should include a physical validation of equipment compared to the recorded documentation of diversity.

Best Practice 7-7-0731, Network Operators should provide physical diversity on critical inter-office routes when justified by a risk or value analysis.

Best Practice 7-7-1065, Network Operators and Service Providers should identify and manage critical network elements and architecture that are essential for network connectivity and subscriber services considering security, functional redundancy and geographical diversity.

Best Practice 7-7-5075, **Network Diversity:** Network Operators and Service Providers should ensure that networks built with redundancy are also built with geographic separation where feasible (e.g., avoid placing mated pairs in the same location and redundant logical facilities in the same physical path).

Best Practice 7-7-5076, Network Operators and Service Providers should ensure and periodically review intra-office diversity of critical resources including power, timing source and signaling leads (e.g., SS7).

Best Practice 7-7-5079, Network Operators and Service Providers should, where feasible, provide both physical and logical diversity of critical facilities links (e.g., nodal, network element). Particular attention should be paid to telecom hotels and other concentration points.

Awareness

As outlined by the following existing Best Practice, awareness training on critical systems is crucial in assisting employees in making proper decisions at the onset of work activities and prioritization.

> **Best Practice 7-7-0588**, Network Operators, Service Providers and Equipment Suppliers should provide awareness training that stresses the services impact of network failure, the risks of various levels of threatening conditions and the roles components play in the overall architecture. Training should be provided for personnel involved in the direct operation, maintenance, provisioning, security and support of network elements.

Standard Operating Environment (SOE)

NRSC is encouraged to continue development of initiatives to provide a SOE for network outage reporting.

- ATIS-0100012 - Standard on Outage Classification

SOE will facilitate the elimination of guesswork and standardize outage analysis on static NORS data fields for future analysis by the NRSC.

SOE is important to synch up providers, vendors, and FCC outage information for better flow-through for TL-9000 SOTS, providers, and NORS systems.

Network Outage Reporting System (NORS)

NRSC should partner with the FCC on continued evaluation of incorporating standard outage classifications and root causes into the NORS system.

Providers and Vendors should adopt where feasible the NRSC Standard on Outage Classification and Examples of Standardized Root Causes documents in their internal tracking systems.

System Sizing Considerations

Providers are encouraged to develop internal processes to establish thresholds, review, and identify critical system sizing issues. It is recommended that these guidelines produce some level of actionable response when critical systems, such as DCS, reach the pre-defined sizing threshold.

Examples of actionable response for these critical systems could trigger;

- Higher level of awareness and focus of system sizing considerations
- More frequent Best Practice evaluations (Critical Infrastructure Diversity)
- Engineering review of system sizing considerations

For more information:

If you have any questions or would like additional information concerning this Bulletin, please contact:

NRSC Committee Administrator

Alliance for Telecommunications Industry Solutions (ATIS)

1200 G Street, N.W., Suite 500

Washington, D.C. 20005

202-628-6380

About ATIS

ATIS is committed to providing leadership for, and the rapid development and promotion of, worldwide technical and operations standards for information, entertainment and communications technologies using a pragmatic, flexible and open approach. Over 1,100 participants from over 300 communications companies are active in ATIS' 22 industry committees and its Incubator Solutions Program.

About NRSC

The Network Reliability Steering Committee (NRSC) provides guidelines and tools to the communications industry, with the ultimate goals of maintaining and improving the high level of network reliability in the United States. Through its team of industry network reliability experts, the NRSC establishes industry guidelines and processes to be used in the collection of network reliability data, documents methods for industry use in analyzing outage data, works with the FCC to identify and analyze emerging outage trends, and makes recommendations aimed at improving the reliability of communications networks.

Published by
Alliance for Telecommunications Industry Solutions

1200 G Street, NW, Suite 500

Washington, DC 20005