

# Defeating Telecommunication System Fault-Tolerant Designs<sup>1</sup>

Andrew P. Snow

*Georgia State University*

*Department of Computer Information Systems*

*asnow@gsu.edu*

M. Whiting Thayer

*Federal Communications Commission*

*Accounting Safeguards Division*

*wthayer@fcc.gov*

**Abstract** -- Telecommunications carriers suffer large-scale outages that impact hundreds of thousands of subscribers by the improper deployment or operation of otherwise fault-tolerant designs. This paper gives examples of such outages in telecommunications signaling, transmission, and power systems. In spite of seven years industry tracking of large-scale outages at the national level, the survivability of the public telephone network has not improved, as the frequency of outages is not decreasing. This surprising phenomenon is all the more remarkable in that well-known outage scenarios continue which defeat otherwise fault tolerant systems. Averting such survivability deficits requires less focus on fault-tolerant designs and more focus on organizations and people. It remains to be seen if local access competition will remedy these survivability problems, as voice, video, and data service offerings are bundled by carriers.

## 1. Introduction

A key technique in providing survivable systems is through fault tolerance. Designers and equipment vendors spend considerable effort developing ingenious techniques that allow systems to cope with hardware and software failure, without appreciably affecting users. In telecommunications, fault-tolerant techniques are applied in transmission, signaling, switching, and power systems. Whenever a network is unable to cope with system failure, an outage occurs which affects users. By investigating individual non-survivable episodes we hope to learn how to improve survivability as we move from the realm of 'what if' to that of 'what happened' [1].

In response to a number of celebrated telecommunications outages in the early 1990's, the Federal Communications Commission (FCC) required carriers to report outages that impacted large numbers of users, emergency communications (E911), airports, and other special facilities [2]. The preponderance of the reported incidents are those that surpass a defined reporting threshold – those outages affecting at least 30,000 subscribers for at least 30 minutes. Remarkably, since mid-1992, there have been about 16 such incidents per month in the United States. This paper discusses some of these outages, which are attributable to the improper deployment, operation, or maintenance of systems intended to enhance survivability. In particular, examples of transmission, signaling and power system failures occurring in carrier networks are presented which defeat fault-tolerant designs.

## 2. Signaling

In the public switched telephone network, Signaling System Number (SS7) is an out of band packet switched network which allows local and tandem switches to cooperate in providing end-to-end connections, and many enhanced services. The SS7 network is completely separate from the voice switching fabrics, but it uses the same transmission systems (copper and fiber cables and related electronics) that are used to carry voice traffic. Without connectivity to the SS7 network, local telecommunications switches cannot process requests for new calls to or from any other building for users attached to that switch. For this reason ANSI Committee T1 standards require each local switch to have redundant access to the SS7 network. In spite of this well-known standard, a common outage scenario involving SS7 is shown in Figure 1. While the figure only shows two switches, network outages reported to the FCC have shown as many as 88 switches isolated from the SS7 network because of a single network failure.

The proper deployment of redundant access ('A' links) to different packet switch nodes (STPs, or Signal Transfer Points) is depicted where the 'A' links are not only connected via separate circuits, but also that those circuits use separate fibers, cables, conduit, paths, electronic components, power supplies, and timing sources. An improper deployment is also shown where the 'A' links are routed in the same path and a fiber cable dig-up severs both 'A' links, isolating the local switches from the signaling network. Unfortunately, this is a common occurrence.

Other SS7 outages have occurred where the 'A' links are not only on the same fiber, but also multiplexed onto the same DS3 circuit. Also, SS7 'A' links are to use separate transmission equipment attached to separate power circuits. There have been a number of instances where a DC fuse blows and takes down both 'A' links because the separated link equipment shared the same power circuit.

Carriers benefit greatly from the implementation of SS7, as it allows revenue-enhancing services such as caller-ID and 800-database access. It is interesting to note that sometimes carriers do not implement the SS7 reliability features according to the standard.

## 3. Transmission

Offering a protection channel usually provides transmission diversity necessary to make a high capacity transmission system survivable. Two common techniques are through digital cross-connect switches (DCS) and fault-

---

<sup>1</sup> The views expressed in this paper are the authors' own and do not necessarily represent the views of their respective organizations.

tolerant SONET rings. Each technique employs failure sensing and a switching capability to an alternate path, in a matter of milliseconds. As DCS rapidly transfers circuits to alternate-working paths in the event of transmission failure, its effectiveness requires path diversity. However, Carriers do not always deem transmission diversity as cost effective, and sometimes chose not to provide it, regardless of the standard. In other instances, the carrier thought there was physical diversity where there was not. This administrative problem was identified by the industry over seven years ago, but it still is contributing to network outages.

These problems also do not escape fault-tolerant rings. Here, the intended fault tolerance is achieved through bi-directional rings, which have primary channels in one-direction and protection channels in another, all in the same cable. If the cable is severed, or a node fails, the ring operates in a simplex mode over the protection channel. A number of reported outages have occurred after a ring operating in a simplex mode sustains another failure at a later date, defeating the intended redundancy. Another reported failure mode is where the ring is installed in a “collapsed” or “folded” mode where both sides of the bi-directional ring are in the same path. Here a fiber cut bifurcates the ring, rendering it inoperable. The collapsed mode of installation has been deployed where unique paths for all sections of the ring are not available, or where the carrier thought the paths were unique. The two major modes of improper operation and deployment of SONET rings are shown in Figure 2.

#### 4. Power Systems

Power systems are typically triply redundant in that there are three sources of power. All communications equipment runs on DC voltage generated by AC fed redundant rectifiers. AC power is obtained from the Power Company and many large or critical communications facilities have backup generators in the event of commercial AC power failure. If both sources of AC power are lost, the last line of defense is battery backup, typically engineered to power equipment for 8-hours. If commercial power is lost and the generators are improperly maintained, an outage will occur if AC power is not restored within 8-hours. However, if both sources of AC power are lost and the batteries are not properly maintained, an outage is assured. Likewise, if both sources of AC power are lost, it is critical that carrier maintenance personnel be notified, as many communications facilities are not locally staffed. Reported scenarios include that shown in Figure 3, where lightning not only disrupted commercial AC, but also damaged the generator. The outage was caused by the improper operation of the alarm system, as 8-hours later the batteries were depleted and the remote network operations personnel were not aware of the problem. In another somewhat similar incident, the alarms worked, but the wrong street address was supplied to the Power Company.

#### 5. Discussion

These outages present recurring examples of outages caused by the carrier industry not following best practices and industry standards developed by that same industry, and promulgated by Federal advisory committees, carrier associations, and consultants such as Telcordia. The reasons seem to be in two classes – (1) situations where the carrier made a conscious decision not to provide redundancy and (2) situations where the carrier thought there was redundancy where there was none. The former is a carrier efficiency tradeoff of interest in business, political and regulatory realms. This paper has dealt mostly with examples of the latter, where otherwise fault-tolerant designs have been inadvertently defeated. However, these two classes of outage events, the fact that the frequency of outage events has been constant for over seven years while the trend for procedural causes is increasing [3], suggests that working harder on fault-tolerant design techniques is unlikely to be a singularly successful approach.

Carrier industry claims in annual reports over the last seven years in response to outage constancy have been fascinating at times. In trying to rationalize this phenomenon, several explanations have been offered:

1. Network reliability remains stable in the face of growth in lines and traffic
2. Outages would decrease if laws were enacted to decrease cable cut incidents
3. If the threshold for outage analysis is normalized (artificially increased) to account for network growth, the network is improving

With respect to the first claim, outages due to traffic were rare before tracking of outages, and remain a non-factor – there is no correlation between traffic load and outages. In addition, to accommodate growth, there have been over a 2-fold increase in fiber optic deployment over the last seven years. If interoffice fiber channels are properly protected, infrastructure growth should not be a factor in the frequency of outages due to fiber.

With respect to the second claim, because of industry lobbying, “one-call” laws (call before you dig) were implemented or strengthened in many states and at the federal level. In spite of these efforts, the outages initiated by fiber cuts continue to increase. Carrier industry reports often confuse the failure event triggering an outage with the cause of the outage. For instance, if a fiber cable is cut and an outage results, is the reason “cable cut” or should in fact the reason be “unprotected transmission facility”? The industry analyses the data and often reports the “cause” as the former rather than the latter. This creates the illusion of others (e.g. construction industry, other utilities) being the cause of the outage. Of course decreasing cable cuts is important, but from a survivability perspective the proper question is “given a cut, how can the network be robust enough to cope with the cut?”

The last claim is a suggestion that since more traffic and lines are in the system, the threshold should be raised for

analysis (but not for reporting) [4]. In their famous treatise on time series of events, Cox and Lewis studied a eighty-year series of coal mining accidents in which at least 20 coal miners died [5]. Just as the significance of 20 deaths is not dependent upon the amount of coal production, how much traffic a network carries, or how many subscribers are connected does not diminish the significance of 30,000 or more subscribers affected for 30 minutes or longer.

Organizational concepts and research which classify telecommunications as risky systems (where “one can expect...processes [that are] unstable [with] unclear goals, misunderstanding and mis-learning, happenstance, and confusion as to means.” [6]) may also be in order as telecommunications infrastructure and services rapidly evolve. Although not synonymous with safety, telecommunications survivability has safety implications, as well as economic and societal implications. In *Normal Accidents* [6], Perrow highlights the difference between reliability theory and normal accident theory: reliability theorists believe that if they try harder things will improve, while normal accident theorists believe that accidents are inevitable because of coupling and complexity.

In his 1999 *Afterword*, Perrow states that reliability theory is only half the job, and that understanding the power in and of organizations is key:

“[we] rarely question how important efficiency goals should be in risky systems, and who has the power to impose those goals, and their contribution to production pressures.....We should address the improvement of safety, but in addition, address the role of production pressures in increasingly privatized and deregulated systems that can evade scrutiny and accountability.” [6]

In the late 1980’s and early 1990’s, there was a move away from rate-of-return regulation and a move towards price cap regulation. If there is no competition in a price cap environment, carriers might be tempted to scrimp on survivability investments (diversity, information systems to map physical paths to logical paths, training, too much concentration to realize economies of scale, etc.) to maximize profit. Perhaps it is time to look at survivability of information systems and networks not only from classical reliability, availability, and survivability perspectives, but also from organizational, regulatory, and competitive perspectives. Perrow goes on to summarize Lee Clarke’s research concerning “fantasy documents”, wherein organizations produce documents “written in a technical language that favors organizational needs and visions of efficiency, converting an ethical problem into a technical one. The moral risks of risky systems are trumped by the bureaucratic standards demanded of fantasy documents and the administrative rationality they signal” [6]. Perrow’s portrayal of Clarke’s research [7] is scathing in identifying the motivation for fantasy documents:

“...organizations create fantasy documents as they try to assuage those who would challenge their constructions of

reality: citizen groups, social movements, and the occasional recalcitrant regulatory agency.”

The Network Reliability Steering Committee<sup>2</sup> annual reports and ANSI T1A1.2<sup>2</sup> technical reports contain rhetoric which are akin to Clarke’s description of fantasy documents, without addressing the core issue – why is outage frequency *not* decreasing?

## 6. Conclusions

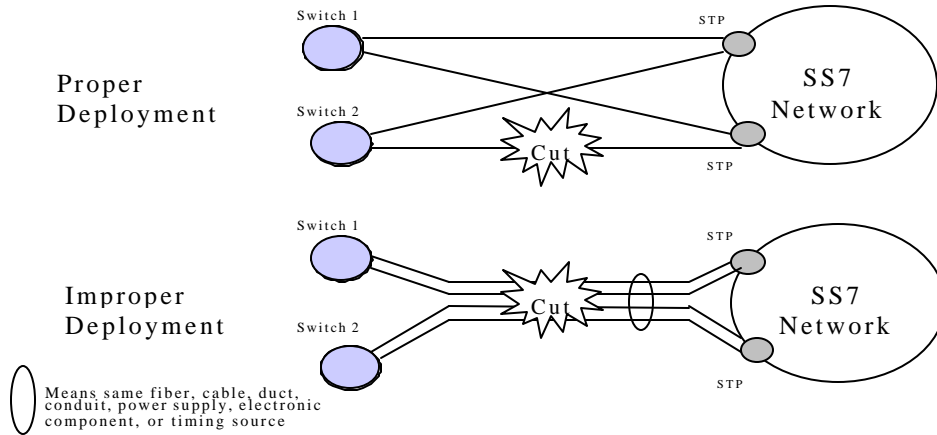
US national policy makers have enacted what they hope to be a remedy for higher quality telecommunication service, more services, and cheaper rates – the Telecom Act of 1996. The intent is to introduce competition. This view argues that competition, and not more regulation, is the answer to the survivability problems presented in this paper. True, some critics believe that so far the only thing resulting from the Act has been industry consolidations through mergers. However, competition is starting to take hold – cable TV companies are offering voice, video and data; likewise traditional telephone companies are offering high speed data (XDSL) and even video. Can you imagine an outage that not only takes down voice (including cellular), but also video broadcast and Internet access? With true competition in local markets, economists believe such attributes as reliability and survivability will improve if customers demand it. With little competition in local transport markets over the last seven years, carriers seem to have acted as if the constant rate of large-scale outages is acceptable. Well-known best practices that take advantage of fault-tolerant designs have often not been implemented. Competition hopefully will become an important factor in carrier “cost effectiveness” studies of diversity, and possibly influence staffing levels and training. Time will tell if accepting outage rates without addressing management and operational improvements is a viable business strategy.

## 7. References

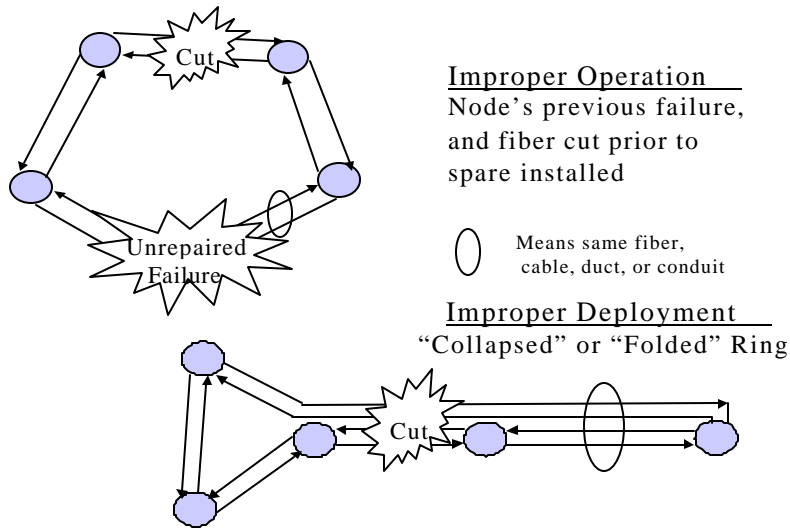
- [1] Snow, Andrew P., “A Survivability Metric for Telecommunications: Insights and Shortcomings”, *IEEE Computer Society proceedings, Information Survivability Workshop – ISW’98* (October 1998) 135-138.
- [2] Code of Federal Regulations; Title 47, Volume 3, Parts 40 to 69, (*47 CFR 63.100*), Rev. October 1, 1998.
- [3] *Network Reliability Steering Committee Annual Report 1999 (For the Year Ending 1999, June 30)*, Alliance for Telecommunications Industry Solutions, Washington, DC, 2000.
- [4] ANSI Technical Report No. 42, *Enhanced Analysis of FCC Reportable Service Outage Data*, August 1995.
- [5] Cox, D. and Lewis, P., *The Statistical Analysis of Series of Events*, John Wiley and Sons, New York, 1966.
- [6] Perrow, Charles, *Normal Accidents: Living with High-Risk Technologies*, Princeton University Press, Princeton, NJ, 1999.
- [7] Clarke, Lee, *Mission Impossible: Using Fantasy Documents to Tame Disaster*. Chicago: University of Chicago Press, 1999.

---

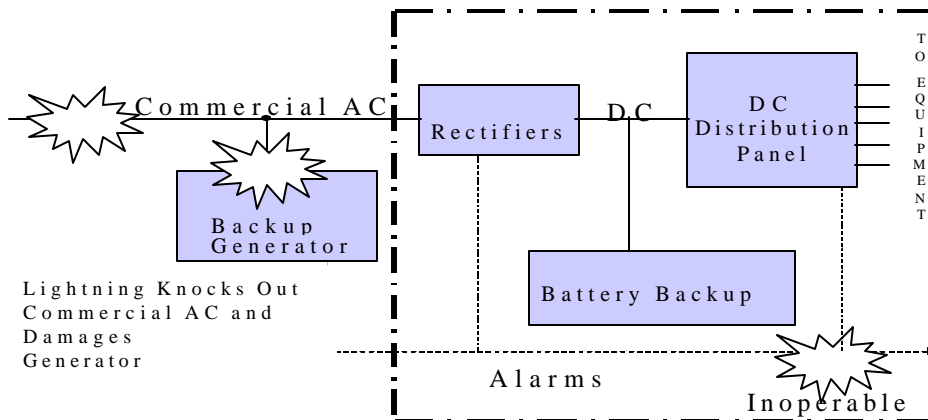
<sup>2</sup> Sponsored by the carrier industry association, the Alliance for Telecommunications Industry Solutions.



**Figure 1. Fault-Tolerant SS7 'A' Links: Proper and Improper Deployment**



**Figure 2. Fault-Tolerant SONET Ring: Unreliable Deployment or Operation**



**Figure 3. Fault-Tolerant Power: Unreliable Deployment or Operation**