THE Locomotive
THE full STORY

What's the Real Threat To High-Tech Telecom? Heat and Power Problems are the Greatest Risks

By Robert Weir, P.E.
What is a telecommunications network? The short answer is that it is digital electronics.

Today's telephone switches are nothing more than expensive computers with sophisticated software that direct voice and data and provide features such as call waiting, caller ID and voice mail, and all the other features we have come to expect.

Like any other computer or sensitive electronic equipment, telecommunications electronics are susceptible to damage from heat, electrical disturbances, moisture, and direct physical damage. When properly protected from these exposures, the electronics that make up the backbone of the telecommunications industry are highly reliable. In fact, the record indicates that it is the supporting infrastructure that represents the most likely cause of failure affecting telecommunications.

Telecommunications Infrastructure

It is useful to examine the infrastructure of telecommunications and to note the ramifications of equipment dependencies. Figure 1 shows that each successive layer of the pyramid is dependent upon all of the layers below it.

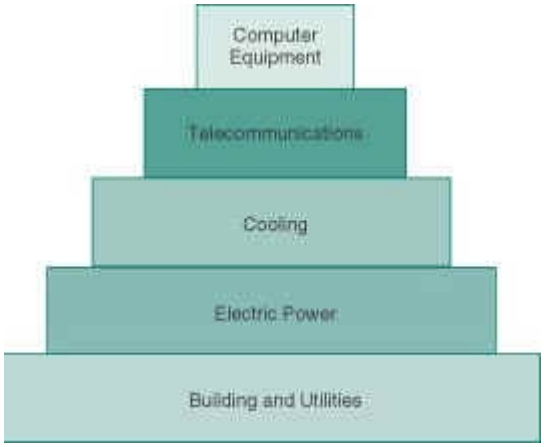

Figure 1

Building and Services

Both equipment and infrastructure elements are usually installed in substantial buildings having extensive physical security and fire resistant construction. Such a structure forms the base of the infrastructure pyramid in the figure. We often tend to take buildings for granted, but they deserve some special respect in this case because of the protection and support they provide.

Not only are telecommunications vital to public safety services, they are important national assets, and can be the target of terrorists or anyone bent upon inflicting damage. A robust, solidly built structure with well-designed security and alarms is an important layer of protection against many kinds of intruders.

Electric Power

Ascending one layer in Figure 1, we come to the next vital layer of infrastructure — the electric power supply. Power supply for telecommunications enjoys the benefit of a long tradition of reliability built into the public telephone network.

The electronic equipment operates on direct current (DC) provided by batteries that can support the electronic equipment for several hours in the event of power failure. Being a constant voltage power source, batteries also isolate the electronics from electrical noise prevalent with alternating current (AC) power. Rectifiers that convert the incoming AC power from the local power company into DC power recharge the batteries. DC power provides a simple, inherently reliable, and clean source of electricity.

During a local power outage, emergency generators can be employed to supply AC power to the battery charging systems during an extended power failure. A major benefit of this arrangement is that power from the AC generator is converted to DC before being used. This completely avoids voltage or frequency

fluctuation — not a trivial matter where sensitive telecommunication equipment is concerned.

Cooling Must Be Adequate

Heat is a natural byproduct of electronics. Most of the electric power consumed by electronics is ultimately released as heat. An installation that consumes 10 kilowatts of electric energy will release the equivalent of those kilowatts as heat energy, or about 34,000 BTU per hour. When installed in a building, it is essential that provisions be made to remove this heat so that ambient temperature will remain within acceptable limits. In tropical climates, more capacity will be needed.

You may ask why heat is harmful. The answer is that it is the natural enemy of electronics. This is so because of the nature of electronic devices. These are complex assemblies of semiconducting, conducting, and non-conducting materials. These materials will perform their intended functions within these assemblies only so long as they do not suffer physical or chemical degradation.

Heat is an enemy of these devices because of its relationship to the rate at which materials degrade. The rule of thumb is that for every 10 degrees Celsius of temperature rise, **the speed of all chemical reactions doubles**. That rule applies to the chemical reactions involved in the degradation of electronics as well as to every other substance. As if that were not enough, many components include thermoplastics that will melt once a certain temperature is reached.

It is essential that operating electronics be maintained at an ambient temperature consistent with reliable operation and satisfactory equipment life. As long as power is supplied to the electronics, sufficient cooling must also be available.

As a final note on the relative importance of cooling, electronics can usually sustain loss of power without physical damage. Of course there will be delays associated with reinitiating software when power is restored, but for the most part, hardware will be undamaged. Loss of cooling, on the other hand, if permitted to raise temperatures to critical levels, will result in widespread electronic failures.

Telecommunications and Computer Equipment

Much of the equipment used in the telecommunications industry is comprised of specialized digital computers. Successful operation of telecommunications equipment is entirely dependent on an infrastructure that comprises things like electrical power and mechanical cooling.

Telecommunication facilities often have extensive self-diagnostic and monitoring systems that report operational status, individual component failures, and loss of

power or environmental control (heating or cooling). Most system cards switch to a spare circuit when a line indicates a failure is imminent.

Good locations have alarm systems with remote monitoring of all critical system functions. The switching and transmission system hardware is very reliable, and is designed to detect and correct errors or switch to spare circuits when necessary. Except for individual line cards, the switching equipment is duplicated with approximately 50 percent of its software and processing power being directed to diagnostics and testing activities.

Almost all problems are detected and corrected before they affect customer service. Switching systems are remotely monitored in Switching Control Centers around the clock, 365 days a year. All alarms for all switching systems are displayed in the control center. Failures are generally caused by software or human errors. Equipment failures are generally limited to small switching components such as line frames or line cards. Fires, floods, volcanoes, earthquakes, espionage, terrorist attacks and other natural events can cause catastrophic failures.

What Can Go Wrong?

The facilities of the telecommunications industry are generally robust, well engineered and highly reliable. When these are combined with the inherent redundancy of the public switched telephone network, the result is an extremely reliable and flexible system. This reliability was powerfully demonstrated by the loss of a major network location in the collapse of the World Trade Center. Serious interruption of regional telephone traffic was not experienced.

That is not to say that equipment losses cannot occur. But the frequency of such events may be significantly lower than what might be expected in other industries that rely on electronics. Furthermore, the design of the electronic equipment for telecommunications service anticipates continuous, uninterrupted operation. The result is a highly modular approach wherein online replacement of components and modules is provided. As a result, an electronic failure temporarily reduces the traffic capacity of the equipment but does not necessarily cause a shutdown. Such equipment is designed to continue operating while repairs are being made.

Replacement Values

The cost to acquire telecom equipment is a good gauge to measure potential loss. While it is unlikely that an entire telephone switch could be taken completely out of service, short of an event such as the attack on the World Trade Center, it is always wise to know the real replacement value of such assets. As a rule of thumb, a telephone switch should cost about $60 per line. That is to say that a 10,000-line switch will cost about $600,000 to replace.

An equal amount on a per line basis should be recognized to cover replacement of transmission equipment. Together, a 10,000 line central office represents about $1.2 million in switching and transmission equipment. This number of lines is probably what one would expect to see in a modest size urban or suburban central office.

Property Damage

The most serious property damage loss scenario would involve loss of cooling in a period of hot weather. High temperatures are the enemy of electronics, and extended exposure to high temperatures will lead to failures. The extent of these failures determines whether a significant property damage loss will occur. Even when fairly extensive damage has been inflicted, the highly modular nature of telecommunications equipment should enable restoration of full capacity by replacement of affected modules or circuit boards.

As has been stated previously, power loss is not likely to be a serious threat to telephone facilities. This is because of the underlying DC power systems that support the electronics. Even in cases where power is lost by failure of backup generation and battery depletion, it is unlikely that the equipment will be damaged when operations are resumed.

The critical equipment in a telecommunications facility need not be the telecommunications electronics itself. The supporting infrastructure can be much more important in terms of loss potential. Electric power, heating, ventilation and air conditioning are frequently just as vital to overall function. Failure of even individual items can cause extensive property damage. This infrastructure should be designed and installed in a manner worthy of telecommunications reliability.

Business Interruption

Business interruption involving telecommunications is difficult to anticipate. Network redundancy mitigates any significant overall loss of business. The telecommunications network is not monolithic. It’s possible that a loss in a facility may significantly reduce one company’s earnings while actually increasing income for another. It is entirely possible that a company suffering from an equipment failure at one of its locations may actually result in a windfall of revenue to another company whose facilities may be called upon to handle the re-routed traffic during the outage.

Contracts define the relationship between telecom companies and are also an important element in assessing potential business interruption losses. When a geographically limited firm is involved, the impact of a single outage at one of its facilities can have adverse business interruption consequences that might not have occurred had it owned a greater portion of the total network.

Legacy Equipment and Industry Forecasts

The current vintages of telecommunications switching equipment include the No.4 ESS and No.5 ESS manufactured by Lucent Technologies, the EWSD from Siemens AG, and the DMS 100 and the DMS 100/200 from Nortel Networks. The No.4 ESS is no longer manufactured and the others are mature and fully developed switches. They are deployed throughout the Telco and Long Distance carrier networks. There are some No.1 ESS machines still working in the local exchange networks. This equipment is also no longer manufactured. These machines were first deployed in the 1960s and are well beyond their technological ages although they still provide excellent service.

Currently, there appears to be no problem acquiring replacement parts for equipment failures of any of this equipment. In the United States, the Regional Bell Operating Companies have very active Plug-In Inventory Control systems. Defective plug-in circuit packs are returned to various vendors for repair. Also, as older equipment is replaced in one office, it is transferred to other offices to accommodate growth. At this stage in the technical lives of all of the switching equipment mentioned above, manufacturers are not spending a lot of resources on further development but are looking forward to the next generation of switches.

The next generation of switches will be ATM (Asynchronous Transfer Mode) and/or IP (Internet Protocol) based switches. This equipment is now in development with some early models deployed in carriers' laboratories. The first deployments will be installed in tandem in the local and long-distance networks. This will occur in the next two to three years. Installations in local-exchange networks will probably begin in the next three to five years.

In Conclusion

The computer electronics that comprise telecom switches and transmission equipment are very durable when housed and operated in a clean, cool and dry environment. Because of the modular design of the equipment, typical failures usually involve replacement of a circuit board for complete repair. And, the redundancy of the network design permits seamless operation of the telecom system even in the unlikely event that an entire switch is lost.

The real threat to high technology telecom equipment lies in the traditional building infrastructure equipment. Since sensitive electronics will not tolerate high temperatures or humidity, the integrity of the building ventilation and air conditioning system is critical to the continued operation of computers and telecommunications equipment.

A failure to the building's HVAC system is the greatest risk hazard to telecom equipment that is not designed to shut itself down on high-temperature

conditions. Similarly, equipment located in a facility with a suspect power system may be at greater risk. Power system failures can impart damaging electrical transients that can destroy the electronic components of telecom equipment. Having adequate system protection and emergency response plans is the best defense against telecom equipment failure.

Robert Weir, a director with The Hartford Steam Boiler Inspection and Insurance Company, is a Professional Engineer and has an extensive background in the design and construction of power generation and industrial equipment and systems. A graduate of the U.S. Naval Academy, he holds a Master's Degree in mechanical engineering from Worcester Polytechnic Institute and is a graduate of Suffolk University Law School. He is a member of the American Society of Mechanical Engineers (ASME), a permanent committee member of the National Fire Protection Association (NFPA 37), and is admitted to practice in Massachusetts and federal courts, including the U.S. Supreme Court. He is a registered patent attorney.