PRINT ME
SAVE AS

Target: Telco Fires

Modern businesses count on a high level of uninterrupted service from their telephone and datacom services

By JEROMIE WINSOR

In May 1988, a disastrous fire ripped through Hinsdale, Ill., a western suburb of Chicago. The ramifications of this fire were widespread, affecting businesses and residences over a wide region. Some 35,000 telephone customers were forced to go without service for nearly a month, including area hospitals.

From the above description, one may think that this must have been quite a large fire. In fact, the fire was limited to a single facility, and the building itself was not entirely destroyed. The damage was primarily limited to the equipment inside: the public telephone switch.

Similar fire events at telecommunications facilities have occurred near Los Angeles, New York City and Toronto. Each time, surrounding facilities and businesses have lost communication services: the vital lifeline of any modern business.

While fires at telecommunications and datacom facilities are extremely rare, the risk involved is great. Even a small fire can end up costing businesses a great deal of time and money. In the case of a telephone and Internet service providers, who own and operate the largest telecommunications facilities, an event like this can mean dangerous liability cases and a loss of clients.

BUILDING A STANDARD: NFPA 76

The process of building a standard for telecommunications facilities began in 1996, when the NFPA received a letter from AT&T requesting that a standard for fire protection be created. After receiving additional interest from the telecom and fire-protection communities, the Standards Council decided to develop a new standard, NFPA 76.

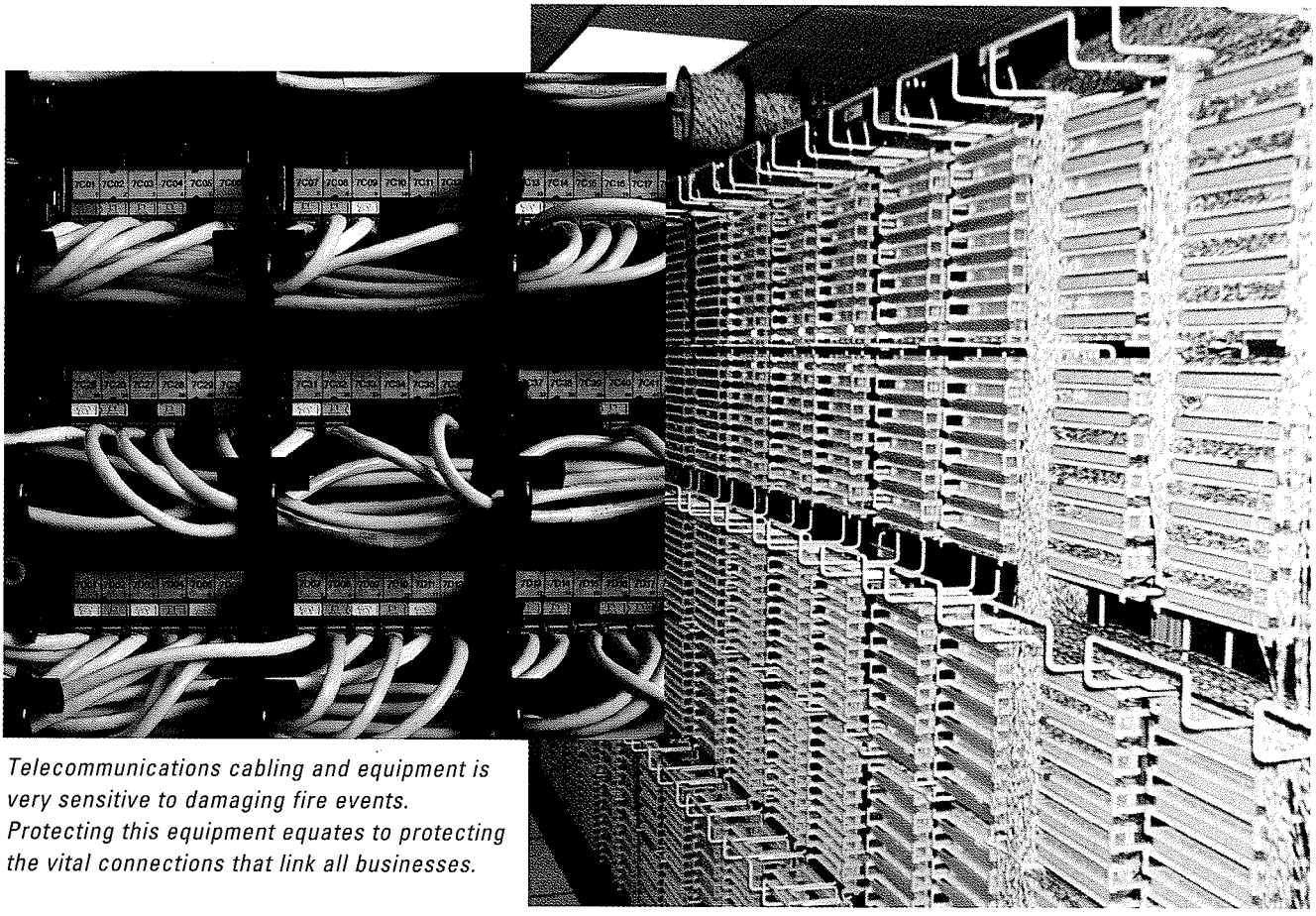
The primary thinking behind this movement was that having a separate standard would not only help to address the unique fire-safety requirements of telecommunications equipment, but it would separate these facilities from being classified under other codes that focus more on life safety.

The first step was creating a telecommunications committee to oversee the standards process. This process is two-fold: first, the committee submits a draft for proposals. Once proposals have been received, the draft is published with the proposals, asking for comments. After comments have been taken, the standards council decides whether or not to publish the standard.

The NFPA 76 standard committee began by publishing an initial draft of the standard for proposals. At first, the standard tried to cover a very broad range of facility types, from the most basic corporate office or strip mall to the more complicated telco hotels or server farms. At this juncture, the plan is first to publish a "recommended practice" that will be limited to large—over 500 square foot—facilities.

Another interesting mission of NFPA 76, according to Mark Conroy, fire engineer with the NFPA, is to help create a mindset among professionals, owners and companies that where critical data is involved, it is important to create redundantly reliable facilities and continually back up data off-site. Focusing on this will hopefully lead to greater awareness of the dangers.

Currently, the recommended practice NFPA 76 is on schedule to be published by February or March 2002. First, it will be up for adoption at the November meeting, where it is open to comments from the general assembly. If everything goes through, the Standards Council will decide in January whether or not to publish it. Plans have already begun for possibly making it a stan-



Telecommunications cabling and equipment is very sensitive to damaging fire events. Protecting this equipment equates to protecting the vital connections that link all businesses.

And business continuity is not the only process that could be affected. If a telecom facility handles a number of ATM transactions for banks, losing the information in even one of these major hubs could harm the financial stability of the country. If the facility is serving a hospital, a loss of service could detract from the efforts of those saving lives.

Quite obviously, building the highest level of redundancy into all areas of a telecommunications facility is the best way to mitigate any risk to operations, including fire.

LIFE-SAFETY RISKS

Over the years, the primary fire-safety focus for computer rooms and telecom facilities has been shifting to put a priority on this uninterruptibility. As always when protecting any facility from fire, guarding life safety is the primary concern. But the life-safety risks in a telecommunications facility are much less than an office building due to the sparseness of people in equipment spaces.

Actually, because the focus is more on uninterrupted service, designing fire protection systems for these facilities lends itself very well to performance-based design. In fact, an upcoming recommended practice from the NFPA—NFPA 76—is one of the first such NFPA documents to include a section outlining performance-based design requirements.

Basically, protecting the operations in these facilities comes down to protecting the sensitive equipment, which typically includes, but is not limited to, switching equipment, servers, routers, computers and cable television equipment that establishes any form of one- or two-way communications.

Telecommunications facilities generally house this equipment in large, conditioned rooms that are owned or leased by a telecommunications company offering wired telephone, cellular, cable television or Internet service. Many individual corporations have rooms within their office facilities that house the equipment as well.

As with any facility, there are many spaces serving different functions. For fire safety purposes, the facility can be divided into two areas: equipment and nonequipment spaces. While nonequipment space is generally designed to stop any fire from spreading into the equipment areas, equipment space must also deal with fires when they are very, very small.

TRADITIONAL FIRE PROTECTION

The prescription for fire safety in telecommunications facilities has continually changed over the last decade. Part of the reason is that the importance of telecommunications has really not blossomed until then.

While most facilities in general require sprinkler systems, for telecommunications equipment the risk of a sprinkler malfunction can actually be greater than the risk of a fire, with water nearly as damaging as fire is to the equipment.

One solution to this problem is to use a dry-pipe sprinkler system, where water pressure is not delivered to a sprinkler head until an initial fire alarm triggers it, followed by a time interval to check the validity of the alarm before water is released.

While this solution may help to mitigate the risk of an erroneous discharge of water, it does not adequately protect the equipment itself from damage in the event of a fire. This task has generally fallen to a halon or clean agent system.

Halon—which was banned from production in the United States due to its global-warming potential—and its subsequent replacements offer a means of putting out fire without doing major damage to telecommunications equipment.

These gaseous substances fill up a space and rob the fire of its oxygen, or its fuel. Although these substances—at certain levels—offer a threat to humans, they are very suitable for telecommunications equipment spaces and have become the suppressant of choice for the industry.

Most of these substances can either be distributed automatically—as triggered by an alarm event and sprayed from the ceiling—or dispersed manually from a fire extinguisher.

FIRE DETECTION

For high-risk telecommunications facilities, however, traditional fire detectors—smoke and heat detectors—generally do not offer the necessary protection. By the time smoke or heat levels reach the proportion necessary to set off these devices, the battle to save the vital communication network has, in all likelihood, already been lost.

As a result, for companies that have a serious stake in ensuring that the phones keep ringing, code-based requirements for detection are not enough. Instead, fire designers are relying on the most advanced detectors around, in an effort to accomplish very fast detection and very fast response. This can be accomplished with the use of "very early warning" detectors coupled with rigorous alarm processing.

There are a couple of different "very early warning" devices at a designer's disposal. A common tool is the aspirating, or air-sampling, detector. Basically, this device collects small samples of air and brings them back into a small box, where the air is analyzed. Another detection device that is specially suited for application in these environments are the spot-type sensor, which offers the opportunity to widely distribute sensors that are tied back into a computer.

Special spot sensors have the ability to be placed within a system or a rack to get very near the source of the fire. These could be used in very small spaces along with an automatic gas suppressant to snuff out a fire very quickly without the need for other intervention.

Using very-early warning detectors is a very important facet of the system, but rigorous alarm processing and response is also key. A minute's time can mean the difference between a system that is destroyed and a fire that has been snuffed out.

see TELECOM, page 13

THE CAUSES OF TELCO FIRES

When creating a fire-safety plan for a telecommunications facility, it is important to understand the events that can trigger a fire in these unique environments. The most typical fire threats originate from building systems, human error, outside fires and within the telecommunications equipment itself.

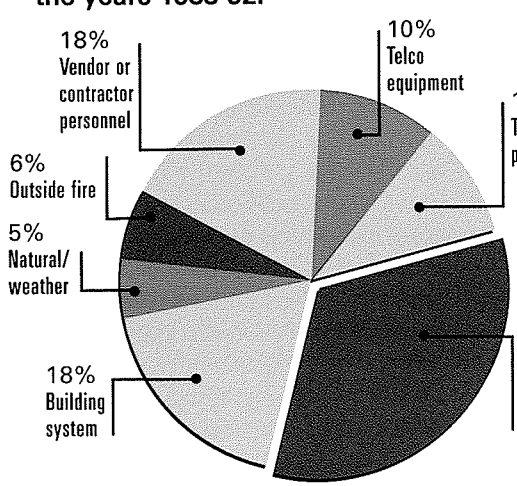
By far, the most common instigator of fire events in telecommunications facilities are building systems, especially the power distribution equipment. As a matter of fact, according to the FCC's Network Reliability Council, electrical equipment caused nearly one-third of all reported telecommunications fires between the years 1988 and 1992 (see graph). Besides the electrical system, the other building systems that can be the source of a fire include the HVAC systems or mechanical areas.

Human error can be initiated by facility staff, but it is far more common that outside vendors or contractors, who are not familiar with the sensitive nature of telecommunications equipment and facilities, are the cause of a fire.

Other causes, such as a fire that spreads from an outside source or natural event (lightning, wind, etc.) or a fire that is caused within the telecommunications equipment, do not occur as often but still offer a challenge for fire safety systems. Fires that originate within the telecommunications equipment, for example, are much harder to effectively detect and suppress.

It is important to remember the high risk involved with protecting these systems, where a momentary loss of service is a major detriment to business continuity and damaged equipment can lead to a financial disaster. With these tenets, any fire threat, no matter how small, must be factored in and planned against.

Root causes of telecommunications fires for the years 1988-92.



Source: FCC Network Reliability Council's Report to the Nation (1992)

Many facilities will have levels of fire suppression built into their system, beginning with the very early warning detection system and a manual response. This can be backed up with smoke alarms and an automatic gas suppression system, often with a standard sprinkler system as the last line of protection.

THE HUMAN FACTOR

The most valuable response mechanism the human response to the initial alarm event. The challenges, however, include the facts that fire events are rare and the equipment has very rigorous requirements that a facility's staff must be fully aware of. When properly educated, a responding staff member can be the most vital link in a fire-protection scheme.

Conversely, when the human response to a fire event is inappropriate, the damage done to telecommunications equipment can actually be worsened. For example, in past events, both the internal and external facility staff have doused these fires with water, something that should not be done unless life or the building itself is in danger. Also, ventilating smoke through the computer room is a big mistake. Fires in nonequipment areas have been ventilated through the computer room in the past, and the smoke can cause serious damage to equipment. Another concern is shutting down the power supply. When the fire department arrives on a scene, quite often one of their first orders of business is to shut down the power supply for the building. Improper, unplanned shut down of telcommunications routers or computers can cause the equipment to function improperly, and the accompanying loss of power for the HVAC system can cause the smoke to accumulate around the equipment, even if the fire itself is outside of the equipment space. Having an on-site liaison that is aware of these issues can be as important as the fire protection system in the space.

THE FUTURE OF TELECOM

The Telecommunications Act of 1996 effectively created a competitive marketplace for the delivery of telephone and datacom services. In addition, the growing reliance on cellular and Internet communications, especially by businesses, has created a need for services that even a depressed market will not kill.

The separation of the winners and losers of the new telcommunications market will largely depend on the ability to provide a high level of service, and telecommunications fire safety can be a big facet of this. By using the latest technology and preparing a thorough plan for fire detection, modern communications companies, and companies in general, can help ensure that their vital connections are not severed. ■