KATHLEEN H. ALMAND, P.E., FSFPE

Safe Data

Understanding the performance of fire protection systems in data centers

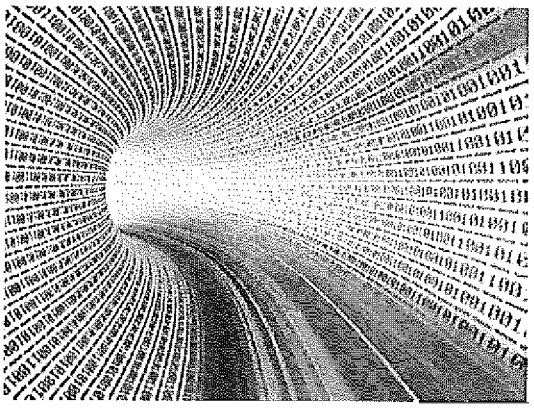
Modern society is highly dependent on the ability to communicate and to access data instantaneously, functions that depend on a global network of interlinked telecommunications systems and data centers. Vast amounts of digital content are stored in multiple locations and retrieved transparently by the user.

EVEN SMALL FIRES in **IT/** telecom centers can result in significant data loss and service interruption.

Fire represents a significant risk for these centers. Even a very small fire can result in significant data loss and service interruption. The indirect impact of fire loss due to business interruption and the loss of critical operations, sometimes geographically very distant from the IT/telecom facility itself, can far outweigh the direct property loss.

In the past few years, there have been dramatic changes in the equipment housed in these facilities, each with its own impact on fire risk. This equipment presents several types of fire safety challenges: fire load, energy density, accessibility, and a high and complex airflow environment to manage waste heat. Each of these challenges affects the design of fire safety systems, including detection, suppression, and emergency response.

Airflow containment—directing high volumes of cooling air at high-energy-generation equipment—is an innovative approach to energy management in these facilities, This results in localized, high airflow patterns and smoke dilution, which, in turn, can pose significant challenges for providing adequate fire detection and suppression. The challenges are both in prediction and performance. Predicting the performance of detection and suppression systems can become an issue, since detector actuation is affected by local air-flow patterns and by smoke dilution, and suppression agent dispersion is affected by the volume of airflow and by obstructions associated with the equipment used to create these containment solutions. Although tools exist to model fire development, detection time, and suppression agent dispersion, they have not been validated for this application.



NFPA 75, *Protection of Information Technology* Equipment, and NFPA 76, *Fire Protection of Telecommunications Facilities,* address fire protection requirements for IT/telecom facilities. Last year, 50 members of the telecommunications and fire protection industries met to discuss research that would meet these standards' needs to provide the technical basis for fire protection system requirements. The result is a research project, now underway, to develop a set of modeling tools that can be used to reliably analyze detection performance in IT/telecom facilities. The program will consist of a review of models, inputs, and available validation for this application.

At this year's SupDet conference, held in March in Phoenix, another aspect of the suppression challenges in data centers was presented. In a business environment where service continuity is paramount, suppression systems designed to protect electrical equipment must at times operate when that equipment is energized. This type of fire hazard challenges the most sophisticated clean-agent protection system. A 2009 Foundation study characterized the hazards associated with fires in energized electrical equipment. By analyzing these hazards, and considering the suppression processes, the properties of a standard test were developed, and the range of values of the most important parameter—the flux of added energy—was estimated. More research is needed to define performance parameters for a given suppression system in this range.

Data centers will continue to evolve, and fire protection systems and the engineering tools needed to evaluate their performance must evolve with them.

KATHLEEN H. ALMAND, FSFPE, is the executive director of the Fire Protection Research Foundation.

Photogra ph: iStockphoto