FIRE PROTECTION

ENGINEERING

Q3 2016 / ISSUE #71

Special Hazards Fire Protection Systems

DATA CENTER FIRE PROTECTION

A CASE STUDY ON OXYGEN REDUCTION FIRE PROTECTION

AN UPDATE ON WATER MIST FIRE PROTECTION SYSTEMS

SFPE
The Official Magazine of SFPE

DATA CENTER

Adapting to a Constantly Changing Environment

LEE A. KAISER, P.E.

DATA CENTER DESIGNS have become a playground for creative problem solvers and new products. The areas of information technology, electrical power, and equipment cooling—The Big Three—seem to be reinvented every five years. This constant reimagining of the data center is driven by the need for a larger capacity to address software and data demands as consistently as possible with zero downtime.

Building designs have become a secondary consideration, adapting to serve the needs of The Big Three. Some building designs have become more complex to reduce size while other designs remain simple but larger.

Despite all these changes, the goals of data center fire protection remain the same: warn early of a fire, give the occupants options, and do no additional harm. If you select fire protection systems with these precepts, then they will parallel the mission of the data center.

A Well-Developed Fire Protection Strategy

The architecture and engineering team for any new data center project must design with these three fire scenarios in mind:

- A fire outside the data center is indirectly threatening it.
- Smoke inside the data center requiring immediate investigation before escalation (with the option for manual extinguishment).
- A fire inside the data center too large to be extinguished manually.

Some examples of solutions include continuous walls surrounding the data center, air sampling smoke detection arranged for Very Early Warning Fire Detection, clean agent-type manual fire extinguishers placed near all room exits, and clean agent fire extinguishing systems. Engineers should remember to focus on asset protection—life safety will be a convenient byproduct of that focus.

NFPA 75 and Enforcement by AHJ Community

The section concerning risk considerations (Chapter 4) is one of the most important parts of NFPA 75, Standard for the Fire Protection of Information Technology Equipment. Fire protection engineers should judge risk assessments against NFPA 551, Guide for the Evaluation of Fire Risk Assessments.

The standard is voluntary in most cases, and many data center designers skip over its usefulness. AHJs also have trouble applying the prescriptive portions when they run into an IT facility. Many are confused by how NFPA 75 applies to the size of IT room. The scope states it is for "…the protection of information technology equipment and information technology equipment areas." This is admittedly a broad definition, but the broad scope points to the importance of a risk assessment. The smaller an IT room, the less equipment it can hold. If loss of the equipment presents a risk to the business, the prescriptive requirements should be followed. But if there is little risk, then the standard may not apply to that room. It should then stand to reason that any large IT rooms or data centers should perform a risk assessment to determine fire protection requirements.

Raised Floors Present Unique Firefighting Challenges

A risky proposition for any firefighter is battling a fire underfoot. Many data centers continue to use raised floor systems to act as an air supply plenum and to conceal power and communications

FIRE PROTECTION

Raised floors are an important, but often overlooked requirement that bears more explanation.

cabling. The 2013 edition of NFPA 75 requires either automatic sprinklers or a gaseous fire extinguishing system below raised floors when one or both of these conditions exist:

- There is a critical need to protect data in the process, reduce equipment damage and facilitate a return to service.
- The area below the raised floor contains combustible material.

Raised floors are an important, but often overlooked requirement that bears more explanation. If a fire occurs in a raised floor space, it will be difficult to access. Manipulating tiles for access is tough and regularly causes injuries in non-fire conditions including sprains, strains, and cuts on sharp corners of the metal framing system. Fill the room with smoke and firefighters now have a new risk not usually found in other structural firefighting conditions.

Virtualization IT Solution Increases the Cost of Fires

Virtualization is the consolidation of multiple computer servers into one device. The concept of virtualization is purely IT-related but increases the value of the equipment inside the data center. The virtualized server has much more computing power, energy consumption, and heat rejection. Servers operate multiple software applications simultaneously and more efficiently than individual servers, but have created a market with server costs of $1–1.5 million (U.S.)—much more expensive than the industry is used to.

Because of the rising costs, virtualization is changing the loss equation. In the mainframe days, the equipment was worth more than the data. Then equipment became cheap, and the data explosion made data loss more expensive than the equipment. Virtualized servers are bringing the two into balance with equal worth.

Fire Ignition Sources

Many in the gaseous suppression industry believe data center fires are under reported for a variety of reasons. A large concern is a fire can damage a company's brand image, exposing vulnerabilities.

The actual number of incidents per year in any given country is unknown, but the reality is data centers have fires. It is this author's experience that there are about two fires per month in the U.S. resulting in a suppression system discharge. The ignition source varies. About 10 percent of the time it is in the IT equipment, but manufacturers have made great strides in making equipment more resistive to causing fires. A little more than a third of the time the ignition source is the power distribution equipment—either inside the IT room or outside in a power or battery room. Uninterruptible power supplies are a frequent source of small fires and smoke events. The remaining causes are less common and can include foreign objects in the data center, human error, or even arson.[1,2]

HVAC and Cabling Designs Should Lead Fire Protection Decisions

Do not develop final designs for fire protection systems until there is a complete understanding of both the HVAC system and electrical raceways present in the space. Without accommodating the HVAC system, performance will inevitably suffer.

Today, air change rates for most data centers require spot smoke detector spacing of 125 Ft^2 per detector, as dense as required by NFPA 72, National Fire Alarm and Signaling Code. Also, facilities use aisle containment systems that complicate installation of both detection and suppression systems. NFPA 75 and NFPA 76, Standard for the Fire Protection of Telecommunications Facilities have requirements for installing fire protection when aisle containment is at play, but the components must be understood early in design. Without adjusting for aisle containment partitions, sprinklers may not work properly, or clean agent systems may not develop concentrations as fast as possible.

Locations of electrical cable trays and bus ducts must be known for proper placement of sprinklers and clean agent nozzles. Improper coordination can impact fire system performance. Furthermore, recent Factory Mutual Research has shown how difficult cable bundle fires can be to extinguish.[3] A fire involving a cable bundle can threaten the entire data center if not extinguished.

Placement and Type of Smoke Detection Key to Detecting an Impending Fire

Large, uncontrolled smoke production causes increased damage, an additional difficulty in response and equipment failures from corrosion of printed circuit boards. Early detection of smoke depends on knowledge of the HVAC system in the space.

For very early warning, locate detectors where the smoke will travel—along the air circulation path. Smoke must arrive in sufficient density to be detectable. If there are not sensors along the airflow paths, smoke may not be detected in time to avoid a larger fire event.

Air sampling smoke detectors can warn data center operators of a smoke condition well before humans can perceive it. A notification scheme using mobile communication devices should be part of a well-thought-out very early warning fire detection system.

Once notified, a facility should have trained personnel search for the source of the smoke. Statistically, the most probable cause of a smoke event is overheated equipment. Personnel investigating should have thermal imagers available to search the space.

When the source of smoke is found, the associated equipment should be powered down according to IT procedures. To extinguish any flaming or active combustion, make sure a manual fire extinguisher is available to address the problem before any suppression system activates.

There is a lot of interest in water mist systems for data centers and several examples of water mist being used as the primary fire suppression system.

Specifying the appropriate type and number of manual fire extinguishers in the data center can be overlooked. Many times specifying extinguishers is left to architects, but engineers should take a more active role in IT facility designs so the correct type is specified. Chapter 8 of NFPA 75 has requirements to follow for extinguishers. Facilities should steer clear of powdered extinguishers in IT rooms.

After Detection Data Center Operations Impact Fire System Decisions

Automatic power and HVAC shutdown is a very hot topic for IT personnel. The NFPA codes and standards generally require powering down equipment in an IT room when a fire is detected as well as turning off HVAC units and closing dampers serving the room. This is not popular with many IT operators.

Within the past five years, it is become en vogue to "ride through" the event because the reality of an immediate shutdown of server equipment is too risky for the primary mission of the data center. NFPA allows exceptions for these "critical operations data centers" if proper justification can be made to the AHJ. Furthermore, this new reality has been realized by the NFPA 2001, Standard on Clean Agent Fire Extinguishing Systems Technical Committee that more Class C fires will be part of the data center fire experience. System designers must make accommodations for this including higher Class C extinguishing concentrations and planning for continual mixing during the agent retention period.

Non-Traditional Data Center Fire Suppression Systems

Clean agent fire extinguishing systems should be selected if the risk analysis shows a low tolerance for an outage. However, several fire protection systems have been marketed for installation in data centers besides clean agent systems including aerosol systems that generate fine particulate which interrupts flame chemistry for extinguishment. The concern with aerosol, however, is the cleanup effort of the particles after a discharge and the high heat during discharge causing secondary fires.

There is a lot of interest in water mist systems for data centers and several examples of water mist being used as the primary fire suppression system. Water mist should be viewed as an alternative to water-based sprinkler systems, not clean agent systems. It is important to remember that they still use water and activate using heat like a sprinkler system as water will pool on any horizontal surfaces. The advantage of water mist over sprinklers is they use less water, typically 50-90 percent less depending on the system.

Data center operators and specifying engineers continue to select very different strategies for fire protection of new data centers. In large part, decisions about the appropriate level of suppression protection and detection are made by showing the data center owners a menu of available options and letting them select at their risk without performing the risk analysis required by NFPA 75. In some cases, selection of the fire protection system is made by the construction manager/general contractor who is delivering the finished space for a certain unit price. Often, the owner believes they have a "critical operations" data center even though the fire systems weren't installed for critical operations.

Many system selection decisions are based on the cost first, what worked the last time, and a hope that no fire will occur, but the reality is the stakes for major IT facilities have never been higher. The public's demand for service with little to no interruption, additions to data consumption, and the significantly increased cost of virtualized servers make the risk of fire exposure to data centers significantly higher today than even just five years ago.

The best strategies for fire protection today are integrated with the operating model of the data center and the disaster recovery plan. A multi-layered approach to fire protection assures that fires and other small thermal events can be dealt with early causing minimum impact to the data center and delivery of service.

LEE A. KAISER is with ORR Protection Systems.

References

1. Hirschman, Dave (AOPA.org), 'ATC Zero': Inside the Chicago Center Fire, www.aopa.org/News-and-Video/All-News/2014/November/06/ATC-Zero-Inside-the-Chicago-Center-fire (November 6, 2014)
2. Judge, Peter (datacenterdynamics.com), Modular data center survives arson attack, www.datacenterdynamics.com/power-cooling/modular-data-center-survives-arson-attack/93151.fullarticle (February 3, 2015)
3. FMapprovals.com, Small-Scale Testing, Large-Scale Benefits, www.fmapprovals.com/product-alerts-and-news-events/approved-product-news/approved-product-news-recent-issues/2015/apn-volume-31-1/small-scale-testing (August 25, 2015)