Protecting Against Fires in Data Centers

BY DAVID RAUSCH

What happens when a fire breaks out in a modern building? If the building is code-compliant, it is equipped with an integrated fire detection, alarm, and sprinkler system. The detectors sense the presence of smoke, alarms sound, and the fire department is summoned. In the meantime, building occupants are given instructions, and the sprinklers activate in the area where the fire is located. The water contains the fire and provides protection for the occupants until the fire department arrives and extinguishes the fire.

In the case of a fire occurring in a data center, the primary problem associated with sprinkler-based protection is one of time. Since the typical fire sprinkler system doesn't operate until the air temperature reaches 500° – 1000°F, critical data and sensitive electronic equipment have already been destroyed by the time the water is discharged.

Of equal concern to data center owners and operators is the length of business interruption caused by a water-suppressed fire. Not only is the damage more extensive, thus requiring time-consuming replacement of hardware, but drying out the data center can also be a massive effort. Depending upon the size and importance of the data center to its owners and users, each hour of downtime can represent thousands of dollars in lost revenue.

So what's the key to protecting a data center and its vital business continuity against fire? Number one, data center operators must look at their facility as a unique area within their building, one that is not adequately protected by a water-based system specifically designed to protect the building structure. Number two, the data center must be viewed as a special fire protection application and equipped with a special hazards fire protection system providing rapid fire detection, integrated emergency response, and waterless fire suppression.

Step 1: Rapidly Detect the Fire

There are two proven methods for detecting a fire in a data center.

The first is by means of a high sensitivity smoke detection system which uses air sampling techniques to identify potential fire situations before there is smoke or open flame. Air from the protected data center—including the room and its subfloor area—is drawn continuously through a piping network into the detector where particles of combustion are measured at levels of obscuration as low as 0.003 percent per foot. This is approximately one thousand times more sensitive than a conventional smoke detector.

Data center operators must look at their facility as a unique area within their building, one that is not adequately protected by a water-based system specifically designed to protect the building structure.

At this stage of a fire, only invisible products of combustion—such as the outgassing of electrical components—are present. This incipient stage is followed by visible smoke, flame, and finally, intense heat. By continuously sampling the air in a data center, the HSSD system can detect airborne particles of combustion and provide the earliest warning possible.

An air sampling detection system often buys the data center manager thirty minutes or more of advance warning in the event of a fire emergency. This time can be used to locate the source of the situation and take corrective actions to prevent the fire from escalating and minimize the damage done to the data center and its vital contents.

The second method of fire detection is through the use of smoke detectors that feature a fully analog, microprocessor-based "brain." The technology built into this type of "smart" detector enables it to function as part of a "distributed intelligence" detection network and make decisions regarding potential fire and alarm situations without time-consuming communications with its central control unit. A "smart" detector can also supervise its own internal readiness status and report back to the control unit.

Smart detectors offer a number of advantages over conventional detectors. Their performance and reliability are vastly superior due to proven microprocessor-based technology. And because they reduce the amount of communications on the detection circuit, smart detectors are far less likely to generate nuisance alarms. Of paramount importance to the cost-conscious data center manager, retrofitting older fire detection systems with new smart detectors often can be accomplished without replacing existing wiring. This saves both installation time and money.

Step 2: Control the Emergency Response

The hub of the fire protection system is the central control unit. Typically mount-

ed right outside the data center, the control unit is also microprocessor-based and acts as the focal point of the distributed intelligence system. It is responsible for monitoring inputs from the detectors and other devices as well as maintaining the communications network necessary to report continuously on the status of the fire protection system.

In the event of a fire, the central control unit receives an alarm signal from one or more of the detectors in the protected area. It then initiates a series of "outputs" including triggering audible and visual fire alarms, notifying the local fire department, and activating the release of a fire suppression agent into the protected data center.

The central control unit also can be set up to initiate building systems management tasks such as controlling the HVAC functions within the data center and shutting down power to the electronic equipment. Through the use of special software, the central control unit can be configured and monitored from a remote location.

Step 3: Suppress the Fire

There are two main considerations when addressing waterless fire suppression in a data center—the configuration of the system and the fire suppression agent of choice.

Waterless fire suppression systems are custom engineered to fit each data center application. There are, however, three basic elements that are common to each type of system: the container(s) to store the fire suppression agent; a network of piping to deliver the agent to the data center; and strategically-positioned nozzles to distribute the agent to all parts of the protected enclosure.

From this point, the configuration of the fire suppression system depends on the size and layout of the data center. Central storage systems feature a bank of agent storage cylinders in one location connected to the data center by a computer-calculated piping/nozzle network. In-cabinet systems, using a multidirectional nozzle attached to piping and a nearby agent storage container, provide waterless fire suppression for high value electronic cabinets, servers, and other enclosures.

Regarding the selection of a waterless fire suppression agent, NFPA provides only a general guideline. NFPA 75, which covers the protection of electronic data processing equipment, states that "where there is a critical need to protect data in process, reduce equipment damage and facilitate return to service, consideration should be given to the use of gaseous agent total flooding systems in sprinklered or nonsprinklered computer rooms." Factory Mutual also recommends a gaseous agent suppression system to protect hardware and software in data centers where thermal and nonthermal damage from a fire can cause a high loss expectancy.

Perhaps the best known waterless fire suppression agent is Halon 1301®. Unfortunately years ago, Halon 1301 was determined to be an ozone-depleting agent and its production halted. Since then the most viable alternative has been FM-200®, a waterless agent with similarities to Halon 1301. Both are gaseous agents that are extremely effective on Class A, B, and C fires. Both agents are electrically nonconductive, safe for people, and require no after-fire cleanup.

But while Halon 1301 production is banned, FM-200 has zero Ozone Depletion Potential (ODP) and is listed on the Environmental Protection Agency's SNAP List as an acceptable alternative to Halon 1301 for use in occupied and unoccupied areas with no restriction. For this reason, FM-200 is the choice of fire protection engineers the world over and has been used in more than one hundred thousand installations in over seventy countries.

An emerging agent is 3M™ Novec™ 1230 fire protection fluid. Novec 1230 fluid offers zero ODP, the lowest atmospheric lifetime for halon alternative agents, and a Global Warming Potential of one, lower than any halocarbon agent acceptable for use in occupied spaces.

Inerting agents provide a third type of waterless fire suppression. An inerting agent is a blend of natural gases that works on a fire by depriving it of the oxygen it needs. Inerting agents have zero ODP and no atmospheric lifetime. They do require longer discharge times than either FM-200 or Novec 1230, and their storage containers take up more space.

Beyond Hardware and Agent

Data center operators, owners, and their insurance carriers should be made aware of the importance of *who* designs, installs, and services their special application fire protection system. They should know that a qualified fire protection company will be able to perform the necessary piping and hydraulic calculations and offer a smooth installation that minimizes any interruption to the facility's operations. Finally, the right fire protection company also will train the data center staff on the basic operation and care of the fire protection system as well as provide 24/7 service.

When it comes to protecting a data center against fire, don't let your data center customers be satisfied with a water-based sprinkler system. Help them calculate what an interruption in the operation of the data center would cost their company, and then specify a fire protection system that is designed to detect a fire faster, control the emergency situation seamlessly, and suppress the fire without the use of water. ❖

David Rausch is Kidde Fire Systems' Product Manager for Clean Agent Systems based in Ashland, MA. He can be contacted by phone at (508) 881-2000 or via e-mail at david.rausch@kidde-fenwal.com.