

Mitigating Fire Risks in Mission Critical Facilities

By Victor Avelar

White Paper #83

APC[®]
Legendary Reliability[®]

Executive Summary

This paper provides a clear understanding of the creation, detection, suppression and prevention of fire within mission critical facilities. Fire codes for Information Technology environments are discussed. Best practices for increasing availability are provided.

Introduction

Today's data centers and network rooms, more than ever, are under enormous pressure to maintain operations. Some companies risk losing millions of dollars with one single data center glitch. Therefore it's not hard to believe that in the event of a catastrophic data center fire, a company may not only lose millions but may also go out of business.

According to the National Fire Protection Association (NFPA), there were 125,000 non-residential fires in 2001 with a total of 3.231 billion dollars in losses¹. Industry studies tell us that 43% of businesses that are closed by a fire never reopen. And 29% of those that do open fail within 3 years. It's no wonder why when designing data centers; fire prevention, detection and suppression are always top concerns. Fires in data centers are typically caused by power problems in raceways, raised floors and other concealed areas. This is one of the reasons why raised floors are not recommended for data centers and network rooms. Fires have also been caused due to arson, corporate sabotage and natural occurrences such as lightning and power surges. Like any other critical system in a data center, fire protection must be redundant and fault tolerant in order to increase the overall data center availability.

Fire prevention provides more protection against fire than any type of fire detection or suppression equipment available. Simply put, if an environment is incapable of breeding a fire then there will be no threat of fire damage to the facility. If a fire does occur the next step is to detect it. Before fire alarms were invented, watchmen were responsible for spotting fires and alerting others. Now there are a number of advanced detectors that can detect fire in its incipient stages and then notify a central center that notifies personnel and suppression systems. Some of the first fire detection devices were nothing more than a water valve tied to a rope with a weight attached. In the event of a fire, the rope would burn through thereby opening the water valve. Fortunately, fire protection systems have come a long way with the advent of technology. Today there are many ways of detecting and suppressing fires, but only a few are recommended for data center applications. In a data center, the main goal of the fire protection system is to get the fire under control without disrupting the flow of business and without threatening the personnel inside.

Data Center Design Standards - NFPA Codes

NFPA, National Fire Protection Association, was established in 1896 to protect the public against the dangers of electricity and fire. Its mission "is to reduce the worldwide burden of fire and other hazards on the quality of life by developing and advocating scientifically based consensus codes and standards, research, training, and education." NFPA today is a worldwide organization with more than 69,000 members.

¹ National Fire Protection Association NFPA, Fire Analysis and Research Division.

*Does not include the events of 9/11/01, where there was \$33.44 billion in property loss.

Throughout NFPA's existence it has created many standards one of them being NFPA 75. NFPA 75 is the standard for the protection of electronic computer / data processing equipment. Several of items listed in the "Industry Best Practices" section are a result of the NFPA 75 standard. One important exception provided by the 1999 edition of NFPA 75 (6-4.2.1) allows data centers to continue to power the electronic equipment upon activation of a gaseous agent total flooding system. This exception is valid for a data center with the following risk considerations (NFPA 75, 2-1):






1. Economic loss from loss of function or loss of records
2. Economic loss from value of equipment
3. Life safety aspects of the function
4. Fire threat of the installation to occupants or exposed property

Gaseous agents will be discussed later in depth. NFPA continuously updates its standards therefore it's recommended that the latest standards be reviewed prior to designing or retrofitting a fire protection system into a data center. One must be aware that in most cases the Authority Having Jurisdiction (AHJ) has final say in what can or can not be done in regards to fire protection systems.

Tutorial on Fire

Fires can be categorized by five classes: Class A, B, C, D, and K. The five classes are described in Figure 1 below and are accompanied by the standard picture symbol used to identify what fires an extinguisher may be used on.

Figure 1 – Classes of fire

Class	Type of fire	Symbol
A	Fires involving ordinary combustible materials such as paper, wood, cloth and some plastics.	
B	Fires involving flammable liquids and gases such as oil, paint lacquer, petroleum and gasoline.	
C	Fires involving live electrical equipment. Class C fires are usually Class A or Class B fires that have electricity present.	
D	Fires involving combustible metals or combustible metal alloys such as magnesium, sodium and potassium.	
K	Fires involving cooking appliances that use cooking agents such as vegetable or animal oils and fats.	

In order for fire to exist, three elements are required. This is often taught as the “Fire Triangle”. Oxygen, Heat and Fuel must all interact for a reaction to take place otherwise known as fire. If one or more of these three elements are taken away, fire cannot exist. Therefore, fire extinguishing methods can vary depending on which element(s) are removed. For instance CO₂ systems reduce oxygen by displacing it with a heavier CO₂ gas. And because the CO₂ gas is much colder than the fire, it hampers its progression by taking away heat.

Once a fire is started it is often categorized in stages of combustion. There are four stages of combustion; the Incipient Stage or pre-combustion, Visible Smoke Stage, Flaming Fire Stage and Intense Heat Stage. As a fire progresses through these stages, many factors increase exponentially, including smoke, heat, and property damage. Not to mention risk of life, which becomes critical as smoke density increases. Fire research has shown that the incipient stage allows for the largest window of time to detect and control the progression of a fire. It’s in this window of time that fire detection systems can mean the difference between availability and unavailability. The longer the fire burns the more products of combustion, which then leads to a higher chance of equipment failure even if the fire is successfully extinguished. These products of combustion are conductive and can corrode the circuits on IT equipment. In these next few sections, we’ll discuss available solutions for detecting and suppressing fires in a data center

Choosing a Fire Protection Solution

For the purposes of designing a fire protection solution for a data center, three conditions should be met; identify the presence of a fire, communicate the existence of that fire to the occupants and proper authorities, and finally contain the fire and extinguish it if possible. Being familiar with all technologies associated with fire detection, alarming, and suppression will ensure a sound fire protection solution. Of course prior to selection of a detection and suppression methodology, the design engineer must assess potential hazards and issues. Will the data center have raised floors? Will it have high ceilings? Will personnel occupy the area? Will detectors be obstructed in any way? These questions, and many more like them, need to be answered before the proper fire protection solution is chosen. For instance, knowing that computer equipment running in a data center will become damaged at a sustained temperature of about 175° F should encourage a designer to implement heat detectors that are sensitive to that range of heat. Although a good deal of footwork must still be done, technology is making it easier and safer to design fire protection solutions.

In 1998 the Building and Fire Research Laboratory (BFRL) of the National Institute of Standards and Technology (NIST), received funding to develop 6 products that would improve building design and construction practices. One of these products is the Industrial Fire Simulation System or IFS2. The BFRL hopes that by 2003 the product will be used by U.S. commerce. The problem with designing fire protection solutions for today’s buildings is that it requires expensive full scale testing that is oftentimes impractical. With a product such as the IFS2, fire protection system performance can be predicted therefore allowing designers to recommend the proper solutions. The following section describes each of the components utilized in a complete fire protection solution for data centers.

Fire Detection System Types

Three main types of detectors are available; smoke detectors, heat detectors and flame detectors. For the purposes of protecting a data center, smoke detectors and heat detectors are far more effective.

Spot type smoke detection

Spot type smoke detectors can cover an area of about 900 square feet (84 square meters). These types of detectors aren't intelligent enough to be desensitized or report their locations therefore are ineffective in a data center. There are two types of spot type detectors; photoelectric and ionization.

Photoelectric detectors work by using a light source and light sensor perpendicular to it. When nothing is in the chamber the light sensor doesn't react. However when smoke enters the chamber, some of the light is diffused and reflected into the light sensor causing it to sound the alarm.

Ionization detectors use an ionization chamber and a small amount of radiation to detect smoke. Normally the air in the chamber is being ionized by the radiation causing a constant flow of current, which is monitored by the detector. When smoke enters the chamber it neutralizes the ionized air thereby causing the current to drop. This triggers the detector into an alarmed state.

Intelligent spot type very early smoke detection

Intelligent Spot-Type Very Early Smoke Detection (VESD) detectors, Figure 2, are very similar to conventional spot-type detectors except that they employ a more advanced detection method using a laser. As particles pass through the detector, the laser beam is able to distinguish them as dust or byproducts of combustion. These types of detectors are individually addressable so that they are able to send information to the central control station thereby pinpointing the exact location of the smoke. Some have the ability to automatically compensate for changing environments such as humidity and dirt accumulation. They can also be programmed to be more sensitive during certain times of the day, for instance when workers leave the area, sensitivity will increase. Intelligent spot type detectors are commonly placed below raised floors, on ceilings and above drop down ceilings. However modified spot detectors are also used in air handling ducts to detect possible fires within the HVAC (Heating Ventilation Air Conditioning) system as seen in Figure 3. By placing detectors near the exhaust and the intake of CRAC units (Computer Room Air Conditioners), detection can be accelerated.

Figure 2 – Intelligent smoke detector



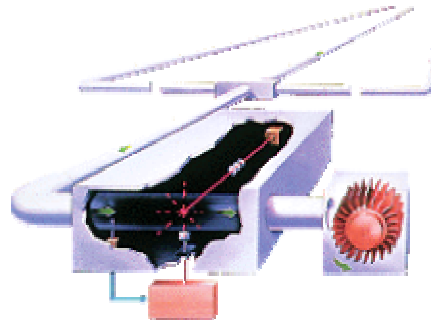
Figure 3 – Duct smoke detector



Air sampling smoke detection

Air sampling smoke detection, sometimes referred to as “Very Early Smoke Detection” as well, is comprised of a network of pipes attached to a single detector, which continually draws air in and samples it. The pipes are typically made of PVC but can also be CPVC, EMT or copper. Depending on the space being protected and the configuration of multiple sensors, these systems can cover an area of 5,000 to 80,000 square feet (465 to 7,432 square meters). Despite the wide area of coverage, the sensors can be centrally located for ease of maintenance and repair. Smoke detection is dependent on three variables; the sensitivity of the detector, how clear the smoke path is leading to the detector and how diluted the smoke will be once it reaches the detector. In an area such as a data center where the airflows are rapid, it becomes difficult to detect smoke with conventional spot-type detectors especially in the incipient stage of a fire. This is what makes VESD an ideal smoke detection solution for high availability data centers. The air sampling system is designed to detect the particles released from PVC wire during the initial stages of heat build up. When the smoke particles drift through the pipes and into the detector, a photo detector or a laser beam differentiates the particle as dust or as a byproduct of combustion. This detection process can be up to 1000 times more sensitive than a photoelectric or ionization smoke detector. These systems are capable of detecting byproducts of combustion in concentration as low as 0.003% obstruction per foot. A typical air-sampling detector is show in Figure 4.

Figure 4 – Air sampling smoke detection system



Linear thermal detection

Linear thermal detection is an effective method of detecting “hot spots” in cable trays or cable runs. It is composed of at least two conductors whose monitored characteristics are heat dependent. When a set temperature is reached, the two conductors cause an alarm condition that is detected at the main control panel. The control panel can then notify personnel where along the length of wire the alarm occurred. This type of detection is highly recommended in a data center environment where multiple bundles of cabling exist. Linear thermal detection is capable of detecting heat anywhere along its length up to about 5,000 feet (1,524 meters) per zone.

It's worth mentioning a different detection method, used for this same application, called Corrosive Gas Detection. One would think corrosive gas detection is unnecessary in a data center; however, it is in this application specifically where it is useful. The premise is that these detectors would alarm during the very

early stages of cable fires. When networking cables or electrical conductors overheat, the PVC (Polyvinyl Chloride) insulation covering the conductors breaks down into Hydrogen Chloride. The hydrogen chloride then reacts with water vapor in the air to form Hydrochloric Acid, which can damage computer equipment. It's the Hydrogen Chloride that will cause the corrosive gas detector to enter an alarm state. Overall this type of detection doesn't provide as an effective a solution as linear heat detection.

Flame detectors

Flame detectors usually use a photo sensor to detect visible flames. This type of detector is very ineffective in an area such as a data center. A flame usually appears after the incipient stage of a fire. It's during this incipient stage where detection is crucial in a data center.

Fire Suppression System Types

Once a fire is detected in a data center, it is critical to quickly extinguish the fire with no effect on the data center operation. To do this various methods can be used, some better than others. Regardless of the method employed, it should provide a means to abort the suppression system in the event of a false alarm.

Foam

Foam formally called, Aqueous Film-Forming Foams (AFFF), is generally used in liquid fires because when applied it floats on the surface of the flammable liquid. This prevents the oxygen from reaching the flames thereby extinguishing the fire. Foam is electrically conductive therefore couldn't be used anywhere where electricity is present. Needless to say it should not be used in data centers.

Dry chemical

Dry chemical or dry powder systems can be used on a wide variety of fire and pose little threat to the environment. Different types of powders can be used depending on the type of fire. They are electrically nonconductive but require clean up. They are used in many industrialized applications but are not recommended for data centers due to the residue left after discharge.

Water sprinkler systems

Water sprinkler systems are designed specifically for protecting the structure of the building (Figure 5). Water sprinklers are discharged when the valve fuse opens. Fuses are usually solder or glass bulbs that open when they reach a temperature of 165-175°F. It's important to note that by the time the fuse opens the temperature around the sprinkler head may be as high as 1000°F. This has given rise to fast acting or quick-response sprinkler systems, which are basically the same but, open at a lower temperature. Water sprinkler systems can be installed in three different configurations: wet-pipe, dry-pipe, and pre-action. Wet-pipe is by far the most common installation and is usually found in insulated buildings to prevent freezing. Dry-pipe systems are charged with compressed air or nitrogen to prevent freezing. Pre-action systems prevent accidental water discharge by requiring a combination of sensors to activate before allowing water to fill the

sprinkler pipes. Normally water sprinklers are not recommended for data centers; however, depending on local fire codes they may be required. In this case a pre-action system would be recommended. Installing a sprinkler system during construction can range from \$1- \$2 / square foot, while retrofitting an existing building costs increase to \$2- \$3 / square foot.

Figure 5 – Water sprinkler



Water Mist Systems

Water mist systems discharge very fine droplets of water onto a fire. One drop ranges in size from 100 to 120 microns, which dramatically decreases water consumption. Because mist systems use less water than conventional sprinkler systems they require less storage space. Water mist systems are extremely safe and pose no threat to the environment. This fine mist of water extinguishes the fire by first absorbing heat from the fire. By absorbing the heat, vapor is produced causing a barrier between the flame and the oxygen needed to sustain it. It is this change of state (liquid to gas) that makes this water mist system so effective. (This is the same phenomenon that is used in evaporative cooling.) Typical applications include gas turbines, steam turbine generator bearings, generator sets, transformers and switchgear rooms. Water mist systems are gaining popularity due to its effectiveness, however, it remains to be seen whether or not water mist systems will one day protect data centers.

Fire Extinguishers

Sometimes the oldest method of fire suppression is the best. Fire extinguishers these days are essentially the same as that have always been in that they are easy to use and can be operated by just about anyone. What makes fire extinguishers so valuable to data centers is the ability to extinguish a fire before the main suppression system discharges. As we noted before, the human nose is the best fire detector, which helps to extinguish a fire in its earliest stages.

A recent type of fire extinguisher has been approved for use in data centers and is replacing Halon 1211. The new agent is HFC-236fa or more commonly called by its trade name FE-36 and can be used in occupied areas (Figure 6). It is environmentally safe and leaves no residue upon discharge since it exits as a gas. Similar to other clean agents FE-36 extinguishes fires by removing heat and chemically preventing combustion.

Figure 6 – Fire extinguisher



Total flooding fire extinguishing systems

Total flooding fire extinguishing systems, sometimes referred to as Clean Agent Fire Suppression Systems, can be used on Class A, B, and C fires. A gaseous agent flooding fire suppression system is highly effective in a well-sealed, confined area, which makes a data center an ideal environment. It typically takes less than 10 seconds for an agent to discharge and fill the room. The agent is contained in high-pressure tanks as shown in Figure 7. The number of tanks used depends on the total volume of the room being protected as well as the type of agent being used. The hidden areas in a data center present the biggest threat of fire. If wires are damaged, loose or otherwise poorly maintained in an open area, a routine visual inspection should uncover the problem and repairs can be made. Discovering a problem in a closed area is far more difficult. Unlike water suppression systems, gaseous agents infiltrate even the hardest to reach areas such as inside equipment cabinets. Later the gas and its byproducts can be vented out of the data center with very little environmental impact and no residue. These agents are non-conductive, non-corrosive and some can safely be discharged in occupied areas. For years Halon has been used as the agent of choice, however, it is being phased out due to its ozone depletion properties. We will discuss Halon alternatives in the next section.

Figure 7 – Gaseous agent cylinders



Gaseous Agents

A fire-extinguishing agent is a gaseous chemical compound that extinguishes a fire, as a gas, by means of “suffocation” and or heat removal. Given a closed, well-sealed room, gaseous agents are very effective at extinguishing fires and leave no residue. Back in the 1960’s when Halon 1301 was introduced; it was widely used throughout various industries given its effectiveness in fighting fires. However, on January 1, 1994, under the Clean Air Act (CAA), the U.S. banned the production and import of Halons 1211, 1301, and 2402 in compliance with the Montreal Protocol on Substances That Deplete the Ozone Layer. Recycled Halon and inventories produced before January 1, 1994, are the only sources available today. Furthermore the EPA (Environmental Protection Agency) published the final rule (63 FR 11084) on March 5, 1998 that bans the production of any blend of Halon. However an exception was made for the purpose of aviation fire protection. In the midst of this ban came two U.S. standards: NFPA 2001 standard on Clean Agent Fire Extinguishing Systems and the Significant New Alternatives Policy (SNAP) from the (EPA). Under these standards alternative agents are evaluated based on their safety, effect on the environment and effectiveness.

Gaseous agents can be divided into two categories; inert gases and halocarbons. Note that the names of the agents are designated under the NFPA 2001 standard. The names in parentheses are the trade names that they are normally referred to.

Inert Gases

Although there are other inert gas agents approved by NFPA 2001, Carbon Dioxide, and Inergen are more widely accepted and are described in further detail. Some other inert gas agents include: IG-55 (Argonite), IG-100 (Nitrogen) and IG-01 (Argon),

Carbon Dioxide

Carbon Dioxide or CO₂ is an inert gas, which reduces the concentration of oxygen needed to sustain a fire by means of physical displacement. Because CO₂ is heavier than oxygen, it settles to the base of the fire and quickly suffocates it. That makes this type of agent unsafe for discharge in occupied areas. If it is to be used in an occupied area, this type of suppression system must use safety mechanisms to reduce the likelihood of a fatal discharge. A safety mechanism would be one that provides audible and visual queues to data center occupants 30-60 seconds prior to discharge. CO₂ is non-conductive and non-damaging. A disadvantage to the use of carbon dioxide is the large number of storage containers required for effective discharge. CO₂ is stored in tanks as a gas and occupies about 4 times the storage volume of Halon 1301. This is obviously a poor choice for any data center where floor space is highly valuable. Some applications are transformer rooms, switch rooms, cable vaults, generators and industrial processes. The typical cost of a CO₂ system is about \$100 / cubic foot. The cost of the agent is about \$3 / pound.

IG-541 (Inergen)

Inergen is an inert gas composed of nitrogen, argon and carbon dioxide, all of which are found naturally in the atmosphere. For this reason it has a zero Ozone Depletion Potential (ODP), an acceptably low Global Warming Potential and does not produce any harmful products of decomposition. Inergen is non-conductive, leaves no residue and is safe to discharge in occupied areas. Inergen is stored as a gas in high-pressure tanks that can be located about 300 feet (91 meters) away from the nozzles. This is convenient considering Inergen requires a storage volume 10 times that of Halon 1301 which would take up precious data center space. Furthermore to reduce the storage volume needed for systems protecting multiple rooms, section valves can be used to direct the agent to the alarmed zone. Inergen is used in data centers, telecommunications offices, and various other critical applications. The typical cost of an Inergen system is about \$3 / cubic foot. The cost of the agent is about \$0.50 / cubic foot or about \$8,000 to fill an 80 liter tank at 150 Bar.

Halocarbons

Although there are other alternative agents approved by NFPA 2001, FE-13 and FM-200 are more widely accepted and are described in further detail. Some other halocarbon agents include: HCFC Blend A (NAF-SIII) and FC-3-1-10 (CEA-410)

HFC-23 (FE-13)

FE-13 has zero Ozone Depletion Potential (ODP) and an acceptably low Global Warming Potential however it does produce toxic hydrofluoric acid (HF) when exposed to high temperatures. FE-13 can be used in occupied areas; however, like in any other fire situation all occupants should evacuate the area as soon as an alarm sounds. One of the main advantages of FE-13 is that the nozzles can be fixed at heights up to 25 feet. The low boiling point of this agent -116°F (-82°C) makes it ideal for applications such as unheated storage areas. Due to differences in vapor pressure FE-13 cannot be retrofitted or “Dropped In” with existing Halon 1301 systems. FE-13 has a storage volume 2.2 times that of Halon 1301. Applications include battery rooms, data centers, and industrial applications that may need to protect unheated areas. The typical cost of FE-13 is about \$3,500 / pound.

HFC-227ea (FM-200)

FM-200 has zero Ozone Depletion Potential (ODP) and an acceptably low global warming potential. It is an odorless, colorless and is stored as liquefied compressed gas with a boiling point of 2.5°F (-16.4°C). FM-200 is discharged as an electrically non-conductive gas that leaves no residue and will not harm occupants. It can be used with ceiling heights up to 12 feet compared to FE-13 which can accommodate ceiling heights up to 25 feet. Of all the alternative agents, FM-200 has one of the lowest storage space requirements, needing only 1.7 times that of Halon 1301. FM-200 chemically inhibits the combustion reaction by removing heat and can be discharged in 10 seconds or less. An advantage to this agent is that it can be retrofitted into an existing Halon 1301 system. Like FE-13, FM-200 decomposes at high temperatures forming hydrofluoric acid (HF), which is toxic. Some applications include data centers, switchgear rooms, automotive, and battery rooms. The typical cost of an installed FM-200 system is about \$2,800 / cubic foot. The cost of the agent is about \$7,700 / pound.

Pull Stations

Pull stations allow a building occupant to notify everyone in the building of a fire. These are usually placed at every exit to the building and once pulled can notify the fire department of the alarm (Figure 8). Pull stations are sometimes the best way to catch a fire in its incipient stage. No matter how sensitive a smoke detector may be, it's still no substitute for the human nose. A person can pick up the scent of smoke much earlier than any smoke detector can.

Figure 8 – Pull station



Signaling Devices

Signaling devices are activated either after a pull station or a detector enters the alarm state. Signaling devices provide audible and / or visual queues to building occupants as a signal to evacuate the building (Figure 9). Audible sounds may include horns, bells, sirens, and may be heard in various patterns. Sound levels range from 75dBA to 100dBA.

Visual signaling devices are crucial to notifying occupants who are hearing impaired. Strobes usually incorporate a Xenon flashtube that is protected by a clear protective plastic. They are designed with different light intensities measured in candela units. The minimum flash frequency for these strobes should be once per second.

Figure 9 – Fire alarm strobe



Control Systems

Regardless of the number of fire suppression and detection products in a building they are useless without a control system. Control systems are the “brains” behind the building’s fire protection network. Every system we’ve discussed thus far is accounted for by the control system. An example of one is shown in Figure 10 below. It controls the sensitivity levels of various components such as smoke detectors and can be programmed to alarm only after a certain sequence of events have taken place. The computer programs used by these systems allow a user to set certain time delays, thresholds, passwords, and other features. Reports can be generated which can lead to improved performance of the fire protection system, by identifying faulty sensors for example. Once a detector, pull station or sensor is activated the control system automatically sets in motion a list of rules that have been programmed to take place. It can also provide valuable information to authorities.

Figure 10 – Fire control panel



Protecting a Mission Critical Facilities

Now that all the fire protection components have been described, the last step is to bring them together to design a robust and highly available data center solution. It's important to note that while various types of detection, suppression, and gaseous agents were described, not all of them are recommended for a highly available data center. The following list of components compliments a data center goal of 7x24x365 uptime.

- Linear heat detection
- Intelligent Spot-Type Detection (VESD)
- Air sampling smoke detection (VESD)
- Fire Extinguishers
- Total flooding fire-extinguishing system
- Halon alternative clean agent
- Pull stations
- Signaling devices
- Control system

Linear heat detection wire should be placed along all wire trays and electrical pathways above and below the raised floor. An alarm here should not trigger the suppression system however it should prompt the control system to sound an alarm.

Redundant air sampling smoke detector systems should be placed beneath as well as above the raised floor. This is to prevent any accidental discharge of the clean agent. Both detection systems must enter an alarm state before the total flooding suppression system discharges. It is also recommended that intelligent spot-type detectors be positioned at every CRAC unit intake and exhaust. If any other ductwork enters the data center, duct smoke detectors should also be installed. Again, to prevent accidental discharge of the clean agent, no individual alarm should be able to trigger a discharge. The recommended Halon alternative clean agent is FM-200 because of its small storage footprint and effectiveness. FE-13 is also a good choice especially in a data center with high ceilings. In addition to the total flooding fire-extinguishing system, fire code may require a sprinkler system to be installed. If this is the case, it must be a pre-action system to prevent accidental water damage to the data center. FE-36 clean agent fire extinguishers should be placed throughout the data center according to local fire codes. There should be pull stations as well as written procedures posted at every exit and signaling devices throughout the building capable of notifying all personnel inside of a fire.

The control system should be fault tolerant, programmable and capable of monitoring all devices. It should also be capable of automatic system overrides. All the detectors should be addressable therefore allowing the control panel to identify the precise location of any alarm. The control system is vital to the effectiveness of the suppression system. It must coordinate the sequence of events that take place immediately following the initial alarm. Some of these include sounding a separate evacuation alarm prior to discharge; closing ventilation dampers to prevent air from escaping, discharging the agent and notifying the local authorities.

And of course this could not all be done without well-written and effective emergency procedures, reinforced with regular training of all data center employees.

Raised floors

Raised floors bring up some important issues with regard to fire protection in mission critical facilities and are worth mentioning here. Raised floor tiles conceal power and data cables as well as any other combustible material such as paper and debris. Therefore it is recommended that all cabling be placed overhead where it is visible and can be easily inspected in case of a detected hot spot. When given the opportunity, raised floors become a breeding ground for human error that poses significant fire risks. In some cases boxes of paper have been discovered under the floor. It may seem very natural to store material under a raised floor without thinking of the fire hazards imposed. For more information on raised floors see APC White Paper #19, "Re-examining the Suitability of the Raised Floor for Data Center Applications". Lastly, raised floors increase the financial cost of properly protecting a data center. Because raised floors create a completely separate plenum, it must be protected with the same level of fire protection as the space above it. When systems like intelligent smoke detection and gaseous agent flooding are used, the cost could approach twice that of a non-raised floor environment.

Industry Best Practices

The following are list of recommend practices for increasing the availability of a data center from a fire protection perspective.

- Ensure that the data center is built far from any other buildings that may pose a fire threat to the data center.
- Emergency procedures should be posted on all annunciator panels and fire alarm control panels.
- A fire alarm system should incorporate multiple stages of alarm.
- A smoke purging system must be installed in the data center.
- All electrical panels must be free of any obstructions.
- All EPO buttons and fire alarm pull stations should be consistently labeled to avoid any confusion.
- All fire extinguisher locations should be clearly identified and should provide information on what kind of fire to use it on.
- Any openings in the data center walls should be sealed with an approved fireproof sealant.
- Each data center exit should have a list of emergency phone numbers clearly posted.
- Enforce a strict no smoking policy in IT and control rooms.
- EPO systems should not be activated by fire alarms.
- Equip the switchgear room with fire extinguishers.
- Fire dampers should be installed in all air ducts within the data center.

- Fire protection systems should be designed with maintainability in mind. Replacement parts and supplies should be stored on site. Systems should be easily accessible.
- Get approval from the fire marshal to continue operating the CRAC units when the fire system is in the alarmed state.
- If a facility is still using dry chemical extinguishers ensure that the computer room extinguishers are replaced with a Halon alternative.
- Pre-action sprinklers should be placed in the data center (if required by AHJ) as well as in the hallways.
- Provide a secondary water source for fire sprinklers
- Sprinkler heads should be recessed into the ceiling to prevent accidental discharge.
- The annunciator panels should have emergency or operating procedures posted near them. Most annunciator panels are located in the security office and may also be located in the engineer's office.
- The fire suppression system should have a secondary suppression agent supply.
- The data center should be void of any trash receptacles.
- All office furniture in the data center must be constructed of metal. (Chairs may have seat cushions.)
- Tape libraries and record storage within the data center should be protected by an extinguishing system. It's recommended that they be stored in a fire safe vault with a fire rating of more than 1 hour.
- Any essential supplies such as paper, disks, wire ties, etc., should be kept in completely enclosed metal cabinets.
- UL approved extension cords used to connect computer equipment to branch circuits should not exceed 15 feet in length.
- The use of acoustical materials such as foam, fabric, etc. used to absorb sound is not recommended in a data center.
- The sprinkler system should be controlled from a different valve than the one used by the rest of the building.
- All data center personnel should be thoroughly trained on all fire detection and extinguishing systems throughout the data center. This training should be given on a regular basis.
- Air ducts from other parts of the building should never pass through the data center. If this is not possible then fire dampers must be used to prevent fire from spreading to the data center.
- Water pipes from other parts of the building should never pass through the data center.
- Duct coverings and insulation should have flame spread ratings less than 25 and a smoke developed rating less than 50.
- Air filters in the CRAC units should have a class 1 rating.
- Transformers located in the data center should be a dry type or should be filled with non-combustible dielectric.
- No extension cords or power cords should be run under equipment, mats or other covering.
- All cables passing through the raised floor should be protected against chaffing by installing edge trim around all openings.
- Computer areas should be separated from other rooms in the building by fire-resistant-rated construction extending from structural floor slab to structural floor above (or roof).

- Avoid locating computer rooms adjacent to areas where hazardous processes take place.

Common mistakes

Some common mistakes made with regard to fire protection systems in a data center environment.

- Having the fire system automatically shut down the CRAC unit. This will cause the computer equipment to overheat resulting in downtime.
- Using dry chemical suppression agents to extinguish computer room fires will damage computer equipment. Dry chemical agents are very effective against fires but should not be used in a data center.
- Storing combustible materials underneath a data center raised floor.

Conclusions

Most fires in mission critical facilities can be prevented if common mistakes are avoided and fire detection is properly specified and monitored. Human error plays a large roll in preventing fire hazards and must be eliminated through training and procedures that are enforced.

References

www.fireline.com

www.hygood.co.uk

www.e1.greatlakes.com

About the Author:

Victor Avelar is an Availability Engineer for APC. He is responsible for providing availability consulting and analysis for clients' electrical architectures and data center design. Victor received a Bachelor's degree in Mechanical Engineering from Rensselaer Polytechnic Institute in 1995 and is a member of ASHRAE and the American Society for Quality.