Fire Protection Options for Data Centres

Mark L. Robin, PhD
DuPont Chemicals & Fluoroproducts
mark.l.robin@usa.dupont.com

Introduction

Modern data centres are characterized by spaces filled with ever-increasing numbers of server racks and various types of electronic equipment, and are regarded as mission-critical facilities that must maintain 24 x 365 business continuity. There was a time when temporary business interruptions were a minor and relatively inexpensive inconvenience to the operation of data centres. However, with the increasing reliance of society upon the interconnected global IT infrastructure for much of what we consider everyday life, the loss of data centre service often has a dramatic effect felt far beyond the affected business, impacting clients, suppliers, whole industries, and society at large. Data processing centers store data in the systems memory, and during an interruption only that data which has not yet been placed in permanent memory is lost – but there is much more than just data loss at stake.

The uninterrupted use of computers and electronic equipment in modern data centres is critical. According to a 2013 Ponemon Institute report, the cost of data centre downtime is high - and getting higher. From 2010 to 2013, the average cost per minute of data centre downtime increased 41%, from $5617 per minute in 2010 to $7908 per minute in 2013.

The total cost of downtime is not limited to revenue losses, but can ultimately also include :

- *Productivity Losses*. Numerous users across an organization rely on IT-delivered services and applications and any downtime will greatly reduce their productivity, often resulting in work grinding to a halt.

- *Customer Disruption*. Customers can suffer from disruptions in customer service and support systems, leading to dissatisfied customers who may take their business elsewhere.

- *Reputation Damage*. Disruptions can negatively impact the reputation of the organization, leading to a loss in future sales.

- *Isolation and Repair Costs*. The cost of downtime also includes the costs to find and fix the problem.

from International Fire Buyer, January 2015

- *Loss of Data and Records.*
- *Lawsuits.*

Costs in addition to the loss of revenue can be significant, as seen in Figure 1 which summarizes the cost of a typical data centre outage.

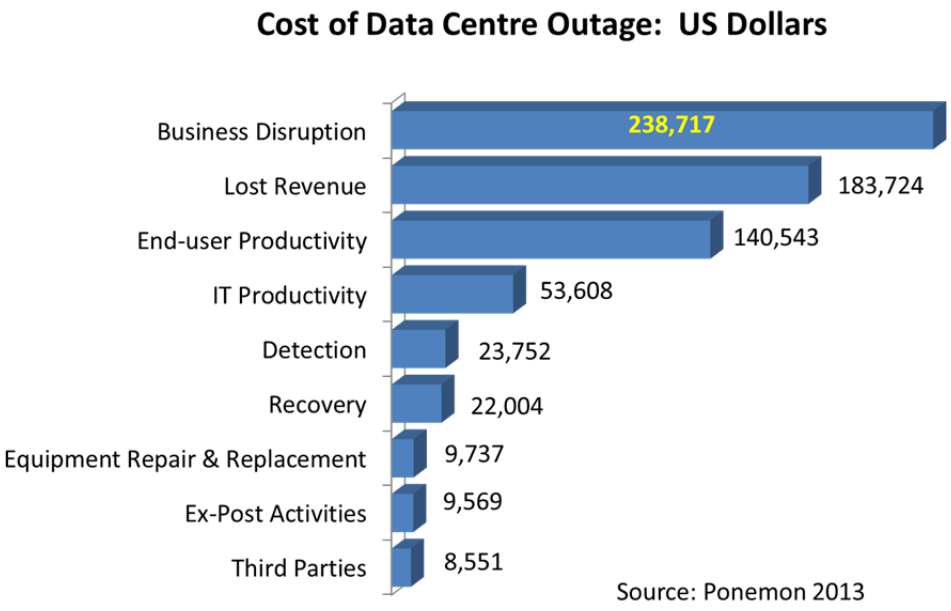

Figure 1. Cost of Data Centre Outages

Fire Protection Options

The high value and sensitivity of the electronic equipment found in modern data centres, combined with the consequences of system interruption, makes fire protection a critical component of any data centre risk assessment. Fires do occur in these types of facilities as evidenced in Table 2, which includes a selection of data centre fires that have been reported within the last several years.

Table 2. Data Centre Fires

Date	Location	Datacenter
2014	Thailand	Cowboyminers
2014	South Korea	Samsung
2014	Argentina	Iron Mountain
2014	USA	Iowa Legislative Building
2013	USA	NSA Spy Center
2012	Canada	Shaw Data Center

A. Water Based Fire Suppression Systems . The primary objective of a sprinkler system is not fire *extinguishment* but fire *control:* confining a fire to its point of origin (preventing fire spread) and controlling ceiling temperatures to prevent structural damage. Sprinkler systems use water, at a typical flow rate of 25 gallons per minute. Water has obvious disadvantages around electronics and electrical systems due to its electrical conductivity. In the event of activation, water damage to the facility and equipment can be substantial, often worse than the fire damage itself, and the cleanup required after sprinkler system activation can be extensive. Sprinkler standards such as NFPA 13 typically require a 30 minute supply of water, and it is common for the two heads nearest the fire to activate – this translates to 1500 gallons of water dumped on the facilities electronic equipment. Sprinkler heads are activated by a thermally sensitive frangible bulb or fusible link which releases water only after the head reaches a preset minimum temperature, usually 135^{o}F or higher. By this time fires are well-developed and considerable direct fire, smoke, and water related damage can be expected (See Figure 2). The extensive cleanup after a sprinkler system discharge, and resulting business interruption, will add to the business cost of a fire. Water is not a three dimensional agent, and cannot readily extinguish hidden or obstructed fires, such as an in-cabinet or in-rack fires. For these reasons, sprinkler systems are best suited for the protection of *structures,* not for the protection of mission-critical assets located within those structures.

Water mist systems are a more recent entrant into the water-based fire suppression arena. Such systems generally require high pressure pumps and special nozzles to distribute a fine water mist into the protected space. Typical delivery rates for water mist systems are on the order of 8 gpm for high pressure water mist systems: a 30 minute discharge from the two closest heads would result in 480 gallons of water dumped on the facilities electronic equipment. Water mist primarily extinguishes via oxygen dilution: steam produced from the mist near the fire displaces oxygen and puts out the fire. Water mist systems perform well on large energetic fires, but have exhibited poor performance on small fires. Water mist, like water, does not fully flood a space and as a result is not suitable for the extinguishment of hidden or obstructed fires, such as an in-cabinet or in-rack fires. While lesser in volume than sprinklers, these systems do leave residual

water following system discharge, necessitating cleanup and added service interruption. Potential water damage to electronics and the incompatibility of water and electricity remain a concern. For these reasons water mist systems, like sprinkler systems, are not recommended for the protection of high value electronic assets and services located within a structure.

Figure 2. Aftermath of pre-action sprinkler activation on an in-cabinet fire

B. Clean Agents. The primary objective of a gaseous clean agent system is to extinguish the fire quickly, limiting fire damage to the object(s) involved in the origin of the fire. Hence, the primary purpose of a gaseous clean agent system is to protect the valuable, sensitive and mission-critical assets within the enclosure. This is clearly fundamentally different from the primary objective of sprinkler systems, as illustrated in Figure 3.

The primary advantages of total flooding clean agents are:

- Clean extinguishment - fires are extinguished without collateral damage due to agent discharge (no residues, no cleanup required
- Rapid extinguishment during early stages of fire growth
- Ability to extinguish shielded, obstructed or three-dimensional fires in complex geometries

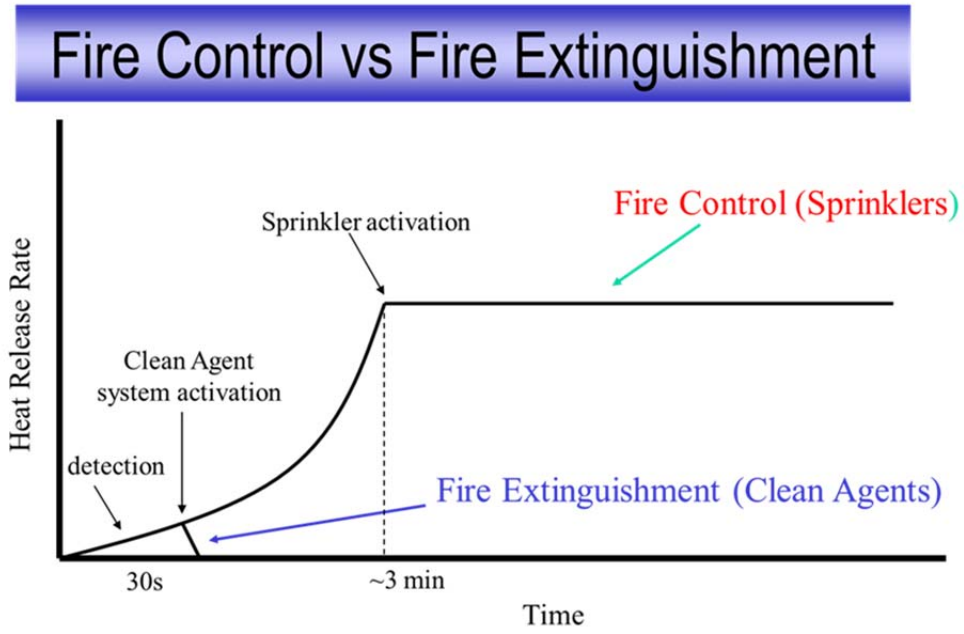

Figure 3. Fire Control vs Fire Extinguishment

Clean agent systems employ a combination of rapid detection and rapid agent discharge, providing extinguishment of fires in their incipient stage, significantly reducing asset damage due to thermal effects or fire combustion products, allowing facilities to quickly return to service after a fire event. Further, clean agents do not leave corrosive or abrasive residues following their use, eliminating the cost and need for cleanup as well as the potential for longer term equipment operational issues. A gaseous clean agent penetrates into hidden or obscured areas and densely packed cabinets and racks . Consequently clean agent systems are ideally suited as the first line of defense to protect electronic equipment in mission critical facilities.

Clean agents can be divided into two classes: halocarbon agents, based on the elements of carbon, hydrogen, and halogen (for example, fluorine) and inert gas agents, based on gases such as nitrogen, argon and carbon dioxide. The two most widely employed total flooding clean agents for data centres are DuPont™ FM-200® and Tyco Inergen® systems. Systems using FM-200® employ HFC-227ea (CF_3CHFCF_3) and extinguish fire primarily through the absorption of heat. Inergen®, a blend of nitrogen, argon and carbon dioxide, extinguishes fire by lowering the oxygen content to below the level required for sustained combustion. Both agents are electrically non-conductive, suitable for the protection of Class A, B and C hazards, and applicable for use in normally occupied areas. Both agents offer optimal safety in use as they are characterized by low chemical reactivity, high material compatibility and low toxicity (e.g., neither agent is metabolized in the body).

The Minimalist Approach to Data Centre Fire Risk Mitigation

In an effort to reduce costs, some facilities choose to provide no fire protection for the mission-critical equipment within their facilities, opting only for the installation of sprinklers. As discussed above, water-based systems are designed to protect the overall structure, not the mission critical assets within the structure. Once a sprinkler system has activated, significant water damage is likely and the resultant business interruption may extend into weeks if not months.

Another minimalist approach to fire protection in mission-critical facilities is to install sprinklers for the protection of the structure and high sensitivity smoke detectors (HSSDs) for asset protection, the theory being that once detected, someone can then find the fire and extinguish it, perhaps with a handheld extinguisher. This approach requires 7x24 manning of the facility, and failure on the part of the operator to find and extinguish the fire could obviously lead to disastrous results impacting both the operator and the facility.

The potential consequences of adopting a minimalist approach to data centre fire protection can be clearly seen in the devastating results of a recent fire at the Shaw data centre in Calgary, Canada, in which the fire suppression system consisted of the minimum protection required by code, i.e., a sprinkler system:

- Knockout out of the primary and backup systems supporting key public services
- Loss of cable, telephone and Internet services by more than 20,000 Shaw business and household clients
- Crippled city services, including 311 emergency services
- Delay of hundreds of surgeries at local hospitals
- ATMs and debit terminals throughout the city affected
- IBM Canada forced to fly backup tapes holding vehicle and property registration data to a backup facility in Markham, Ontario
- Extensive water damage to furniture, walls and sensitive electronic equipment on the floors below the top story fire location
- Temporary relocation of over 900 Shaw employees while damage is repaired
- Six days of service outage

According to media reports, an electrical fire triggered the facility's sprinkler system which ran for more than two hours, soaking furniture, walls and sensitive electronic equipment on floors below. The total cost of the incident is not limited to the costs associated with the above items, but will ultimately also include costs due to loss of data and records, lawsuits and the loss of customer confidence.

from International Fire Buyer, January 2015

The Clean Agent Approach to Data Centre Fire Risk Mitigation

The advantages of clean agent fire protection for mission-critical data centre assets can be seen in the results of a recent fire in the Iowa State Legislature Building in the United States. At approximately 3 PM on February 18, 2014, a transient-voltage surge suppressor (TVSS) located in the basement of the Iowa State Legislature Building failed, resulting in significant damage to the TVSS unit and the production of smoke throughout the room housing the unit. An employee activated a manual release station, discharging over 2,400 pounds of FM-200® clean fire-extinguishing agent into the room and raised floor. Within minutes of receiving the signal from the building's automatic fire alarm system, the local fire department arrived on the scene to find the fire extinguished and personnel already engaged in damage assessment and working to restore operations. By 9 PM the data centre was completely cleared of damaged equipment, and by 2 AM major Iowa government websites and agency systems were restored. By 3AM – 12 hours from the start of the fire – all remaining agency applications were restored. Unlike the Shaw outage, which lasted six full days, the use of a clean agent system resulted in a return to normal operations within a period of 12 hours, with losses limited to direct fire damage.

Ensuring Business Continuity

To ensure business continuity in mission-critical facilities, protection of both the structure and its contents is required. The added cost of installing a clean agent system is justified by its ability to provide what sprinkler systems cannot - protection of the sensitive, expensive and mission-critical assets located within the facility, and the minimization or complete elimination of business interruptions in the event of a fire.

As demonstrated by the recent fire in the Shaw facility in Calgary, opting for minimal fire protection of such critical facilities can lead to devastating results. Sprinkler systems and clean agent systems are fundamentally different in their purpose: sprinkler systems serve to protect the structure, whereas clean agent systems serve to protect the contents of the structure. Substantial risk reduction at very high benefit/cost ratios may be realized by protecting mission-critical facilities - such as data centres - with both a clean agent system and a sprinkler system.

from International Fire Buyer, January 2015