Data Center Fire Protection: A False Sense of Security

Solutions For High Value, Mission Sensitive or Mission Critical Computer Rooms and Local Data Centers

TAMPA, FLORIDA, US, February 16, 2022
/EINPresswire.com/ --


Lloyd Aronoff, Consultant

Historical Risk Analysis

The multiple life safety benefits derived from a professionally designed smoke detection system that is installed in every high value, mission sensitive or mission critical facility, is unchallenged. Traditional data center designs recommended smoke detectors to be mounted under the raised accessible access floor, if applicable, and on the ceilings in all computer rooms. This basic design scenario is a decades old boilerplate industry standard.

Sometimes these smoke detectors, or ASD (Aspirating Smoke Detection) sampling points when cross zoned and when activated, are mated to a state-of-the-art fire suppression system. The usual suppression specifications are designed to extinguish a fire with an approved suppression agent, mathematically designed and discharged from within the calculated cubic area of the computer room.

> “Innovation is the only way to win.”
>
> *Steve Jobs*

The historical basic need for the electronic detection of particles of combustion, or smoke, in an almost sterile computer room, is driven by two basic factors:

1) Code Driven: To protect human lives and facility property by providing an “early warning” notification system, signaling the occupants to evacuate the building immediately because of the detection of smoke or an in-progress fire.

2) Convenience Driven: The blame game starts. If the computer room or data center stops functioning, the loss of revenue because of a technical disruption is enormous. The facilities insurance companies have a huge financial interest to find technical faults of a specific computer systems chassis, or line voltage conduit system, or cooling systems that failed, reviewing historical logs of real alarms vs. false alarms, or discovering simple operator errors.

This includes conducting a detailed forensic investigation starting with the original detection system design, installation, sub-contractors, scheduled inspection reports, preventative maintenance measures or operator training errors, all searching for faults.

The “Economic Loss” Paper Trail

Who will compensate the facility for the loss of revenue? A reason, a fault or a discrepancy must be discovered that caused a computer room or data center to shut down as the result of any incident. Any loss of revenue as the result of the initial incident and future potential revenue streams has both legal and subsequently financial consequences. The facility stockholders require answers from facility management. The subsequent discovery and litigation efforts is usually time consuming and economically exhausting.

The key word in this analysis is "early warning". The issue is how much time is really considered to be early. When does the damage clock start to tick: When micro-arcing starts, when actual arcing of line voltage powered conductors starts, when coils are starting to overheat? When plug-in connectors become loose and arc? When terminal strips loosen from constant heating and subsequent cooling? When plastic insulation on conductors starts to melt? Or when drive bearings overheat or when enough particles of combustion are produced with a large enough quality and density that a detection system analyses an abnormal level of particles of combustion and activates the Fire Alarm system and possibly, the suppression system.

The evidential damage financial loss clock will be forensically documented, and subsequent economic damage assessment will be calculated from the initial time of the incident.

"A False Sense of Security" Ends in a Realtime Incident continues.....To continue readings about "False Sense of Security" issues in data centers and computer rooms, please follow: https://www.tampabaynewswire.com/2022/02/10/data-center-fire-protection-a-false-sense-of-security-105482

ABOUT STERLING LANGLEY LLC
After 35 years in the Life Safety Systems industry, Lloyd Aronoff established Sterling Langley LLC. As an Open Innovation Product Developer, the company is motivated to uncover hidden value in a manufacturers existing investment of electro/mechanical products and create new innovative peripheral devices. All too often, a manufacturers R&D staff have been reduced or eliminated for corporate economic survival. Subsequently, brand new innovative product market share erosion may be recognized too late to economically adjust to competitive market demands.

“Designer-At-Risk” is an exclusive industrial engineering business model designed by Lloyd Aronoff. Sterling Langley LLC is compensated only if the client agrees with their creativity, ideas and intellectual property that includes new features, new functions, and new benefits, for their clients’ own commercialization.

Additional information about "Creating Value Through Innovation" can be found by visiting: https://www.sterlinglangleyllc.com Lloyd Aronoff can be reached at laronoff@sterlinglangleyllc.com or (954)-980-9074.
# # #

Lloyd Aronoff
Sterling Langley LLC
+1 954-980-9074
laronoff@sterlinglangleyllc.com
