White paper

Ten ways to ensure the safety of data center employees

The data centers of today are far bigger and consume more energy than could have been imagined just a few short years ago. Size-for-size, today's data centers use approximately 30 times the power needed to run the average office building. In total that's about 80 million megawatt hours of electricity a year, which provides ample opportunities for danger.

The consequences of an electrical event in a data center can be dire. Some studies estimate the minimum cost of an electrical accident at $750,000. Other consequences include an OSHA investigation, protracted legal proceedings and most tragically and significantly, the loss of human life.

Today's data center owners and operators face a delicate balancing act. They must walk a fine line between ensuring the safety of personnel, facilities and equipment while maintaining 24/7/365 availability of mission critical systems. The two need not be—and, indeed, cannot be—mutually exclusive.

There are steps the data center operator can take from a product, system and policy standpoint to minimize employee risk. Here are 10 activities to help improve the safety of data center employees.

#1. Develop and embrace a culture of safety

Because of the vast amounts of power consumed by data centers, safety cannot be a part-time job, a far-off department or a mere box on an organizational chart. Instead, safety needs to be an ongoing, transparent management commitment and a way of doing business. Successful, safety oriented data centers are ones that create a culture and thought process dedicated to safe working practices and that affect everything done within the data center walls.

Ideally, each data center should have a dedicated "safety czar." This should be an executive-level position—preferably staffed by someone with an electrical engineering background—who is responsible for all safety activities, including establishing and communicating clear, easy-to-understand policies; developing rigorous training programs; investigating and acquiring high-quality safety equipment; conducting periodic audits and inspections; and continually monitoring and actively complying with changing safety standards and practices.

#2. Understand the relevant standards

Accidents involving electricity have taken place since the beginning of its use. But data centers are comparatively new concepts. And because most data centers are more the domain of IT professionals than electrical engineers, the act of maintaining power systems is typically not in the comfort zone of most data center staff.

For that reason, data center operators should understand and follow the critical safety standards for facilities that allow employees to work on electrical equipment. These standards include:

- NFPA 70 edition 2002: National Electrical Code.
- NFPA 70E edition 2000: Standard for Electrical Safety Requirements for Employee Workplaces.

– IEEE Standard edition 1584-2002: Guide for Performing Arc Flash Hazard Calculations.
– OSHA 29 Code of Federal Regulations (CFR) Part 1910 Subpart S.

In addition, OSHA requires that facilities strictly adhere to a six-point plan to minimize and protect workers from arc flash incidents:
– Provide and be able to demonstrate a safety program with defined responsibilities.
– Calculate the degree of arc flash hazard.
– Use correct personal protective equipment (PPE) for workers.
– Train workers on the hazards of arc flash.
– Use appropriate tools for safe working.
– Provide warning labels on equipment.

Of particular interest to data center operators should be two particular sections of the OSHA standard, usually referred to as "lockout/tagout" procedures. The standard for The Control of Hazardous Energy (Lockout/Tagout), OSHA 29 Code of Federal Regulations Part 1910.147, provides clear practices and procedures for disabling machinery or equipment to prevent the release of hazardous energy while employees perform service and maintenance activities. The standard outlines measures for controlling hazardous energies, including electrical, mechanical, hydraulic, pneumatic, chemical, thermal and other energy sources.

In addition, OSHA Title 29 Code of Federal Regulations (CFR) Part 1910.147 outlines requirements that must be met to protect employees who work on electric circuits and equipment. This section requires workers to use safe work practices, including lockout and tagout procedures. These provisions apply when employees are exposed to electrical hazards while working on, near or with conductors or systems that use electric energy.

Data center operators must clearly understand and abide by these standards. According to OSHA, compliance with these standards prevents an estimated 120 fatalities and 50,000 injuries each year.

#3. Observe safe working practices
For all data centers observing standards and ensuring worker safety should begin before the facility is even constructed. A critical part of complying with electrical safety standards is that an arc flash hazard analysis be completed for the facility's electrical distribution system. This analysis is a complex engineering study usually made up of three parts: a short circuit study, a protective device time-current coordination study and the arc flash-hazard analysis itself.
The analysis provides a detailed assessment of the potential energy at each point in the system that would be released in the event of an arcing fault within the equipment. Based on this analysis, the data center operator can determine the degree of the hazard and the appropriate personal protective equipment (PPE) employees must employ.

#4. Have the right PPE equipment for the job
PPE equipment is the last line of defense against injury or death due to an arc flash event. PPE includes cotton and flame-resistant (FR) clothing, voltage-rated gloves, hard hats with full face shields, full-coverage flash suits and insulated blankets. PPE is necessary whenever a worker crosses the Flash Protection Boundary, but the type and amount of PPE required varies with the hazard.

Determining the appropriate level of PPE is based on the risk anticipated. Too little PPE exposes a worker to potentially lethal injury or death. Too much PPE can be bulky and may restrict vision and movement, which increases work time and difficulty and the chance of an accident. NFPA 70E Table 130.7(C)(1)(a) discusses the appropriate PPE for use in all cases.

#5. Use informative warning labels
All equipment that may be subject to arc flash must carry warning labels. It is important to understand that the responsibility for marking the equipment lies with the data center operator, not the equipment manufacturer or installer. For maximum protection, arc flash warning labels should carry additional information beyond what is required by law.
A sticker that reads "Danger. High Voltage," while in compliance with standards, is nevertheless too generic and is likely to be ignored. By providing more information on the sticker, workers have the information they need to make informed choices for safety procedures. Many organizations choose to label equipment with the specific values determined in the flash hazard analysis. The current standards do not require labeling the equipment with these values, but it is a good practice for workplace safety.

#6. Understand and observe safe working areas
Arc flash boundaries are required around data center electrical equipment such as switchboards, panelboards, industrial control panels, motor control centers and similar equipment when an individual works on or in the proximity of exposed energized components. Activities that are subject to arc flash boundaries include examining, adjusting, servicing, maintaining or troubleshooting equipment.

Specific boundaries include:
– Flash protection boundary. An approach limit at a distance from exposed live parts within which a worker could receive a second-degree burn if an electric arc flash were to occur. Workers who enter the flash protection region must be outfitted in the appropriate PPE.
– Limited approach boundary. An approach limit at a distance from an exposed live part within which a shock hazard exists. A person crossing this boundary and entering the limited region must be qualified to perform the job or task.
– Restricted approach boundary. An approach limit at a distance from an exposed live part within which there is an increased risk of shock, due to electrical arc combined with inadvertent movement, for personnel working in close proximity to the live part. The person crossing this approach boundary and entering the restricted space must have

a documented work plan approved by authorized management and wear the right PPE for the work being performed and the voltage and energy level involved.
- Prohibited approach boundary. An approach limit at a distance from an exposed live part within which work is considered the same as making contact with the live part. The person entering the prohibited space must have the proper training to work on energized conductors or live parts. Tools used in this space must be rated for direct contact at the voltage and energy level involved.

#7. Beware of Electrocution

The most obvious and commonly understood danger to data center personnel is electrical shock, or electrocution. To receive a shock, the worker needs to physically touch an energized surface, such as a terminal or bus bar, and becomes part of electrical path. The current flows through the body, causing injury or death.

The keys to avoiding electrocution are relatively straightforward. Employees must strictly follow OSHA guidelines for wearing the correct protective clothing and unplug or otherwise de-energize live equipment before working on or near it.

To further mitigate the risk of electrical shock, today's data centers are increasingly built with low- and medium-voltage touch-safe panelboards, breakers, switches and other devices that are double insulated and help prevent worker exposure to live parts. This allows employees to maintain them without the risk of electrocution and without the need to de-energize large portions of the data center.

#8. Understand the risk of arc flash incidents

Arc flashes represent perhaps the gravest danger to data center employees. As multi-megawatt facilities, data centers are prime candidates for arc-flash events, which can cause substantial damage, fire, injury or death. Arc flashes strike anywhere from five to 10 times a day across the U.S. alone, with about 20% occurring in motor control centers and switchgear and another 18% taking place in custom control panels.

Only in the last 20 to 30 years have the dangers of electric arc been fully understood. The existence and associated danger posed by arc flashes came to the forefront in 1985 in a paper, "The Other Electrical Hazard: Electric Arc Blast Burns," by Ralph Lee, which was published in the IEEE Transactions on Industrial Applications.

The National Fire Protection Association (NFPA) defines an arc flash as "a dangerous condition associated with the release of energy caused by an electric arc." The degree of hazard to workers is related to the available short circuit current in the circuit and the arc duration.

Arcs occur when electric current flows between two or more separated, energized conducting surfaces. Arc flash causes range from operator error such as a tool slipping or by touching a test probe to the wrong surface, to equipment failure, to simply operating a breaker. When an arc is created, the surrounding atmosphere is suddenly heated to an intense temperature of up to 20,000 degrees K and plasma is generated. Conductors are vaporized and metal changes state from solid to gas. This expansion also creates an explosive pressure wave that can reach pressures of 500 pounds per square inch, is powerful enough to shear off 3/8" bolts and blow apart entire substations. It even generates enough force to compress a person's chest to kill without burning.

Electric arc burns make up a substantial portion of the injuries from electrical malfunctions. The scorchingly high temperatures unleashed by arcs can reach 35,000 degrees F, nearly four times that of the surface of the sun. The result can be fatal burns at up to about five feet and significant burns at up to 10 feet.

The fireball generated by the arc flash travels at 5,000 feet per second and contains metal droplets and copper vapor that act as shrapnel and injure not only the worker but also nearby people. The intense light produced by the arc can temporarily and sometimes even permanently blind or cause eye damage to people. Sound levels can reach a deafening 160 dB—compared to a typical rock concert at 115dB—and can result in permanent hearing loss.

"An arc flash is just like a grenade going off," says Mietek Glinkowski, Director of Technology at ABB. "Just like a grenade, you don't have to be in physical contact with it; you just need to be close enough to be injured or killed. It's amazing to me that some people still don't understand or appreciate this danger."

In addition to the potential for injuries and loss of life, arc flashes can also destroy equipment, causing extensive downtime and requiring expensive replacement and repair. They can also ignite nearby flammable materials, resulting in secondary fires that can destroy entire facilities.

#9. Use products that protect against arc flashes

The immense amount of power available at a data center's switchgear and motor control centers poses an ideal opportunity for arc flash occurrences. Today's data centers are increasingly embracing products that guard against arc flash events in one of two ways: by containing its energy or by quickly cutting off the source of the arc event.

Products that offer passive protection against arc flash

Products that offer passive protection against arc faults attempt to limit the arc flash to its area of occurrence, thus minimizing damage to equipment and people. Many data centers are installing arc-resistant switchgear, which is designed to reduce the potential of employee injury and equipment damage. In the case of an arc fault, this equipment routes the expanding hot gases through a system of vents and flaps away from workers at the front, rear and sides of the switchgear.

The switchgear doors, walls, and panels are reinforced and sealed to withstand the temporary pressure surge until relief vents and flaps operate. This design helps ensure that damage is contained in the compartment of fault origination, rather than spreading to adjacent compartments.

Products that offer active protection against arc flash

Products that offer active protection against arc faults seek to reduce or eliminate the energy of the arc flash itself. These products are designed to quickly detect the enormous and nearly instantaneous increase in light intensity—up to several thousand times normal ambient lighting levels—that accompanies an arc flash fault, and then act to limit its arcing time.

Arc flash detection products are capable of issuing a trip signal in as little as 2.5 milliseconds after initiation of the arcing fault. One such product is a low-voltage detection and relay system that detects the flash using a fiber optic sensor, quickly processes that signal and sends a trip or disconnect signal to kill the arc.

Another type of product combines several components, including detection and release electronics and corresponding primary switching elements, which initiate a parallel three-phase short-circuit to earth in the event of an arcing fault. The extremely short switching time of the primary switching element, often less than 1.5 milliseconds, along with the rapid and reliable detection of overcurrent and light, ensures that an arc fault is extinguished (shunted) almost immediately after it arises. This solution enables switchgear to achieve the highest possible level of protection for both workers and equipment.

Products that perform remote monitoring

In addition to using products that offer protection against arc flashes, many companies employ products that remotely monitor and diagnose electrical equipment. This limits direct employee exposure to equipment and reduces the hazard of exposure to an arc flash incident.

These monitoring products take many forms, ranging from small, equipment-specific ones such as remote temperature sensors for power buses to centralized systems, such as ABB's DecathlonTM DCEM solution, which monitor virtually all data center functions. The latter often feature interlocks or lockouts that prevent workers from operating a potentially unsafe device or provide alternate control methods to ensure safe operation while maintaining uptime.

#10. Don't be complacent

When it comes to ensuring the safety of data center employees, no amount of regulations, standards or safety czars can replace basic common sense. "Whenever you have human beings working on a piece of electrical equipment, there's always an inherent risk," Glinkowski says. "That's why we have standards, and that's why the standards need to be followed to the letter. But do not be complacent."

Indeed, perhaps the biggest risk in a data center environment may well be the false sense of security that comes from routinely and successfully performing maintenance procedures. That sense of security can turn into complacency—which must be avoided. "Treat every task as if it were energized and dangerous," Glinkowski advises. "Never assume that something is disconnected and grounded just because someone said it was. Double check to make sure it is. And most of all, never deviate from the standards."

Conclusion

Electrical events in data centers can be catastrophic, resulting in loss of life, OSHA investigations, protracted legal proceedings and millions in costs. Today's data center owners and operators need to ensure the safety of personnel, facilities and equipment while simultaneously maintaining 24/7/365 availability of mission critical systems.

Data center operators must implement products, systems and policies to minimize employee risk. This begins with embracing a culture of safety and understanding and observing the standards—such as NFPA 70 edition 2002, NFPA 70E edition 2000, IEEE Standard edition 1584-2002 and OSHA 29 Code of Federal Regulations—for facilities that allow employees to work on electrical equipment. As such, operators must ensure that employees observe safe working practices, have the right PPE equipment for the tasks at hand, use informative equipment warning labels and understand and observe safe working areas.

Operators must also be keenly aware of the risks of arc flashes, which strike from five to 10 times a day across the U.S. alone and represent perhaps the gravest danger to data center employees. To protect against such events, they should embrace products that offer both active and passive protection against arc flashes.

Finally, all data center employees must understand the inherent risks of working on electrical equipment and exercise maximum caution and common sense when doing so.

ABB Data Centers
125 East County Line Road
Warminster, Pennsylvania, U.S.A.
Phone: +1 800 HELP 365

www.abb.com/datacenters

9AKK105408A8196