Data center safety:
More power means more risk mitigation

As data centers grow larger and more sophisticated, so too do the electrical systems that power them.

In fact, electrical systems at many data centers are less like their predecessors of five or 10 years ago than they are like the systems that run heavy industrial operations. They now include not only low- and medium-voltage (15-38 kV) subsystems, but increasingly incorporate higher-voltage components as well. They deliver more power, flexibility and reliability than older systems, but they also require industrial-strength safety solutions that are new to many data center operators.

"Large IT companies that are in the business of running data centers know this. They have dedicated departments dealing only with infrastructure – power infrastructure being one of them. They manage the electrical system more like the industrial environment," offers Mietek Glinkowski, Global Head of Technology for Data Centers at ABB. But at the next level – data centers that operate in support of another kind of business – he observers "there may be need for further education on this topic."

The IT-centric culture of data centers is more focused on servers and networks than electrical power infrastructure, he notes. "You can have extremely knowledgeable people walking down the aisles of these facilities without a full understanding the nature of the electrical hardware around them."

The essential risk in electrical equipment at any voltage level is a short circuit – simply the flow of current along an unintended path. As voltage levels increase, the strength and consequence of a short circuit increases too. An explosive arc flash presents some level of risk at any time equipment is charged, but it's a particular concern at specific moments:

- When it is being powered up;
- When it is being powered down;
- When a panel or enclosure is opened for maintenance.

An arc flash can generate temperatures in excess of 30,000 degrees (F), vaporizing its conductors and causing an explosion that rains plasma and molten metal. It ruins the piece of equipment. If uncontained, it can kill or injure nearby workers. It also can damage other nearby equipment, causing extended downtime and costly repair.

There are a handful of strategies to manage the inherent risk in operating and maintaining a powerful electrical system. Generally all these strategies are applied in some combination.

System integration

Integration of electrical systems with the Data Center Infrastructure Management (DCIM) system used to automate data center operations is the most comprehensive approach to risk mitigation and safety. Until recently, true integration wasn't possible. Electrical components could be hard-wired to provide specific data to system operators, but creating such inputs is costly, complex and didn't always provide the sought-after level of transparency and control.

This means every problem that arises during operations requires at least two solutions – one for the systems managed through DCIM and one for the electrical controls. While these solutions must combine to resolve whatever need has arisen, any positive result is largely attributable to the wits and know-how of the people who run them.

One ABB expert discussing the similar situation in an industrial setting describes it as "institutionalized crisis management."

Now, however, due to the rise of open standards for communication between electrical components, technology exists to provide true integration – allowing electrical systems to be managed right along with every other data center system. ABB's Decathlon DCIM system is among the first to offer this capability; it can use data from electrical components to understand and respond to state changes as capably as it does with asset management and HVAC, to name just two.

Such integration is a big deal, according to Mark Reed, Director of the Data Center Initiative at ABB. It allows the entire data center to be managed from a single interface, using a unified stream of data. This allows for improvements in efficiency, flexibility, reliability, cost control and – of course – risk mitigation.

For example, it provides remote diagnostic capability of breakers and switchgear. "Instead of having to go into the electrical room and expose yourself to the panels, you do can do that work remotely through your control system," Reed says.

As another example, it's standard practice to mechanically lock out electrical system components before opening them for maintenance. But when the electrical system is integrated with the DCIM, "you can do a lockout on the control system in addition to the mechanical one. This keeps all system operators informed and updated." If the locked out components will affect other operations – such as reducing HVAC capacity – the system can quickly compensate.

Just the act of powering up or down an electrical system puts stress on equipment that can cause faults and shorten equipment life. An integrated electrical system allows such procedures to be programmed and coordinated with other data center subsystems to prevent faults, lengthen equipment life, and avoid other unintended consequences from cascading through the data center.

As an example, Reed points to management of the HVAC system.

"Maybe you're having trouble with one section of your HVAC; you'd lock it out mechanically and electrically before working on it," Reed suggests. "By also being able to lock it out with the operating system, you can automatically reduce demand on the specific servers that might require the extra cooling or, just as important, that might tax the electrical system while part of it is shut down."

Modeling and alarm management are other areas where integration provides risk mitigation for workers and equipment. For example, when new control loops are programmed, they can be modeled and validated in the DCIM

before being rolled into operations – where small coding errors can lead to major downtime and damage.

And by wrapping the electrical system in with the DCIM's alarm management capabilities, operators can respond more quickly and effectively without having to train on multiple interfaces and systems.

"If you don't have moment-to-moment understanding of what's occurring in your electrical system, you really can't manage the entire data center at a strategic level," Reed says. "That was a limitation we all simply had to accept. But not any more. The ability to achieve true integration changes the way you can address everything in the data center – beginning with fundamental safety."

Fault reduction

While integration provides a systems management approach to safety, fault reduction puts the power of automation at the place where short circuits are most likely to occur.

At its heart is advanced power electronics technology – essentially smart devices that replace simple on/off controls throughout the electrical system. This allows devices to adjust quickly and incrementally to changing conditions in order to prevent circuits from overloading and faulting.

Widely used in industrial applications, such as drives and motion controls, power electronics are now also being applied in wind, solar and other power-conversion applications to "dial down" sudden surges in power, according to ABB's Glinkowski. And data centers are beginning to use them as well.

"It's an emerging capability that offers a new paradigm in terms of managing the power and the impact of power in data centers from the point of view of safety," he says. "It brings controllability half-cycle by half-cycle" in such devices as power converters, inverters, rectifiers and – most commonly – uninterruptible power supplies. "They finish their work before a human could even know something was happening," he says. "They do more than limit damage from a fault; they improve reliability by preventing the fault in the first place."

While use of power electronics is new in the role of data center safety, Glinkowski points out that it's consistent with an industry cycle of refreshing IT infrastructure every two to five years. "The power infrastructure needs to be modified to keep up with IT," he says. "Adding power electronics to protect sensitive IT assets is simply good practice."

Current reduction

Another approach to mitigating risk from electrical faults is to reduce the current moving through equipment – putting less stress on systems and reducing the intensity of any potential fault. This can be done both passively and actively.

"At the top level, it can be achieved by selecting different topologies in data center electrical systems," Glinkowski says. "For instance, if you want to deliver 20 MW of power, you can design a system that will instead provide two separate flows of 10 MW each, therefore reducing short-circuit current."

System components also contribute. For example, installation of high-impedance transformers can reduce fault current levels by 20 or 30 percent.

These solutions are passive – offering design that has inherently lower risk. Fault current limiters provide active current reduction in medium-voltage applications. They work through the use of superconductors that, when overloaded, convert to regular conductors – thus reducing current output. A new class of device, fault current limiters are capable of responding during the first current rise – less than a millisecond – which is usually quickly enough to prevent a fault of any kind. Glinkowski says they can be retrofitted into existing systems based on analysis to identify areas of elevated risk.

Containment

Integration, fault reduction and current reduction all seek to prevent events from occurring. The return on investment for these technologies is measured in increased reliability and reduction of downtime.

But even with those safety strategies in place, efforts need to be made to contain the impact if an event does occur.

Containment essentially puts a box around electrically charged equipment, so in the case of an arc flash, nobody gets hurt and nothing else gets damaged.

While such enclosures have long been standard, the moment when a worker needs to open a panel to maintain it has always been an instant of high risk.

Now certain types of equipment such as switchgear are being built with arc-resistant designs. Some, for example, use plug-in electrical modules, like Lego – meaning they never have to be opened while charged. To maintain or replace them, the module is pulled out, which essentially unplugs it. After it has been properly discharged, it can be opened and repaired. And then, once closed, it is racked in again. So there is no instance when a person is exposed to an open panel containing electrically charged equipment.

Such design doesn't mitigate the risk of incident, Glinkowski emphasizes. But it does contain damage while going a long way to reduce the potential for injury.

Personal protective equipment

Safety regulations stipulate appropriate personal protective equipment (PPE) that must be worn when working on or around electrical equipment. While a mandatory first step in any risk management effort, it is really only a last resort and is the least effective form of risk mitigation. It builds a protective barrier between workers and charged equipment, but it doesn't reduce the likelihood or severity of a damaging fault. Further, cumbersome Level 3 and Level 4 PPE can slow down the work, which is costly and increases the time of exposure to the hazard.

Contact us

For more information please contact:

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

www.abb.com

9AKK105713A8947

Power and productivity
for a better world™