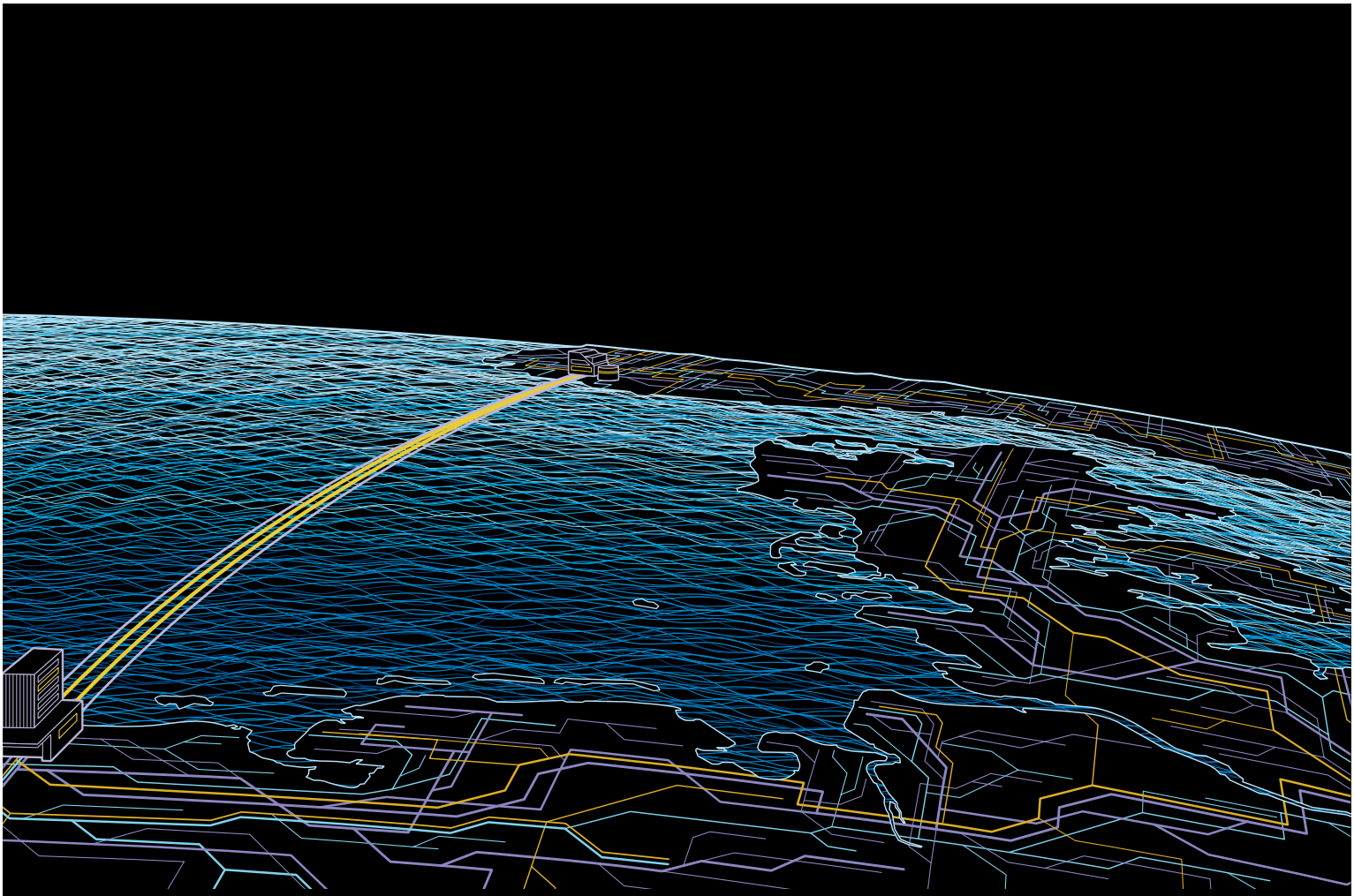


ABB white paper

Industrial-strength solutions to reduce risk in the data center

Power and productivity
for a better world™

Data centers are unlike any other operation. They look and act like administrative support offices, managing sophisticated IT assets to keep information moving in government and military functions. But unlike administrative support offices, they can't afford mistakes, and they can never close. As a result, identifying and managing risk is a critical task.

A major source of disruption and downtime in data centers is human error. And their largest safety hazard is in the increasing size of the electrical systems that power them. Both of these risks can be addressed at two important levels: design of the center and its critical systems and the improvement of day-to-day operations.

As government and military data center managers look to manage risk and safety in these areas, they will also find meaningful opportunities to improve reliability. They will find automation solutions that reduce error-prone human intervention. And they will find electrification technologies that reduce hazards and disruptions.

The systems used to manage data centers have largely evolved out of building management systems that run office facilities. Today, however, the power consumption of data centers and their need for finely honed performance is closer to the profile of industrial facilities, which often must manage unstable processes involving extraordinary amounts of power on a 24/7-basis.

That's why public-sector data centers are now looking to solutions developed in the industrial arena to address their most perplexing challenges and greatest risks.

Managing risk in the data center can be compared with managing quality in manufacturing. Here's why: For most of the 20th century, quality assurance meant placing an inspector at the end of a production line or process to identify and discard defects. But the Total Quality Manufacturing (TQM) movement of the 1980s offered this revolutionary premise: Building quality into each portion of the manufacturing process. This has a twofold benefit:

1. It eliminates defects at the end of the line; and
2. It reduces waste and improves the efficiency of processes.

TQM was so successful that it's all but disappeared as a distinct discipline; it's just how business is now done.

Today a similar revolution is taking place around managing risk in the data center. Technology now exists to build reliability into the very infrastructure of the data center — not just the IT assets, but also the environmental systems, electrical network, security and safety processes, and the controls that manage them.

This is an important advance for at least three reasons:

1. Reliability. Downtime in a data center can incapacitate an entire department, building or military site, and in some cases is even a matter of national security. And because of the sensitive equipment at the heart of any data center, tolerances for such variables as climate control and electrical power quality add complexity to the job of maintaining smooth operations at all times.

2. Availability. Data centers — particularly those in Tiers 3 or 4 of the ANSI/TIA 942 Uptime standard — cannot afford to take systems offline for emergencies or even for routine and scheduled maintenance. So cost-effective redundancy must be built in.

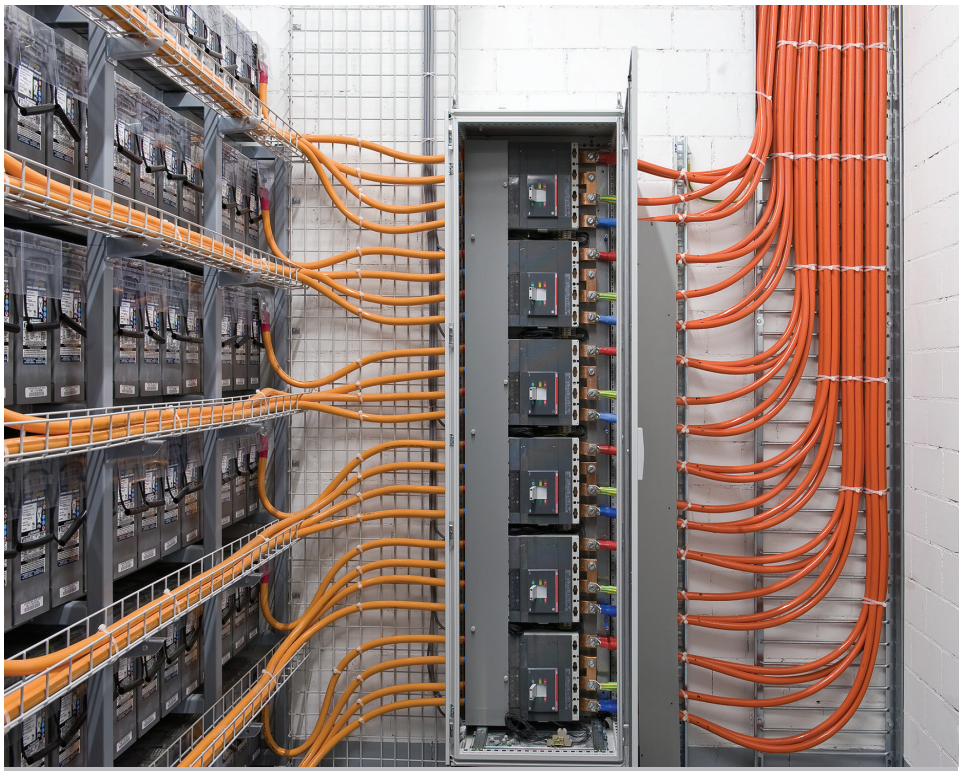
3. Safety. Data centers operate in a more hazardous climate than other back-office operations. On-site electrical substations, along with the presence of power-distribution equipment throughout, put people and millions of dollars in capital assets in close proximity to high- and medium-voltage installations.

These characteristics are unlike any other office setting. In fact, they are more like the profile of large industrial facilities, where variable processes involving extraordinary amounts of power must be maintained around the clock.

For the past decade, the industrial sector has been building reliability into the core of operations in the same way it implemented TQM during the 1980s. It is achieving unparalleled uptime and improvements in risk management.

Data centers have the same opportunities, with the biggest potential gains residing in areas that don't generally receive primary consideration: control systems and electrical systems.

Nothing has a bigger impact on reducing the risk of human error than the automation capabilities of the control system.



Control system strategies

A primary source of disruption in the data center is people. In fact, in the 2010 *National Survey on Data Center Outages*, the Ponemon Institute reported 51 percent of all outages involved human error as a root cause, and 80 percent of respondents in the survey noted some or all of these outages could have been prevented.

Nothing has a bigger impact on reducing the risk of human error than the automation capabilities of the control system.

Nothing has a bigger impact on reducing the risk of human error and heading off unplanned outages than the automation capabilities of the control system. Built-in monitoring and intelligence can identify problems, apply solutions and otherwise handle a vast array of tasks that require speed and timing. That's the promise of Data Center Information Management (DCIM). But what passes for such a system in many data centers may offer very little in the way of true automation — and a lot in the way of room for error.

The goal of DCIM is to integrate all critical systems: energy management; power and load management; building management and environmental systems; and asset management and server optimization. Being able to monitor the status of all these areas in a single interface is only a first step.

Developing a control system that also reduces human input is a bigger job. It takes more planning and may incur more capital expense than upgrading specific devices and equipment. But it can provide the most dramatic impact on reliability and safety over time, while reducing day-to-day operating costs that grow over the system's lifetime. And nothing can do more to reduce the human element of risk than a properly designed — and well-used — control system.

Like industrial facilities, not all data centers are the same. There are four standardized tiers of data centers, defined by their desired level of reliability. But developing appropriate risk management solutions isn't standardized. There is no cafeteria-style plan allowing players in each tier to select from a predetermined set of solutions. Each center's risk must be managed individually.

In the industrial environment, control platforms exist that allow flexibility to build appropriately scaled solutions on a common platform, and the same opportunity exists for data centers, providing flexibility to increase reliability objectives as requirements change. Typical ROI on such systems can range from 12 to 18 months, with benefits accruing for a decade or more.

Following are some key areas where advanced automation can improve reliability and safety.

Improved security

The first level at which the control system can reduce risk is through improved security to prevent accidental misuse as well as malicious tampering.

A DCIM with user-specific levels of access can be easily customized to assure that users have access only to the system functions for which they have been approved and trained.

This obviously helps to protect against malicious use. But from a perspective of risk management, there are other more prosaic issues. Good security also protects against people who, with the best intentions, get in over their heads. For instance, with high-voltage power equipment in and around the facility it is important that only people trained to manage such equipment have access to manage it.

Paired with controls developed and hardened in the punishing industrial setting, a robust DCIM can provide the ability to create and change user-based permissions on the fly to provide anti-tamper security, as well as accidental disruptions and injuries from unauthorized use.

An example of this function in practice is to allow all operators to monitor certain control loops while only specific operators can actually manage them. In another example, a supervisor's approval might be required before certain operator requests are allowed to take effect. Such levels of security require configuration capabilities down to the control loop level — a function that has obvious value in the increasingly sensitive data center environment.

> 51 percent of all outages involved human error as a root cause

Alarm management

The job of alarm management is to get to the root of an emerging problem as quickly as possible. In an environment where multiple systems are at work, that in itself can be a complex process, which is why alarm management is subject to a handful of industry standards. A first level to risk mitigation is to ensure that the center's DCIM system supports these standards.

As an example, when any kind of crisis occurs, operators may be overwhelmed with dozens of alarms, all demanding immediate attention.

Some of these may be critical while others may be a low-priority byproduct of the crisis. Effective alarm management does more than list everything that's going wrong; it helps operators to quickly understand the root cause of the problem, bringing high-priority issues to the top and even suppressing other alarms until there are no higher priorities to be addressed. Compliance with alarm management standards implements established protocols for dealing with these and other complexities, and demonstrates the organization's commitment to safety.

Typical symptoms of a sub-par alarm management system include:

- alarms that operators learn to ignore;
- critical alarms that are obscured by lower-priority notifications;
- missing alarms due to a lack of integration of some systems and components

In chemical production and other process industries, where sudden changes in process states can result in disaster, the

science of alarm management has been tested and refined over several generations of technology. Today, data centers are utilizing capital technology that carries enough risk to warrant application of such robust systems.

Improving alarm management will address these symptoms to provide the following benefits:

- Faster identification and response to operating issues as they arise;
- Fewer critical issues that result in disruption or downtime;
- Reduction in downtime when disruption does occur;
- Potential reduction in human resource costs due to simplified monitoring and response requirements;
- Improved compliance recording;
- Improved analytic capabilities

For Tier 1 or 2 data centers, where system redundancy is limited and round-the-clock onsite monitoring may not occur, advanced alarm management also can provide new levels of remote notification and response that go well beyond standard capabilities of sending e-mails and text messages to designated managers.

As an example, ABB operates a Remote Operations Center staffed to support site personnel. Critical alarms can be sent automatically by the Decathlon DCIM to the center's experts who are trained to quickly diagnose and resolve faults.

Condition-based maintenance

Preventive maintenance is the enemy of reliability. When all equipment is maintained according to the calendar, it means high-performing equipment gets the same attention as equipment that may be nearing failure. As a result, service time and replacement parts are wasted on equipment that is running well while equipment needing attention may not get it in time. In contrast, condition-based maintenance, sometimes referred to as predictive maintenance, allows data centers to spend their resources only on equipment when it requires attention.

Use of smart devices

Achieving the level of efficiency promised by condition-based maintenance requires investment in smart devices with the ability to report performance data as well as the integration of those devices with the control system. When any device begins to operate outside normal performance parameters, the control system signals an appropriate alarm.

As an example, a fan drawing more current than specified may indicate a clogged filter or a worn bearing. Such condition-based monitoring allows fast response to changing conditions without the high cost and unneeded disruption of preventive maintenance.

In another example, the flow of fluids through many cooling systems is measured with simple turbine meters, devices that are inexpensive to build into new equipment, but which require high maintenance and frequent repairs. When they need to be replaced, more advanced meters, such as electromagnetic flow meters, offer some distinct advantages. While more costly to install, such meters run for years with little or no maintenance and automatically report when they are out of calibration.

Achieving the level of efficiency promised by condition-based maintenance requires investment in smart devices with the ability to report performance data as well as the integration of those devices with the control system.

Computerized Maintenance Management

Computerized Maintenance Management (CMM) systems automate the process of scheduling maintenance work. They can identify replacement parts that need to be ordered, list training requirements and certifications needed by the person who will conduct the repair, and notify system operators when the repair is commencing so they are prepared for any cascading effects that may occur throughout the center. When paired with advanced monitoring of smart devices, CMM becomes even more powerful. CMM can ensure that a device running outside normal parameters is appropriately prioritized for attention without requiring any human intervention until the moment a technician executes the work/repair order. Thus, it is a powerful tool to reduce risk at the most critical time — when part of the system requires maintenance.

Full use of standards and protocols

One of the main advances in the ability to monitor and manage electrical systems is the standardization of protocols, such as fieldbus architecture and, more recently, the International Electro Technical Commission's IEC 61850 communications standard.

IEC 61850 is considered a "smart grid standard," one of a range of international standards designed to allow faster and easier communication throughout the electrical system. It applies specifically to communication within and between substations, and has a goal of making such compliant equipment "plug and play," regardless of the manufacturer.

One of the big selling points for using IEC 61850-compliant equipment is "future-proofing." Any system that utilizes compliant equipment today will integrate easily as it is expanded, updated and connected to other outside systems such as those used to bring electricity from alternative energy sources into the data center. A strategy of compliance to specific industry standards is important as an enabling prerequisite for a number of other risk management strategies, such as full interconnectivity between critical databases.

Thanks to a trio of nuances in the way IEC 61850 is written, it's proving transformational:

1. It is a truly global standard, common for both IEC and ANSI
2. It provides a flexible open architecture both for medium- and high-voltage devices
3. It is based on Ethernet communications so it offers fast, reliable and secure communications and interoperability among electrical devices with the flexibility to adapt as new communication technologies arise

Interconnectivity of databases

If the purpose of an automated control system is to reduce the need for error-prone human intervention, the ability of databases to trade and use information seamlessly is critical.

Historically it's been a difficult task. But while IEC 61850 was developed for communication in the electrical system, it also can be used to achieve more transformational results such as true integration between the electrical system and the control system. To realize the benefit of interconnectivity, compliant smart devices need to be installed throughout the electrical system — a job that can be done incrementally as individual devices are retired and replaced — and the control system needs to be designed with integration in mind.

There are multiple risk-reduction facets to this important capability. Information from all systems can be analyzed as if it came from a single source, allowing faster identification and response to changing states. Further, automation is enhanced. The control system has two-way communication with devices in each system. Once it has received data to analyze a change or fault, it can also signal relevant devices to resolve the issue. A control system with robust intelligence and automation capabilities can often do this within milliseconds, before human operators have time to see or acknowledge an event is occurring.

Finally, for procedures that are not automated, operating complexity is reduced and training requirements along with it. Operators only need to learn to use a single interface, and they can control each system as if it is part of the control system.

For example, if a data center's monitoring equipment indicates a primary transformer at the onsite substation is nearing failure, there will typically be a hard-wired mechanism in the switchgear to trip the transformer to prevent major damage. But after the transformer trips, everybody has to go into crisis mode to minimize electrical consumption. Use of the climate control system must be curtailed, meaning servers may need to be powered down while the alternative power source such as onsite diesel, or perhaps a second transformer at a separate substation are brought online.

By contrast, if the control system is designed to integrate IEC 61850-compliant devices, it can receive information about the transformer trip and handle all of the necessary responses in milliseconds without human intervention. The advantage of such speed is reduction of risk to people and equipment and improved reliability as equipment stays online for longer and gets attention more quickly when needed.

So far this is not the norm. In fact, today ABB's Decathlon system is the only DCIM that is built to comply with IEC 61850 — owing to its origins with the energy and industrial process industries. But it's a feature that offers a level of visibility, speed and control that will become vital as data centers seek to improve efficiencies and achieve 100 percent reliability.

Electrical security

The electrification requirements of data centers are quickly outpacing the capabilities of most DCIM systems. Driven by efforts to manage operating costs and increase electrical reliability, operators are moving into new frontiers of the Smart Grid. They are developing their own microgrids with on-site power generation and storage capabilities to reduce dependency on the grid. They are seeking to participate in emerging energy markets, drawing electricity not only from local utilities but from generators half a continent away.

ABB is working with a major IT equipment provider to demonstrate the feasibility of a net-zero energy data center using DC power and relying heavily on such renewable energy sources as wind and solar. However, the variables surrounding these capabilities present challenges that few DCIM systems are designed to address.

For example, when a data center begins generating its own electricity, it must conduct real-time modeling to ensure it is using the lowest cost power available at any moment.

Further, monitoring capabilities may need to expand beyond the data center's four walls to include the substation, distributed energy resources like wind and solar, and sophisticated energy storage devices.

The electrification requirements of data centers are quickly outpacing the capabilities of most DCIM systems.

Technology to manage these functions already exists and is being widely used in the energy industry. Integrating these capabilities with DCIM systems for data centers can support risk management associated with pricing volatility in today's energy.

The electrification requirements of data centers are quickly outpacing the capabilities of most DCIM systems.

Whether it occurs at the utility or within the data center, an electrical interruption that might have lasted several hours may now last only a few minutes.

Electrification strategies

Control system strategies manage risk by increasing automation and reducing potential for human error. The other significant risk data centers must begin to manage is the rising hazard that results from the increasing scale of electrical networks that serve data centers.

While the size and power of an electrical system increases risk, it also presents the opportunity to achieve greater efficiency and flexibility that might not be economically justified for smaller networks.

Substation design

Data centers are unique in their need for reliable electrical supply. Today, a substation must:

- Deliver power from the utility with the lowest risk of disruption;
- Facilitate the process of smoothing over brief disruptions;
- Allow seamless introduction of the various alternative power sources data centers are using to assure the supply and cost of electricity.

Traditionally designed substations may fall short in any or all of these areas. Depending on the size and configuration of an existing substation, a small range of technologies can be applied to achieve dramatic improvements in reliability. With proper design and equipment modifications, a substation with current MTBF (mean time between failures) of 0.5 can reduce failures from once or twice a year to as little as once every 30 to 200 years.

The same technologies serve to shorten the duration of outages. Whether it occurs at the utility or within the data center, an electrical interruption that might have lasted several hours may now last only a few minutes, a short enough time that it can be covered easily with a battery energy storage system (BESS) or other onsite power supply.

Whether it occurs at the utility or within the data center, an electrical interruption that might have lasted several hours may now last only a few minutes.

The up-front price for such reliability may be 30 percent to 50 percent more than standard substation designs, but the return on investment has become easier to calculate. It reduces maintenance and operating costs in some cases by up to 90 percent and it can be designed into the substation by degrees.

Partnering with an equipment manufacturer experienced in the design of transmission and distribution systems, and knowledgeable about setting up microgrids and making utility connections, can provide clear cost-benefit analysis for a range of substations designs.

Here are some key technologies for smaller, safer and more flexible substation design that would be evaluated in such a process.

Dry-type transformers. Air-cooled transformers require less space than conventional, oil-filled units. They present reduced risk of fire or explosion so they also require less safety-zone space around them. As a result, dry-type transformers are often used for indoor applications but are finding increasing applications for outdoor locations as well. These transformers also require less maintenance than traditional transformers for increased reliability and reduced lifecycle cost.

GIS technology. Gas-insulated switchgear (GIS) technology uses compressed SF6 gas rather than air as an insulating medium for switchgear and other components. One benefit is that GIS units are smaller, sometimes occupying just one-third the footprint of older designs.

Further, enclosure of components in a sealed SF6 environment reduces environmental impact on substation equipment, eases maintenance and eliminates such periodic disruptions as animals getting into electrified equipment. Overall reliability gains can reach 1,000 percent.

GIS technology is more costly than Air Insulated Switchgear (AIS). However, because components are self-contained and connected through bus systems, they create a modular system that enables future expansion of the substation without ever taking the substation offline for construction. As a result, capital investment to build a new substation can be limited to the cost of meeting current demand, with future expansion being funded only when it is actually needed.

More purposeful substation design. Another advance in substation design is the range of configurations used to join the substation to the electrical utility. One connection is typical, with a backup power supply for short disruptions, but

reliability is improved by having a second connection to the utility, ideally through a different substation.

There are a variety of configurations for utility hookups, each with its own set of cost-benefit tradeoffs. Tier 1 data centers have different requirements and cost limitations than Tier 4 centers. Currently, there are no established industry standards for substation design based on a data center's energy or uptime requirements; however expert design can ensure necessary power at best cost.

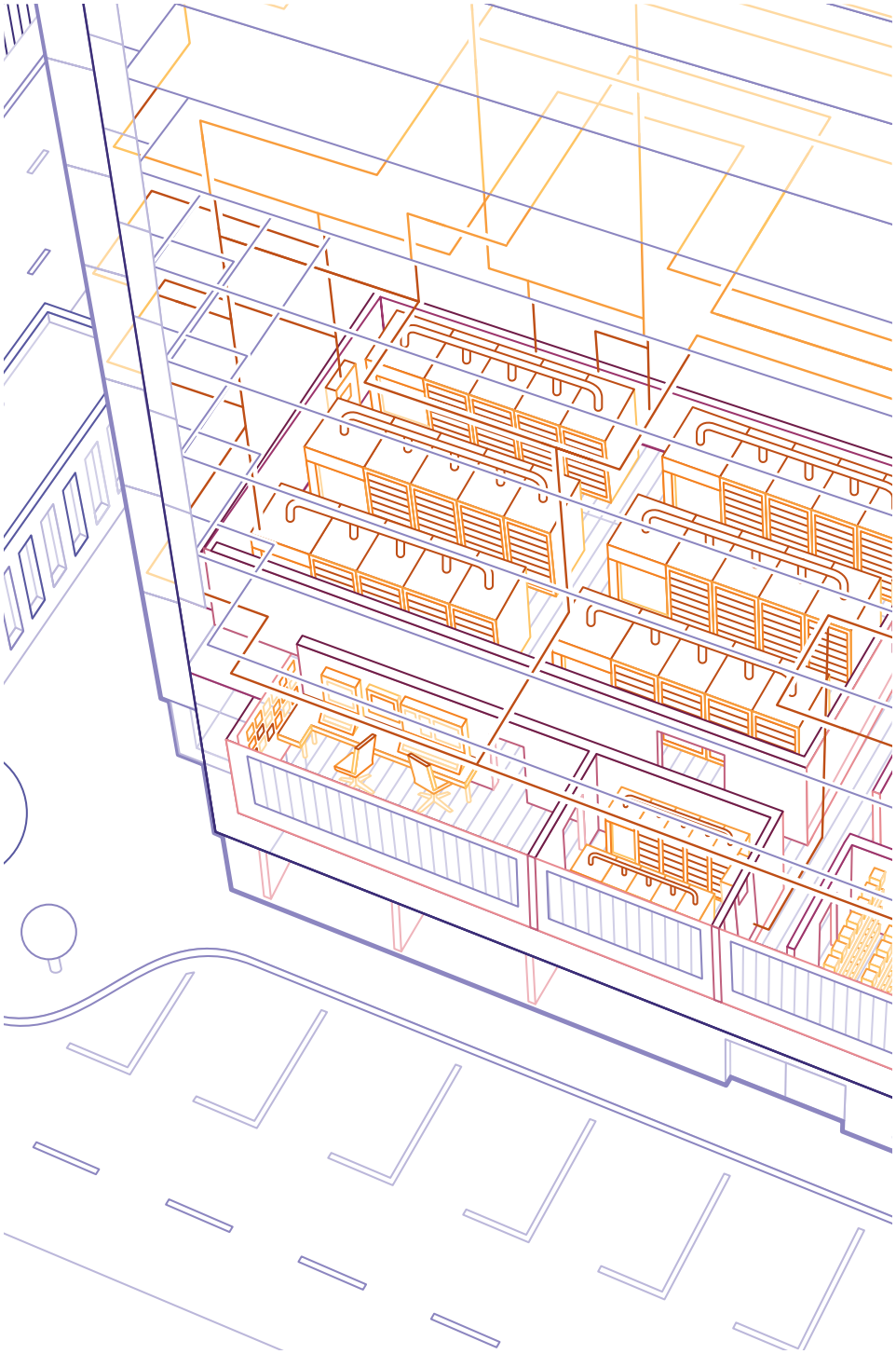
Smart sensors and monitoring

To facilitate control system integration discussed earlier, electrical system updates should include installation of IEC 61850-compliant sensors and devices. These devices heighten control and monitoring of the electrical system even when it isn't fully integrated with the control system. They improve fault detection, isolation and restoration (FDIR) capabilities, providing early warning and the ability to resolve problems before they affect operations. They are centralin the transformation to condition-based maintenance.

If these devices are installed over time as the system components require maintenance or replacement, the facility will move incrementally toward greater integration.

Arc flash hazard mitigation

The increasing hazard that electrical systems present in data centers may be a relatively new concern for many data center operators, but it's nothing new for regulators and first responders. Equipment inside the facility can be extremely dangerous, even deadly, if not properly maintained and operated. Because all electrical equipment is now enclosed, the primary danger from electrified equipment in a data center is arc flash. An arc flash can generate temperatures in excess of 30,000 degrees (F), causing an explosion of plasma and molten metal. It can occur at any time, but is a particular risk when equipment is being powered up or down, and when enclosures are opened for maintenance.



According to The Institute of Electrical and Electronics Engineers (IEEE) estimates, there are more than 2,000 arc flash incidents per year. Further, eight of 10 injuries to electrical workers result from arc flash explosions rather than electrical shock. Risk of arc flash can be been assessed through an arc flash study, which delivers a clear set of recommendations on managing each piece of equipment.

Today, though, that process is in flux. IEEE 1584, the international standard for calculating arc flash hazard is being revised in a process expected to conclude by late 2013. The changes may be significant. In this environment of uncertainty, data center operators are expected to comply with current safety standards, prepare for new standards and maintain confidence that they've addressed the actual risk in a meaningful and economically justifiable manner. Achieving these objectives requires the strategic combination of four key approaches.

Fault-limiting technology

Arc flashes are caused by electrical faults,

and their severity is a function of both current and time. Reducing either variable serves to reduce arc flash risk.

For example, power electronics can be used to replace simple on/off controls throughout the electrical system in such applications as drives and motion controls found in a data center's environmental systems. They allow for quick and incremental adjustment to changing conditions in order to prevent circuits from overloading and faulting, essentially "dialing down" sudden surges in power before a fault can occur.

Current reduction
Another approach is exemplified in ABB's Ultra-Fast Earthing Switch (UFES), which initiates a three-phase short circuit to earth in the event of a fault. The extremely short switching time combined with the rapid detection of the fault, ensures a fault is extinguished as soon as it arises.

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

At the top level, it can be achieved by selecting different topologies in data center electrical systems. 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, thereby 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 a 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 and reduce current output. Fault current limiters are capable of responding during the first current rise in less than a millisecond, usually fast enough to prevent a fault of any kind. They also can be retrofitted into existing systems based on analysis to identify areas of elevated risk.

Containment

Fault reduction and current limitation seek to reduce events and their impact. The return on investment for these technologies is measured in increased safety and reliability, and through improved operating efficiency. Even with those strategies in place, efforts need to be made to contain the impact if a major event does occur. This is where arc flash-resistant design comes in.

Containment is a two-fold design strategy. It uses topologies that limit the likelihood of an arc flash and it surrounds the equipment in an enclosure that absorbs the force of an arc flash and/or vents it safely away from people and other nearby equipment.

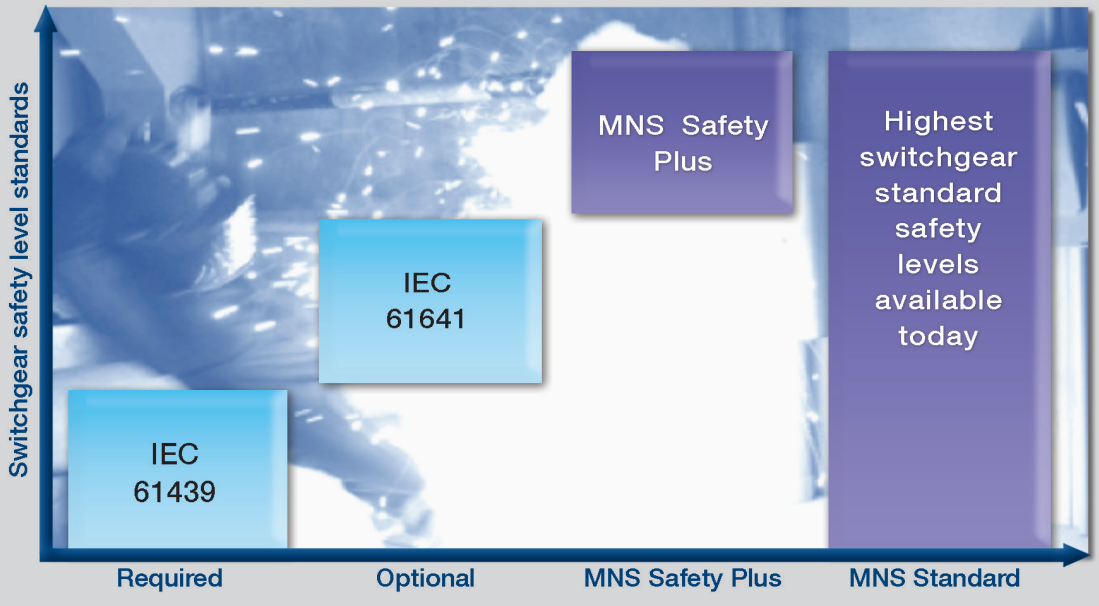
While such enclosures have become standard in medium-voltage applications, they are now increasingly being applied to low-voltage equipment as well in equipment such as motor control centers and low-voltage switchgear.

The arc-resistant features of these devices include the following:
- withdrawable drawers with power and control terminals located in the vertical wireway – designed to be installed or removed with all doors closed;
- horizontal buses of up to 4,000 amps accommodating greater load so the additional bus units are not required;
- bus splice windows in the vertical wireway to allow visual inspection of connections;
- enhanced enclosures featuring non-flammable and non-hygroscopic housing that insulates phases from each other and ground to create an arc-free zone.

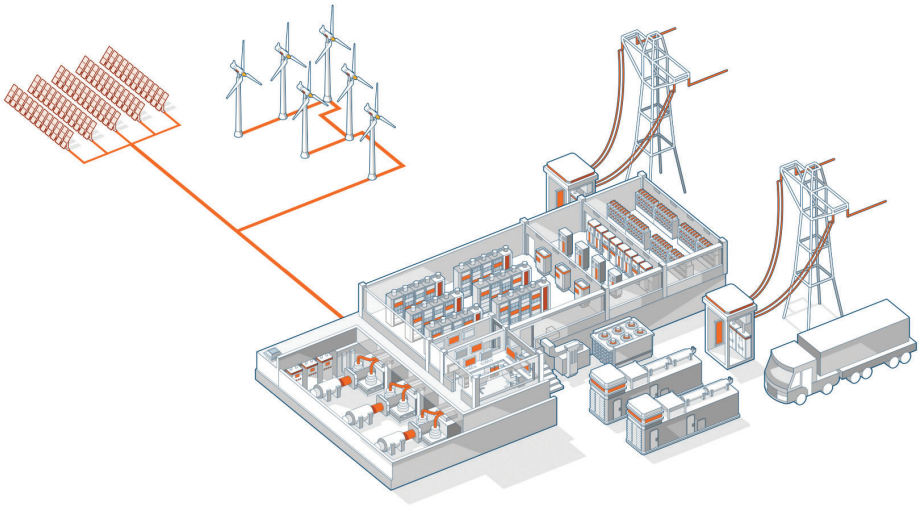
Personal Protective Equipment
Safety regulations stipulate appropriate

Minimize risk of deadly arc flash incidents

The MNS low voltage switchgear solutions meet and exceed the IEC 61439-1/-2 and IEC 61641 safety standards for arc flash protection.



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, PPE is really only a last resort and is the least effective form of risk mitigation. It builds a protective barrier between workers and energized 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.



Conclusion

Reducing hazards and managing risk are an ongoing part of the job in the data center as in any commercial or industrial setting. In a quest to eliminate disruption and downtime, data centers are growing larger, more powerful and more sophisticated, and so too are the solutions to their risk management challenges.

Two key areas that have not always been the focus of risk management efforts now need to be addressed: the unpredictable and error-prone impact of human intervention in the operation of sophisticated management systems, and the hazard presented by increasingly powerful electrical networks.

Solutions for these concerns are often technology based, and reside both in a facility's day-to-day operations as well as its design, which extends to the design of systems, substations and electrical networks.

Data center managers seeking to embed safety, risk mitigation and improved reliability in their everyday operations now need to explore higher levels of integration and automation through industrial controls developed specifically for the needs of the data center. And they must embrace electrical network design built around the increasingly complex power requirements of their business.

For more information on data center technology:

Marty MacDonald
Director, U.S. Federal Markets
ABB
1455 Pennsylvania Ave., N.W., Suite 1130
Washington, DC 20004
Phone: +1 614 818 6456
Email: Marty.MacDonald@us.abb.com

www.abb.com

9AKK105713A9702

Power and productivity
for a better world™