THE MAGAZINE OF 7x24 EXCHANGE INTERNATIONAL

NewsLink

SPRING 07

BEST POWER PRACTICES IN ENSURING BUSINESS RESILIENCE

WHAT TO PROTECT AGAINST?

DISASTER AVOIDANCE VERSUS DISASTER RECOVERY

SOMEONE HAS TO LEAD

ADVANCED

STS Communication

- New Wavestar communications package
- Triple redundant logic and power supplies
- Redundant LCD screen with Waveform capture
- Industry's first biometric security system

NEW KITS & VOLTAGE VERSION

Branch Circuit Monitoring System

- Kits for any existing distribution cabinets
- Track, report and manage current, voltage and power measures to server level
- Manage current voltage and power in server cabinets
- Communicate through modbus or SNMP protocol and/or local monitor

IMPROVED

PDU Performance

- Re-engineered rigidized doors
- Vision panels and improved locks
- Hinged interior panels
- Fits BCMS with no alterations
- Flexible custom designs

Power Distribution, Inc.
4200 Oakleys Court
Richmond, VA 23223
800.225.4838
804.737.1703 fax
e-mail: sales@pdicorp.com
web site: www.pdicorp.com

PDI

creating the perfect wave

Contents

7x24 Exchange INTERNATIONAL

The end-to-end reliability forum.

www.7x24exchange.org

DIRECTORS & OFFICERS

322 Eighth Avenue, Suite 501
New York, NY 10001
(646) 486-3818

by Robert J. Cassiliano

Chairman's Letter

I hope springtime has everyone energized!

Wall Street's dramatic resurgence highlighted with the DOW hitting a record high is a key indicator of an economic comeback. We are seeing strong signs of this surging market in the Mission Critical Industry as well as hiring of permanent staff and consultants is occurring on a pre 911 pace, projects on hold are being given the go ahead, and funding for new projects, in particular relocations and build outs are being approved. This is great news which presents tremendous business opportunity for those companies that can react quickly with quality resources and innovative solutions.

The 7x24 Exchange can assist you in meeting these challenges by conducting conferences which provide participants with insights to client strategies, an understanding of how complex projects are planned and executed, knowledge of how to improve day to day Mission Critical support, lessons learned, and the newest techniques and tools to solve mission critical problems. The 7x24 Exchange will address these key elements to assist you by providing the following:

Insights to client strategies – present conference keynotes that are client executives that can deliver a message focused on client goals and strategies for meeting those goals. Our Spring Conference presents Fran Dramis as the conference keynote a renowned technology visionary and change agent.

An understanding of how complex projects are planned and executed – include more real life case studies at conferences presented by the team that delivered the project including a client representative.

Knowledge of how to improve day to day Mission Critical support – provide conference topics and NewsLink Articles focused on support. Conference participants should take advantage of all networking venues.

Lessons learned – ensure talks at conferences and NewsLink articles with some additional focus on Lessons Learned. Conference participants should utilize conferences for sharing information.

Newest techniques and tools to solve Mission Critical problems – provide tutorial sessions by industry experts focused on the latest and most effective methods to solving problems.

The Board of Directors will continue to "Raise the Bar" when it comes to providing value to 7x24 Members and Conference Participants!

I look forward to seeing you at our Spring Conference in Boca Raton, Florida.

Russelectric custom engineers every power control system to specific customer requirements

"When we upgraded our Russelectric system, we wanted SCADA to monitor and control our old gear as well as the new. A canned package would have meant kluging something together.

Russelectric custom SCADA integrates our entire system... not just the new equipment."

At Russelectric, special requirements or unusual designs are not interruptions of our business... *they are our business.*

Russelectric specializes in using proven technologies and components in innovative ways to satisfy even the most exotic customer requirements. We'll never compromise on quality, safety, or performance. And, above all, we'll never ask our customers to settle for less than exactly what they want.

Independently owned and operated, Russelectric has only one goal... to take care of our customers.

1-800-225-5250
www.russelectric.com

Russelectric
Power Control People You Can Rely On

Best Power Practices in Ensuring Business Resilience

by Jim Neumann

ABSTRACT: According to headlines in leading IT periodicals, the list of IT-savvy companies whose business operations have been adversely impacted by electrical power-rooted problems reads like a "Who's Who" of the leading e-commerce, transaction processing, networking, software, financial services, and IT services business leaders.

Because electrical power and IT operations are so tightly interwoven, power problems cut directly into a company's ability to keep its mission-critical computing on-line... and prevent them from maintaining a high degree of insight into power-related problems.

This article examines the symbiotic relationship between electrical power and IT systems, including new "Power Analytics" strategies that give facilities owners and operators unprecedented insight into the health of these two interdependent infrastructures.

If you Google the terms "power outage" and "data center" together, you'll find 98,400 reasons why the most important element in data center design – and the most unpredictable wildcard in getting it right – is electrical power infrastructure. Reading through the search results, chances are good that you'll see your ISP… your cellular phone carrier… your bank… your credit card company… and other very familiar names.

The economic impact of electrical power problems in data centers has grown in correlation with the digital economy itself, with staggering implications for data center operators:

- 40% of all business downtime now stems from power quality problems[1] and fully 80% of those electrical disturbances originate inside the company's own facilities… most caused by the day-to-day operation of ordinary equipment[2] like computer and networking gear.
- More than 500,000 businesses and consumers experience electrical power problems every day, with the average power outage lasting two hours[4]. The annual cost to the U.S. economy due to these power disruptions is estimated as high as $164 billion... not including up to another $24 billion due to power quality phenomena that falls short of full-blown power outages.
- The seriousness of an unplanned power outage to an individual company varies by industry and application – ranging from "costly and disruptive" to "costly and life-threatening" – with some industries losing as much as *$6.45 million per hour* of business downtime[3].
- Even the daily cost per for planned mission-critical application downtime ranges from $167,200[5] to $800,000[6] depending on the size of the company.
- For large companies, a gain of just one percentage point of availability is worth $7,358,400 per year. Even at an average size company, one hour of downtime translates to $10,000 off the bottom line; with a 5% power availability gap, such companies risk $3,679,000 per year.[7]

Companies slammed by power problems, even as technology-savvy as they may be about IT, have learned the hard way that failing to understand the symbiotics between their IT systems and their electrical power infrastructure can create operational and financial havoc. Because electrical power and data center operations are so interdependent, power problems greatly jeopardize companies' ability to ensure business continuity… or even just maintain a sufficient level of insight into power-related problems.

"Six-nines" reliability

To operate with the utmost reliability, your data center must achieve 99.9999 percent uptime. PowerCommand® pre-integrated power generation systems from Cummins Power Generation help give you end-to-end reliability. They're specifically designed to fit and work together—providing 24/7 assurance of uninterrupted power, exceptional data reporting and the capacity to match your expanding infrastructure.

Our network of local distributors is at your service to deliver everything from design assistance and installation to 24/7 maintenance and support.

Contact your local distributor today or visit www.cumminspower.com/local

Our energy working for you.™

Power Generation

Power control you can count on

PowerCommand standby power systems combine a micro-processor-controlled generator set with switchgear, paralleling equipment, digital master controls and transfer switches. Because they are designed by one manufacturer, these components deliver better performance with increased functionality.

For more information, contact your local Cummins Power Generation distributor or visit www.cumminspower.com/powercontrol

CRITICAL BENEFITS OF POWER ANALYTICS SOLUTIONS FOR DATA CENTERS

1. Adaptive, real-time situational awareness
2. Predictive diagnostics based upon actual operating conditions (not just extrapolations of historical data)
3. Intelligent alarm management that filters irrelevant alarms
4. Global consolidation and management of assets
5. Energy, capacity, and resources management
6. Reliability-centered maintenance
7. "What if" simulation environment to drive design and maintenance considerations
8. "Black Box" data restoration and analysis in the event of anomalies

A Costly Pound of Cure

Despite the overwhelming financial incentives and imperatives, many companies still are still flying blind when it comes to their power systems infrastructure. They frequently **overestimate** the capabilities of their internal preparedness (UPS, generators, etc.) and at the same time **underestimate** the severity and the speed with which power problems strike: for example, the 2003 Northeast Blackout surged across the Great Lakes and northeast regions like a tsunami, knocking out 250 power plants across a million square miles in only eight minutes.

Knowing that advance warning isn't always possible, businesses have made continuity their highest priority, at whatever costs. The first-generation approach to mitigating – short of preempting – the effects of data center power problems are monitoring and SCADA technologies… coupled with banks of fault-tolerant systems, UPS, generators, battery rooms, etc.

For organizations concerned about maintaining business continuity, these technologies were a wise investment for reducing post-outage business disruptions. Many modern-day facilities still rely solely on these approaches… knowingly operating in reactionary mode, and responding to alarms as they arise. In times of trouble, these alarms deluge users with thousands of lines of information per second, making it nearly impossible for data center operators to gain an accurate understanding of the precarious health of their power system operations. So, like the car alarm that has become more of an annoyance than an alert that a car is being stolen, operators often ignore – or even just turn off – these systems.

"The biggest challenge in data center design is striking a balance between continuity versus costs," explained Mark A. Ascolese, co-founder of the Critical Power Coalition, a national organization whose mission is to develop common public policy and establish a unified industry voice to ensure the quality, reliability, and continuity of electrical power within critical industries, businesses and public services.

"Too frequently, organizations over-invest in standby and recovery equipment, when all that is really needed is greater visibility into how power infrastructure will respond to changes in the operating environment under varying conditions," Ascolese added. "It's like paying to install airbags throughout the interior of your car, when collision avoidance alternatives are readily available, less expensive, and offer safety benefits far beyond what airbag can. In the past year, Power Analytics has emerged as a proven, cost-effective, and forward-looking methodology for providing the insight required to identify, isolate, and prevent electrical power problems long before they can jeopardize data center operations."

An Ounce of Prevention

The term "Power Analytics" is the electrical power counterpart to "Business Analytics," those sophisticated mathematical models that help financial institutions to assess a consumer's real-time financial health, determine FICO scores, prevent fraud and predict lending risks.

Power Analytics enable data center operators to assess the real-time integrity of their electrical power infrastructure, prevent anomalies, and predict the nature and location of electrical power problems the instant they become theoretically possible. Over the past year, since its introduction at the **Spring 2006 7x24 Exchange Conference**, Power Analytics technology has emerged as the "collision avoidance" solution data center operators sought to successfully predict and prevent electrical power problems from occurring.

With successful installations nationwide with the Federal Aviation Administration (FAA) and several undisclosed corporate data centers, the technology has proven successful in helping companies gain an unprecedented understanding into the innermost workings of the power systems supporting their IT infrastructure, ushering in a new era in data center management and planning; one executive compares it to the revolution that occurred in the medical field when CT scanners and other diagnostics technologies were introduced.

How Power Analytics Work

The comparison to medical technologies is an apt one: Power Analytics systems allow unprecedented insight into power systems infrastructure for a simple reason: every element of power systems design – from the largest piece equipment to the smallest circuit breaker – is codified with the operating specifications, system parameters, and all other pertinent data for every component that comprises the overall system.

Just as all components of the human body have normal and abnormal "vital signs" – and irregular signs like high temperature, elevated blood pressure, heart rate, or respiration rate are indicators of potential longer-term health problems – so does electrical power infrastructure.

So, just as physicians rely on a full range of patient monitoring systems to observe vital signs – right down to the real-time respiration and cardiac output of a patient – data center owners now have the means to understand systems-level reliability and capacity, right down to the smallest power cable or circuit.

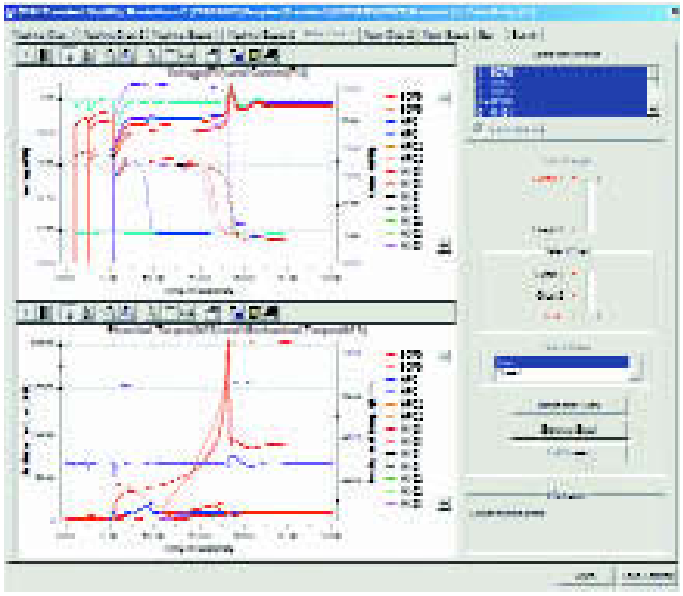


Image One: Once a Power Analytics model is created, it serves as a "flight simulator" that not only detects potential design miscues, but allows data center managers to conduct important "what if" scenario testing of their operational environment.

Model-Driven Design, Diagnostic, & Deployment

The principal benefit of the "model-driven" Design/Diagnostics/Deployment approach for data center operators is that it removes all major variables, unknowns, and uncertainties from the entire project. Because specifications for every component – and the interrelation of all components to one another and the surrounding infrastructure – are known early in the design stage, they can also serve as the basis for downstream diagnostics and deployment.

Thus, operators know precisely how their infrastructure is going to perform during the three crucial phases:

- **Design Phase:** A Power Analytics platform creates more than a typical CAD blueprint or one-line diagram of a facility: it creates a dynamic, "virtual model" of the power distribution system and its components and controls logic. Within this virtual model, detailed manufacturers' specifications for all equipment and components are stored; by recognizing "normal" power system readings on a component-by-component basis, data center operators are assured of the system-level integrity on a sum-of-the-parts basis…

  Armed with this information, potential electrical infrastructure problems can be easily designed out of a facility before it is constructed or modernized; safety considerations (arc flash, protection coordination, etc.) are addressed; and a detailed understanding of systems-level capacity and reliability are attained in order to ensure that the data center design is "perfect on paper" before proceeding.

- **Diagnostics Phase:** Once completed, this Power Analytics virtual model is used as the basis for simulating and validating the operational parameters of the overall electrical distribution system, to ensure system-wide integrity before it is constructed. Reusing the data in the virtual model, important "what if" problems, even ones that are beyond the scope of operational probability, can be quickly and easily addressed. Better still, these diagnostics can identify design modifications that will further improve the operational performance and resilience – power flow, power quality, component sizing, etc. – of the finished facility.

- **Deployment Phase:** The true value of Power Analytics becomes apparent in the deployment phase. Unlike traditional one-line diagrams, the virtual model can be switched from "design mode" to "surveillance mode" once the facility is constructed. In this mode, a facility's target operating specifications as encoded in the virtual model, are compared to actual online data from the facility's physical equipment, to ascertain when and where anomalies have the potential to occur.

  Power Analytics systems know how to check, interpret, and cross-reference "symptoms" deep within data center infrastructure… whether locally, or in remote locations managed by a central operator. In comparing the "actual" and "virtual" performances of the electrical infrastructure, Power Analytics software is able to detect the most negligible variations, even those involving seemingly unrelated components. This actual-to-virtual methodology accurately predicts yet-to-fail components or operating conditions that, left undetected, could result in a power outage.

  Over time, "normal" power system readings consist of more than just the original manufacturer's equipment specifications used to launch the facility: historical operating measurements, including day-to-day readings of equipment in routine operation, are also factored in. Negligible deviations in measurements from any component – combined with other readings in a seemingly unrelated area – can be probed to determine if they could be an indication of the early stages of power anomalies.

Image Two: After a Power Analytics system is deployed, thousands of arcane electrical components making up a data center's power systems infrastructure can be presented in easily understood charts, graphs, and diagrams depicting only relevant information for specified users.. including the economic impact of operational decisions.

The Big Picture: Millions of Smaller Ones

But these millions of micro-details are pointless unless they can be translated into actionable measures by data center operators. Like Business Intelligence (BI) visualization tools – which companies use to consolidate, analyze, and present information about their operations – Power Analytics systems have advanced, customizable data reporting tools that can generate individualized real-time status reports; these reports can be tailored for the informational needs (technical, operational, financial) and technological knowledge of appropriate people within the organization.

This flexible visualization capability prevents one of the most frequently-cited problems resulting in data center power outages: information overload. In case after case, human error – specifically, incorrect human action caused by misinterpretation of systems readings – has been shown to worsen, if not directly cause, the severity of power outages.

Acting as both an on-board electrical power system expert and translator, Power Analytics systems intelligently filter the power system sensory data, help data center operators understand the real-time health of their electrical power infrastructure, as well as diagnose whether that health is improving, stable, or deteriorating.

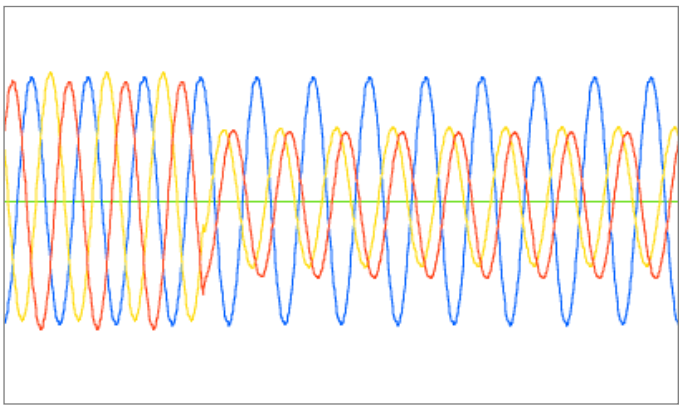


Image Three: Thin-client Internet Explorer Viewer, with an actual Square D CM4000T waveform displayed. This waveform capture – taken from a live, non-disclosable client application – displays the effect of a power anomaly on all three voltage phases, time-stamped to the millisecond.

When a reading that warrants further investigation is detected, Power Analytics systems help operators understand the impact of surrounding components to scrutinize and determine when and where problems could be in the formative stages. As a result, Power Analytics provide a far more detailed assessment of potential electrical power problems… in most cases, long before they actually occur and can have a devastating effect on a company's bottom line.

Thus – like the difference between a checkup and an autopsy – business-impacting questions rooted in the health and reliability of electrical power can be answered immediately, not after a problem occurs. As examples:

- How much more capacity can our existing facilities accommodate, before it becomes necessary to make arrangements for new facilities?
- What would be the operational impact of adding new equipment, changing configurations or adopting new technology?
- If we were to outsource our manufacturing – or we needed to monitor our suppliers' facilities to ensure the integrity of their systems – how could we do so?

Summary: Implications for Data Center Owners

Forward-thinking data center operators are recognizing that Power Analytics presents a dramatically new best practices paradigm over traditional IT/power systems methodologies.

For the first time, companies are now able to comprehensively and confidently view power systems infrastructure synergistically with their IT planning and facilities management.

Armed with these capabilities, facilities across America are now operating at peak levels of uptime… and more importantly, unprecedented insight into the health, reliability, and capacity of their facilities for the long term.

For businesses for which electrical power serves as the central nervous system for their global operations, Power Analytics is emerging as one of the most promising new business continuity technologies of the e-business era.

Jim Neumann is Vice President of EDSA Micro Corporation. He can be reached at jneumann@edsa.com.

Sources and Footnotes:
1) Sandia National Laboratory
2) Electric Light & Power magazine
3) EPRI (Electric Power Research Institute)
4) Contingency Planning Research
5) IBM Corp., "Best Defense Against Worst-Case Scenarios"
6) Oracle Corp. research report
7) Oracle Corp. research report

Seven (7) Most Common Operational Mistakes Found in Data Centers

by Todd Bermont

"We need more budget…. Tier II isn't enough. We need a Tier III or maybe even a Tier IV data center." Have you heard those words coming from your CIO or Facilities Manager lately?

With regulatory pressures and the cost of downtime soaring, organizations and government agencies alike are pouring huge sums of money to make their data centers more resilient. In most cases this makes absolute sense. A data center that supports a trading desk could have a downtime cost of over $40 million per minute. An outage to a data center that supports a manufacturing line could run into the millions of dollars per hour. In cases such as these, a Tier III or Tier IV data center is certainly justified.

However, just throwing money at a data center does not guarantee that you will never experience an outage. Certainly, the design and Tier level of a data center have a major impact on the ability to mitigate the risk of downtime. After all, if you don't have the proper redundancies built into your systems, it will be very tough to maintain those systems and avoid potential single points of failure. But, a stellar design and a high Tier Level rating will not guarantee uptime.

Many studies have shown that the leading causes of downtime are actually human error and infrastructure failure due to improper maintenance and hardware failure. (Fig.1) Our experience has been that a large percentage of outages in data centers can actually be prevented. What we have found is that by putting the proper emphasis on ongoing maintenance and operations of mission-critical facilities significantly increases uptime and resiliency.

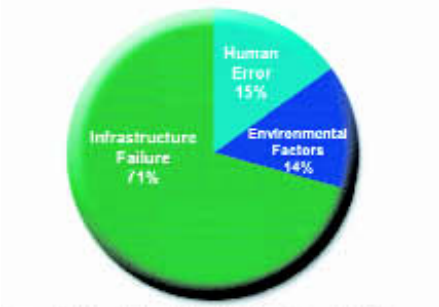


Figure 1: Infrastructure Failure & Human Error total 86% of preventable cause of downtime in mission critical facilities[1]

[1] Source: "The Critical Role of High Availability Infrastructure Support Services" E. Rocco, D. Igou, Gartner Research January 2004

In conducting assessments on hundreds of data centers, large and small, across the country, we have found seven common operational mistakes.

1. Staff Level does not correspond with Physical Infrastructure

Perhaps one of the most surprising mistakes we have found in data centers is that the staff responsible for running the data center is not congruent with the impact of the data center to the business, as well as the investment made in that data center.

In assessing a large, Tier III data center for a major financial institution, we noted that there was only one facilities manager who understood the infrastructure of that data center. This manager was only there during standard business hours and lived over an hour away from the facility. To conduct major preventative maintenance activities, this person often had to work weekends.

One of the major benefits of a Tier III facility is that they are designed with a great deal of redundancy so that if any one component fails, it should not impact the operations of the rest of the facility.

So, with spending all of that money on the infrastructure, the company had put itself at risk because indeed it had a very major single point of failure - the facility manager. Forget the proverbial what happens if "he gets hit by a bus," what happens if one of this company's competitors decided they wanted to offer the facilities manager a higher salary to manage a data center that was closer to home and that person quits? Now what?

Who can replace this person? Who else knows the ins and outs of the facility? Who else knows the equipment? Who else has witnessed and written procedures for that facility? Who else has the ability to react if there is a major disaster occurring within the facility? With only one person… no one!

You never know what circumstances can present themselves. The key is to build in redundancies within your staff as well as your infrastructure. Your facility should never be dependent on the knowledge and expertise of just one person.

2. Preventative Maintenance Not Performed

Amazingly, in conducting assessments across the country, it was discovered that routine and proper preventative maintenance (PM) is not being performed on critical equipment. This is a significant issue. In fact, what we have found is as little as 50% of all contracted PMs are ever completed. That means that while companies have actually paid for these preventative maintenance activities to happen, more times than not, the work is never done.

HOW CAN THIS BE?

Well to schedule just one PM visit, it can require literally over two dozen contacts via phone, email, etc., just to coordinate. Often, it just falls through the cracks, many times because there is not enough staff to be focused on preventative maintenance.

Secondly, finding the appropriate maintenance windows and maintaining those can be difficult. Invariably, something will come up that does not allow the PM to happen because there is a major business issue that can not afford to have the data center down for maintenance.

Thirdly, even if the PM is performed, often the corrective action that is required isn't properly documented or followed up on.

Just recently we fielded a call from a facilities manager who experienced a thermal shutdown in their data center because one of the belts on their computer room air conditioner failed, causing the unit to chill and fail. By loosing that one unit, the room heated to a point where the equipment was experiencing a thermal shutdown. That caused a significant outage in the facility which could have easily been avoided by conducting routine preventative maintenance.

3. Lack of Contingency Plans for Key Staff

Earlier, we spoke of potential single points of failure when it comes to staffing levels. The third common mistake related to this issue is that in many data centers there is a lack of a formal contingency plan for the key facilities people responsible for the facility.

We have seen in numerous instances that when the facilities manager goes on vacation or is sick, there is no proper contingency plan in place to replace the person who is out. "Ah, that's ok…he has a pager and a cell phone. If there is an emergency, we can always call him." Right, let's say he is in the hospital where you can't use a pager or a cell phone or let's say he has gone fishing up in the mountains where there is no cell service for miles? Now what are you going to do when an emergency hits?

The key is to not only have redundancy in trained personnel, but to also have the right contingency plans in place so there is always someone readily accessible for that facility when needed.

4. Limited or No Documented Procedures

Properly documented Methods of Procedures (MOPS) is imperative, For example, a CIO for a major consumer products manufacturer endured a 28+ hour outage at his data center. What was the cause of this outage? A maintenance technician for the HVAC accidentally pushed the emergency power off (EPO) button and caused the entire facility to crash.

There are several things that could have prevented this from occurring. The first of which is having properly documented Methods of Procedures (MOPS) for the maintenance of critical equipment.

We have found that many data centers either have outdated MOPS or do not have them at all. It is critical to have tested, comprehensive and accurate MOPS on every critical component in your data center facilities down to the switch level. A MOP that was written three years ago may not be sufficient today depending on if there were changes to the configuration and or changes to your facility.

In addition to MOPs, many data centers lack fully documented Standard Operating Procedures (SOPS) for the proper ongoing operations of equipment, safety procedures and emergency operating procedures (EOPS) when an event or disaster happens in the facility.

Each documented procedure should be tested and validated for accuracy. With human error being one of the leading causes of downtime in data centers, the lack of fully tested and documented procedures is one of the major contributors to that fact.

5. Limited or No Supervision of Maintenance Activities

In thinking about your facility, when is the last time one of your staff members supervised the maintenance being done within your facility. Commercial airlines always use a pilot and a co-pilot to fly a plane. That is for redundancy and both have responsibilities to ensure the flight goes according to plan.

We find in data centers that all too often there is no co-pilot with the flight pattern in place (MOP) to ensure that the maintenance person is properly conducting service on the equipment. The MOP

Sure, you have the server capacity... But what about the power?

If you don't have adequate power availability and protection, your operations can come to a screeching halt!

Don't overlook the most important aspect of your data center infrastructure.

Depend on **MGE UPS SYSTEMS** to help design and integrate power solutions that not only meet the current demand of power hungry servers, but are scaleable to accommodate future growth. MGE's experts in power infrastructure, UPS systems, sophisticated power management software and around the clock services make sure that you don't have unexpected capacity problems.

Need more info?

Visit **www.mgeups.com/dc** to register for one of our informative webcasts or for a free white paper on *Optimizing the Cost of Business Continuity.*

With over 40 years of global UPS experience, MGE's products and services provide the ultimate protection for enterprise-wide applications. Contact us today to learn how our power experts can safeguard your critical infrastructure.

800.523.0142

MGE
UPS SYSTEMS

www.mgeups.com

serves as the roadmap. The case of the maintenance technician accidentally pressing the EPO button would most likely have never happened if there was a co-pilot from the company overseeing the maintenance.

When you are conducting maintenance in your facilities, first, make sure you have a fully tested and documented MOP. Secondly, be sure to have one of your employees overseeing the maintenance technician as the work is being done to ensure the work is being done according to the MOP.

6. Limited or No Documentation of Maintenance Activities

Having a procedure is one thing. However, in your facility are you keeping accurate and legible records of what activities have been performed? This is critical to be able to conduct predictive failure analysis and is even more critical when it comes to required corrective actions.

All too often necessary corrective actions that result from preventative maintenance visits are lost or never completed due to the fact that either the handwriting from the maintenance technician was not legible or the fact that the action was not properly documented with a specific action plan for completion.

Make sure that all maintenance activities are fully documented, in a legible fashion, in a central and easily accessible place.

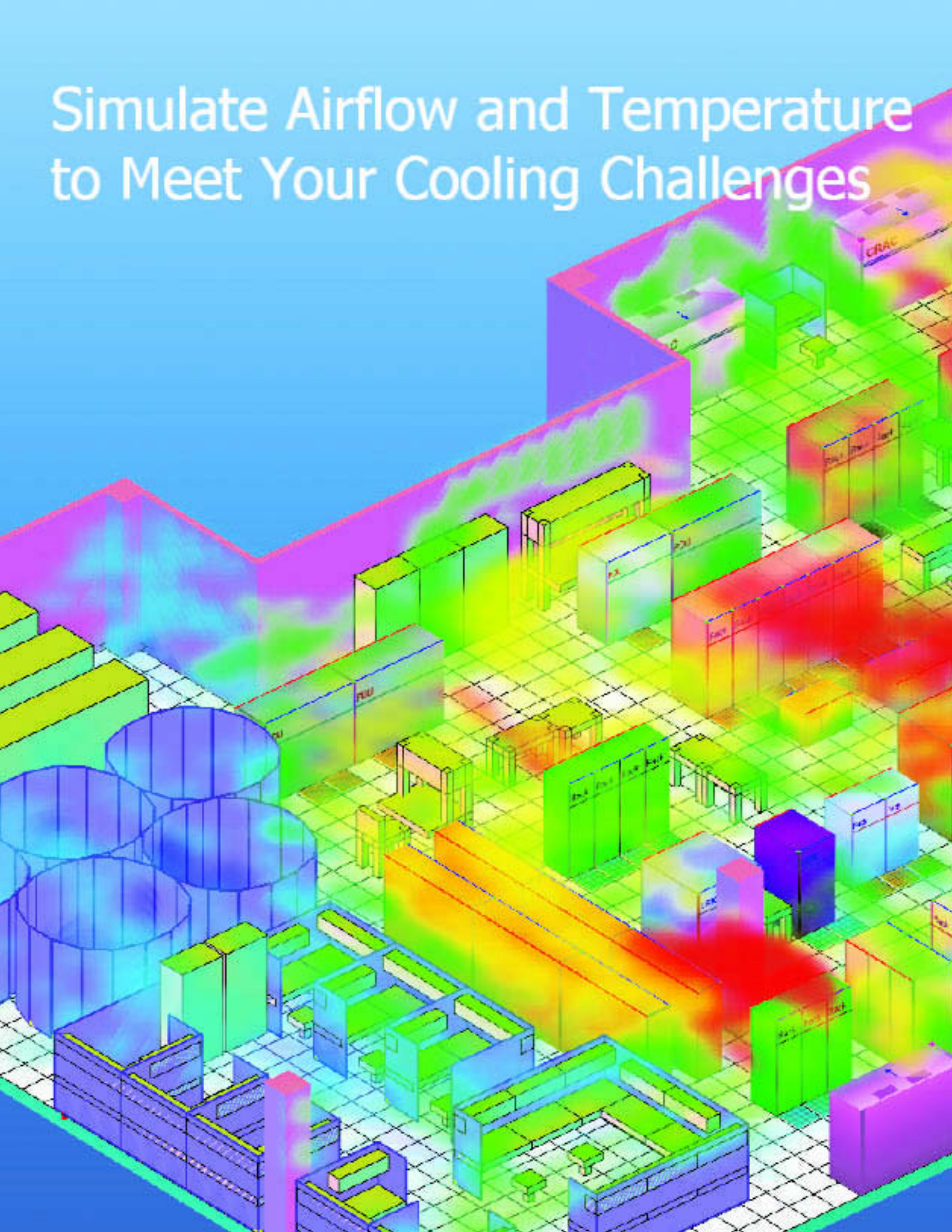
7. Outdated or Non-Existent Drawings & Site Operation Guides

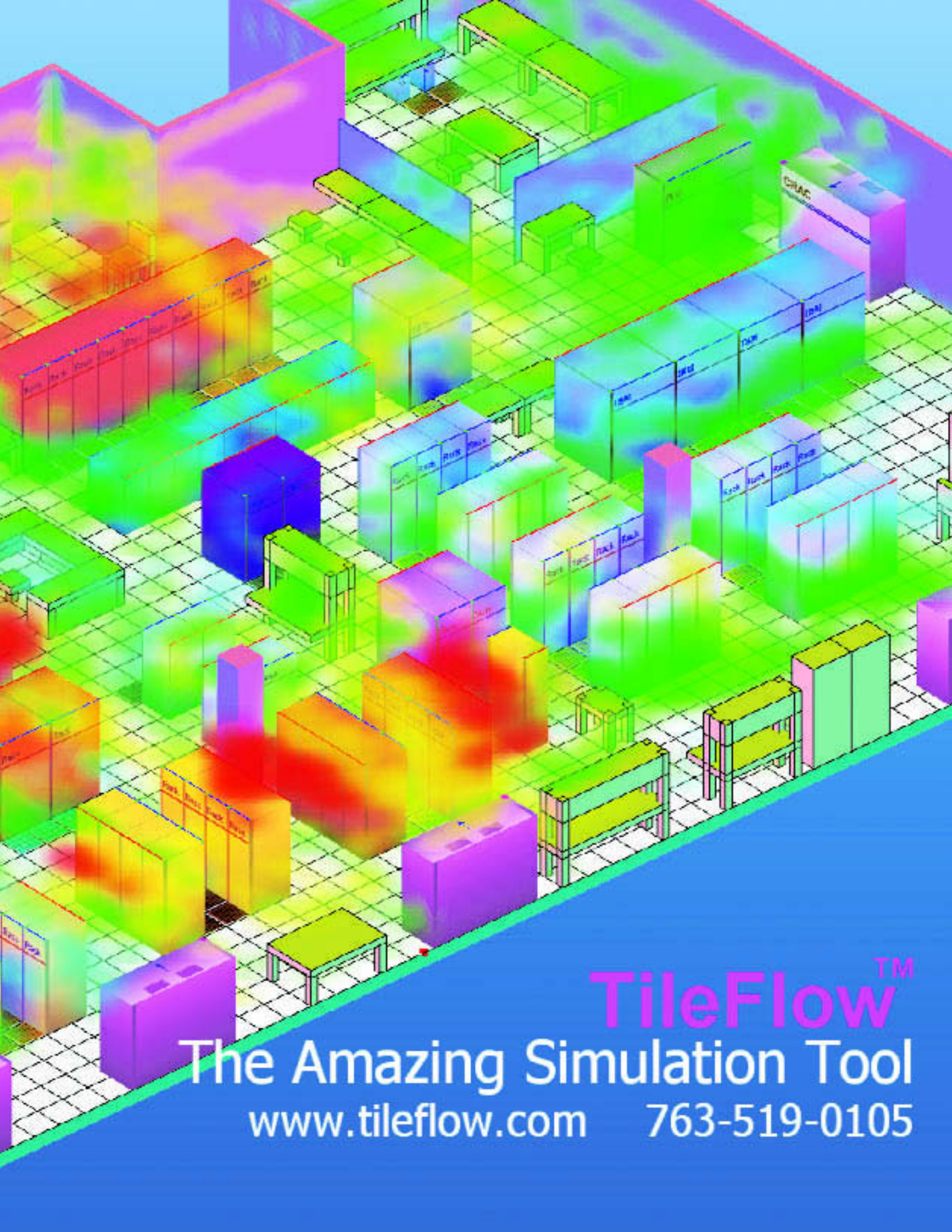
The seventh critical mistake is the lack of current "as-built" and electrical "single-line" documents. Not keeping these up to date is asking for disaster. First, breakers, Power Distribution Units (PDUs) and other critical infrastructure can easily become overloaded without keeping proper track of connected equipment and devices. Secondly, especially during an emergency, not having accurate drawings and documentation could present a safety hazard as well as make complete disaster recovery very difficult in the event something disastrous happens in the data center.

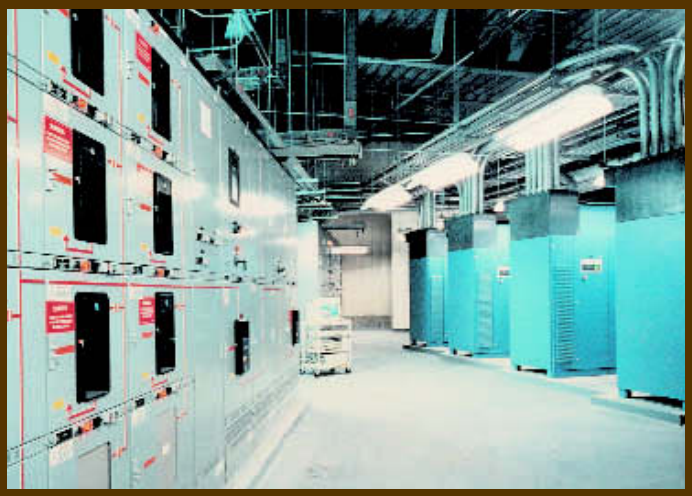
In summary, while it is important to invest in the right design and build-out of your data center and other mission-critical facilities, make sure to pay equal attention to the day-to-day operations of the facility. With human error and hardware failure being the top causes of downtime in facilities, by just focusing on eliminating the seven common mistakes you can significantly enhance the resiliency of your facilities.

Todd Bermont is Regional Director of Total Site Solutions. He can be reached at tbermont@totalsiteteam.com.

Simulate Airflow and Temperature to Meet Your Cooling Challenges




TileFlow™
The Amazing Simulation Tool
www.tileflow.com 763-519-0105



11 METROTECH CENTER

by Thomas E. Reed, PE

At 11 MetroTech Center's topping-out ceremony in 1994, then-Brooklyn borough President Howard Golden remarked that "the mission of those who will work here will be a vital link in the life of every New Yorker." Little did he know of the gravity of his words in the years to follow when New York City would survive 9/11 and the Northeast Blackout of 2003. Located in downtown Brooklyn, the five-story 358,000 SF facility houses the data processing and dispatch for all five New York boroughs emergency response agencies including the New York City Police Department (NYPD), the New York City Fire Department (FDNY), the Emergency Management System (EMS), and the Department of Information Technology and Telecommunication (DoITT). For Philadelphia-based KlingStubbins, the Interior Architecture (representing DoITT) and base building and fitout engineering team responsible for designing the failsafe 24/7 infrastructure, the project challenges were not confined to the aggressive criteria of the City, but the intense focus on cost-consciousness of the design as well.

Through the years, 11 MetroTech, one element of the entire MetroTech Center developed by Forest City Ratner companies, has not only helped transform the urban center of Brooklyn, but it has undergone its own internal transformation. The facility was initially designed for the City of New York's Department of Information Technology & Telecommunications (DoITT) and the NYPD's Public Safety Answering Center. In 1996, the FDNY computer and dispatching functions were folded into the building, followed by EMS' move some eight years later. The consistent internal shuffling of departments required a surgical reconfiguration of equipment needed to ensure that not a single 911 call or piece of data was dropped or lost due to the renovations. Because KlingStubbins was successful at making this happen when the facility was first opened, the firm was retained for subsequent enhancements and new agency tenant improvements.

Systems are designed to withstand long-term outage of most all municipal services such as electric power, natural gas, and domestic water utility services. The emergency generators and paralleling switchgear provide utility paralleling and supply power to the facility. Critical reinforcement of the uninterruptible power supply (UPS) system maintains continuous service to the computer facility even with a loss of two of the four modules in the either UPS. The chilled water plant, consisting of four electric driven 400-ton centrifugal chillers, afford diversity in cooling sources and distribution. The design circulates water through the computer center, with no interruption of cooling to the computer room equipment during emergency modes of operation.

The approximate $65 million internal expansion of 11 MetroTech required a sizeable team effort, which included developer Forest City Ratner; interior architect Swanke Hayden Connell; technology consultant IMI; members of the DoITT, NYPD, EMS and FDNY planning groups; and First New York Management, the organization that would manage and operate the building. The complexity of reconfiguring power distribution systems as each new emergency response agency was added to the building ultimately played out during the coordinating efforts between the agencies themselves. As KlingStubbins Engineering Design Principal Gerry Murray, PE recalls, "There was an urgent need to provide highly reliable back-up systems, while maintaining separation of systems dedicated to each agency, NYPD, FDNY and DoITT. During our very first Design Session, the criteria was set that the reliability and redundancy strategy must include a "separation of systems" on a day-to-day basis, while allowing overlapping back-up resiliency in the design." This kick-off meeting would set the tone for the rest of the planning process.

Even though the emergency response agencies shared the mutual mission of serving the public good in a timely fashion, KlingStubbins would need to convince them that diverse distribution and multiple system redundancy were a vital strategy to providing availability of the infrastructure. The KlingStubbins design team faced the challenge of allowing the agencies to operate exclusive of one another and yet still act as a source of power for the other in the case of catastrophe.

Central to the design was the need for sophistication, while providing for simplicity in operation. Working with First New York management, a team that has successfully maintained and operated the facility since its original commissioning, Kling developed methods of procedure for operations as well as the trade contractors that would perform the upgrades.

Throughout the design process, the team met weekly with members of the City agencies as well as the City's Design and Construction agency DCAS. This assured that new requirements could be quickly integrated into the design and construction process. The constant

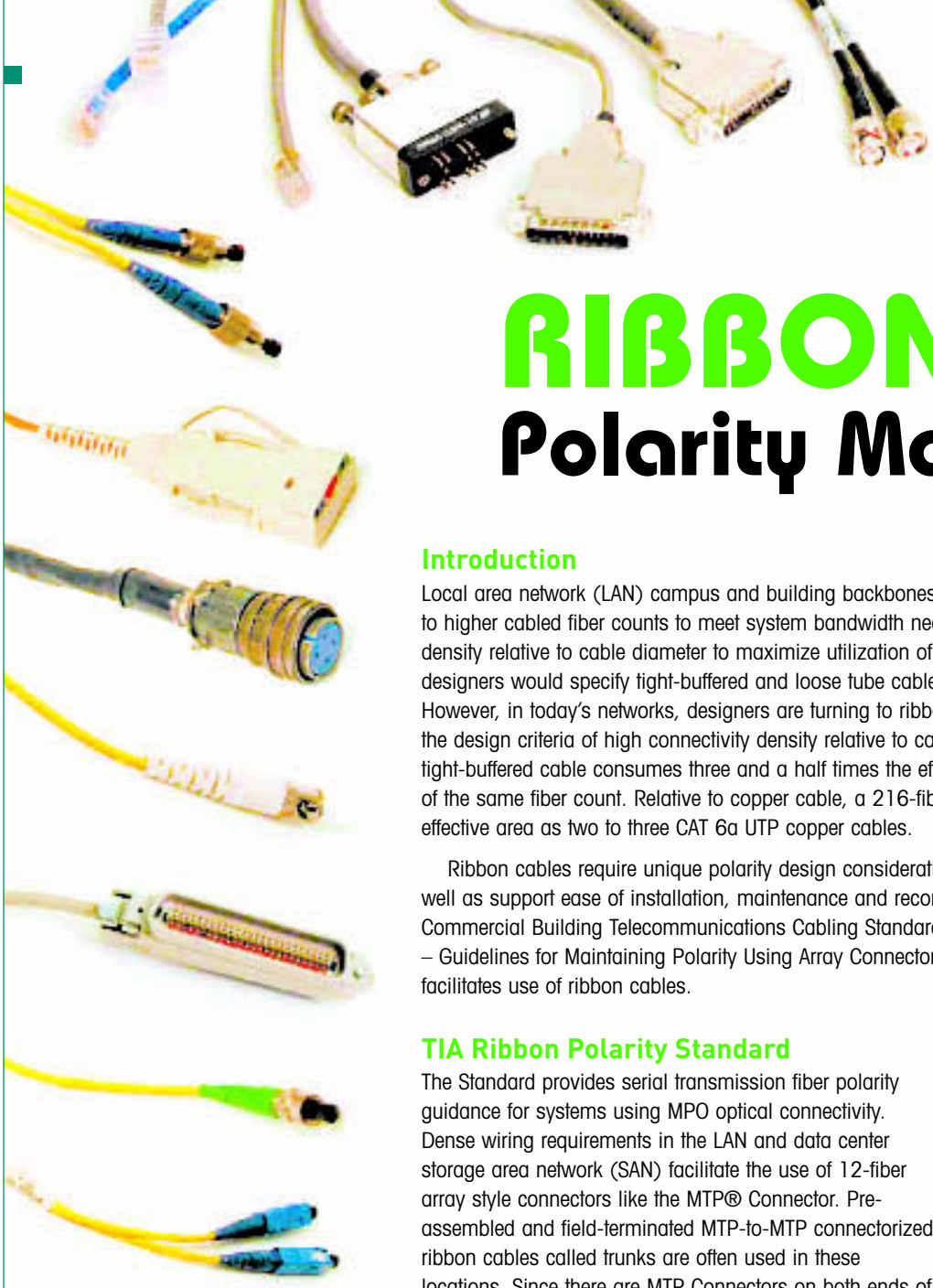
Thomas E. Reed, PE is Principal and Senior Director of KlingStubbins' Technology and Government Practice. He can be reached at treed@klingstubbins.com

demands placed on the City agencies such as police, fire, and information technology required the design and construction process to be unlike any other private or public project. DCAS and the City team worked non-stop with both the development, design, and construction teams as well as Police, Fire, EMS and IT agencies to establish a Change Control Procedure that had "military precision", and assure cost control, while accomplishing the ever-changing needs to the First Response agencies.

Projects that house such critical public safety functions are most difficult on management, design, construction, and financing. This project not only succeeded but excelled in each of these fields, mainly due to the quality, dedication, and talent of the individuals involved from each aspect of the project.

PROJECT TEAM:

Developer/Owner:	Forest City Ratner Cos.
Project Management/Leadership:	DCAS (Department of Citywide Administrative Services)
Tenants:	DoITT, NYPD, FDNY, EMS services
Design team:	KlingStubbins Engineer; Swanke Hadden Connell Interior Architect
Construction:	JLS, New York
Property Management:	First New York Management
Technology:	IMI Inc.; Gartner Group, Winbourne & Costas, Inc.



RIBBON CABLE
Polarity Management

by Doug Coleman

Introduction

Local area network (LAN) campus and building backbones as well as data center backbones are migrating to higher cabled fiber counts to meet system bandwidth needs, as well as provide the highest connectivity density relative to cable diameter to maximize utilization of pathway and spaces. Until recently, network designers would specify tight-buffered and loose tube cable designs for these backbone applications. However, in today's networks, designers are turning to ribbon cable designs because of its ability to meet the design criteria of high connectivity density relative to cable diameter. For example, a 144-fiber unitized tight-buffered cable consumes three and a half times the effective area compared to a ribbon plenum cable of the same fiber count. Relative to copper cable, a 216-fiber ribbon plenum cable consumes the same effective area as two to three CAT 6a UTP copper cables.

Ribbon cables require unique polarity design considerations to ensure reliable system performance as well as support ease of installation, maintenance and reconfiguration. ANSI/TIA-568-B.1-7-2006, Commercial Building Telecommunications Cabling Standard, Part 1 – General Requirements, Addendum 7 – Guidelines for Maintaining Polarity Using Array Connectors, was ANSI approved in January 2006 and facilitates use of ribbon cables.

TIA Ribbon Polarity Standard

The Standard provides serial transmission fiber polarity guidance for systems using MPO optical connectivity. Dense wiring requirements in the LAN and data center storage area network (SAN) facilitate the use of 12-fiber array style connectors like the MTP® Connector. Pre-assembled and field-terminated MTP-to-MTP connectorized ribbon cables called trunks are often used in these locations. Since there are MTP Connectors on both ends of these trunks and the end equipment typically has standard duplex transceiver ports, the trunks are plugged into factory-made breakout furcations called modules that transition from the MTP connector to a duplex connector/adapter style. (See Figure 1.)

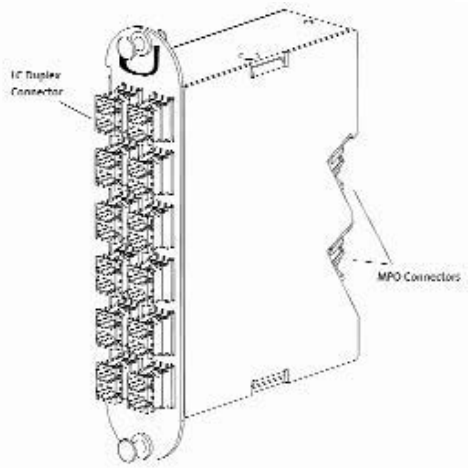


Figure 1: MTP connector

Each 12-fiber ribbon translates into six 2-fiber serial optical circuits that require polarity management that can be achieved using one of numerous methods. Like simplex and duplex connectors and adapters, the MTP Connectors and adapters are also keyed to ensure the proper orientation is maintained when connectors are mated. With MTP Connectors, this keying establishes the orientation of one fiber array in one connector relative to the array in the mating connector, but does not ensure that duplex fiber pair polarity is maintained.

The Standard includes guidance on three sample methods identified as Method A, Method B and Method C. It is important to note that the Standard states in paragraph 3.1 that "While many methods are available to establish polarity, this Standard outlines sample methods that may be employed." The word "may" implies that alternate polarity methods are available to accomplish the same result that are not discussed

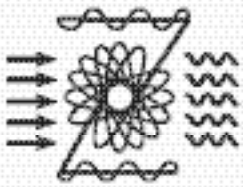
LOAD BANK RENTALS

Right. Ready. Reliable.

Call the professionals:

ComRent® International

Successful load testing begins with *ComRent*.



Founded in 1997, *ComRent* fills the need for quality test equipment. Our equipment is used to test the design, installation and reliability of mission critical power systems. ComRent's capabilities can handle load testing projects up to 90+MW at medium voltage for commissioning of large power systems. Smart load tests now mean future reliability. *ComRent* makes your next load test easy. We provide rentals, service, professional experience, logistics and confidence with every job. Look for the 3 R's that *ComRent* can deliver: Right. Ready. and Reliable.

ComRent® International **1.888.881.7118** **www.loadbanks.com**

Locations: CALIFORNIA (LA & Bay Area), MARYLAND, TEXAS (Austin), CHICAGO, NYC. New Locations: TAMPA/ORLANDO, HOUSTON.

Predictive Maintenance for Electrical Switchgear + Critical Equipment

- 24/7 real time thermal monitoring
- On-going trend analysis + alarms
- Plastic IR sensors fit <u>inside</u> enclosures

Identify Failures <u>BEFORE</u> They Happen

- Continuous thermal monitoring - not just a periodic inspection
- Non-contact, permanent installation within enclosures
- Ultra reliable passive IR sensors - require no power
- Instant on-line trend analysis + Two stage alarm per sensor
- Monitor all key points where heat change signifies malfunction
- Easily installed - new - retro fit - expandable
- Integration with over 400 BMS / bus / SCADA systems

Power Service Concepts Inc.
599 Albany Avenue, North Amityville, NY 11701
Phone: 631 841-2300 www.psc-exertherm.com

EXER THERM
PREDICTIVE MAINTENANCE

or included in the Standard. Thus, the Standard shows three examples and recognizes that other valid methods also exist such as the universal polarity management method that will be discussed below.

Method A

Method A (see Figure 2) uses a single module type wired in a

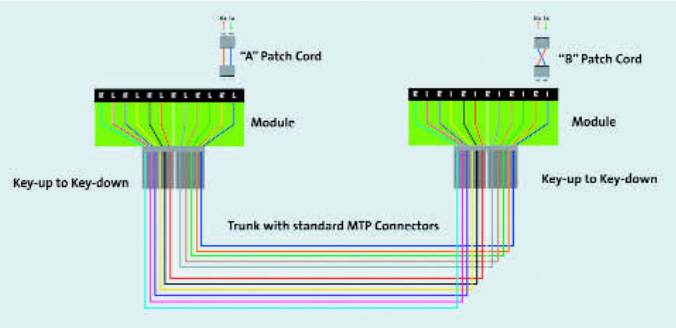


Figure 2

"straight-through" configuration and two different patch cords in an optical circuit. One patch cord is straight wired and the other with a pair-wise flip. All components in the channel are mated key-up to key-down. No guidance is included in the Standard to differentiate where the patch cord with pair-wise flips should be used and how it should be made so that it is easily recognizable from the regular duplex patch cord "straight-wired." Because polarity is addressed in the patch cords, the end-user is ultimately responsible for managing it.

Method B

Method B (see Figure 3) uses a single module type wired in a

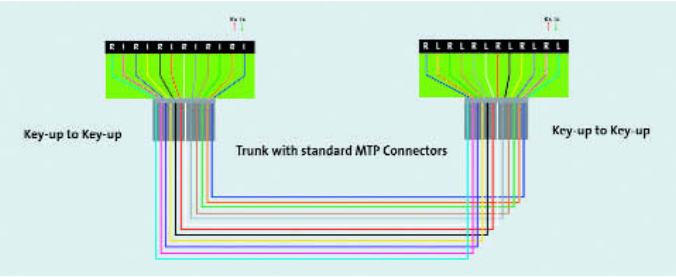


Figure 3

straight-through configuration and standard patch cords on both ends. The differences are that all components in the system are mated key-up to key-up. When the link is configured in this fashion, physical position #1 goes to physical position #12 on the other end. A module on one end is inverted so logically (label-wise) position #1 goes to position #1. This method requires advance planning for module locations in order to identify the module types and location of the inverted module in the optical link. This adds complexity to the polarity management. Using an MTP Connector key-up to key-up configuration does not allow use of an angled polished (APC) single-mode connector.

Method C

Method C (see Figure 4) uses a pair-wise fiber flip in the trunk cable to correct for polarity. This enables the use of the same module type on both ends of the channel and standard patch cords. Because

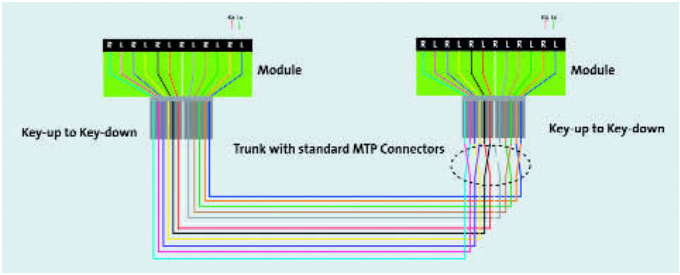


Figure 4

polarity is managed in the trunk, extending the links requires planning of the number of trunks in order to maintain polarity. The TIA Standard does not include text regarding the ability to migrate to parallel optics for Method C, but parallel optic capability can easily be achieved with a special patch cord to reverse the pair-wise fiber flips in the trunk.

Universal Polarity Management Method

The Plug & Play™ Universal System polarity management method (see Figure 5) is an enhanced polarity management method that is

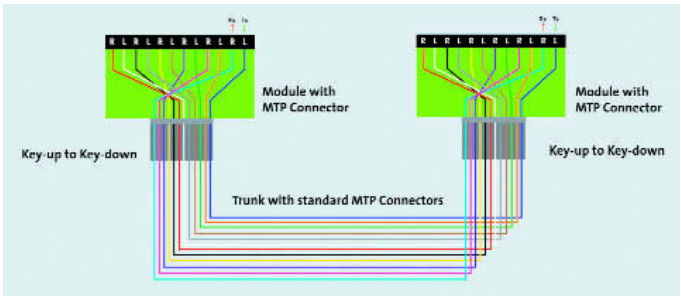


Figure 5

not included but meets the intent of the TIA Standard. The method uses the same module and patch cord type at both ends with no inversion or reconfiguration needed to maintain polarity. Polarity is easily accomplished and managed with the modules internal fiber wiring scheme. The system is mated key-up to key-down. The method supports simple concatenation of multiple trunks without effecting polarity. The method easily accommodates all simplex/duplex connector types as well as single-mode fiber APC MTP connectors. Similar to Methods A, B and C, the Universal polarity management method easily facilitates migration to parallel optics. The wired modular system components enable fast and simple networking moves, adds and changes without polarity concerns associated with special polarity-compensating components used in Methods A, B and C.

Each of the methods works when the rules of that method are followed. The user is cautioned, however, not to mix and mate component parts from the various methods. This will not necessarily work. The Addendum No. 7 Standard states that one method should be chosen and used throughout the network.

In summary, numerous ribbon polarity methods are available to consider. It is essential that end-users and system designers evaluate each method before implementing to ensure that criteria such as reliability, ease of installation, maintenance and reconfiguration, as well as the ability to easily migrate to higher-data-rate solutions that may require parallel optics, are addressed and satisfied.

Doug Coleman is Manager of Technology and Standards for Corning Cable Systems. He can be reached at doug.coleman@corning.com

WHAT TO PROTECT AGAINST? DISASTER AVOIDANCE VERSUS DISASTER RECOVERY

by Gene Kern

Avoidance, Recovery, Continuity

Businesses can be interrupted by events as simple as a network outage, or as devastating as a tornado, fire, or even an act of terrorism. The most appropriate step you can take to reduce the impact of a disaster is to first realize that it could happen to your business.

Let's make sure we're all on the same page, definition-wise. *Disaster Recovery* (DR) describes the strategy an organization employs to deal with potential technology disasters so that the effects will be minimized and the organization will be able to either maintain or quickly resume its mission-critical functions. It follows then that Disaster Recovery Planning (DRP) needs to focus on the data, hardware and software critical for a business to restart operations that have been shut down by a disaster.

Disaster Avoidance, as the name implies, is the process of *preventing* or significantly reducing the probability that a disaster caused by humans, machines, or forces of nature will occur; or if such an event does occur that the effects upon the organization's technology systems are minimized to the greatest extent possible.

Business Continuity (BC) procedures kick in as soon as a disaster is triggered. These procedures are a progression of preordained tasks, manual or autonomic, aimed at enabling an organization to continue serving its customers during and after a disaster. It precedes, and ideally minimizes or precludes, the recovery process.

Business Continuity Planning (BCP), explained below, is an excellent starting point for a business to focus because it yields valuable input that can be used to develop cost-effective *Disaster Avoidance* policies. The BCP process requires the business to identify its mission-critical operations and indispensable processes and data that are essential to keeping the business functioning as a disaster is occurring. Only by knowing the value of the processes and data you are protecting can you have a basis for effectively allocating dollars towards protecting them with Disaster Avoidance methodologies.

After the BCP has prioritized the key business processes, the next step is to identify the specific and significant threats that could disrupt normal operations. And, finally, devise mitigation strategies to ensure effective and efficient organizational response to the challenges these specific threats create during and after a crisis.

While there are certainly overlapping features and objectives of these three strategies, it's important to understand and benefit from the distinctions, because they are certainly not mutually exclusive. Disaster Avoidance policies and procedures will minimize your exposure to certain disasters. Business Continuity Planning will maximize your ability to keep mission-critical processes working as a disaster unfolds or to resume as soon as possible afterwards. And, the main objective of a Disaster Recovery Plan is to bring operations back as quickly and seamlessly as possible after they have been interrupted by an event.

If the BCP process can cost-justify implementing all three, your business will be positioned to face fewer disasters, experience far less disruptions in operations, and will be prepared to recover more quickly when operations are halted.

The Impetus for Disaster Planning

Business preservation is the primary overriding force that supports all efforts to protect your operations from disasters. The internal need, desire and want to survive that are shared by the company's stakeholders, are constantly being challenged by an assortment of external forces and pressures.

To remain competitive in the marketplace, a business simply can't afford to fall easy prey to disaster-related outages and downtime. Customer service suffers, production halts, product deliveries fall behind, and vital communication channels are disrupted. All of which contribute to lost sales, lost customers, and eventually, unless remedied, a failed business.

As more methodologies emerge to assist companies in achieving increasing rates of uptime, competition intensifies further. Businesses that readily adopt and implement these new disciplines and practices are able to increase market share at the expense of the laggards who are not willing or able to allocate resources towards more diligent disaster planning. Some specific examples of these entities and their methodologies include:

- ***Six Sigma*** is a highly disciplined tactic that focuses value-based strategies to increase marketplace performance, increase customer satisfaction, minimize lead time and reduce costs.
- ***The International Organization for Standardization (ISO)*** specifies requirements for state-of-the-art products, services, processes, materials and systems, and for good conformity assessment, managerial and organizational practice.
- ***The American National Standards Institute (ANSI)*** oversees the creation and use of thousands of guidelines that directly impact businesses in nearly every sector.
- ***The Information Technology Infrastructure Library (ITIL)*** is a globally recognized collection of best practices for information technology service management including DRP and BCP.

Within the last decade, the natural desire to survive is being matched in intensity by legislated requirements to survive. Governmental compliance rules are mandating that companies protect stakeholders by maintaining persistent and on-demand access to, and availability of, data, as well as the preservation of communiqués and other electronic records. Some of the more pervasive regulations that have placed on businesses the demand to implement policies and procedures to maximize data integrity include:

- ***Sarbanes-Oxley Act of 2002***, a result of the large corporate financial scandals, represents the biggest modern change to federal securities laws on record keeping.

- ***SEC Rule 17a-4*** requires that member brokers and dealers preserve all original communications that relate to their business for up to three years with easy access for two years.
- ***Gramm-Leach Bliley Act*** includes provisions to protect consumers' personal financial information held by financial institutions.
- ***1996 Health Insurance Portability and Accountability Act (HIPAA)*** establishes regulations for the use and disclosure of any information about an individual's health status, provision of health care, or payment for health care (Privacy Rule).
- ***USA Patriot Act*** requires financial institutions to implement identity verification procedures, antiterrorism regulations, and capabilities to identify customers and flag suspicious transactions.

And, to add insult to injury, some post-911 and post-Katrina laws are even requiring that data survive even when the business doesn't.

Sources, Perpetrators and Categories of Disasters

Be sure to pick your battles. Because, in the disaster abatement world, everything has a price. Certain types of disasters lend themselves to avoidance. With other types, the best you can hope for is a quick recovery.

Take natural disasters, for example. They can't be avoided. No amount of preparation will stop an F4 tornado from running through your community or flood waters from breaching a levy. They're going to happen, so a Disaster Recovery Plan is just smart business. The more exposure to natural disasters your business experiences, the more resources you'll need for DR.

Fortunately, natural disasters, which wreak the most havoc, are also the least common. While frequency statistics for the various sources of disasters differ greatly, depending on their source, there is one recurring conclusion among them all – human error is a major cause of disasters that lead to data loss (32% according to *Strategic Research Corporation*). Collectively, SRC sites hardware and software failures as the leading cause at 58%. Virus attacks are the culprits 7% of the time and, as expected, natural disasters are responsible for only 3% of data loss incidences.

FEMA, which is primarily concerned with the most serious of disasters that effect communities or even greater geographic areas, focus almost all of their energies on three major sources of disaster: Natural causes (meteorological, geological, celestial), human error, and more recently, terrorism.

Ultimately, most studies agree that human behaviors, whether accidental or intentional, will continue to be a leading cause of disasters. When you combine these with mechanical and software failures you are accounting for the vast majority. And, fortunately, many of these can be prevented by implementing *Disaster Avoidance* procedures.

Procedures, Processes and Reporting in a Perfect World

It's the good news/bad news scenario. The good news – fairly capable technology is available for implementing very effective avoidance, recovery and continuity strategies. The bad news – the DR and BC responsibilities are very often managed too low within the organization, with disparate lines of reporting, to yield a cost-effective, optimum implementation of the technology. Normally, DRP is under the auspices of the IT department, while *Business Continuity Planning* can be found within a business unit, operations, or even managed by corporate security.

The result of this scenario will often be a collection of disjointed plans that exhibit superfluous spending and unproductive duplication of efforts. Since there is much overlap in the tasks and resources required to achieve the objectives of DRP, BCP and even Disaster Avoidance, all would benefit greatly from a coordinated, integrated process.

Imagine how streamlined and efficient these plans could be if they were developed by a committee comprised of professionals from

Disaster Recovery Tier Definitions

Criticality Tier	Corporate Impact Description	RTO	RPO	Minimum IT Requirements	Minimum Facilities Requirements	Costs	Data Center Tier
Tier 1	**Mission Critical** Applications defined as being of a critical nature to the success or failure of the corporation	4 hrs	≤ 1 Min	Virtualized Server Environment Geographically Disbursed Clustered Servers Geographically Disbursed Clustered Database Geographically Disbursed Mirrored SAN	Redundant Power System Redundant UPS Redundant Dedicated HVAC Redundant Generator Redundant Fuel Systems Sites Hardened	$$$$$	Tier IV
Tier 2	**Enterprise** Applications or systems defined as impacting the entire corporate environment or a very large % of employees		≤ 1 Min	Virtualized Server Environment Geographically Disbursed Clustered Servers Geographically Disbursed Clustered Database Geographically Disbursed Mirrored SAN	Redundant Power System Redundant UPS Redundant Dedicated HVAC Redundant Generator	$$$$	Tier III
Tier 3	**Departmental** Applications impacting a single department but not defined as critical	24 hrs	≤ 2 hrs	Locally Clustered Servers Locally Clustered Database Locally Mirrored SAN Storage	Redundant Power System Redundant UPS Redundant Dedicated HVAC Redundant Generator	$$$	Tier III
Tier 4	**Local** Applications impacting a single location or small group of users or individuals in differing departments	72 hrs	≤ 36 hrs	Redundant Power Supplies (even numbers) Local Database Local Storage Data and OS Backed Up	Redundant UPS Redundant Predator HVAC Dedicated Power and Cooling Generator	$$	Tier II
Tier 5	**Other** Applications that are not vendor supported, run on out dated OS, are legacy apps that are just reviewed for data, kept to meet regulatory requirements, or are used by a very small segment of the corporate population	≥ 1 week	≤ 1 week	Single Power Supply Single Server Database on local server Local Storage Data Backed Up	Dedicated Power Dedicated Cooling Conditioned Power (UPS)	$	Tier I

multi-disciplines – engineering, finance, operations, IT, and facilities management. And, what if this committee had direct reporting responsibility to a C-level executive? Optimum planning, with top-level buy-in, would certainly maximize the successful results when these strategies are ultimately implemented.

As for the overall process, *BCP* is the most logical starting point, since it includes a *risk assessment* that assigns to each category of disaster, a probability of occurrence over a specific time span. It also defines the impact each type of disaster would have on the business.

Another outcome of the risk assessment is the identification of *Recovery Time Objectives (RTO)*. The RTO specifies how long a particular system can be down before having a major impact on the business' ability to survive. The third benefit of the risk assessment is the determination the Recovery Point Objective (RPO) for each application/system. The RPO identifies how much data can be lost before the business is unable to recover the system in question.

From the RTO, RPO, probabilities of occurrence, and identification of affected systems, an *hourly rate of downtime* can be calculated. At this point, finance and accounting processes are used to cost justify proper levels of spending for disaster avoidance, disaster recovery and business continuity. And finally, assuming the committee has a direct line of report to a C-level executive, approval by a chief decision-maker can more easily be obtained after presenting the resulting recommendations and supporting empirical data.

This is the process that would unfold in a perfect world. An ambitious, but worthwhile goal to aim for.

An Ounce of Avoidance...

Perhaps the only thing more important and cost-justified than a well documented Disaster Recovery Plan is a well devised Disaster Avoidance strategy and a well implemented disaster avoidance architecture.

The most effective disaster avoidance architecture will be impacted by the previously defined requirements and commitments for business continuity, which include budget, resources and management support.

Disaster Avoidance planning assists in understanding the costs and benefits of various architectures through careful consideration of certain key inputs derived from the BCP, including…

- How much redundancy is possible in your application architecture?
- What is your desired Recovery Time Objective (RTO), defined as the amount of downtime that can be tolerated in the event of a disaster?
- What is your desired Recovery Point Objective (RPO), defined as the amount of data loss that can be tolerated in the event of a disaster?

So, what constitutes a well implemented disaster avoidance architecture? Some of the basic elements include:

- Fully-redundant power and environmental systems in all data centers
- Comprehensive disaster recovery plans for each data center
- Annually executed internal and external Disaster Recovery audits
- Perimeter system security consisting of firewalls, virus protection, Spyware prevention and persistent patch management
- Physical alarm and security systems, peripheral security with video surveillance, access security
- UPS and emergency generators

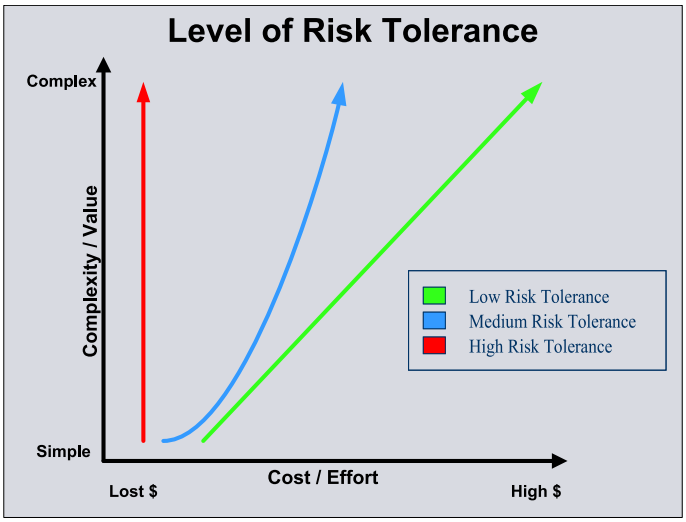
Since we define disaster avoidance as taking all feasible steps to safeguard the physical, informational, and communication assets of the business, where the risk assessment findings determine there is cost-justification, a disaster avoidance architecture can also incorporate a wide range of state-of-the-art technologies, including:

- Enterprise-class, fault-tolerant servers with high 9's availability
- Mainframe technologies, which still provide reliable fail-over capabilities
- Data vaulting, replication, and mirroring
- Fail-over software technologies
- Virtualization, which allows for rapid provisioning of application instances
- SAN storage replicated between sites
- Highly availability systems designed in clusters

Is an ounce of avoidance worth a pound of recovery? Consider that each dollar spent helping the business achieve disaster avoidance, is just that, a dollar spent. But, a dollar spent on disaster recovery, doesn't end there. Far more dollars will be consumed during the outage than will be spent preventing it.

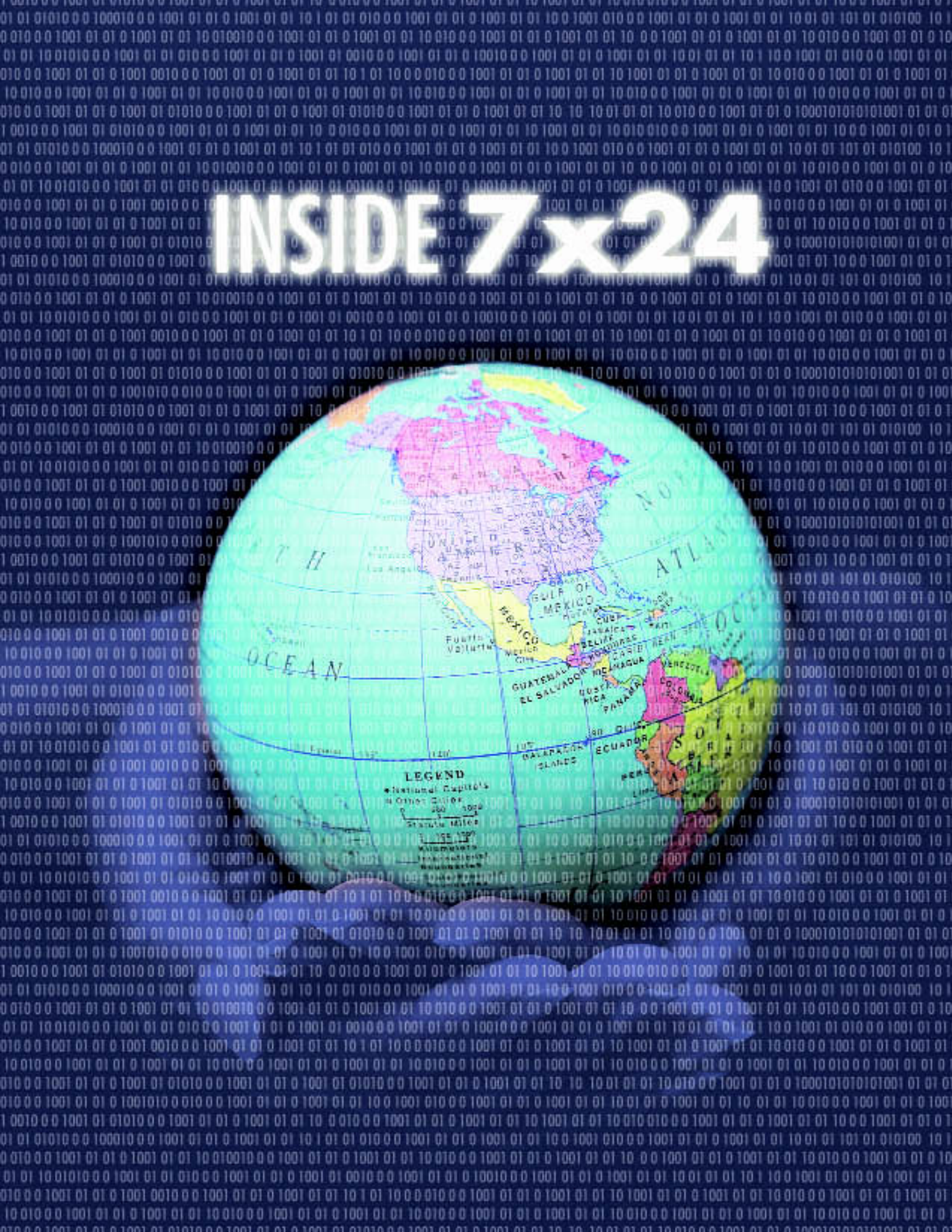
Summary

With modern day global unrest, global warming, and global competition, mitigating the impact of pending disasters isn't a discretionary endeavor; it's a matter of survival. And, the optimum approach is to adopt coordinated strategies for disaster avoidance, disaster recovery and business continuity, since each plays a unique role in the preservation of the business.



Gene Kern is Executive Vice President of WAKE Technology Services, Inc. He can reached at gkern@waketsi.com

INSIDE 7x24



2007 Spring Conference Highlights

The Spring Conference themed "End-to-End Reliability: Mission Critical Standards" will be held June 3-6 at the Boca Raton Resort & Club in Boca Raton, FL. The Spring Conference will feature compelling keynotes, concurrent and tutorial sessions, an all new common hospitality area, a spectacular vendor event, and more...

Fran Dramis

The opening conference keynote address entitled *"Managing the Virtual Data Center"* by Fran Dramis, former Executive Vice President & Chief Information Officer for Bell South will address issues facing CIOs and heads of infrastructure as they manage what is increasingly becoming the virtual "glass house". Back by popular demand on Tuesday morning is Kevin Kealy of AT&T on the topic of *"Voice Security in Today's World"*. If you use a cell phone, Bluetooth, or voice over IP you'll want to hear this presentation. Wednesday's sessions will kick-off with a presentation by Intel entitled *"Data Center of the Future: Concept Versus Realization"* by Gary Howard and Karl Wyatt, Ph.D.

New this conference is a common hospitality area themed "Voo Doo Lounge". Take a stroll on down to the BIG Easy and enter at the sign marked Bourbon Street! Don't stop there... to enjoy Mardi Gras you must keep pounding the cobblestones... Make some stops along the way and don't forget to visit the vendors at the following local establishments..."Famous Door", "Felix Restaurant & Oyster Bar", "Four Corners Blues Bar", "Desire & Oyster Bar", "Jean Lafitte's Old Absinthe House" and the "Cat's Meow". Inside each location you will meet new vendors and enjoy New Orleans style entertainment all night long. The Big Easy awaits...

In addition to enhanced programming 7x24 Exchange International presents "Casino Grande". Get ready for an evening of Blackjack, Craps, Roulette, Slots and other casino favorites! What's that?...You say you don't play...come anyway and enjoy other games like pool, darts and others. If dancing is your thing don't forget your dancing shoes as the rip roaring band "3 Grand" plays your favorites all night long. ***Special thanks to the following organizations for making this event possible:*** **ABB, Data Space Advisors, APC/MGE, Eaton, SIEMENS, Russelectric, PDI, Danaher Power Solutions, Cummins, The Markley Group, Starline Track Busway, Detroit Diesel, Kohler Power Systems, Data Aire, Mitsubishi Electric.**

For the complete Spring Conference program and registration information please visit 7x24exchange.org or call (646) 486-3818.

CORPORATE LEADERSHIP PROGRAM MEMBERS *(at press time)*

Spring Conference 2007

End-to-End Reliability: MISSION CRITICAL STANDARDS

Silver Members

ACTIVEPOWER

APC | MGE
Critical Power and Cooling Services

CATERPILLAR®

Cummins Power Generation

mtu

DETROIT DIESEL

EATON

PDI
creating the perfect wave

SIEMENS

SYSKA HENNESSY GROUP

Key Members

ABB

DANAHER POWER SOLUTIONS

DA DATA AIRE INC.

DataSpace ADVISORS

KOHLER POWER SYSTEMS

MARKLEY GROUP

MITSUBISHI ELECTRIC UPS Division

Russelectric
Power Control People You Can Rely On

SKANSKA

SQUARE D

STARLINE TRACK BUSWAY

t.a.c

INTERESTED IN PRESENTING AT THE FALL CONFERENCE?

Visit www.7x24exchange.org and download the Call for Presentations

Theme: Mission Critical Systems

Deadline: June 22nd

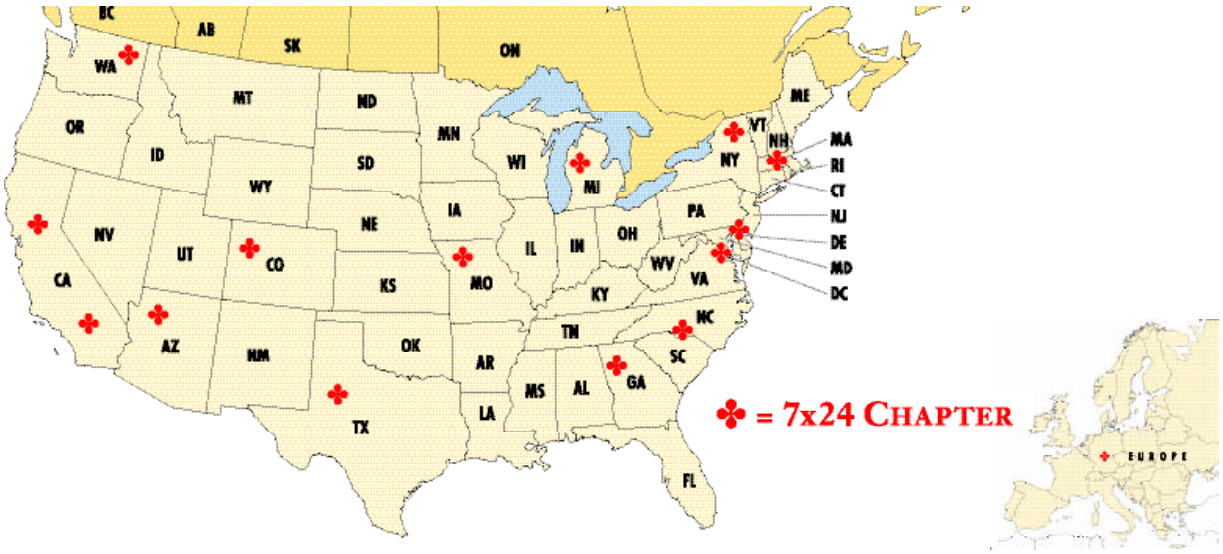
SUBMIT AN ARTICLE FOR THE FALL NEWSLINK

Visit www.7x24exchange.org and download the Call for Articles

Deadline: July 9th

BECOME INVOLVED IN YOUR LOCAL 7x24 CHAPTER

INTERNATIONAL CHAPTERS INCLUDE:



- Arizona
- Atlanta
- Bay Area (San Francisco)
- Boston
- Southern California
- The Carolinas
- Delaware Valley
- Europe (London, UK)
- Lake Michigan Region
- Lone Star (Dallas)
- Midwest (Kansas City)
- Metro New York
- Northwest (Seattle)
- Rocky Mountain
- Greater Washington DC

Visit www.7x24exchange.org today to participate in your local chapter!

7X24 Exchange INTERNATIONAL

The end-to-end reliability forum.

THE PREMIER ORGANIZATION SERVING THE UPTIME INDUSTRY

MEMBER FORUM:

Post ideas...solutions...ask industry related questions!
Both end users and vendors are welcome to use this discussion forum that was built with the 7x24 Exchange Mission in mind, to promote end-to-end reliability among those individuals who design, build, use and maintain mission critical enterprise information infrastructures.

CAREER CENTER ONLINE:

7X24 Exchange Career Center is the premier electronic recruitment resource for the industry. Here, employers and recruiters can access the most qualified talent pool with relevant work experience to fulfill staffing needs.

- **POST A JOB**
  Target your recruiting and reach qualified candidates quickly and easily. Simply complete our online Registration Form and start posting jobs today!
- **POST YOUR RESUME**
  Whether you're looking for a new job, or ready to take the next step in your career, we'll help you find the opportunity that's right for you.

Visit www.7x24exchange.org and Take Advantage of These New Services Today!

NEWSLINK OPPORTUNITIES

Following are the Editorial Guidelines for Newslink together with the Member Advertising Rate Card. Advertisers interested in placing an ad may fax the insertion order to 7x24 Exchange at 212.645.1147 or email to jeremy@7x24exchange.org. Questions? Please call Jeremy O'Rourke at 646.486.3818x109.

NewsLink Member Advertising Rate Card

BLACK AND WHITE RATES

Size	1X	2X	3X
Full Page	$1,500	$1,300	$1,100
2/3 Page	1,100	1,000	900
1/2 Page Island	900	800	700
1/2 Page	700	600	550
1/3 Page	600	550	500
1/4 Page	500	450	400

COVERS & PREMIUM POSITIONS – INCLUDES 4 COLOR

Size	1X	2X	3X
DPS	$5,000	$4,500	$4,000
2nd / 3rd Cover	2,500	2,200	2,000
4th Cover	3,500	2,750	2,500

COLOR RATES

Process Color (4/c)	$900
PMS Colors (add per color)	$600
Process Colors (add per color)	$500

Revisions and Proofs: $50

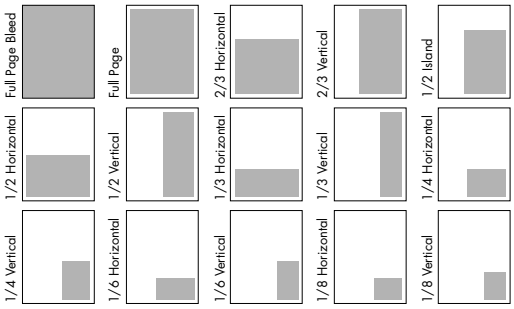
Position Guarantee: 15% premium

*Non-Members add 40% to all rates

NON-BLEED AD DIMENSIONS

Size	Width	Length
Full Page	7.5″	10″
2/3 Horizontal	7.5″	6.5″
2/3 Vertical	5″	10″
1/2 Island	4.875″	7.5″
1/2 Horizontal	7.5″	4.875″
1/2 Vertical	3.625″	10″
1/3 Horizontal	7.5″	3.25″
1/3 Vertical	2.5″	10″
1/4 Horizontal	4.5″	3.25″
1/4 Vertical	3.25″	4.5″

8 1/2″ x 11″ MECHANICAL REQUIREMENTS



Live Area: 7.5″ x 10″
Trim Size: 8.5″ x 11″
Bleed Size: 8.75″ x 11.25″
Halftone Screen: 133 lines up to 150 lines

DPS Mechanical Requirements:

Live Area: 16″ x 10″
Trim Size: 17″ x 11″
Bleed Size: 17.25″ x 11.25″
Halftone Screen: 133 lines up to 150 lines

Advertiser indemnifies 7x24 Exchange against losses or liabilities arising from this advertising. 7x24 Exchange assumes no liability whatsoever, except to the extent of a one time paid advertisement of the same specification, in the next or similar publication, if any proven or admitted errors or omissions have occurred. Payment is due upon receipt of the invoice. Interest shall be charged at 2% per month compounded to yield 26.82% per year on overdue accounts. Revisions to previously submitted ad copy are subject to additional charges. A charge of $30.00 will be levied for returned checks. In the event of a contract cancellation, the advertiser or agency agrees to repay 7x24 Exchange any discounts granted for multiple insertions less any discount applicable for the number of insertions completed in the contract. All cancellations must be received in writing prior to the advertising sales deadline. All premium positions are non-cancelable. Prices are net of agency commission.

EDITORIAL GUIDELINES FOR NEWSLINK

Manuscript specifications: Feature articles vary in length from 500 to 2,000 words. While Newslink accepts articles in a variety of formats, it prefers to receive materials on CD. All articles must be received by the deadline to be considered for a specific issue. Material submitted after the deadline will be considered for the following issue.

Bylines: All articles should include a brief (1-2 sentence) author biographical sketch at the end of the article, that includes the author's name, title, affiliation, address, and phone number. Photos of authors are never used. Newslink does not pay authors for contributions.

Visuals: Authors are encouraged to submit photographs and charts, graphs, or other illustration that will help readers understand the process being described, though it does not guarantee that visuals will be used with the article. Submit all charts, graphs, and other artwork separately; do not incorporate them in the body of the article. Indicate caption material separately. Newslink reserves the right to publish submitted visuals.

Editorial procedures

All articles are reviewed for suitability. Accepted materials are then edited for grammar and to conform with Newslink's editorial style. All attempts are made to preserve the author's writing style, however, Newslink has the right to edit for style, clarity, and to fit space allotments, and to make final selection on headlines, subheads, and graphic treatment. Manuscript submission implies author agreement with 7x24 Exchange's Editorial Policies.

Copyright

Newslink requires first serial rights for submitted articles. This means the author(s) grant Newslink the right to publish the article for the first time. We also request permission for electronic distribution on 7x24 Exchange's web site, www.7x24exchange.org.

Disclaimer

The responsibility for accuracy remains with the author. The opinions and information in bylined articles in this publication are those of the authors and do not necessarily reflect those of the Officers and Board of Directors of 7x24 Exchange.

Just one of our state-of-the art solutions for ensuring power reliability.

RELIABILITY

Turn it on.

For more than 100 years, Square D® has been the nation's leading electrical brand. Not just because of the products. But also because of our people. Experts who know how to create the right power system for you.

From engineering studies to turnkey project management, our critical power experts are dedicated to solving your most challenging power problems and delivering unsurpassed power reliability. With a host of Square D power management, power control and power distribution products, you can be confident the experts will create the right solution for you.

So you'll always have the power you need.

Turn reliability on. Sign up for a critical power information kit at www.criticalpowernow.com/kit.cfm.

a brand of Schneider Electric

SQUARE D