PUBLISHED BY 7X24 EXCHANGE INTERNATIONAL

7X24 Exchange INTERNATIONAL

THE END-TO-END RELIABILITY FORUM™

Theresa Payton
2015 Fall Conference
KEYNOTE SPEAKER

COLLABORATION GUIDES DATA CENTER DESIGN

FALL 2015 • www.7x24exchange.org

CONTENTS

As a service to assist our valued members in staying informed about our dynamic industry, 7x24 Exchange is pleased to publish 7x24 Exchange® Magazine, offering articles by leading professional experts on current and future trends, best practices, and the state of our industry. Please note that the opinions and views expressed in these articles are those of the individual authors themselves, and do not necessarily reflect the views of 7x24 Exchange or any of our members.

7X24 Xchange INTERNATIONAL

The end-to-end reliability forum.™

www.7x24exchange.org

DIRECTORS AND OFFICERS

Chairman & CEO
ROBERT J. CASSILIANO
Business Information Services, Inc.

President
DAVID SCHIRMACHER

Vice President
CYRUS J. IZZO, P.E.
Syska Hennessy Group

Director – Marketing, Vendor Representative
JULI IERULLI
Caterpillar

Director – Chapter Representative
MICHAEL SITEMAN
M-Theory Group

STAFF

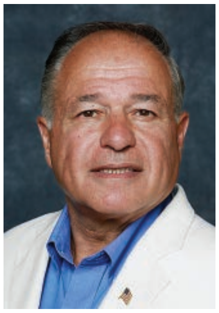
Director – Chapter & Member Relations
KATHLEEN A. DOLCI
646-486-3818 x103

Programs Director & Editor, 7x24 Exchange Magazine
TARA OEHLMANN, ED.M.
646-486-3818 x104

Senior Director of Conferences
BRANDON A. DOLCI, CMP
646-486-3818 x108

QUESTIONS?
Call (646) 486-3818
www.7x24exchange.org

CHAIRMAN'S LETTER



Robert J. Cassiliano

As summer fades away we look forward to the rejuvenation of the fall season!

The Mission Critical Industry was created to ensure the continuous processing of information required for business operation. Data is the key component of that information, which makes protecting that data of utmost importance. Big Data complicates the data landscape with its facets of volume, velocity, and variety. Protection is achieved on a number of fronts. First the technology hardware and software must ensure the data is processed without corruption or loss of data and there is the proper level of redundancy and backup. Next the building infrastructure supporting the technology must have the reliability and resiliency to provide a fault tolerant facility so there is no interruption of data processing. A robust data security program must also be in place consisting of data protection across computer hardware and software, storage devices, networks, and all peripheral equipment and edge devices. Today there is an additional need for a cyber security program that protects against such attacks as a denial of service or a hack that causes a business shutdown. The cyber security program should have the ability to monitor for potential threats, detect an attack, prevent an intrusion, remediate the problem, and recover from a cyber incident. In the Mission Critical world data is king and we as professionals in the industry have the responsibility to protect data integrity and data processing.

7x24 Exchange's conference goal is to provide attendees with the best of education, networking, and information sharing all in an environment designed for a memorable experience for you and your guests. 7x24 Exchange is committed to providing value to members, conference participants, and their companies.

The theme for the 2015 7x24 Exchange Fall Conference being held at the JW Marriott San Antonio Hill Country in San Antonio, Texas November 15 – 18, 2015 is **End to End Reliability: "Commitment to Excellence".** Conference highlights are as follows:

- Welcome Reception
- Sunday Tutorial
- Conference Keynote: "Big Data and the Internet of Things: Boon or Bust for your Cybersecurity" by Theresa Payton
- Keynotes by Fran Dramis & Yahoo!
- Presentations by Compass Datacenters, CPS Energy & Sentinel Data Centers
- Monday evening: "Marquis Plus+ Partner Showcase"
- Talks from Oracle, National Bank of Abu Dhabi, The Green Grid & ASHRAE
- Exchange Tables on specific topics at Tuesday lunch
- An End-User Exchange Forum Luncheon

Sponsored Event: **"A Night at the Rodeo"**

The program content is designed to provide value to conference participants and their companies by focusing on important topics of the day. Cyber Security, colocation, and modular design are highlighted at this year's Fall event.

I look forward to seeing you at the Fall Conference in San Antonio, Texas!

Sincerely,

Bob

In keeping with its commitment to social responsibility, Chairman & CEO, Bob Cassiliano presented the conference keynote speaker Mark Kelly with a $5000 donation on his behalf to America's Vet Dogs.

COLLABORATION

GUIDES DATA CENTER DESIGN

SAN ANTONIO'S CPS ENERGY BUILDS THE AREA'S CONTROL/DATA CENTER BACKBONE FACILITY

by **Will Hodges, P.E., Val Loh and Bob Stickney**

A national hot bed for data center growth, the city of San Antonio is home to some of the country's most high-profile mission critical facilities. So when local utility provider CPS Energy set out to design and build a new 75,000 sq. ft. flagship mission critical facility of its own, called "**Project ECHO**," it needed to champion reliability, redundancy, scalability and flexibility.

But, challenges were abundant. For one, CPS Energy prides itself on being a steward of energy conservation. Considering the City of San Antonio's continual pursuit of data center projects (and with as many as 10 stand-alone data centers already within five miles of the facility), ECHO had to lead by example — to be a real showcase of energy efficiency. Additionally, ECHO needed to accommodate the next 20 years of growth while simultaneously functioning today as a redundant site for two existing CPS Energy control/data centers.

The solution was a single overarching principle that guided the entire project from start to finish: collaborative design.

IT ALL BEGAN WITH A DESIGN CHARRETTE

In order to meet the project's goals from both an MEP and Technology systems perspective, Syska Hennessy Group worked collaboratively with the entire building team — from architects to end users and every building team member in between — beginning with a pre-design charrette.

The charrette set the tone for ECHO by establishing four Guiding Principles that would serve as the foundation for the basis of design documents. These principles streamlined the efforts of building team members from design to construction and post-occupancy, ultimately ensuring that the original objectives were met in the final facility.

1 Silicon Realities. This first Guiding Principle addresses ***reliability, maintainability, functionality, flexibility and a robust system architecture.***

This principle established design parameters early on that directly resulted in an established basis of design and increased collaboration since the building layout took shape with the contractor at the table in the early design phase. Similarly, when it came to designing the data center's cabinet layout, reliability and functionality were key. Therefore, CPS Energy and Syska's team required that a physical mockup of a typical row of cabinets be created. This mockup included the full complement of infrastructure, including the back-of-rack cooling solution, overhead busways, cable tray and lighting so CPS Energy could see what their system would look like and how these individual components would all be accessible between each row of cabinets. Again, this helped eliminate questions and future operational maintenance issues in the field.

To build in flexibility for future expansion on site, Syska designed an MEP/IT infrastructure that would be ready for a Phase II build out, with the ability to expand the building for additional cabinets and utilize existing back of house spaces to accommodate an additional generator, UPS, chillers, and piping, etc. to support Phase II. The goal was to preserve the ability to expand while minimizing the impact to ongoing whitespace operations.

Increased efficiency and reliability were established at ECHO by eliminating the raised floor and replacing traditional computer room air conditioner (CRAC) units with a refrigerant based back-of-rack cooling solution. With no raised floor, the EPO system could be eliminated. Instead of traditional CRAC units supporting the whitespace, pumped refrigerant units were installed in galleries adjacent to the space, keeping all chilled water piping located outside of the critical spaces.

2 Carbon Creature Comforts. This Guiding Principle tackled ***consistency, survivability, daylighting and a softened security experience.***

ECHO's control rooms are a case in point for this Guiding Principle. Together, Syska's MEP/Technology team and the architects at Corgan Associates began control room design by defining how many operators would be working in the areas, which led to deciding how large the space would be, how many display screens, size of screens and ultimately, the owner's requirements for low-voltage systems. Syska's MEP/Technology team utilized 3D modeling software to fine-tune control room designs, which resulted in a recessed well in the operator consoles to accommodate desired sightlines and an articulated monitor mounting solution that could pivot at the top and bottom to enable control room operators to see beyond their own monitors onto the main display wall screens. This process was critical to meeting the operator's requirements while optimizing the design and coordination of architectural lighting, MEP and technology.

While the facility is a mission critical control/data center, CPS Energy made it a priority to create a positive human interface for those working inside. For example, a floor path between the two control rooms was created with artwork and creative lighting and ergonomic desks were specified for employees. One of the biggest design challenges was to segregate the two control rooms per federal regulations — with a six-wall separation. How can a working separation be maintained while not duplicating areas that could be deemed common space? To achieve the separation between different function areas, the design team worked closely with CPS Energy's project committee members and Project Manager Bill Badger, who was responsible for coordinating the needs of each group. The results of this coordination allowed for efficient floorplan design without duplication of common use space. A successful space plan for facilities such as ECHO requires a commitment from the owner to actively be involved with the design team, including decision makers during the design process.

THE 4 GUIDING PRINCIPLES

3 Good Neighbor. This Guiding Principle addresses the *public perception, stewardship and the building's site-scaping.*

CPS Energy was sensitive to the fact that their new facility would be adjacent to a single-family residential neighborhood. It was important that the facility design respect the surrounding context in both scale and appropriateness. Heavy landscape elements were placed between ECHO and the residential area on the north side to create an image of a park-like setting. The service areas and equipment were evaluated and screened to minimize acoustical concerns. The facility itself is also set back over 100 feet from the property line to provide a buffer zone between the neighborhood and the building. The softer aesthetics of the office facade (including a lower building height, a café and an exterior courtyard) were located on the north side facing the residential neighborhood. This was done to provide a connection between the CPS Energy employees and the neighborhoods they serve.

Typical Cabinet Placement. No raised floor and open plenum above.

4 Responsible Corporate Image. This Guiding Principle ensured ***sustainability, marketability, demonstrability, xeriscaping and display of energy conservation.***

LEED Gold certification was a key goal for the ECHO project. To support this goal, special consideration was given to the mechanical cooling system selected. Multiple HVAC systems were studied to determine which one made the most sense from both reliability and energy efficiency standpoints.

Syska's team developed a computational fluid dynamic model (CFD) to find the optimal system layout to cool the racks on the computer room floor and aid low-voltage and MEP systems coordination. This led to the specification of an efficient back-of-rack, refrigerant-based cooling system. The system's back of rack heat extractors have variable speed fans that modulate to control the rate of heat transfer between the air and the refrigerant. This unique solution provides a "room neutral" design where the discharge air is cooled back to room temperature prior to re-entering the space. The refrigerant to water heat exchangers were designed to be installed outside of the critical space, so that only the refrigerant piping and back of rack units are located within the critical space, minimizing the coordination needed to support all the infrastructure. In addition, the design of the system allows a single refrigerant pumping unit to be taken down for maintenance while the cabinets served by this unit can continue to operate through alternate feeds from the adjacent pumped refrigerant row.

Through energy model simulation, the selected HVAC system results in ~13% energy savings over the ASHRAE 90.1 baseline case of a packaged direct-expansion system. This, coupled with the IT virtualization energy savings of ~39%, produces a very energy efficient system that matches CPS Energy's charge to minimize energy consumption and maximize energy efficiency.

COMING FULL CIRCLE

Team collaboration was the key to success for ECHO. From day one to move-in, it set the tone for building a reliable, redundant, scalable and flexible mission critical facility that met all the owner's objectives and brought the team's Guiding Principles to life.

"The Syska Hennessy/Corgan team, combined with Turner Construction, translated some basic requirements into a state-of-the-art facility on a modest budget. By asking questions, listening carefully and then coming back with options and recommendations at every step of the process, the design and construction teams assimilated our underlying mantra of reliability, availability and maintainability for this data center. They were the consummate collaborative partners," said Bill Badger, Project Manager, CPS Energy. "We would sketch out ideas on a dry erase board or over a web conference. In short order, those ideas were integrated into the design and construction of the building. For CPS Energy, this was the perfect integration of owner, designer and builder. ECHO is the tangible result of the best teamwork on the planet."

VITAL STATS:

CPS Energy Mission Critical
Control and Data Center

San Antonio, Texas
75,000 sq. ft.
Opened 2015

The CPS Energy's Mission Critical Control and Data Center (ECHO) was built with concurrently maintainable goals in mind, with a feed from two utility sub stations, allowing for a robust system while maintaining the overall budget constraint. Supporting multiple operating groups under a single roof, the facility is awaiting LEED Gold certification. ECHO features a control center operating space of 10,000 to 15,000 sq. ft. The facility's data processing or white space area is currently comprised of another 10,000 sq. ft. of space, with design provisions to double the space and critical IT load for future expansion.

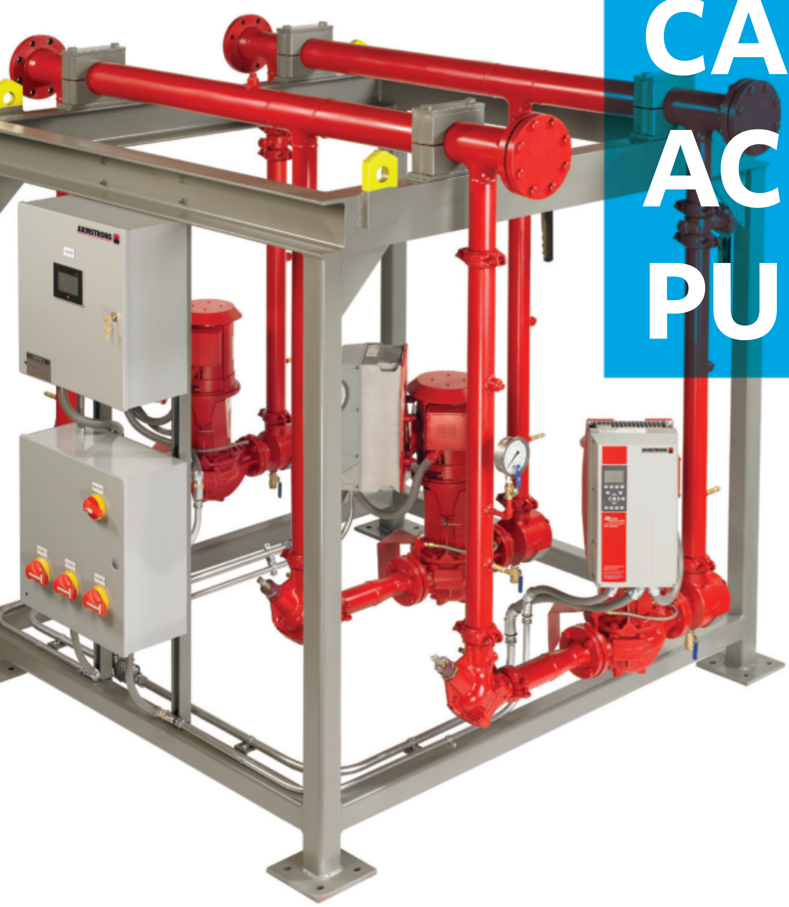
Bill Badger, CPS Energy Project Manager

Refrigerant-based laminar cooling system located on the back panel of each rack.

Will Hodges, P.E. is Senior Associate at Syska Hennessy Group. He can be reached at 972-638-5406
Val Loh is Principal at Syska Hennessy Group. He can be reached at 212-556-3404
Bob Stickney is Principal at Syska Hennessy Group. He can be reached at 972-638-5420

ARMSTRONG

ARMSTRONG CAN HELP YOU ACHIEVE YOUR PUE TARGETS



Modular, integrated cooling solutions to maximize your uptime and increase efficiency.

Our ultra-efficient cooling systems are designed for part-load conditions and offer a scalable approach to your system requirements.

DESIGN ENVELOPE

Design Envelope is a revolutionary technology pioneered by Armstrong that offers simplified pump selection, lowest installed cost, expanded application flexibility and optimized energy efficiency.

BENEFITS

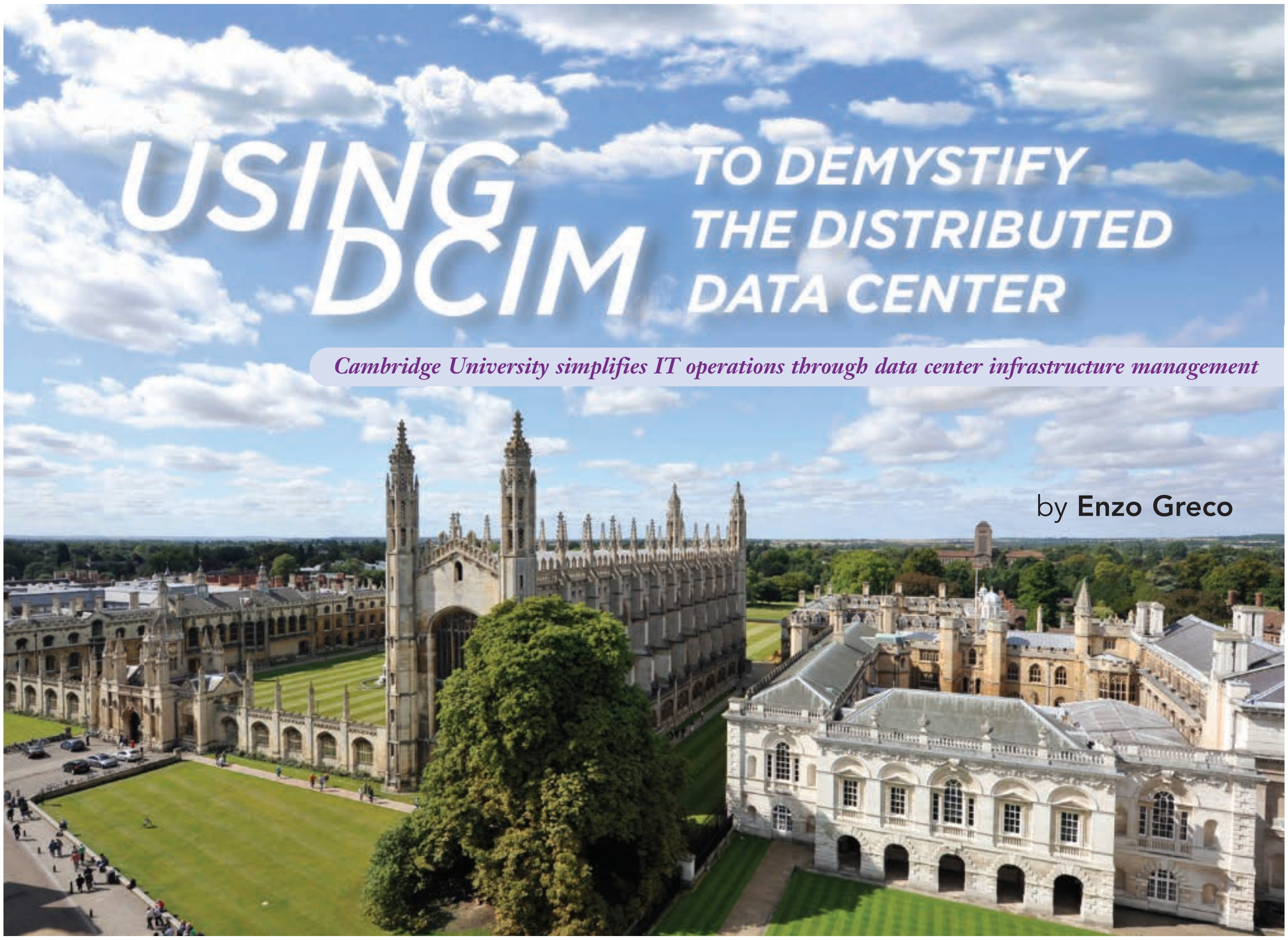
Energy Efficiency

Time to Market

Performance Reliability

ARMSTRONG FLUID TECHNOLOGY
ESTABLISHED 1934

ARMSTRONGFLUIDTECHNOLOGY.COM



USING DCIM TO DEMYSTIFY THE DISTRIBUTED DATA CENTER

Cambridge University simplifies IT operations through data center infrastructure management

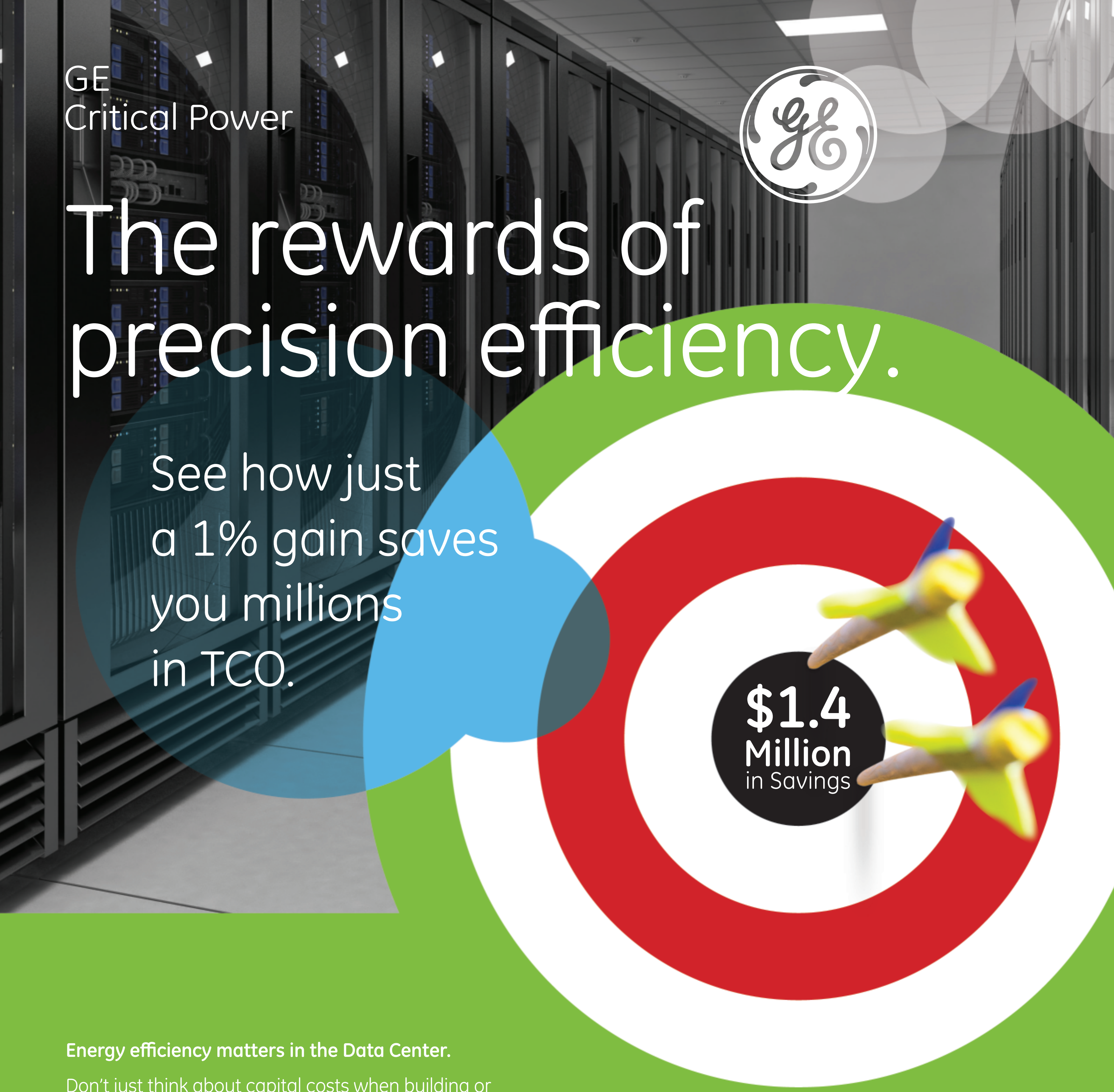
by **Enzo Greco**

Data center infrastructure management—real, dedicated DCIM—is about a decade old (barely), and already has evolved into something its creators didn't expect. DCIM was designed for a different time and a vastly different data center—the swollen facilities of the early 2000s that housed row after row of servers and were built to add even more. No one could imagine a reason why things wouldn't continue that way, and organizations needed to track and manage those assets in increasingly virtualized environments. Because necessity, as they say, is the mother of invention, DCIM was born. No, scratch that. This was when DCIM was conceived. Birth came later, and that's an important distinction.

DCIM gestated while the need for greater visibility and asset management increased. But something else happened during this time—the data center evolved. Server capacity increased, energy efficiency across systems became a priority and enterprise data centers became something of an endangered species. Hyperscale—think Google, Amazon and Facebook—emerged with its own unique architectures, and cloud and colocation facilities started to siphon computing away from traditional enterprise facilities. As DCIM became fully formed, it emerged as and remains a valuable solution in these environments.

But there's another vein of data center evolution—distributed networks, with IT closer to end users and smaller data centers at the hub. These networks can have multiple small computing modules spread across different locations, providing local computing and storage while still networking with each other and with the small data center at the network's center. Individually, these are simple IT resources—often just a rack with a server or servers, power distribution, maybe some

DIESEL | GAS | POWER PLANTS | RENTAL
ST. ALEXIUS MEDICAL CENTER
CAT


$1.4
Million
in Savings

basic thermal management, and networking capabilities. Simple, right? But taken collectively, these are complex networks with considerable management challenges. It might not be what the earliest DCIM engineers had in mind, but the distributed data center is a challenge today's DCIM solutions are built to address.

Case in point: Cambridge University

Cambridge University in England is one of the world's leading research institutions and has been for more than 800 years. The institution's dedication to learning and innovation extends beyond academics and into its operations, including IT. The university values unified technology support that enables and drives achievement, but maintaining an integrated IT infrastructure has been a challenge. As the campus and various departments grew and evolved, separate micro networks popped up. Each department had the option to integrate its servers with the campus's main data center, but it wasn't required. As a result, the campus ended up with more than 200 server rooms serving 120 departments, and most of them operated independently.

None of this is all that unusual, but it's an inefficient way to operate—and the IT personnel at Cambridge knew it. All of these separate, independent IT nodes eliminate the benefits of consolidated management, standardized service delivery and improved security and availability. On top of that, each department was free to build its computing capabilities to its own specifications—and using whichever equipment manufacturers it liked. That's 200 loosely connected server rooms with little or no consistency in terms of server or infrastructure vendors—again, not a model of efficiency.

The university's IT staff understood the need to improve visibility and management of this computing quilt, believing it was the key to optimizing computing performance and efficiency and reducing skyrocketing operational costs. Their solution? Consolidating some of the far-flung IT rooms in a single modern data center and uniting the new facility and remaining distributed computing sites under a single DCIM system.

DCIM in a Distributed Environment

While the distributed model is relatively new, applying DCIM to improve visibility and control of a web of hard-to-see IT assets is more or less exactly what the technology was developed to do. The physical location and heterogeneous nature of the Cambridge facilities just added another layer of complexity. Ultimately, the desire was the same as it is for any DCIM customer: to see and control multiple assets—not just servers, but every component across the network—from a single location.

Cambridge settled on Emerson Network Power's Trellis™ platform, a DCIM solution that enabled management of multi-vendor IT, power and cooling resources through a single pane of glass. The consolidation, data migration and DCIM implementation is an ongoing process, but the early returns are overwhelmingly positive.

The system works with output from the various pieces of equipment including critical infrastructure, configuring and organizing data from multiple sources and translating it into a set of unified actions. It allows the university to reduce both capital and operational expenses by virtualizing platforms and refreshing equipment, using the central data center space intelligently, and implementing evaporative cooling systems. It has made everything the university does around its IT systems smarter, and we would expect nothing less from a place like Cambridge.

Enzo Greco is Vice President and General Manager, Software, Data Center Solutions at Emerson Network Power.
He can be reached at Enzo.Greco@Emerson.com

A Business Service Management Approach for High Performance Computing (HPC) Data Centers

by **Abdullah Aldhamin & Bander Alotaibi**

Abstract – In recent years, there has been a growing practice among IT organizations to deploy Business Service Management (BSM) solutions. In this paper we describe and share Saudi Aramco's EXPEC Computer Center (ECC)—a leading scientific HPC-based data center—experience and recommendations in choosing and deploying a business service management solution to model, manage and monitor our IT resources.

I. INTRODUCTION

Built in 1982, the Exploration and Petroleum Engineering Computer Center (ECC) is designed to provide state of the art technologies and computing power to enable Saudi Aramco geologists, geophysicists and petroleum engineers to explore, develop and manage Saudi Arabia's oil and gas reserves. While the majority of these technologies and services are powered by high performance clusters, a significant number of services are still hosted on traditional servers.

In Saudi Aramco's exploration activities, HPC continues to play a critical role in enhancing geologist's and geophysicist's ability to interpret the subsurface of the earth more accurately. The ability to run complex codes and algorithms on large amounts of seismic data and outputting very detailed images of the earth are only possible by utilizing the massive computing power of clusters. Similarly, major resources are required to allow petroleum engineers to simulate large geological models of reservoirs to understand fluid flow behaviors [1].

Although HPC provides the resources to addresses the high computational needs in the oil and gas industry, many challenges are associated with the large amount of hardware in data centers and the growth rate of the that hardware. One of the main challenges is ensuring the availability of the entire IT infrastructure by utilizing the appropriate IT infrastructure monitoring solution.

A wide variety of monitoring solutions exists in today's market, ranging from free monitoring systems such as Nagios [1] and Zabbix [2] to

PDI
PowerWave
Wavestar® RPP
PowerHub® PDU
Wavestar® PowerPak PDU
Wavestar® STS
JCOMM® BCMS Retrofit

POWERING DATA CENTERS
EMPOWERING GENERATIONS

SMART SWITCHGEAR SOLUTIONS FOR YOUR DATA CENTER NEEDS.

LEARN MORE ABOUT OUR ADVANCED PRODUCTS

WWW.THOMSONPS.COM 1.888.888.0110

REGAL

Thomson Power Systems
Quality • Reliability • Commitment

commercial products such as HP OpenView and IBM Tivoli. Additionally, available solutions differ based on the nature of the business and the required usage such as Web application monitoring solutions designed for monitoring transactions by simulating user transactions. Even solutions in the same category such as IT infrastructure monitoring differ in their licensing strategy and for high growth environments solutions that charge by device or monitor can quickly increase the cost.

In this paper, we will share Saudi Aramco's EXPEC Computer Center experience in choosing the proper monitoring solution for data centers that mainly use HPC systems and what considerations need to be taken.

A. IT SERVICE MANAGEMENT

An effective monitoring solution of IT resources is a main part of IT service management (ITSM), an approach necessary for organizations to manage large-scale IT systems. ITSM is a process based approach to manage an organization's IT systems with a focus on IT services rather than IT systems [2]. It aligns an organization's IT services with business processes to ensure customer needs are effectively met. It introduces management processes to cover the entire life cycle of an IT service including; planning and designing of a service, delivering the service, support and finally continual service improvement [3]. Several of these processes are dependent on IT systems monitoring such as change management, problem management, incident management and configurations management [4].

Having effective IT service management should be a strategic goal for any organization, especially organizations with medium to large IT systems such as an HPC in our case. Today, various best practices exist that if implemented will ensure effective ITSM. Available frameworks include, but are not limited to Information Technology Infrastructure Library (ITIL) [3], Capability Maturity Model Integration (CMMI) [4], Microsoft Operations Framework (MOF) [5] and Control Objectives for Information and Related Technology (COBIT) [6], where standards include ISO 20000 and ISO 9000.

II. BUSINESS SERVICE MANAGEMENT

A common element in an Information and Communications Technology environment is the Business Service Management (BSM), which is a standard approach to model, monitor and manage IT infrastructure in a customer-centric and business-oriented configuration. It is normally positioned on top of ITSM to ensure that business and customer objectives provide an input to define the ITSM model, and the business services offered by the IT organization. The BSM process has driven the development of the traditional network monitoring software industry to use complex layers of differing technologies to close the gap between knowing the problem from a technical point-of-view and the business impact. BSM has been identified by the ITIL as a best practice for IT infrastructure management and operations.

BSM consists of both a structured process and enabling software, allowing IT organizations to operate by service rather than by individual configuration items (CIs) or technology. This has led organizations to prioritize their efforts, and ultimately improve the services delivered to upstream users. That said, BSM is a way to bring together many disjointed processes and applications, and develop quantifiable improvement in efficiency and ability to view IT infrastructure relevant to business processes.

Also, BSM, as a process, is not software by itself. However, there are tools and software solutions that are considered critical enablers to implement BSM in an organization [7] [3]. Thus, BSM software and tools have been popular over the years.

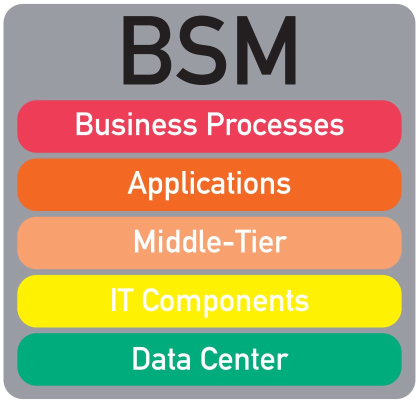


Figure 1: Key Elements to Build a BSM.

Unlike legacy network management systems, BSM software [7] [8] provides a unified view for data center administrators to view and manage devices, applications, networks and events usually from a common dashboard. Traditional network management systems focus on measuring and monitoring the technical availability and performance metrics of IT infrastructure, such as CPU and memory utilizations. However, these tools do not provide the necessary information to determine the business impact of a specific problem. For example, if a server and a storage filer fail at the same time, legacy tools cannot determine which of these two elements is more critical to the business or which business processes have been impacted by the failure.

III. FACTORS TO CONSIDER

In recent years, there has been a rapid development of software solutions to help organizations implement the BSM process. As a leading scientific data center, ECC has the experience

CLUNE
Construction Company

AN AWARD-WINNING GENERAL CONSTRUCTION FIRM — SERVING CLIENTS THROUGHOUT THE USA

Chicago | Los Angeles | New York | San Francisco | South Florida | Washington, DC
clunegc.com

with evaluating and deploying several legacy network management tools and BSM software solutions. This experience allows us to share some key considerations when it comes to implementing solutions in an HPC-driven scientific data center.

A. DATA CENTER OPERATIONS

One of the first factors to consider is the way the data center operations are handled. An unmanned data center operations strategy requires a complex backend solution to run the whole process in an automated manner. Whereas manned data center operations would require a different type of solution, which is user friendly, and offers the required capabilities. In addition, the level of tasks assigned to the operators in response to received events determines the needed capabilities and functions from the BSM solution. These considerations though seemingly primitive, are important starting points that help direct what to look for in a BSM solution.

B. BUSINESS SECTOR

Understanding the business sector where the data center operates is yet another key factor to consider. Service providers, financial institutions, public sectors, and scientific data centers have different types and architectures of technologies, and, hence, operate differently. While financial institutions are more interested in keeping a tight control on each single transaction and ensure it is successfully completed, service providers are more concerned about infrastructure devices such as network devices and servers. The main reason for this difference is the business objective, in which a service providers' business is affected by an availability issue of servers and other devices. In a scientific HPC-based data center, however, the criticality of nodes can be completely different. Typically, such an environment is based upon commodity hardware vulnerable to hardware failures and it is normal to have several nodes totally unusable for maintenance. Hence, the BSM must be configured so that it does not panic on each node failure, unless necessary.   That said, a good BSM solution for a data center in one industry may not deliver the required business value for another data center in a different industry. Therefore, knowing what each BSM vendor in the market provides and the industries where their solution is more dominant provides a strong insight on steering the decision for the BSM solution.

C. LICENSING MODEL

Licensing model plays a crucial part in determining the cost efficiency of the monitoring solution. The licensing model also defines the required administration efforts by support. In general, software licenses are categorized into the following: proprietary licenses and free and open source license. Proprietary licenses grant the use of the software solution to users, while the ownership of the software remains with the developer, and, as such, modifications can only be done by the developer.

Free and open source software licenses, however, allow users and developers to use, modify and share the software and the source code behind it. Table 1 summarizes the main differences between both proprietary and open source licenses. There are different methods to define the scope of the license for the proprietary commercial BSM solutions. For example, they could be licensed per monitoring point, which is measured by what needs to be monitored, e.g., disk utilization and CPU. They could be licensed per monitored device, measured by the number of devices to be monitored. Finally, they could be offered with an unlimited site license model.

In addition, there are two proprietary licensing models commonly used for BSM solutions: subscription and perpetual license models. In the subscription license model, the owner is entitled to utilize the software based on the number defined in the license scope. This means that the cost associated with the software

	FREE AND OPEN SOURCE	PROPRIETARY
Cost	Mostly Free.	Free or paid.
Copyright	Licensed, credit given to original developer when modified.	Licensed by developer only, user granted rights to used
Source Code Ownership	No ownership rights.	Developer owns rights.
Source Code Modifications	Anyone can modify.	Only developer can modify.

Table 1: Comparison between Proprietary vs. Open Source License.

changes in each cycle depending on the number in the license scope. Thus, the owner is entitled to install, run, and request maintenance and support for the software as long as an active subscription is maintained. In the perpetual license, however, the owner pays an initial cost to purchase the use of the software for the defined number in the license scope. The initial cost usually is inclusive of maintenance services for the first year. In addition, the owner may opt not to have official maintenance services for subsequent years without affecting his rights to the use of the solution. Table 2 summarizes the main differences between these two license models.

Considering the case of a high performance computing (HPC) data center with a large number of nodes (in thousands), a perpetual site license will be more effective. It is expected that all of the HPC nodes need the monitoring template, with a few exceptions to cater to some business requirements. Thus, the site license will be more efficient since all managed devices are almost identical.

D. AGENT VS. AGENTLESS

There are two approaches to apply the monitoring to computing infrastructure components: agent-based and agentless monitoring. Each approach brings its own pros and cons. A key decision on choosing a monitoring solution is to decide whether to look for agent-based or agentless solutions. The agent-based monitoring solution consists of a of software component, typically a small application, residing on the client server and collecting data. The data is then returned to the monitoring station based on a policy within the local agent, or as requested by the monitoring server. In this practice, the agent is very lightweight but able to access granular metrics for better monitoring, alerting and reporting, as well as deeper levels of root-cause analysis and trouble shooting. In addition, advanced capabilities and functions, such as patching and configuration management, can be encapsulated within the agent itself. Furthermore, agent-based solutions allow for more flexibility with the creation of customized service monitors.

However, some agents are very heavy consumers of resources and can stress the servers they are monitoring; this could eventually reduce the performance of the servers they are monitoring. This is an important decision when considering HPC data center monitoring, in which resource utilization is crucial. In addition, agents introduce considerable support and administrative overhead to ensure their compatibility with the running system's health, and that they do not introduce any security breaches to the environment. Moreover, agent-based solutions could limit the scalability of the solution to the number of agents it can manage, which is an important metric for a large HPC environment. The agentless solution, however, does not require specific software component to deploy the monitoring, which solves most of the problems introduced by the agent-based solution. Generally, they rely on standard system APIs or network packet analysis methods.

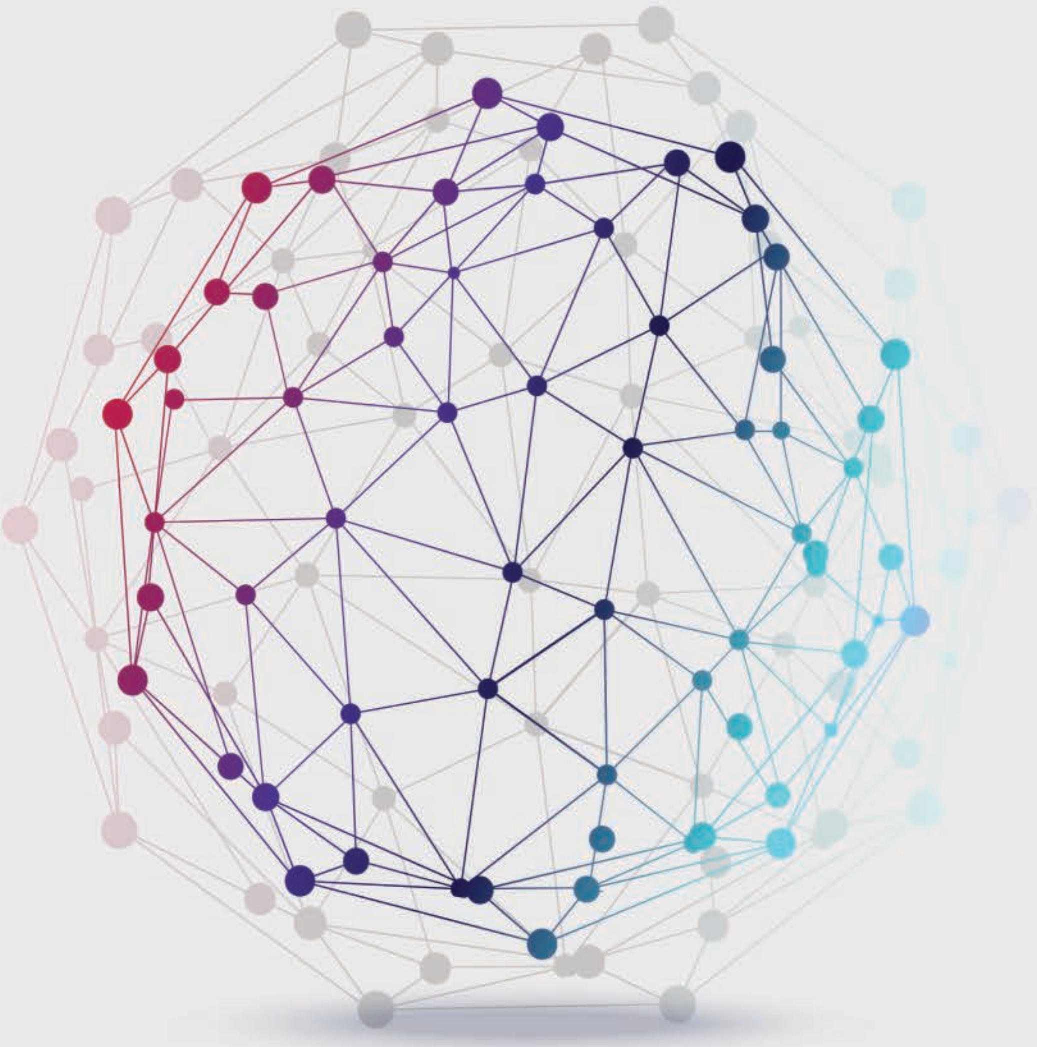
There are different methods used in practice for agentless monitoring: such as SNMP (Simple Network Management Protocol) for Linux/UNIX, network device and storage filers; WMI (Windows Management Instrumentation) for Windows-based systems; SSH (Secure Shell) for Linux/UNIX systems [9]. For SNMP to work, however, the SNMP agent must be configured and enabled to send/receive SNMP traps. But, it is still widely accepted that SNMP monitoring is considered agentless since the agents are standard software components within the monitored systems. Thus, agentless does not require any specific software to install on managed devices, eliminating all overhead associated with agent-based systems.

On the other hand, agentless solutions will be affected by networking issues. Also, when monitored systems are highly utilized, which is the norm in HPC environments, agentless solutions might lose the ability to connect to those servers and collect required data.

	SUBSCRIPTION LICENSE MODEL	PERPETUAL LICENSE MODEL
Cost	Annual recurring payments.	One-time payment.
Validity	12 months.	Perpetual.
Entitlement	Software license, support, updates and upgrades.	Software license only. Usually include 1st year maintenance and support.

Table 2: Comparison between Subscription and Perpetual License Model.

Always at full speed
is no way to run a
cooling system.



The trade-off between the advantages and disadvantages of both methods can be challenging, but careful consideration of the target environment can help reach a strategic decision. In ECC's Linux-based HPC environment, we rely on agentless SSH-based monitoring, which we believe can provide all of the necessary monitoring requirements with the least administrative overhead.

E. SCALABILITY

Another important metric to consider when acquiring a monitoring solution is scalability, which determines the number of devices it can monitor. There are several factors affecting the scalability of BSM solutions. The most common factor is the number of monitors applied coupled with the number of managed devices. It is expected that increasing the number of monitors on each of the managed devices decreases the number of devices monitored by the solution. Such limitation is influenced by the technique used for monitoring.

There are different approaches practiced to address the scalability limitations of BSM solutions. The most commonly used is the distributed monitoring approach. In this architecture, the solution is deployed in different identical servers (slaves), in which each slave is responsible for a certain amount of the load. A master server is deployed on top of these slaves, which interacts and manages the slaves. In addition, it acts as the gateway to end-users, creating a seamless environment on how the monitoring infrastructure is deployed. This architecture allows for greater flexibility to scale the monitoring solution horizontally and vertically, without imposing certain specifications on hardware resources or other limitations. This architecture must be tested and verified against possible scalability thresholds or limitations in order to deliver the required optimal results.

Another approach is to fragment the BSM solution into several components based on functionality. Typically, these solutions consist of a software package to monitor network devices, a package for monitoring servers, a package for application monitoring, and another package for reporting. Although such architecture might have a solution for scalability limitations, it also introduces several complexities, administrative overhead, as well as additional costs.

F. SECURITY

Data is the most important intellectual asset of any data center. Thus, maintaining a secure environment for this data is as important as the data itself. By deploying a new BSM solution into your environment, it implies that a new component will have access to your IT assets, including stored data. This access is required by such solutions to run the necessary monitoring and management tasks. Understanding how the solutions do each task, and what access is associated with it is essential. There are cases where the solution is not aligned with an existing security standard or regulation. In addition, some solutions might require unnecessary authority to access some systems, in which there are alternatives. Moreover, an agent-based solution might introduce additional security concerns and require further efforts to perform patching tasks.

Thus, it is important to have a complete understanding how each monitoring task is performed by the BSM solution. This includes, but is not limited to: access privileges and protocol required, files to be accessed, processes run by the software, and whether there is outbound traffic forwarded to outside servers. For example, a read-only SSH access to system related files for Linux/UNIX based systems is considered a best practice method of performing comprehensive monitoring without compromising security measures.

G. FRAGMENTED VS. UNIFIED

To cater to the capabilities required to monitor the different computing resources, BSM solutions can be categorized into two distinct types: fragmented and unified. A fragmented BSM solution consists of several function-based and independent software applications. Each of the applications delivers a monitoring function and works independently from other

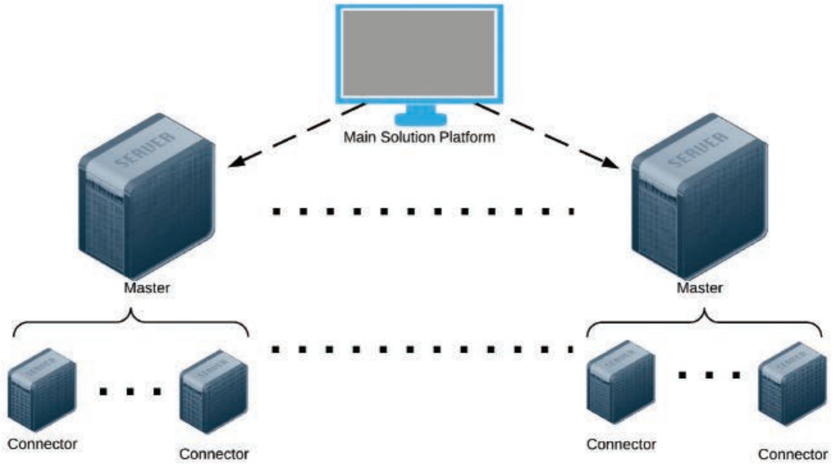


Figure 2 : Typical Distributed Monitoring Architecture.

applications. In some implementations, the set of these applications can be controlled through a single platform that provides analytics and correlations between the different events received from these applications.

The fragmented BSM solution allows for greater flexibility for the solution developer to expand monitoring by making it technology specific. This can enrich the monitoring capabilities with significant details. On the other hand, each of the applications of the same solution could have its own licensing model – even though they are part of the same BSM solution. For example, you might have an application licensed per monitoring point, and another licensed per device. Moreover, fragmented solutions impose significant amount of administrative overhead that might require a dedicated support staff. In some cases, support staff might spend more time performing routine administrative tasks, such as patching, upgrading, troubleshooting internal issues or unusual application behavior, than actually delivering business value. In addition, without a tight, reliable and dynamic integration between these applications, the BSM solution might not deliver the intended business value. These factors contribute to higher costs associated with such solutions.

A unified BSM solution, however, joins the major functionalities of monitoring, analysis and reporting into a single platform with embedded software modules. That is, there is no specific software installed for server monitoring and another for network device monitoring. Strategic partnerships with the OEMs are a key enabler to provide a unified solution, as BSM solution providers can focus on the most important metrics to monitor directly from the devices or applications. Hence, it leaves out all unnecessary details for the OEMs to cover through their technology specific management solutions. This is a widely adopted approach, since most of the complex technologies are equipped with their own management software, intended for very specific installation, advanced administration and management, and diagnostic and troubleshooting tasks. Nevertheless, unified BSM solutions can still benefit from OEM software through API integrations and other means, if deemed necessary for certain business requirements. In general, however, this is very rarely needed for HPC data centers.

Furthermore, unified BSM solutions eliminate much of the training and support overhead imposed by fragmented solutions, resulting in less cost of ownership (TCO). In addition, they allow for functionality expansion through integration with third-party applications, especially when considering an open-source approach.

H. SOLUTION INTEGRITY AND INTEGRATIONS WITH THIRD-PARTY SOFTWARE

Another important factor that plays an important role on the selection of a BSM solution is its integrity and integration offerings with third-party software allowing for functionality and capability expansion. The genuine integrity between different components of a fragmented BSM solution is crucial to deliver optimal business value. Some solutions require an additional integration module for each of its applications, adding more complexity to the solution architecture. Such requirements, in turn, introduce even more integrity and reliability concerns to the whole platform. These integration points within the same platform might also require additional licenses and, hence, additional associated costs. Unified BSM solutions are not impacted by this issue since essential components are already integrated within the BSM platform.

Integration with third-party monitoring, configuration management and systems management solutions expand the functionality and capabilities of the monitoring solution. Thus, it is important to understand the available integration offerings of the BSM solution and how they could be utilized. In an HPC environment, integration with the jobs scheduler and resource management system, such as PBS and Univa Grid Engine, as well as an HPC configurations management solution, such as Puppet, add important details about what is happening in the HPC environment and help the BSM to create better correlation between events – both from systems and applications. It is worth noting that such integration is beneficial in both fragmented and unified BSM solutions, even though some vendors might promote the opposite and rely solely on their product. Also, it is important to understand how these vendors make such integration offerings and whether they require additional licenses or software installations. The most practical approach for such integrations is to use out-of-the-box APIs and perform customizations as deemed necessary. Most propriety solutions, which are also fragmented, require special licenses and software components for integration with third-party application.

I. CMDB CONSIDERATIONS

Configuration Management Database (CMDB) is a fundamental part of any BSM solution. It serves as a data warehouse about all of the data center components, both physical and

At 4 a.m. the most **reassuring** sound in a data center is the quiet hum of a **flywheel**.

You'll be amazed at the strength
of ASCO's innovative solutions.

logical, relationships and dependencies, as well as their criticality to the business, where each entry in the database is referred to as a configuration item (CI). The Information Technology Infrastructure Library (ITIL) treats the CMDB as the central source of data for Configuration Management process to understand how the data center assets are composed and services delivered to end users.

While it seems that CMDB is an integral part of any BSM solution, it is also used by other processes such as Change Management and Incident Management. Thus, the decision whether to treat it as part of the BSM or decouple it is very important. That said, by understanding the demanding work associated with populating and maintaining the CMDB, it becomes more practical to decouple the CMDB related activities from the BSM framework.

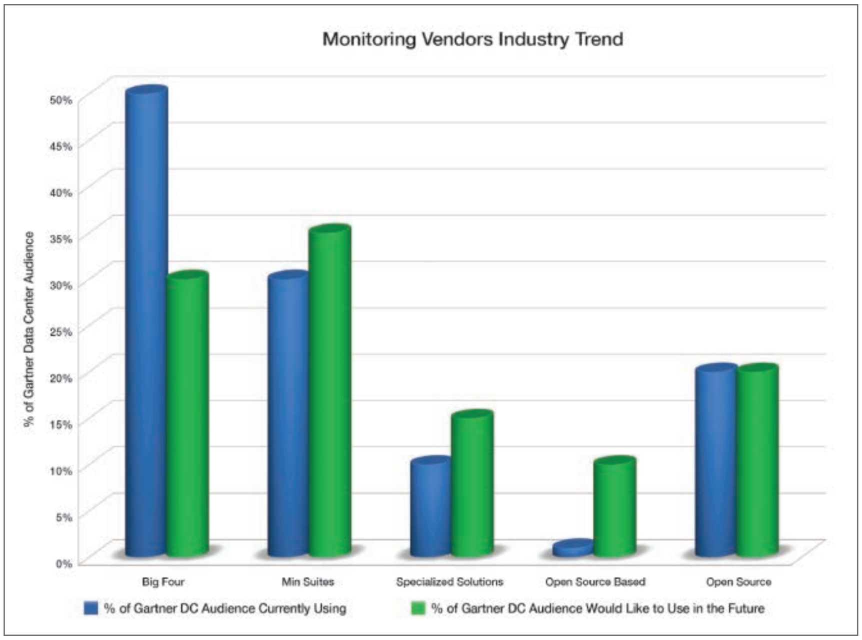


Figure 3: Gartner's DC Audience Current and Future Monitoring Platforms.

By decoupling the CMDB from the BSM, we can utilize more advanced and specialized CMDB solutions, such as BMC Atrium CMDB and PuppetLabs' configuration management system - Puppet. This approach addresses the challenges associated with controlling the CMDB system, and maintaining data integrity, validity and consistency. In addition, it allows for further development of the CMDB by including the data into the CMDB from other sources, such as Asset Management. This process, referred to as federation, transforms the CMDB into a federated CMDB such that the source of the data retains control of the data. This has become a common practice in today's complex computing environments.

Utilizing an independent CMDB as the source of data for all of the IT assets for the BSM is more practical. It allows the BSM solution to focus on what it should, while ensuring the availability of a reliable source of data. Furthermore, it leads to a less complex solution architecture for the BSM.

	DETAILS
Administration Overhead	Higher for fragmented solutions.
Installation Requirements	Generally, fragmented solutions tend to need more components.
Cost	Generally, higher for the fragmented solutions.
Functionality Offerings	More capabilities are usually offered by fragmented solutions.

Table 3: Main Differences between Fragmented and Unified BSM Solutions.

J. OPEN SOURCE APPROACH: OFFERINGS AND LIMITATIONS

In recent years, the open source software industry has gained a huge popularity and been a key competitor to market leaders, who have been driving the industry for years, as shown in Figure 3. Similarly, open source BSM tools and solutions have been popular and widely adopted at the enterprise level.

They aim to associate the concepts of both open source and propriety software together. That said, they offer the flexibility of open source solutions. Users can access the source code and customize the solution to the business needs. They can also integrate with third party solutions, at no additional cost, to expand their capabilities. Often times, these integrations are provided as an out-of-the-box feature utilizing generic

TEST BETTER
F1
F2
F3
F4
+
I
O
−

APIs or web services. Moreover, they are equipped with advanced functionalities, such as application performance monitoring by simulating the user experience using the synthetic transaction monitoring concept, service modeling, auto discovery and many other capabilities. Furthermore, open source solutions are widely used and popular among popular data centers. There are community forums you can utilize for help and support in the event you come across a critical technical issue.

Open source monitoring solutions differ in nature depending on their capabilities. They range from primitive availability monitoring tools, such as Nagios and Icinga projects, to more advanced monitoring solutions, such as Zenoss. Nagios, for example, is a primitive open source monitoring software project that has been widely used in different data centers, and serves as the fundamental ground for several other monitoring projects.

K. SUMMARY

In summary, the selection process of a BSM solution is subjective, and highly dependent on several factors defined by the business needs and objectives. This includes, but is not limited to the nature of the data center operations, business sector requirements and objectives the center serves, solution architecture, solution capabilities and offerings, and the security factors.

IV. CONCLUSION AND FUTURE WORK

Our growing need to provide world-class and highly available HPC resources to serve Saudi Aramco's Oil and Gas Upstream operations has given us the opportunity to study the BSM industry and evaluate several products. In conclusion, the BSM concept leads the way data center monitoring is delivered. It aims to close the gap between IT service [10] organizations and the upstream business of the organization. Choosing the right software solution for that purpose plays a crucial part in delivering this objective. In this paper, we provided some insights based on our experience on how to choose a cost-effective solution to an IT organization, with more focus on HPC data centers in an Oil and Gas industry.

Our future work includes expanding our BSM model to include data center facilities components, mainly monitoring power and cooling infrastructure. In addition, we are working on evaluating the performance of several enterprise BSM solutions. This performance evaluation, together with the considerations provided in this research, will further help organizations to better address their BSM business needs [9].

ACKNOWLEDGMENT

The authors would like to thank the EXPEC Computer Center (ECC) at Saudi Aramco for their invaluable support and contributions to conduct this research.

REFERENCES

[1] "Nagios," [Online]. Available: https://www.nagios.org/. [Accessed 13 January 2015].

[2] "Zabbix," [Online]. Available: http://www.zabbix.com/. [Accessed 13 January 2015].

[3] ITIL, "Information Technology Infrastructure Library Official Website," [Online]. Available: https://www.axelos.com/best-practice-solutions/itil.aspx?utm_source=itil-officialsite. [Accessed 9 July 2015].

[4] "Capability Maturity Model Integration Institute," [Online]. Available: http://cmmiinstitute.com/. [Accessed 1 June 2015].

[5] "Microsoft Operations Framework," [Online]. Available: https://technet.microsoft.com/en-us/solutionaccelerators/dd320379.aspx. [Accessed 1 June 2015].

[6] "Control Objectives for Information and Related Technology," [Online]. Available: http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx. [Accessed 1 June 2015].

[7] R. Crosby, "Data Center Optimization: The Value of Business Service Management," 25 03 2008. [Online]. Available: http://www.cio.com/article/2436918/legal/data-center-optimization--the-value-of-business-service-management.html. [Accessed 13 July 2015].

[8] J. Kowall, "Toolkit: IT Operations Monitoring Assessment and Rationalization," Gartner, 2012.

[9] E. Wilson, "Network Monitoring and Analysis: A Protocol Approach to Troubleshooting," p. 350, 9 January 2000.

[10] T. Schaaf and O. Appleton, "FitSM," [Online]. Available: http://fitsm.itemo.org/files/FedSM-ITSM-intro.pdf. [Accessed 6 July 2015].

[11] BizTech Magazine, "High Performance Computing's Role in Energy Exploration," 18 July 2014. [Online]. Available: http://www.biztechmagazine.com/article/2014/07/hpc%E2%80%99s-role-energy-exploration. [Accessed 01 July 2015].

[12] Information Systems Audit and Control Association, "Control Objectives for Information and Related Technology," [Online]. Available: http://www.isaca.org/cobit/pages/default.aspx. [Accessed 05 August 2015].

[13] M. Rouse, "ITSM Definition," TechTarget, [Online]. Available: http://searchcio.techtarget.com/definition/ITSM. [Accessed 05 August 2015].

Abdullah Aldhamin is Computer Operation Systems Specialist at EXPEC Computer Center, Saudi Aramco.
He can be reached at abdallah.aldhamin@aramco.com
Bander Alotaibi is Group Lead - Data Center Support Group at EXPEC Computer Center, Saudi Aramco.
He can be reached at bander.otaibi.3@aramco.com

STARTING FROM SCRATCH
VISIONING YOUR DATA CENTER

by **Raymond Johnson, II, PE**

The construction industry is littered with projects that have failed to meet the owner's expectations. The reasons for the missed expectations range from the failure to meet the construction budget requirements, schedule requirements, space needs, capacity needs – and the list goes on. Based on years of experience and research, it is apparent one of the primary reasons cited for these failures is poor early planning. Proper early planning can limit rework in future phases, the need to ask for additional capital, and wasted time.

Like most other construction projects, data center projects often fail because of poor planning. Too often the owner falls short of budget because they used old rules of thumb or an online tool to project the cost of construction. At other times data centers are over/under built due to failure to project business needs or operational requirements. And at still other times a proper understanding of construction sequencing, equipment lead times, regulatory action or utility acquisition can result in scheduling delays. Most of these issues can be mitigated through proper planning.

PLAN THE PLAN

Most owners starting the process of constructing a data center are literally starting from scratch. Once the business need is established, the owner quickly finds that in addition to the normal building construction challenges, there are numerous additional technical and logistical issues that need to be overcome in a data center project. The construction of a data center is significantly more challenging today than it was just a few years ago. There are many system and technology options to choose

ATLANTA | AUSTIN | BALTIMORE | DALLAS | DENVER | HOUSTON | NEWPORT BEACH | ORLANDO | PASADENA | PHOENIX | RALEIGH-DURHAM
REDWOOD CITY | RICHMOND | SACRAMENTO | SAN DIEGO | SAN FRANCISCO | SAN JOSE | TAMPA | WASHINGTON DC | WEST PALM BEACH

from that were not previously available. Which systems to choose and how they apply will depend on how the owner intends to operate their facility. Determining whether to build the facility to meet the future size and capacity needs, or to allow for scalability to grow into the future needs, can depend on operational factors as well as systems chosen. The determination of these and many other issues can be iterative, and if not controlled, can have capital budget and schedule impacts. To control the process it is recommended an architect, engineer or data center planning professional be brought onto the team once the business need is established.

As IT professionals are aware, a data center project is far more than just the construction of the facility itself. The planning of a data center is a complex array of interdependent elements (see Figure 1). These elements and their planning can greatly impact the project capital cost and schedule. To maintain control of the planning, a two-part process is recommended. This process is adapted from a similar model being used in other areas of the construction industry. The first step establishes overall project goals. The second step looks critically at the project to facilitate the determination of a preliminary concept.

STEP 1 Visioning Session

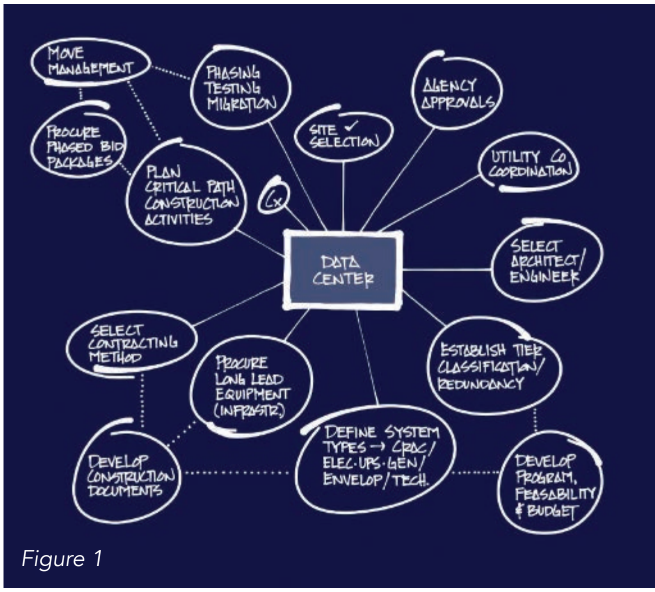
The first step in the planning process consists of a visioning session or preliminary meeting. During the first meeting the architect/engineer/planning professional meet with the primary stakeholders. These are the stakeholders who have the primary decision making responsibility. The stakeholders should be members of the project leadership team, as well as executives responsible for the success of the project. They could include the CIO, CFO, director of facilities, etc. The goals of this meeting would be to familiarize the leadership team with the process, relate the business needs, establish the project goals, and determine the project bumpers.

Project bumpers are project limitations that the planning, construction and implementation must stay within for the project to be successful. An example of a project bumper might be that the data center project cannot exceed a fixed capital expenditure or it will not fit the business model for the company. Another bumper may be that the project schedule is being driven by the need to leave an existing space by a contracted date.

If the company's internal project manager is not a primary stakeholder, he/she should still be included in this meeting. This assures that both the architect/engineer/planning professional and the internal project manager have heard the same goals, needs and project bumpers. It is also important to have at least a general understanding to the existing capacity and projected future needs for this meeting. This will be used in the second meeting to help estimate the equipment and service sizes, and the types of systems to be considered. The better the existing and future capacity requirements can be projected, the more reliable the estimated construction cost will be.

STEP 2 Concept Planning

The second meeting, sometimes called a design charrette, brings together the architect/engineer/planning professional with the owner's primary facility and IT stakeholders. These should be the stakeholders who are responsible for the daily operation and maintenance of the building systems and network. They could include the facility's operations director, IT director and selected specialists. The goal here is to drill down into how the existing systems are operated and what changes are envisioned for the new facility. The use and operation of the facility and systems can have a dramatic impact on the configuration and make-up of the data center. Critical information like the kW capacity, uptime expectations, redundancy requirements, rack density, etc. should be available for discussion. Any one of these can have a profound impact on the capital budget and require re-evaluation and assessment of savings alternatives should the capital budget be exceeded. As stated above, this can be an iterative process where a change in one parameter will result in changes elsewhere.


MOVE MANAGEMENT
PHASING TESTING MIGRATION
AGENCY APPROVALS
PROCURE PHASED BID PACKAGES
SITE ✓ SELECTION
UTILITY CO COORDINATION
PLAN CRITICAL PATH CONSTRUCTION ACTIVITIES
Cx
DATA CENTER
SELECT ARCHITECT/ ENGINEER
SELECT CONTRACTING METHOD
PROCURE LONG LEAD EQUIPMENT (INFRASTR)
ESTABLISH TIER CLASSIFICATION/ REDUNDANCY
DEFINE SYSTEM TYPES → CRAC/ ELEC·UPS·GEN/ ENVELOP/TECH.
DEVELOP CONSTRUCTION DOCUMENTS
DEVELOP PROGRAM, FEASABILITY & BUDGET
Figure 1

Various design alternatives should be considered in this meeting. The process should utilize the project parameters to narrow in on the systems and configurations that meet the requirements and quickly eliminate those that do not. This is where the architect/engineer/planning professional brings their value to the table. The experienced professional is

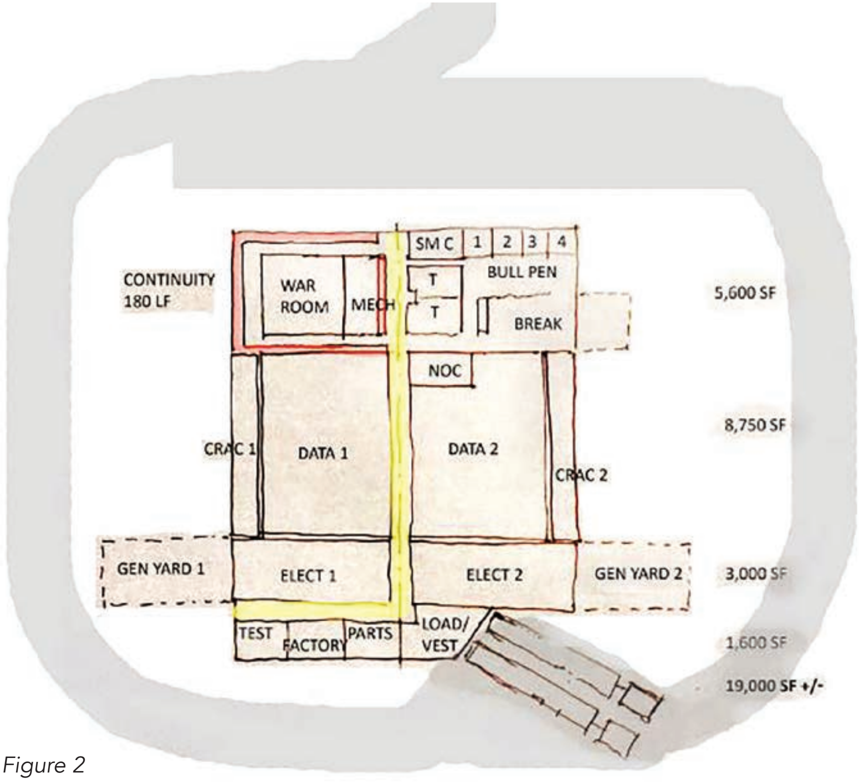


Figure 2

able to facilitate the discussion to efficiently focus on the items that will meet the requirements, while helping eliminate those that will fall out. They are also able to help consider the various alternatives that might be available to allow flexibility to meet the 'what if' scenarios that always come up in these discussions.

Once a sufficient level of information is gathered and agreed upon, and a reliable capital budget projection is created, the architect/engineer/planning professional takes some time aside to rough out a concept plan. This plan should approximate space allocations, adjacencies, white space areas, growth areas, approximate equipment locations, etc. An experienced professional should be capable of performing this task in just a few hours. Once completed to a sufficient level of detail, the stakeholders are brought back to challenge the concept plan. Those challenges are discussed and modifications are agreed upon prior to the conclusion of the meeting. Once all are in agreement, the architect/engineer/planning professional finalizes the concept plan. This can be done at the meeting or shortly after the meeting (see Figure 2).

An important aspect of this meeting is that all stakeholders are actively engaged. It is recommended the stakeholders are able to remain focused on the process. This process can take a couple of days, so time should be allocated to allow their participation.

STEP 3 Project Budgeting

Once the concept plan is developed and agreed upon, the capital budget estimate can be developed. Because of the level of detail that can be generated in a short period of time, the estimate should be relatively detailed and not just a rule of thumb estimate. This level of detail will allow for a more reliable capital estimate that can be utilized to make informed business decisions. The concept plan will also raise the level of comfort for all involved that the facility under consideration will meet the operational needs of those charged to make it work.

THE RESULT

YOUR PLAN

A reliable early planning process that quickly guides a project to its successful conclusion is essential. The result of the process must be a capital budget owners can rely on to make sound business decisions, and a level of certainty that the proposed facility will meet the business and operational needs of the owner. When properly performed, this process can meet those objectives.

This process is normally performed quite quickly and as a result can be quite intense. The participants need to be "in the moment" and dedicated to the successful outcome. The desired outcome of the process it to achieve a reliable capital budget, create a concept that will meet the business and operational needs, and just as importantly, garner the necessary "buy-in" from the stakeholders. This early planning process allows these goals to be achieved in a relatively short period of time.

Raymond Johnson, II, PE, is Director of Mission Critical Design at Wendel. He can be reached at rjohnson@wendelcompanies.com

Everything you need to know about NIAP PROTECTION PROFILE 3.0

by **Michael Parvin**

If we've learned anything from, OPM, Target, Sony, JP Morgan Chase, eBay or any of the countless other high-profile, high-cost cyberattacks of the past two years, it's this: there are vulnerabilities everywhere. Hackers can pillage companies or agencies through anything connected to the network … and today, everything is connected to the network.

We live in the era of the Internet of Things. Hyper-connectivity isn't just possible, it's swinging the pendulum between success and failure for multi-billion dollar businesses. Device-to-device communication streamlines everything we do, and visibility and management of these connected systems enables increased productivity and efficiency. But there's a catch; every one of those connections creates a potential vulnerability, and there are plenty of smart people with bad intentions trying to exploit them.

Simply put, everything from the heart of the data center to any desktop, laptop, keyboard or mouse connected to the network is a potential risk.

Do I have your attention?

THE EVOLUTION OF NETWORK SECURITY

Even some of today's best Intrusion Detection Systems aren't enough to stop all of today's advanced persistent threats, which are designed to burrow into the network from virtually anywhere and siphon data over time undetected. It's critical to identify and secure access points to avoid, mitigate or manage data breaches. That task includes often-overlooked computing peripherals. These are devices that by their nature are difficult to secure, because so many people have access to them. Keyboards, video monitors, even the mouse–anything that could be connected to a KM or KVM switch–falls under this umbrella. These are the devices the National Information Assurance Partnership (NIAP) sought to secure with the release earlier this year of the Protection Profile for Peripheral Sharing Switch version 3.0 (PP 3.0).

The previous protection profile dealt with the pre-2000 security landscape, but cybersecurity must evolve as threats become more advanced. PP 3.0 includes security enhancements for modern peripheral switching technologies and standards designed to (1) defend against these evolving threats, and (2) provide assurance that the switch will not propagate attacks if they occur. These standards require the following:

- Higher isolation between computer ports from digital and analog leakages.
- Optical data diodes to enforce unidirectional data flows.
- Much stronger protection for USB ports.
- Complete isolation of power domains to prevent signaling attacks.
- Analog audio diodes to prevent audio eavesdropping (TEMPEST levels).
- Emulation of display EDID, keyboard and mouse to avoid direct contact between computers and shared peripherals.

Agile.
Secure.
Innovative.

- Much stronger anti-tampering and tamper resistance.
- Strong protection from social attacks and malicious USB devices (such as BadUSB).
- Non-volatility requirements.
- Secure administrator access and log functions.
- Much deeper protection for video signals.

KEY POINTS IN PP 3.0

Security must be included in the initial design:

In the previous protection profile, non-secure KVMs could be reinforced to be deemed secure and pass the independent evaluation that leads to NIAP certification. In PP 3.0, security must be designed into the product. This ensures a heightened focus on security.

More products are included:

PP 3.0 applies to a number of new products that can be tested for use in secure environments. These products include traditional KVM switches, KVM combiners, video wall processors, matrix KVM, KM switches with cursor navigation, isolators and filters, USB gateways, and multi-domain smart card and biometric readers.

Stronger testing replaces Evaluation Assurance Levels (EAL):

Instead of relying on EAL to indicate product security strength, PP 3.0 requires detailed testing specifications. This eliminates some of the gaps in classification. The level of testing in PP 3.0 is higher than EAL 5 products, and PP 3.0 requires 30 times as much testing as previous versions. New testing in PP 3.0 covers areas such as deep packet inspection and TEMPEST level isolation in critical areas such as audio.

Future-proof technology is added:

The previous protection profile was optimized for VGA video and PS/2 peripheral protocols, which are rarely in use today. PP 3.0 includes support for the most modern KVM technologies, including USB (USB 1.1, 2.0, 3.0 and Type C), HDMI and DisplayPort video, and MHL to support mobile devices and not only computers.

Architecture

Engineering

Interior Design

Planning

Program Management

Construction Management

Commissioning

www.jacobs.com | Worldwide

JACOBS

PP 3.0 is internationally recognized:

The previous protection profile was not widely adopted outside the United States, with many countries developing their own requirements over the years. This caused a lack of standardization in the security of peripheral sharing switch products. PP 3.0 is a true international effort, having passed through agencies and certification bodies from Australia, Brazil, Canada, France, Germany, Greece, Israel, Italy, Japan, UK, Poland, Spain, Turkey and NATO.

THE BOTTOM LINE

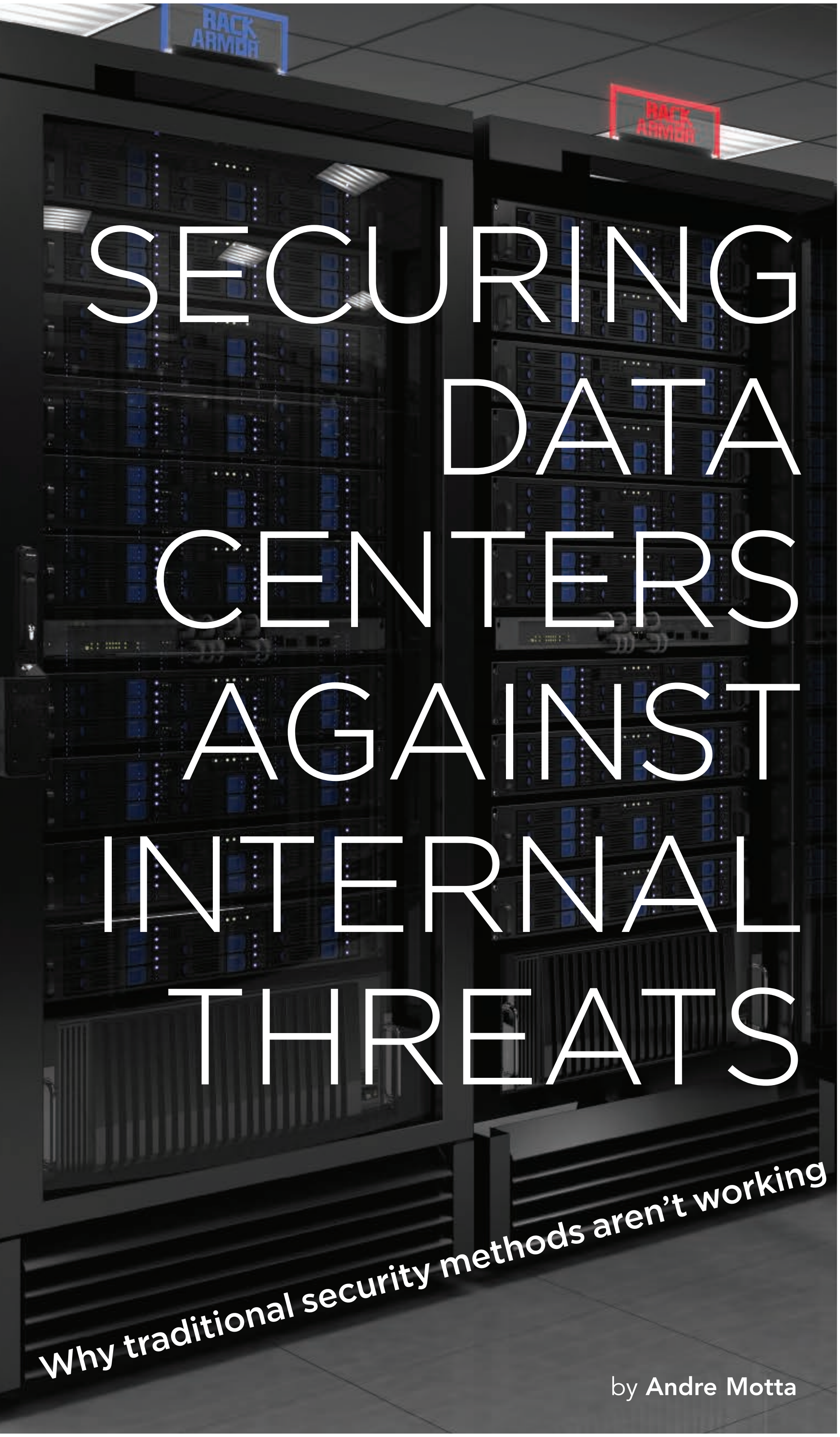
This is a good thing, and a significant step toward more secure networks. But don't worry—no one needs to go out and start ripping and replacing non-PP 3.0 compliant devices. In fact, the first PP 3.0 compliant KVM systems are only just now becoming available. However, the next time your organization purchases a secure KVM, ensure that unit complies with the new protection profile. Your business will be more secure for it.

THE ROAD TO PP 3.0

The National Information Assurance Partnership (NIAP) understands security threats as well as any such organization can, but it understands its blind spots—namely seeing security and security technologies from the perspective of the companies who rely on those technologies. For that reason, NIAP typically enlists industry experts from companies that develop security technologies to help with updates to security guidelines and requirements.

After receiving concerns from security consultants related to peripheral device security, NIAP reached out to Emerson Network Power for assistance with PP 3.0. Emerson's Michael Parvin became the technical editor and led the development of the document that spells out the new protection profile. Parvin and the PSS Technical Community started their work in January 2014 and met—either in person or via phone—every other week until the final document was released in January of this year.

Michael Parvin is Product Manager for the Secure and Standard Desktop Products at Emerson Network Power.
He can be reached at Michael.Parvin@Emerson.com



SECURING DATA CENTERS AGAINST INTERNAL THREATS

Why traditional security methods aren't working

by **Andre Motta**

Edward Snowden. In 2013, his name became linked forever with a significant and highly publicized data breach that rocked the world of data security. As an authorized insider for the National Security Agency, Snowden was responsible for one of the most significant security leaks in U.S. history. His actions sounded the alarm on the rising incidence of data theft worldwide, and the need for enhanced security measures.

During the past several years, most companies and data centers have focused primarily on enhancing cyber security to minimize threats from the outside. Yet a growing body of evidence reveals that internal threats to data breaches are equally as menacing. In fact, as stated in its 2013-2014 report, Understand the State of Data Security and Privacy, Forrester Research (a global information technology market research firm), found that insiders were responsible for 36 percent of the breaches during a 12-month period.

At data centers, insiders include anyone who has access to the facility–employees, clients, visitors, or contractors. The threat they pose, whether malicious or accidental, has been overlooked by many companies and data centers. Although data centers provide physical access control systems and surveillance at the perimeter, facility, or room levels, few offer adequate physical access control and monitoring where the data actually resides–at the rack level.

Vulnerability at the rack level leaves data centers and their tenants (or clients) open to a variety of potentially catastrophic consequences: loss or theft of sensitive data and/or company trade secrets; significant fines and penalties levied by regulatory agencies; loss of customer (current and potential) trust and business, and a tarnished reputation. According to the Ponemon Institute's 2015 Cost of Data Breach Study, the average cost of an organizational data breach in the U.S. in 2014 was $6.5 million. That's a high price to pay for an incident that could be prevented with advanced physical server protection.

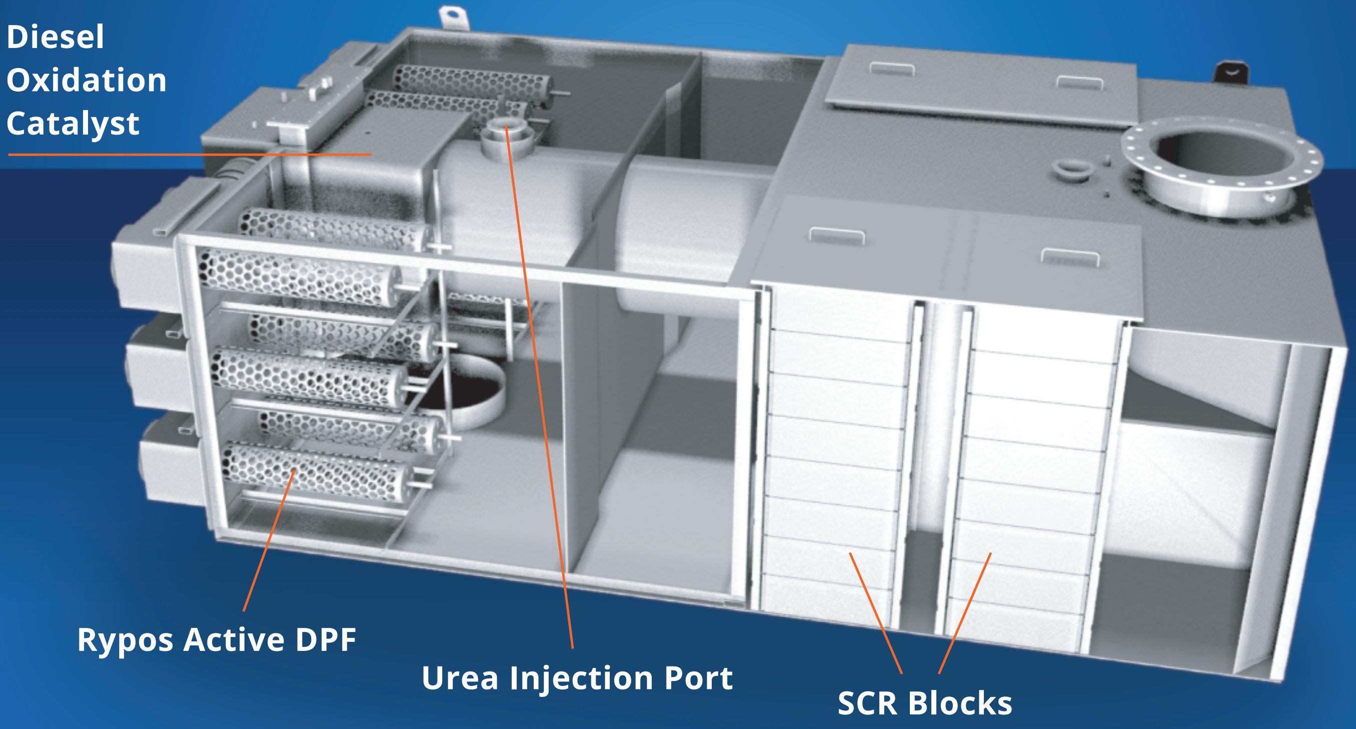
KOHLER Power Systems
KOHLER
Power Systems
2000
KOHLER
KOHLER
Power Systems
KOHLER
Power Systems
TRANSFER SWITCH

The MIRATECH AT-IV

Designed for Mission Critical applications, like yours.

- Reduces NOx, CO, VOC, and DPM to Tier 4f standards
- Active technology works at idle and variable load conditions
- Active self-regenerating DPF, technology by Rypos
- SCR pre-heating function
- Compact design fits in engine rooms; on or in containers
- Integrated silencing – 25dB(A) with options for additional ratings
- Pressure loss consistent with engine manufacturer specifications

Active Tier 4F compliant and beyond!



ENGINEERED TO PERFORM™
800-640-3141 | MIRATECHCORP.COM

MIRATECH

EMISSIONS CATALYSTS • HOUSINGS • SILENCERS • SCR • DPF • SERVICE • TRAINING • TURNKEY

WHERE CURRENT SECURITY MEASURES FALL SHORT

Most data centers use a combination of surveillance, personnel (security guards), and identification and access control technologies to control physical access to perimeters and facilities.

When it comes to internal security, such as that within the server room, one of the more traditional components of a security system is the cage that contains server racks. Intended to deter theft, cages can be visually intimidating. In the evolving world of data security, however, this old-school look is no longer an advantage. Customers today include multi-billion dollar companies, where appearance can make or break a deal. They expect data centers to combine sophisticated aesthetics with modern technology.

In terms of securing the cabinets within a room, one available option is end-of-row placement, where one reader or access control device is located at the end of a row of cabinets. In order to gain access to any cabinet in the row for which the user is authorized, s/he must use the reader at the end of row. For each cabinet, the user must walk back to the end of the row and present required credentials again in order to unlock the specified cabinet. End-of-row access control is not as convenient as systems that house control devices at each cabinet.

Another disadvantage of end-of-row systems is their inability to provide auditing at the rack level. Furthermore, installation is difficult and labor intensive. Therefore, moving end-of-row systems to change the layout of a room or floor can cause major headaches. The associated rewiring process is especially cumbersome.

Whether a data center hosts a single company, or operates as a colocation center, it is common for personnel from one or more organizations to be in the server room at the same time, accessing or servicing their own equipment. Both cages and server cabinets are frequently left unlocked and open while various people are working in the server room.

With such relaxed security practices in place, who is to say that everyone in the server room is actually authorized to be there? Essentially, servers are vulnerable to anyone walking through the room. Keys can be stolen or replicated. Lock combinations can be compromised. The potential for data theft, sabotage, or accidental damage to hardware is monumental.

DATA CENTERS SCURRY TO MEET PRIVACY AND COMPLIANCE DEMANDS AT THE RACK LEVEL

With the mounting threat of data theft, data centers are challenged to provide physical security systems that comply with both their clients' and the regulatory authorities' requirements. They have an obligation to safeguard every bit of sensitive and confidential data they store for medical, educational, and financial industries, to name a few. Privacy rules and regulations include PCI DSS, FISMA, SOX, and HIPAA, among others.

Take for example, The Federal Public Key Infrastructure (PKI) Policy Authority's recent policy update. The agency now requires that certified data centers provide a multi-party control environment. Essentially, the data center's physical security system must operate so that a second authorized credential must be presented at the reader to authorize the action of the first card.

In fact, PKI cyber security experts often advise customers on the importance of ensuring multi-party control to PKI servers and cryptographic keys. "One of the areas that often takes a lot of customization to implement is managing access to data center racks," says Mark B. Cooper, President & Founder of PKI Solutions. "Data center security should include a physical security system at the rack level that makes it easy to define rules which require two or more authorized people to allow access to the rack contents."

Other looming industry and governmental regulations will require data centers to show they can protect and monitor access to confidential data, as well as demonstrate they will be alerted in real time when a breach occurs. Because risk at the cabinet level is under increasing scrutiny by regulatory bodies, data centers also will be required to provide a data trail that shows who was accessing servers, when, where, and for how long.

If data centers don't comply with data protection laws, they face stiff fines and penalties. While noncompliance, alone, is costly, consider the cost of a data breach. Data centers (and their clients) may face legal fees and a tarnished reputation, as well as loss of customer confidence, and loss of current and potential business.

KEY COMPONENTS TO A COMPREHENSIVE SOLUTION AT THE RACK LEVEL

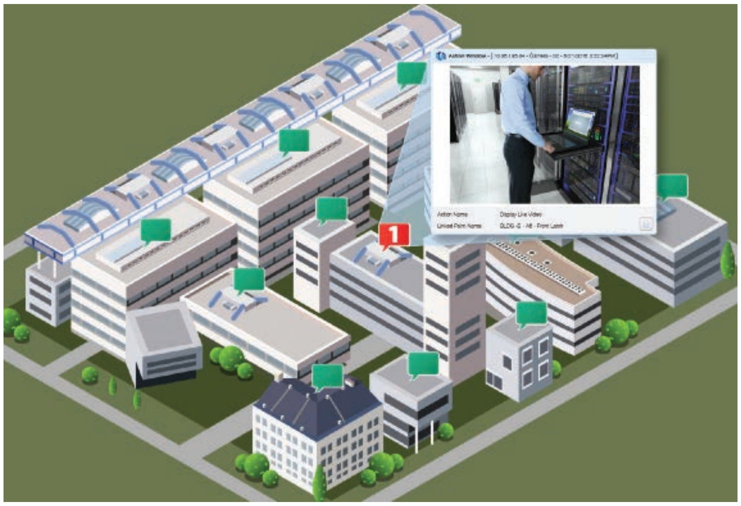
There's more to physical access control at the cabinet level than a card reader or input device. In fact, most solutions are missing one or more of the following additional critical components. Before selecting a physical security system for server racks, be sure to ask your security solutions provider if their system offers these features:

Easy monitoring of the security system status

Many data centers employ security guards to escort visitors to the server room or physically check that the server racks are properly secured after work at the rack is completed. New physical data security systems enhance worker productivity by eliminating these manual processes.

Consider these features:

- A graphic display in real time to instantly visualize the security status of server racks across multiple locations.
- Instant verification of the security status for both front and back doors of each cabinet and rack access panel.
- When an alarm is activated at the rack level, the ability to quickly drill down to pinpoint and display the rack's exact location.
- Icons that show whether a door has been forced or a key has been used, and display the status of three access points: doors, locks, and swing handles.
- Immediately send an email alert, sound an alarm, display a light, or call-up video if the server cabinets are unsecured.
- Remotely and immediately lock, unlock, or lock out a rack through the software.



Live and recorded video of transactions

Although the server room may be fitted with video surveillance, surveillance at the rack level is often minimal or nonexistent in most data centers.

Consider these features:

- Integrate with leading manufacturers of video management systems for facility and rack-level video cameras.
- Instantly view live video, and record and store video logs of cabinet access and server rack activities.
- Open live video feeds from different areas of the security system software including dynamic maps and alarm acknowledgement windows.
- Link recorded video to specific access transactions and include these links in audit reports.

Multi-party control (aka two-man rule)

Leading consultants recommend multi-party control to prevent an individual from having access to the server rack without having someone else also present a valid card.

Consider this feature:

- Multi-party control built into the software for ease of implementing within the data center's security system.

Reporting and auditing capabilities

Some regulatory bodies require auditing capabilities. Data centers that have the capability to generate these audit reports that include the length of time a particular user has had access to the server rack, may increase revenues by charging tenants an additional fee for the report.

Consider these features:

- Knowing who accesses server racks, where, when, and for how long is essential to an effective physical security solution.
- Customized reports that may be exported as Excel, Word, RTF, or PDF files are important for the tenants and provide an additional revenue stream for the data center.
- A Scheduler Wizard makes it easy to automatically schedule, save, and email reports to authorized recipients at pre-determined times.

Easy installation at the point of entry

Be sure that you understand how a system will be installed and the associated installation costs. Some systems that are promoted as simple, low-cost solutions often require an end-of-row installation which is more labor intensive and takes up premium wall space with mounting of hardware enclosures and conduit on the wall. Moving end-of-row systems to change the layout of a room or floor can cause major headaches and the associated rewiring process is especially cumbersome.

Consider these features:

- Hardware that is installed directly on the server cabinet door and doesn't take up valuable wall space.
- All electronics at the door are powered over Ethernet meaning fewer wires during installation.
- Factory-wired hardware eliminates mistakes during installation and greatly reduces labor costs.

Eliminating the need for cages

New physical security solutions can make server rack cages virtually obsolete. There are a number of benefits to their elimination, including the following:

- Cost savings for the tenant. By removing cages, tenants can use racks that are 48 inches deep (instead of 40 inches), which can be configured in fewer rows to save space. Tenants also may eliminate the expenses associated with cage use, including reconfiguring them and running cables.
- Increased income potential for the data center, which may have more space to lease to additional tenants.
- Savings on the cost of power. By eliminating the need for cages, data centers can position rows for optimal airflow to cool racks and reduce energy costs. Improved cooling can also extend the life of the tenants' equipment and improve performance by reducing hardware failures.

INTERNAL DATA BREACH: IT CAN HAPPEN TO ANY COMPANY

Organizations of all sizes and types are vulnerable to data breaches–whether accidental or malicious, internal or external.

The traditional means of restricting and managing physical access at data centers focus primarily on the center's perimeter and facility, while internal security at the server rack level–the source of valuable data–is minimal or nonexistent. Data centers must be able to track and record access to the rack, including the user's credentials, date, time, and duration of access. Doing so positions a data center as a modern, progressive, facility in a highly competitive marketplace.

Failing to provide superior access control at the rack level leaves data centers and their clients vulnerable to data breaches that can result in devastating and costly consequences: loss or theft of sensitive data and/or company trade secrets; significant fines and penalties levied by regulatory agencies; legal fees, loss of customer (current and potential) trust and business, and a tarnished reputation.

Andre Motta is General Manager at IDenticard® Access Control. He can be reached at access_control@identicard.com

Sources: *Shey, Heidi. Understand the State of Data Security and Privacy: 2013 to 2014. Forrester. October 1, 2013.*
2015 Cost of Data Breach Study: Global Analysis. Ponemon Institute. May 2015.
Cooper, Mark B. President and Founder of PKI Solutions.

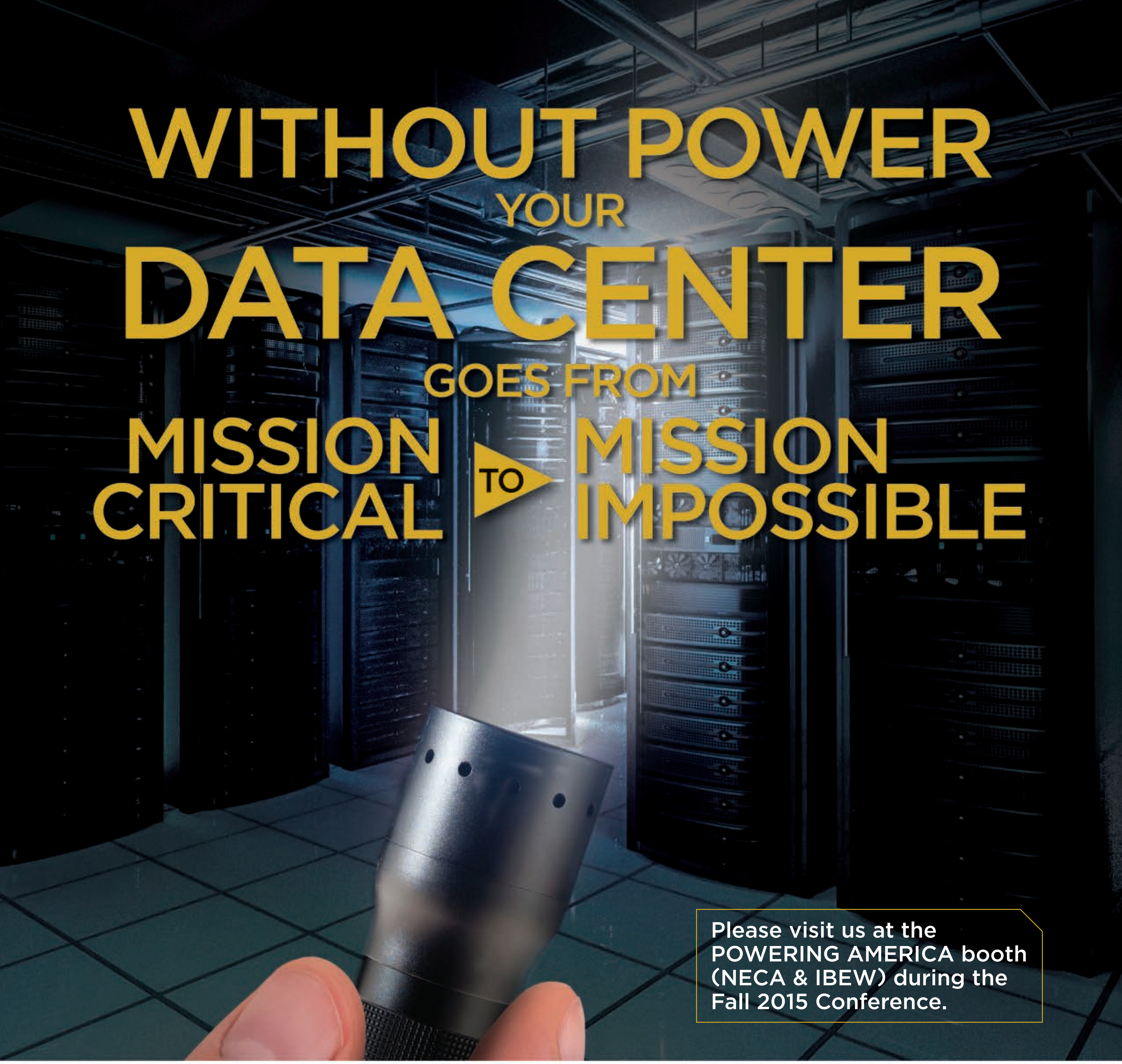
SHORTER UPS RUNTIMES: WHY MANY HAVE REALIZED THAT LESS IS MORE

by **Todd Kiehn**

For decades, data centers and other mission critical applications required several minutes of ride-through time for their UPS systems. The longer runtimes assured that a facility could remain operational if a backup generator failed to function properly or utility power was disrupted for an extended period of time.

BUT IN RECENT YEARS, THIS HAS CHANGED.

The industry has seen a dramatic evolution in UPS runtime specifications–from 15 minutes a decade ago to one minute or less today–due to advances in technology. Customers are no longer willing to pay for it as many simply don't require extra UPS autonomy. In this day and age of doing more with less, facility owners and operators are only purchasing and installing the amount of runtime



Please visit us at the POWERING AMERICA booth (NECA & IBEW) during the Fall 2015 Conference.

POWERING AMERICA PROFESSIONALS ARE IN THE BUSINESS OF KEEPING BUSINESSES RUNNING.

It's a simple fact: Powering America contractors and electricians are better equipped to help you meet critical power needs. Ongoing training in cutting-edge technologies and a focus on business needs mean you're working with professionals who understand it's about more than keeping the lights on. It's about delivering the data that keeps America running. You think that's important, and so do we.

NECA IBEW
POWERING AMERICA

For more information: **www.Powering-America.org**
Online video magazine: **www.electrictv.net**

needed. Generators can now start and fully support a load much faster than in decades past, and the advent of cloud computing and virtualization have also contributed to this growing trend.

Longer UPS runtimes are a byproduct of an era when backup generators were slow to start or unreliable, or when generators were not present and the UPS had to carry the load as long as possible until utility power returned. By contrast, most modern on-site generators can be online within 10 seconds, making multiple minutes of UPS stored energy redundant.

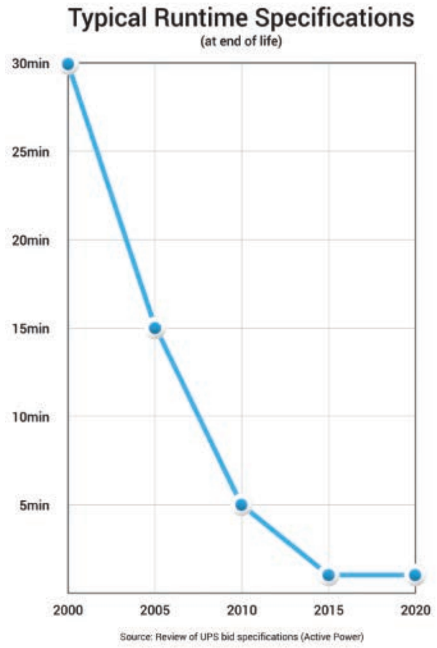
Additionally, some critical facilities have failover safeguards in place where operations are switched over to a backup data center or cloud environment. These transitions also happen fairly quickly, usually taking less than 60 seconds.

So if multi-minute UPS runtimes are no longer necessary, why pay for more when less will do? That's a question that many customers across all industries are asking themselves, resulting in a growing acceptance of shorter ride-through times. In this post-recession era, facility operators are constantly looking for ways to save money and floor space, with many finding that smaller, more affordable UPS systems can help them achieve both goals.

Extended ride-through times are generally achieved through attaching large quantities of valve regulated lead acid (VRLA) batteries to the UPS. These extra batteries increase costs in multiple ways: at first purchase, increased maintenance and monitoring costs, and in periodic (4 to 6 year) battery replacements. VRLA batteries must also be kept at specific temperatures, meaning cooling equipment and costs must be built into the budget.

Since extra runtime is no longer valuable, this equipment represents an unnecessary and unjustifiable expense for owners and operators of mission critical facilities. The less runtime required, the fewer batteries are needed, adding up to significant savings over time. For operators willing to consider emerging technologies such as flywheel-based UPS systems, the savings can be even larger, as these units require less maintenance and replacement than their battery-based counterparts and can withstand much higher ambient temperatures. In data centers and other mission critical facilities, square footage comes at a premium, and smaller UPS systems free up floor space for other applications and hardware.

While many within the industry have recognized the benefits of shorter UPS ride-through times, others are still apprehensive towards change. This presents an opportunity for manufacturers to continue educating customers about the evolution of critical power protection equipment and to explain why runtimes have diminished in recent years. This also presents an opportunity for operators to rethink conventional electrical infrastructure prior to the start of a new design build. For those with equipment already in place, question whether what's deployed is really worth the cost and space. When all designers, engineers and operators trust that they can reduce costs without jeopardizing the overall system's reliability and availability, only then will multi-minute UPS runtimes truly become a thing of the past.



Source: Review of UPS bid specifications (Active Power)

Todd Kiehn is Vice President, Product Management and Modular Infrastructure Solutions at Active Power, Inc.
He can be reached at tkiehn@activepower.com

L1
20A
CIRCUIT 6
L3
20A
CIRCUIT 5
36
35
34
33
32
31
30
29
28
27
26
25
Raritan
DAISY CHAIN TERMINATION ON / OFF
IN / OUT
CONSOLE / MODEM
SENSOR
USB-A
USB-B
FEATURE
ETHERNET
CURRENT(A)
VOLTAGE(V)
POWER(W)
UB LOAD(%)
SENSOR

THE DREADED DOWNTIME

Preventive Maintenance Keeps Data Centers Running without Disrupting Business

by **Paul Lachance**

If the power went off at a data center in the final moments of the Super Bowl, fans in the stands might not notice. But all of the Twitter users and live bloggers feeding their thoughts into cyberspace through that data center certainly would. And the maintenance manager for the facility could easily become the goat of the game.

To avoid such disastrous scenarios, maintenance professionals at data centers schedule crucial Preventive Maintenance (PM) tasks so they do not run the risk of disrupting business activity for their clients–whether those clients are social media companies experiencing peak volumes during a sporting event or stock brokerages buying and selling on a busy trading day.

The best tool for managing those PMs is a modern Computerized Maintenance Management System (CMMS). Essentially a software solution for managing and tracking maintenance activities, CMMS automates a variety of functions that keep data centers running smoothly.

At RagingWire, a world-class data colocation service based in California, a CMMS eases the burden of maintaining dozens of generators and UPS units as well as several hundred cooling units at the company's various data center facilities.

"When I started 13 years ago, we relied on spreadsheets and tribal knowledge for knowing when we last fixed a piece of equipment and when we needed to fix it again," said Chris Thames, Sr., Director of Critical Facilities Operations at RagingWire. "We needed to automate that process with a CMMS."

Understanding the various capabilities of a CMMS enhances the ability of data center managers to reap the benefits of using this key tool in their day-to-day operations, in place of spreadsheets or paper binders. Here is a closer look at those capabilities:

All the capabilities you want...
and some you may not have considered!

Custom Designed and Built Power Control Systems

With mission-critical data and life safety at stake, why would you try to make do with a standard catalog power control system? Why would you settle for a less than optimal solution?

Don't compromise. Insist on a powerful, flexible, fully-integrated Russelectric Power Control System... custom-designed and built with your specific needs and wants in mind. Russelectric will custom tailor a power control system that not only provides all the operating, monitoring, and reporting capabilities you want, but one that is intuitive and easy to use because it is based on your way of doing things. And because Russelectric specializes in custom systems, we can often suggest features and capabilities you never even considered.

1-800-225-5250 russelectric.com
An Employee-Owned Company / An Equal Opportunity Employer

Russelectric
POWER CONTROL PEOPLE YOU CAN RELY ON

PREVENTIVE MAINTENANCE

PM management lies at the core of the CMMS and undergirds a variety of its functions.

On the basic level, PMs are assigned to each piece of equipment or building system in a data center and the PM calendar generates Work Orders (WO) to alert technicians to specific maintenance tasks. PM calendars can be viewed on a daily, weekly, monthly, quarterly, or annual basis – or in any other time configuration needed. In addition, readings from meters and monitors on equipment or infrastructure systems can directly interface with the CMMS to generate automatic PM notifications.

At RagingWire, PMs could contain more than 100 line items for servicing a data center generator, including checking the engine, intake exhaust, fuel system, generator controls, and fuel tanks. And each line item might require technicians to complete 15 to 20 specific inspections or repair steps that are then checked off and documented in the CMMS.

"Our CMMS helps us not only track all assets, but we can also forward-think when the next PM is due," Thames said. "And if we miss the PM, the CMMS will calculate that we were late and reschedule it for us."

PMs also contribute to worker safety when they are set up to remind technicians to refresh skills or complete professional certification requirements. And PMs are useful for tracking updates from manufacturers as well.

But beyond these specific capabilities, the CMMS serves as a catalyst to shift attitudes from a reactive, "fix-it-when-it-breaks" mentality to a pro-active, preventive maintenance mindset. The true beauty of the CMMS lies in its ability to keep an eye on machine components before they break down – and to generate PMs to prevent them from doing so. In data centers, where uninterrupted service is critical, a CMMS offers a clear benefit in terms of reducing or eliminating downtime for crucial infrastructure systems.

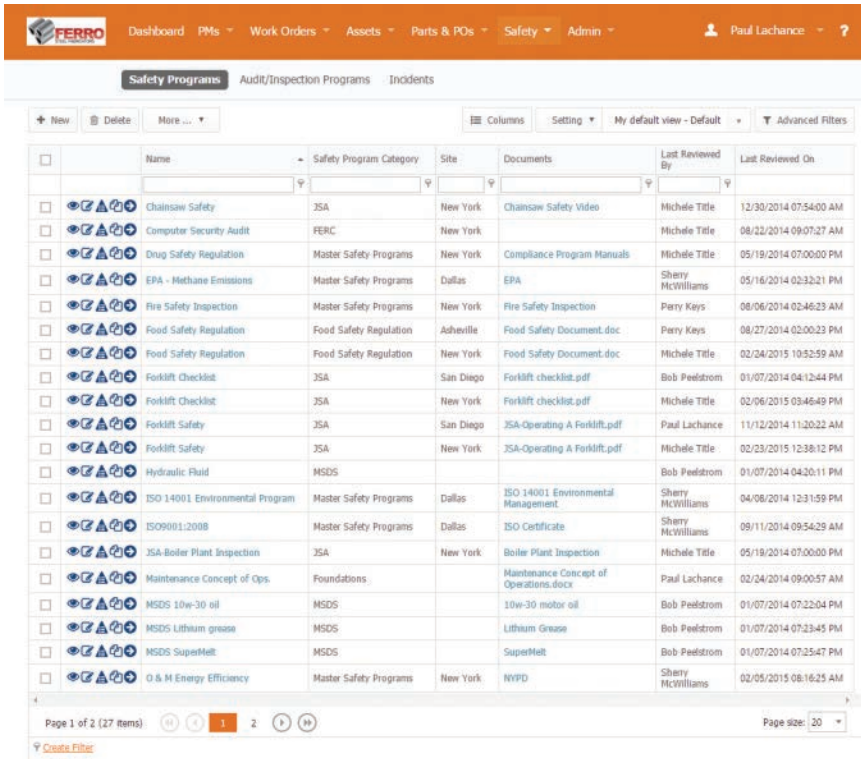
The preventive maintenance approach is also well suited to the unique demands placed on data centers. Because PM tasks are set up in advance, they offer managers more flexibility with work assignments, and as noted, PMs can be scheduled to avoid colliding with a customer's peak activity times.

ASSET PLANNING AND MANAGEMENT

In terms of managing assets, a CMMS gives managers access to crucial information, such as unplanned repairs vs. PMs for specific assets.

During the course of completing PMs as part of the workday, technicians use the CMMS to document the status of repairs, creating an archive of information on assets. That archive becomes an invaluable tool for asset analysis.

Data center services provider ViaWest relies on CMMS – and scheduled PMs – to handle maintenance for backup generators, UPS, cooling infrastructure equipment, fire equipment and more. Each piece of equipment is assigned a PM, based on timed frequencies, such as quarterly, annually, or biannually.



□	Name	Safety Program Category	Site	Documents	Last Reviewed By	Last Reviewed On
□	Chainsaw Safety	JSA	New York	Chainsaw Safety Video	Michele Title	12/30/2014 07:54:00 AM
□	Computer Security Audit	FERC	New York		Michele Title	08/22/2014 09:07:27 AM
□	Drug Safety Regulation	Master Safety Programs	New York	Compliance Program Manuals	Michele Title	05/19/2014 07:00:00 PM
□	EPA - Methane Emissions	Master Safety Programs	Dallas	EPA	Sherry McWilliams	05/16/2014 02:32:21 PM
□	Fire Safety Inspection	Master Safety Programs	New York	Fire Safety Inspection	Perry Keys	08/06/2014 02:46:23 AM
□	Food Safety Regulation	Food Safety Regulation	Asheville	Food Safety Document.doc	Perry Keys	08/27/2014 02:00:23 PM
□	Food Safety Regulation	Food Safety Regulation	New York	Food Safety Document.doc	Michele Title	02/24/2015 10:52:59 AM
□	Forklift Checklist	JSA	San Diego	Forklift checklist.pdf	Bob Peelstrom	01/07/2014 04:12:44 PM
□	Forklift Checklist	JSA	New York	Forklift checklist.pdf	Michele Title	02/06/2015 03:46:49 PM
□	Forklift Safety	JSA	San Diego	JSA-Operating A Forklift.pdf	Paul Lachance	11/12/2014 11:20:22 AM
□	Forklift Safety	JSA	New York	JSA-Operating A Forklift.pdf	Michele Title	02/23/2015 12:38:12 PM
□	Hydraulic Fluid	MSDS			Bob Peelstrom	01/07/2014 04:20:11 PM
□	ISO 14001 Environmental Program	Master Safety Programs	Dallas	ISO 14001 Environmental Management	Sherry McWilliams	04/08/2014 12:31:59 PM
□	ISO9001:2008	Master Safety Programs	Dallas	ISO Certificate	Sherry McWilliams	09/11/2014 09:54:29 AM
□	JSA-Boiler Plant Inspection	JSA	New York	Boiler Plant Inspection	Michele Title	05/19/2014 07:00:00 PM
□	Maintenance Concept of Ops.	Foundations		Maintenance Concept of Operations.docx	Paul Lachance	02/24/2014 09:00:57 AM
□	MSDS 10w-30 oil	MSDS		10w-30 motor oil	Bob Peelstrom	01/07/2014 07:22:04 PM
□	MSDS Lithium grease	MSDS		Lithium Grease	Bob Peelstrom	01/07/2014 07:23:45 PM
□	MSDS SuperMelt	MSDS		SuperMelt	Bob Peelstrom	01/07/2014 07:25:47 PM
□	O & M Energy Efficiency	Master Safety Programs	New York	NYPD	Sherry McWilliams	02/05/2015 08:16:25 AM

Page 1 of 2 (27 items)

Intensium® Flex
Perfect compact power for UPS systems

© Saft – © Photos : Saft, Fotolia – C238 - IBG 057-2-12

Intensium Flex is the ideal backup solution for high power UPS and DC power systems in confined spaces.

- Reliable, maintenance-free lithium-ion technology
- Compact lightweight battery package
- Modular flexible archicture
- Optimized supervision through remote control and diagnostics

www.saftbatteries.com

SAFT

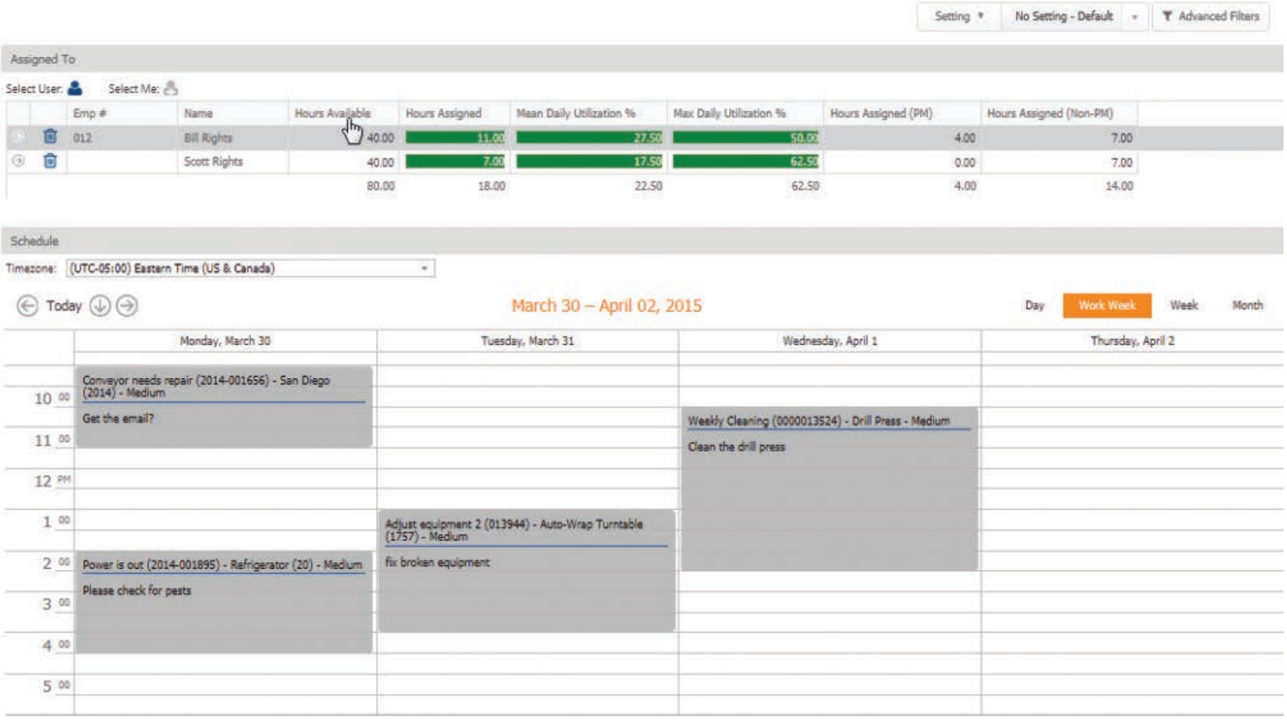
ViaWest also looks at the overall operational state of a unit, and uses a CMMS to do a detailed analysis of all unplanned repairs. Was the event discovered when a technician was executing a PM or monitoring equipment during rounds; or did a customer notify the team? Beyond that discovery, what was the type of repair and how well did the technician perform? ViaWest takes those data points and looks for inconsistencies that can lead to predictive action. The age of the equipment, frequency of events over the year, and the severity of each event contribute to the decisions around replacing equipment or based on the technician scorecard, renegotiating service contracts.

AUDIT/COMPLIANCE MANAGEMENT

Regulatory demands, client certification needs, and evolving legislation all challenge the ability of data center mangers to address compliance issues and respond to audits. With a CMMS in place, documentation and reports on maintenance activity can be pulled at a moment's notice, making managers audit-ready at any time.

At an in-house data center for one financial services company, for example, the CMMS made it possible for managers to quickly respond to auditor's questions about maintenance compliance with Sarbanes-Oxley Act (SOX) regulations. As part of the process, auditors wanted to know exactly what type of PMs have been performed on backup generators used for maintaining the UPS at the data center. The chief facilities engineer tapped the CMMS to produce reports showing all the PMs completed during specific time periods, as well as upcoming PMs planned for the future.

The need for optimal infrastructure maintenance will continue to rise as data centers age and face new technological challenges. And a modern CMMS – with its preventive and predictive maintenance, asset capital planning, and audit-managing capabilities – will also continue to become intertwined with all the other mission-critical systems that keep data centers running in peak condition.



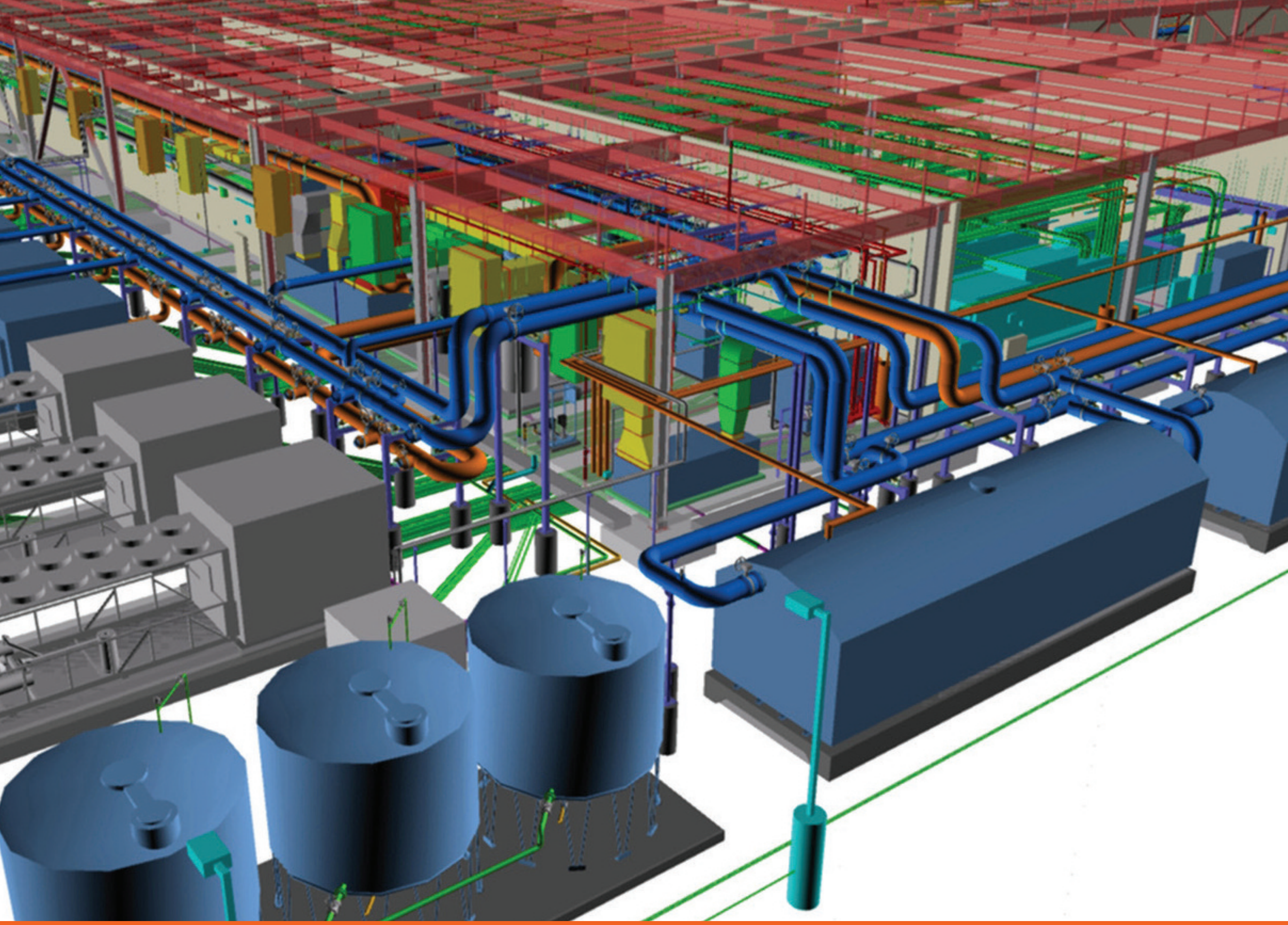
Emp #	Name	Hours Available	Hours Assigned	Mean Daily Utilization %	Max Daily Utilization %	Hours Assigned (PM)	Hours Assigned (Non-PM)
012	Bill Rights	40.00	11.00	27.50	50.00	4.00	7.00
	Scott Rights	40.00	7.00	17.50	62.50	0.00	7.00
		80.00	18.00	22.50	62.50	4.00	14.00

Timezone: (UTC-05:00) Eastern Time (US & Canada)

March 30 – April 02, 2015

	Monday, March 30	Tuesday, March 31	Wednesday, April 1	Thursday, April 2
10 00	Conveyor needs repair (2014-001656) - San Diego (2014) - Medium Get the email?		Weekly Cleaning (0000013524) - Drill Press - Medium Clean the drill press	
11 00				
12 PM				
1 00		Adjust equipment 2 (013944) - Auto-Wrap Turntable (1757) - Medium fix broken equipment		
2 00	Power is out (2014-001895) - Refrigerator (20) - Medium Please check for pests			
3 00				
4 00				
5 00				

Paul Lachance is President and Chief Technology Officer for Smartware Group, Inc. He can be reached at paul.lachance@bigfootcmms.com



Hooray! They're opening 10 new sites per month.

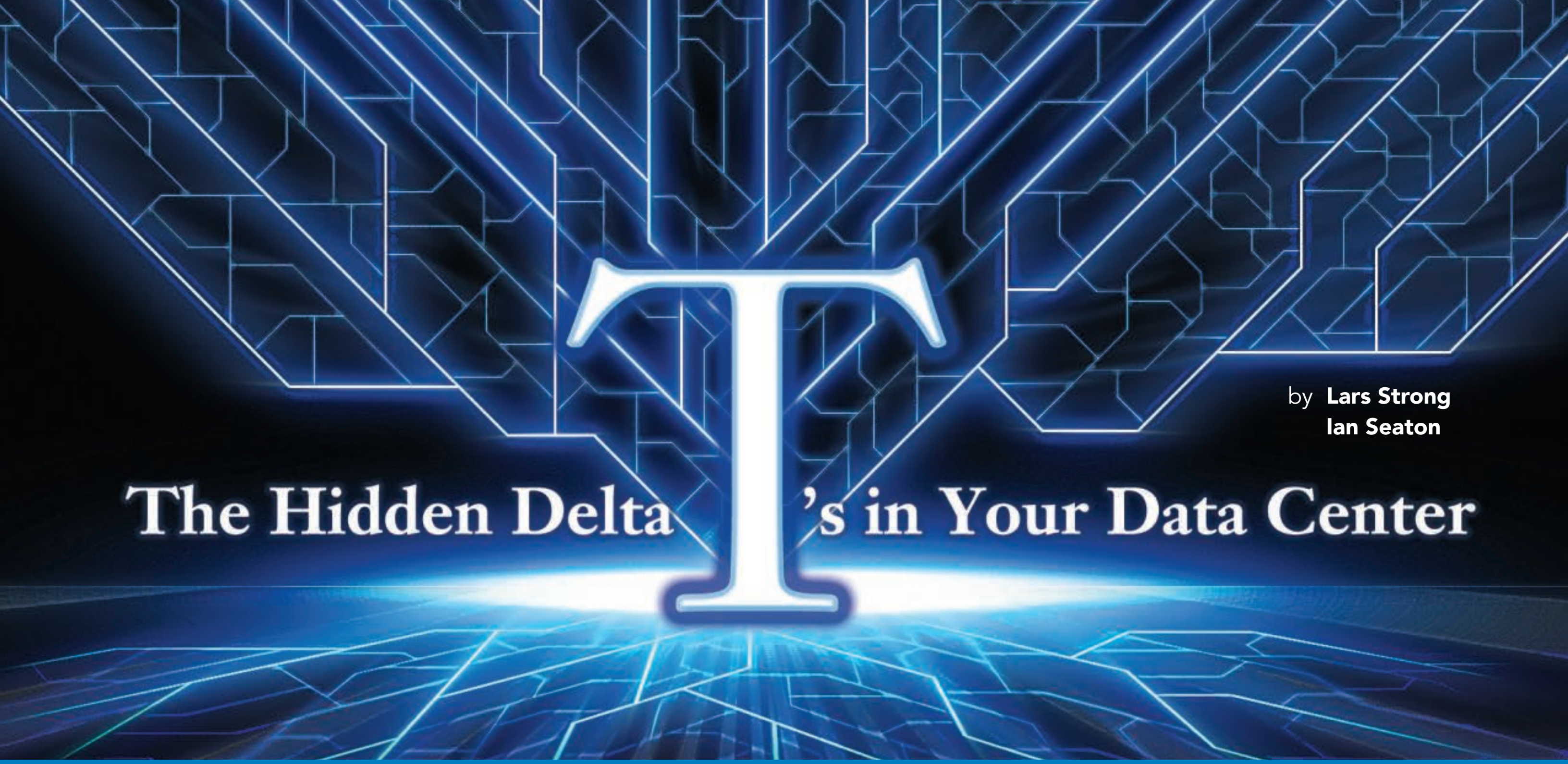
Hooray! Now set up IT infrastructure and take care of existing sites too.

See how easy it is to manage and standardize it all with SmartCabinet™.

Visit *EmersonNetworkPower.com/SmartCabinetVideo*

EMERSON™
Network Power

EMERSON. CONSIDER IT SOLVED.™



The Hidden Delta T's in Your Data Center

by Lars Strong
Ian Seaton

HOW MEASURING LESS-COMMONLY KNOWN DELTA T'S CAN HELP IMPROVE YOUR COOLING EFFICIENCY.

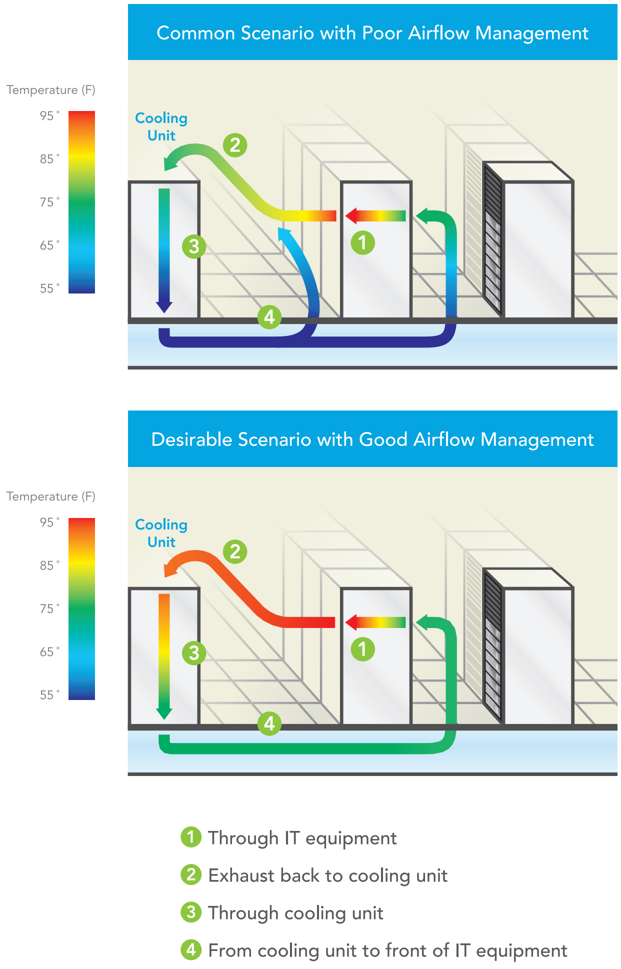

Common Scenario with Poor Airflow Management
Temperature (F)
95°
85°
75°
65°
55°
Cooling Unit
1
2
3
4
Desirable Scenario with Good Airflow Management
Temperature (F)
95°
85°
75°
65°
55°
Cooling Unit
1
2
3
4
1 Through IT equipment
2 Exhaust back to cooling unit
3 Through cooling unit
4 From cooling unit to front of IT equipment

Figure 1: Map of the four ΔT's

Within the data center, two types of temperature differentials are frequently considered as a single metric:

- The increase in air temperature as it passes through IT equipment, picking up and removing the heat produced within that equipment.
- The temperature differential across the cooling equipment cooling coils, or the difference between supply and return air temperatures.

Frequently, these two ΔT's are discussed as the ΔT, but there are good reasons to consider them separately and monitor how they differ. However, there are two additional ΔT's beyond these that are not commonly thought of: the temperature differential from IT equipment exhaust to cooling unit return and from cooling unit supply to IT equipment intake. They will often account for unexpected differences between the IT equipment ΔT and cooling equipment ΔT.

In an ideal data center, the ΔT across the IT equipment would be the same as the ΔT across the cooling coils (or cooling source) and there would be zero ΔT between the IT exhaust and the cooling return intake and/or between the cooling supply and IT equipment intake. Understanding the sources of these differences can help mitigate cooling and inefficiency problems and help return a data center to optimum efficiency.

Commonly Known ΔT: Through IT Equipment

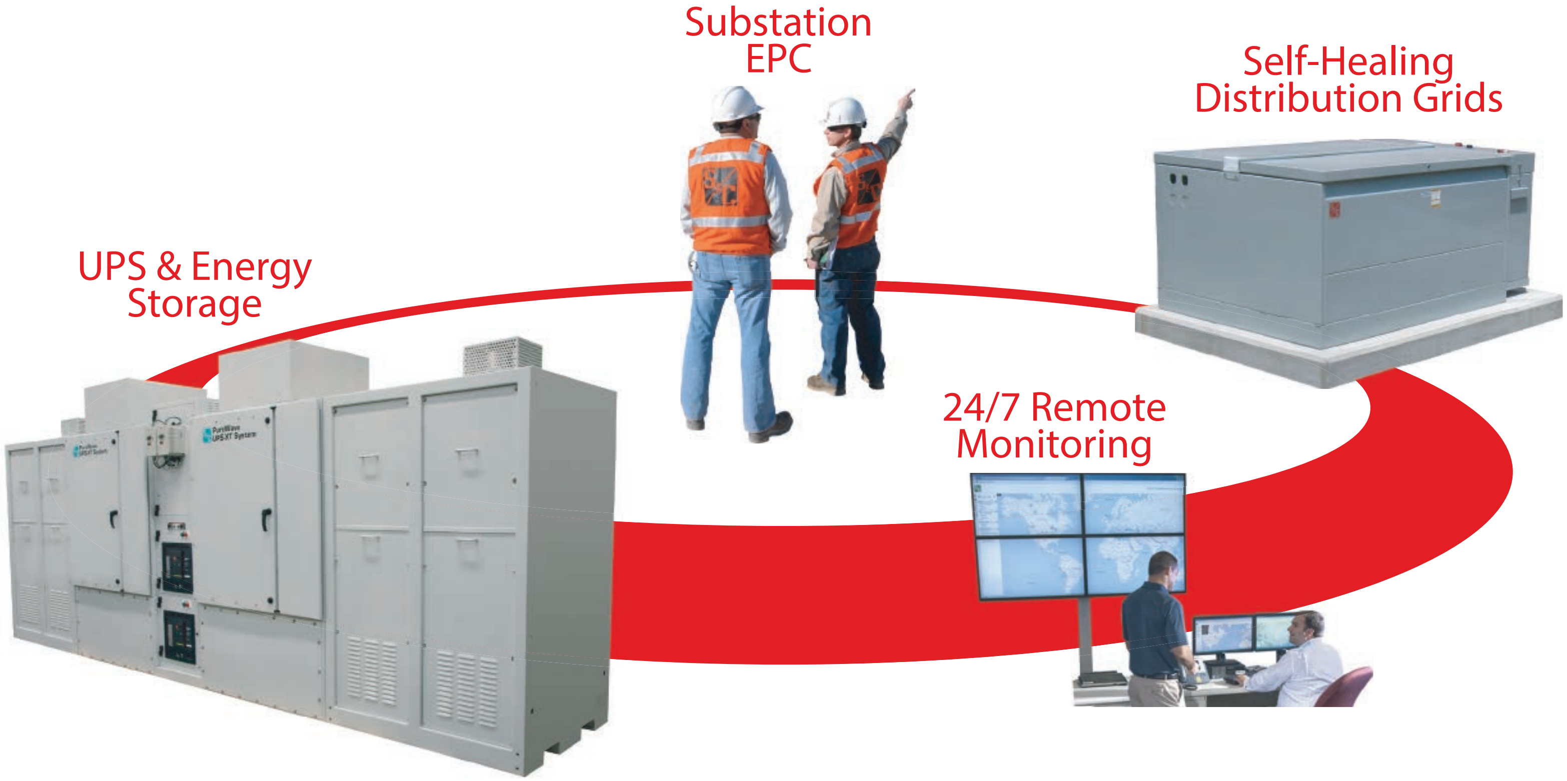
(#1 in Figure 1)

Keeping abreast of ΔT's is one of the most important jobs in a mission critical environment. Usually, ΔT is discussed within data centers as a single metric which is based on the temperature drop across cooling equipment or rise in temperature across IT equipment. While there can be many reasons as to why these two values may be different, they generally fall into two categories: either the return air to the cooling units is being cooled by bypass airflow or the supply air is being warmed due to hot air re-

Let Your Power Be Our Priority

Relax. You have enough to worry about when it comes to your data center's operations. Trust S&C's medium-voltage experts to make sure that your power system's reliability and availability are taken care of.

Your Data Center Medium-Voltage Experts for



Substation EPC

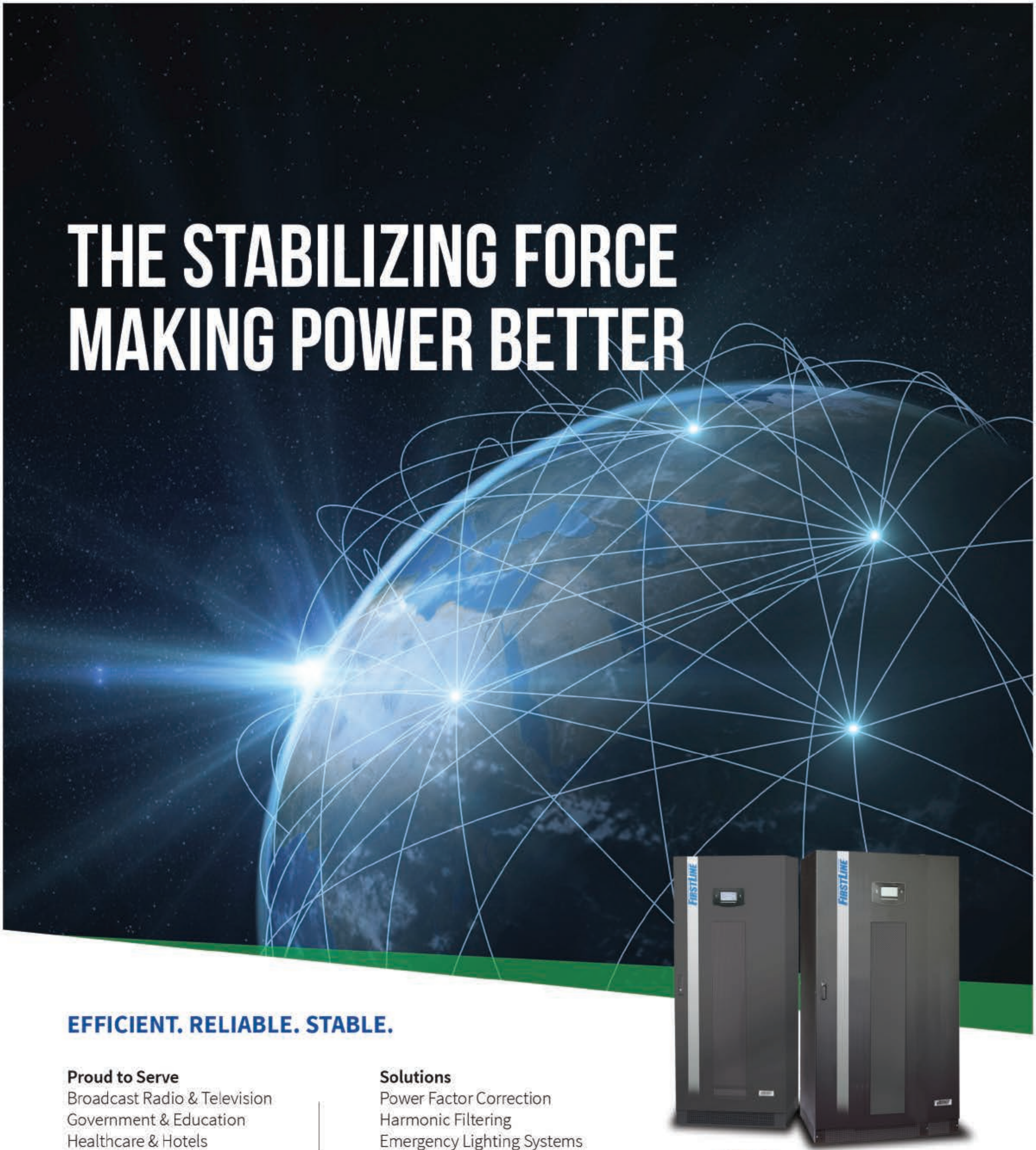
Self-Healing Distribution Grids

UPS & Energy Storage

24/7 Remote Monitoring

Learn more at
sandc.com/MVexperts

S&C ELECTRIC COMPANY
Excellence Through Innovation



EFFICIENT. RELIABLE. STABLE.

Proud to Serve
Broadcast Radio & Television
Government & Education
Healthcare & Hotels
Water Treatment
Manufacturing
Data Centers
Telecom
Oil & Gas

Solutions
Power Factor Correction
Harmonic Filtering
Emergency Lighting Systems
Frequency Conversion
Uninterruptible Power Systems
Voltage Regulation
Battery Monitoring
Power Conditioning

WWW.STACOENERGY.COM

STACO ENERGY®
PRODUCTS CO.

circulation. Regardless of the airflow management effectiveness in the data center, the IT equipment airflow temperature rise will be the constant[1].

Table 1 charts the fixed relationship between airflow, temperature differential and heat within the data center. The following equation is used to establish these values:

$$\Delta T = 3.1W \div CFM$$

IN THIS FORMULA:

- *3.1 is a constant coefficient at sea level*
- *W = watts*
- *CFM = cubic feet per minute airflow*

The coefficient changes for calculations at higher altitudes and in Celsius, for airflow measurements in liters per second or cubic meters per hour, and for heat measured in kW or BTU. Regardless of the unit of measure being considered, there is a fixed relationship between these three factors. In practicable applications, the ΔT across IT equipment typically ranges from around 20˚F up to around 35˚F, depending on the type of equipment. For example, blade servers typically produce a higher ΔT than traditional rack mount servers.

Commonly Known ΔT: Through Cooling Units

(#3 in Figure 1)

The other established data center ΔT occurs across cooling units. Ideally, this delta should be the same as the delta across the IT equipment, indicating that the cooling resource is in sync with the heat load it serves. Unfortunately, due to several factors this is rarely the case. In legacy Direct Expansion (DX) CRAC units, there is typically little allowance for variation from baseline ΔT. For example, increases in return air temperature often result in an associated increase in supply air temperature, so a 5˚F increase in return air temperature might result in a 3˚F or 4˚F increase in the supply temperature. This results in the overall ΔT increasing slightly, but nowhere near the proportion possible with water-cooled coils. Modern water-cooled CRAH units can remove heat equivalent from a 45˚F to 65˚F temperature drop across the cooling coils. Given the mathematical relationship between heat, airflow and ΔT previously discussed (CFM = 3.1W/ΔT), the higher ΔT across those coils equates to removal of more heat, which results in the CRAH unit operating much more efficiently. Under most circumstances increased efficiency is welcome. However, if the ΔT across the IT load is still only 20˚F, then excess heat is not effectively being removed. Instead, the inefficiency of the overall airflow management scheme is being accommodated, which is only a short-term solution.

The ΔT across the cooling source is also affected by set points. For example, if there is a great deal of bypass airflow in the data center, it is possible that the return air can actually be below the set point and therefore returned to the data center without any additional heat being removed (ΔT = zero). Further, with a standard return set point established (similar to a home or office thermostat setting), the CRAHs will be working to bring the data center temperature down to that set point, resulting in ΔT's which could range from 0˚F to over 20˚F. Finally, if the CRAHs are operating with a fixed supply temperature, the ΔT could range from 20˚F to 35˚F based on the types of servers deployed in that space or the cooling coils could see less than 10˚F if there is wasted surplus cooling in the space (up to over 40˚F if there is a cumulative hot air re-circulation effect).

IT Equipment Required Flow Rate

Required Flow Rate (CFM)		IT Equipment Delta T (deg F)					
		15	20	25	30	35	40
IT Equipment load (kW)	0.5	105	79	63	53	45	40
	1.0	211	158	126	105	90	79
	1.5	316	237	190	158	135	119
	2.0	421	316	253	211	181	158
	2.5	527	395	316	263	226	198
	3.0	632	474	379	316	271	237
	3.5	737	553	442	369	316	277
	4.0	843	632	506	421	361	316
	4.5	948	711	569	474	406	356
	5.0	1,053	790	632	527	451	395
	5.5	1,159	869	695	579	497	435
	6.0	1,264	948	758	632	542	474
	6.5	1,369	1,027	822	685	587	514
	7.0	1,475	1,106	885	737	632	553
	7.5	1,580	1,185	948	790	677	593
	8.0	1,685	1,264	1,011	843	722	632
	8.5	1,791	1,343	1,074	895	767	672
	9.0	1,896	1,422	1,138	948	813	711
	9.5	2,001	1,501	1,201	1,001	858	751
	10.0	2,107	1,580	1,264	1,053	903	790

Table 1: Relationship between airflow and ΔT

THE LESS COMMONLY KNOWN DELTA T'S

Beyond these well-established ΔT's, there remains two hidden areas of ΔT that can help data center owner/operators understand the differences between IT and cooling coil ΔT's and suggest possible remediating strategies. These are: from cooling unit to front of IT equipment (#4 in Figure 1) and from exhaust back to cooling unit (#2 in Figure 1).

Often Ignored ΔT: From Cooling Unit to Front of IT Equipment

(#4 in Figure 1)

The ΔT between the cooling unit supply output and the server inlet is

not often monitored, yet is extremely important. For example, if 55˚F is being supplied (fairly typical), the data center is more than 5˚F below the recommended minimum temperature for data processing equipment, per ASHRAE environmental guidelines. However, this low temperature is often not a problem for IT equipment because by the time the airflow reaches the IT equipment, it is typically a much higher temperature.

How does this ΔT occur? Often, supply air can become heated before it enters the computer room from under the floor. For example, perforated floor tiles located too close to CRAHs can actually draw warm air into the space beneath the floor due to the low pressure being created by high velocity supply air (the Venturi effect). Additionally, underfloor obstructions can also create vortices which result in low pressure pockets that pull air from outside of the room into the underfloor space. This unwelcome air mixes with the supply air and is another factor in increasing the temperature before it even evacuates through perforated tiles into the data center.

Even once the supply air enters the computer room, it is subject to conditions which can further increase the temperature. Openings in server racks – either open rack mount spaces or unsealed areas around the perimeter of the equipment mounting area – can allow the server waste air to leak back into the cold aisle and raise the temperature of the supply air. The problems caused by inadequate airflow due to

STARLINE

I e C E
Indirect Evaporative Cooling Equipment

Introducing

STULZ IeCE

STULZ IeCE™ is an indirect evaporative cooling solution, designed to remove heat by exploiting the evaporation of water. Indirect evaporative cooling takes advantage of the cooling potential from outside air without introducing contaminants or humidity into the data center.

Start saving energy now by utilizing STULZ IeCE or one of the other outdoor air handling solutions:

- Indirect Evaporative
- Direct Evaporative
- Custom DX & Chilled Water
- Packaged Rooftop
- Modular

STULZ IeCE

STULZ CyberCon

STULZ CyberHandler

STULZ CyberPack

Email us: info@stulz-ats.com • Call us: (301) 620-2033 • See our products: www.STULZ-USA.com

STULZ®

Outdoor Cooling		Indoor Cooling			Retrofit & Conditioning		
Modular Container	Air Handler	Ceiling	Row	Perimeter	Humidification	EC Fan Retrofit	Replacement

underfloor issues result in increases in hot air re-circulation over the tops of cabinets or around the ends of cabinet rows. A common response to address high IT equipment intake temperatures is to increase cooling airflow volume or reduce temperature setpoints.

Often Ignored ΔT: Exhaust Back to Cooling Unit

(#2 in Figure 1)

In contemporary data centers, the ΔT from servers back to the cooling source is usually negative; the temperature of the return air tends to decrease after it is exhausted from the IT equipment as it makes its way back to be re-cooled. This makes sense, as the excess cooling air is bypassing the data center heat load and returning to the cooling units, reducing the temperature of the return air along the way. There are several causes of such bypass airflow:

- Improperly located perforated floor tiles that can cause cool air to bypass the heat load.
- Large underfloor pressure differentials which may result in high pressure zones that pump significant quantities of air into a cold aisle in excess of the demand indicated by the intake fans of the associated IT equipment.
- Unsealed cable access holes in tiles located toward the rear of server racks that will result in cold air joining the exhaust air inside the back of the server rack. This source of bypass airflow can be especially troublesome when managing cooling efficiency issues via ΔT's, as it can mask the true IT equipment ΔT. Before monitoring or taking corrective action in response to this ΔT, plug any holes in the unsealed floor cut-outs in the rear of server racks to help eliminate false measurements.

REMEDIAL CONSIDERATIONS

When server inlet temperature is more than 5˚F above the supply temperature being produced by cooling units, there is hot air re-circulation occurring from open pathways between a hot and cold aisle, inside or around the server racks, or an inadequate flow zone that may require CFD analysis to determine the source of pressure variations under the floor. If the return air intake of the cooling units are more than 5˚F lower than the exhaust temperature from the IT equipment, there is a bypass airflow problem. Areas to check include improperly placed floor tiles, unsealed floor openings, or simply excess airflow being delivered into the room.

These 5˚F guidelines for calibrating ΔT's are only suggestions to help increase the efficiency of the data center. The overall goal (particularly if free cooling is available) is to get the differentials between the server exhaust and the cooling unit return intake and between the cooling unit supply and the server intake as close to zero as possible. That alignment will result in a better harmonization between expenses made for cooling and the true cooling work required. It will also increase opportunities for more free cooling hours if free cooling is part of the data center's design.

In most circumstances, optimum efficiency in the data center will be achieved when:

- There is minimal difference between the supply air temperature and the server inlet temperature (#4 in Figure 1).
- There is minimal difference between the IT equipment ΔT and the cooling coil ΔT (#1 and #3 in Figure 1).
- The supply temperature can be elevated to a temperature approximating the maximum specified upper threshold for the space (once the above two conditions are met).

Monitoring all four ΔT's can provide valuable information for calibrating the data center to meet its ideal performance level, regain stranded capacity and reduce operating cost.

[1] There will be some conditions in which the ΔT will not remain constant, especially with the proliferation of variable speed fans in IT equipment. When inlet temperatures are allowed to exceed the maximum recommended threshold and move toward the upper allowable levels, many servers will increase fan speeds to protect equipment, thereby reducing the ΔT through the IT equipment. Additionally, with the increased adoption of cloud-based data centers, large caches of work can be transferred between data centers with the resultant increased work load producing higher chip temperatures and, therefore, higher ΔT's. Nevertheless, in normal conditions, the equipment ΔT remains a constant.

[2] http://www.upsite.com/blog/equipment-delta-t-flow-rate-impact-data-center

Lars Strong is Senior Engineer of Upsite Technologies. He can be reached at lds@upsite.com
Ian Seaton is Technical Advisor to Upsite Technologies. He can be reached at iseaton@upsite.com

Mission Critical Subject Matter Experts Needed

Cleveland Community College*, in conjunction with Examplify, LLC, is asking for subject matter experts for the following purposes:

- Developing course content and assessments that align to an outline of learning objectives by participating in one or more of a series of week-long development workshops. Meals, a stipend, travel reimbursement, and lodging will be provided.
- Taking a beta version of a certification exam.

If you are interested in one or both of these opportunities, please email **examdev@comptia.org**

*In 2013, the United States Department of Labor awarded Cleveland Community College (in Shelby, NC) and its partner schools a $23.2 million dollar grant to develop a training program and workforce for mission critical operations. From the grant, the partners created the National Consortium for Mission Critical Operations (www.NCMCO.us). Part of the grant includes developing new college courses in mission critical operations.

NCMCO
NATIONAL CONSORTIUM FOR MISSION CRITICAL OPERATIONS

Examplify
A CompTIA Company

What:

This is a beta version of the NCMCO Mission Critical Operations Certification Exam.
Passing the beta exam qualifies you as a Certified Mission Critical Operator (CMCO).

Who:

Anyone with one year's experience or education in the mission critical field can take this exam.

When:

This is a limited-time opportunity and will be granted on a first-come, first serve basis.

Cost:

$50.00 with the promo code MCOBeta15; 50% off for the first 100 test takers
using the promo code MCOBeta100

Exam time:

120 minutes (plus 30-minute non-disclosure review)

Purpose:

This exam will certify that a successful candidate is able to perform entry-level operational tasks within a mission critical environment. This includes maintenance, reporting, and incident response.

Content:

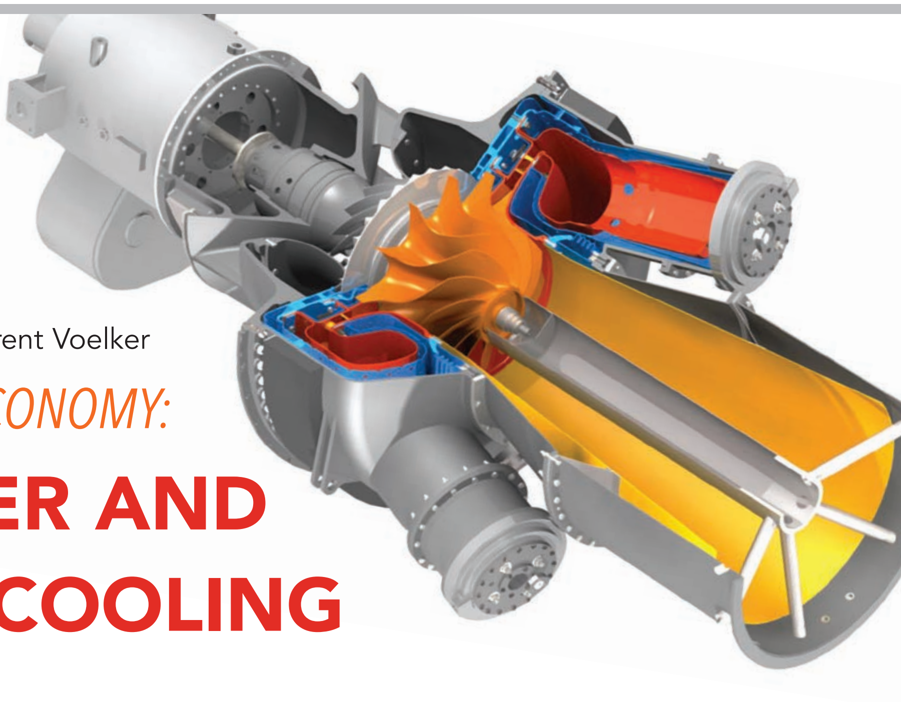
Topics covered on the exam include infrastructure, safety, security, emergency response, operations, and procedures.

A detailed list of exam objectives is available at
exams.ncmco.us

If you are interested or would like further information, please contact
examdev@comptia.org

CERTIFIED
MISSION
CRITICAL
OPERATOR

CMCO



by Brent Voelker

FUELING THE INFORMATION ECONOMY:

RESILIENT POWER AND COGENERATED COOLING

As the discretionary operation of diesel generators becomes increasingly restricted and the recently announced Clean Power Plan enters the implementation phase, a pivot toward cogenerated cooling from resilient dual-fuel gas turbines will become essential to the boomer data center industry. And radial gas turbines rated at 1.8MW are ideally designed for data center applications. Coupled with an absorption chiller, a single turbine generator displaces 2300kW of electric power from the grid. But more importantly, a dual-fuel turbine is capable of smoothly switching from 100% natural gas to 100% diesel at full load without power interruption in the event that the utility gas supply is disrupted. Such turbines can single-handedly provide superior reliability of prime electric power and equipment cooling during normal operation and in times of emergency, reducing or eliminating requirements for backup diesel generators, UPS, and associated maintenance.

Data centers are large power consumers and heat producers, requiring backup generators and redundant cooling to qualify for high reliability ratings. Diesel generators sufficient to power the electronics and electric cooling (normally powered from the grid) have been the standard for data center standby power due to their ability to startup rapidly in the event of a power outage. Uninterruptible Power Supplies (UPS) bridge the gap to maintain power during the ten seconds it takes for the diesels come on line. Despite tightening restrictions on exercising diesel engines for maintenance and reliability checks, gas reciprocating engines have not displaced diesels. Gas engines are slower to start and bring up to full load, so they must be accompanied by higher-capacity UPS. Further, the probability of gas supply disruption during a major disaster results in unacceptable system reliability for the gas option. While some gas generators can be operated on diesel as well, they typically required a minimum diesel flow at all times, making extended operation unacceptable unless expensive emissions controls are employed.

Enter the dual-fuel gas turbine, capable of smoothly switching from 100% natural gas to 100% diesel at full load without power interruption in the event that the utility gas supply is disrupted. The generator is operated 24/7 on 100% natural gas in parallel with the grid, transitioning seamlessly to island mode when grid power is interrupted. In order to maximize value during normal operation, an absorption chiller powered by turbine exhaust provides continuous equipment cooling to the facility. Excess chiller capacity is employed in a turbine inlet cooling (TIC) system to boost generator output.

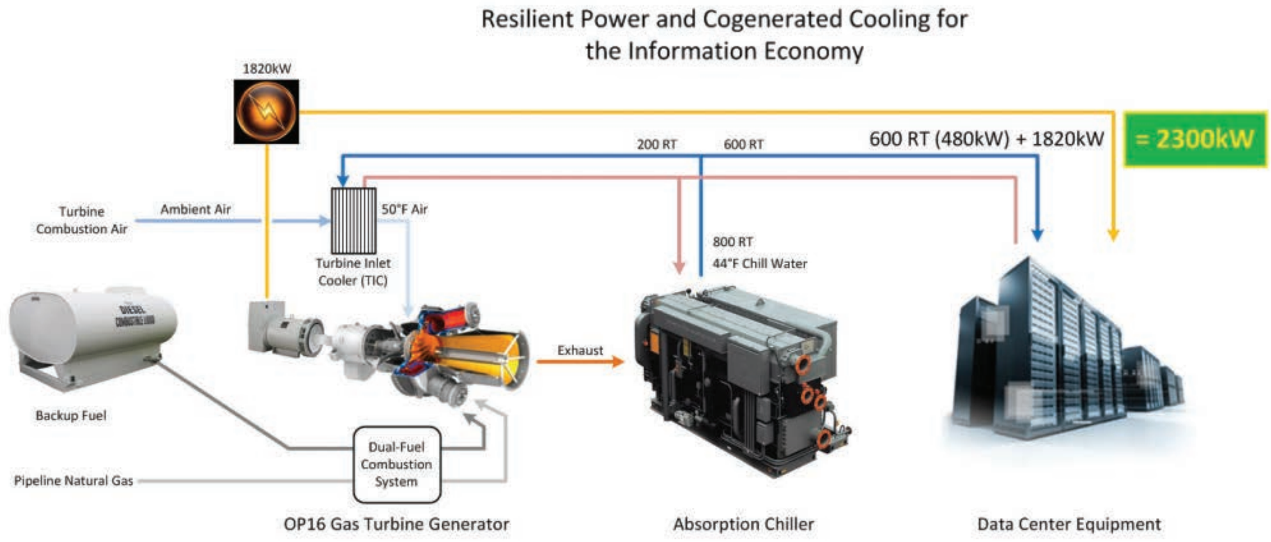
ARE YOU AFRAID OF THE DARK?

The
DATACENTER
Where IT, Facilities and Design Meet
Journal
"Unbiased, Quality Content Every Day!"
Visit www.datacenterjournal.com today

Coupled with an absorption chiller, a single turbine generator designed for distributed cogeneration displaces 2300kW of electric power from the grid: it produces 1820kWe to power electronic equipment plus 600 Tons of Refrigeration (RT), which would normally draw 480kW when electric chillers are employed. Further, substantial additional energy is available in the turbine exhaust to power redundant chillers should the data center require it: total exhaust energy from one 1.8MW turbine is sufficient to produce 1560 RT. Data centers typically employ backup generators in 2-2.5MW increments, so the gas turbine with cogenerated cooling will perfectly support a typical facility strategy of modular incremental expansion. But unlike backup diesel generators, the gas-fired turbine will provide its own additional return on investment by reducing the cost of energy for the facility during normal operation.

Fuel control should be tuned for a six-second transition time for switchover from 100% gas to 100% diesel or from diesel back to gas. A small receiver in the gas line or a run of large-diameter pipe ensures adequate gas pressure through the switching transient after the gas supply is lost. The turbine will require 14,000 gallons of U.S. conventional diesel to operate continuously for 72 hours in the event of a crisis. During normal operation, an automated maintenance action will switch from gas to diesel and perform diagnostic checks to periodically demonstrate reliability of operation on the backup fuel. Total time operating on diesel for these routine checks will be less than 15 hours over the course of each year.

The small gas turbine generator represents a sea change for power in the data center industry. While some large data centers are accompanied by enormous investments in redundant high voltage power lines or independent gas lines, these strategies remain vulnerable to system-wide disruptions. At a fraction of the cost, the small gas turbine can automatically and literally transform the data center into an island unto itself, fully insulated from electric grid and gas supply outages. And in addition to the avoided cost of UPS and backup diesel generators, a gas turbine with cogenerated cooling will provide exceptional value during normal operation by reducing energy costs while continuously demonstrating the availability of reliable power to carry the center through times of emergency.


Resilient Power and Cogenerated Cooling for the Information Economy

Brent Voelker is the Director of Sales for Kinsley Energy Systems.
He can be reached at bvoelker@kinsleyenergy.com.

INSIDE 7x24

2015 FALL CONFERENCE

END-TO-END RELIABILITY: MISSION CRITICAL FACILITIES

COMMITMENT TO EXCELLENCE

Register Before October 23rd for a Chance to Win One of Three MacBook Airs

2015
FALL CONFERENCE
END-TO-END RELIABILITY: MISSION CRITICAL FACILITIES
COMMITMENT TO EXCELLENCE
November 15-18, 2015
JW Marriott San Antonio Hill Country
San Antonio, TX

SAVE THE DATE!

2016 Spring
Navigating the Future
June 5 - 8, 2016
Boca Raton Resort & Club
Boca Raton, FL

2016 Fall
Theme TBD
October 23 - 26, 2016
JW Marriott Phoenix Desert Ridge
Phoenix, AZ

For information about sponsoring a 7x24 Exchange event please contact Brandon Dolci, CMP at 646-486-3818 x108

INTERESTED IN PRESENTING AT THE NEXT SPRING CONFERENCE?

Visit www.7x24exchange.org and complete the
Call for Presentations or call 646-486-3818 x104

DEADLINE: **JANUARY 8, 2016**

SUBMIT AN ARTICLE FOR THE NEXT SPRING ISSUE OF 7x24 EXCHANGE MAGAZINE

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

DEADLINE: **FEBRUARY 26, 2016**

PUBLISHED BY 7X24 EXCHANGE INTERNATIONAL
7x24 Exchange International
THE END-TO-END RELIABILITY FORUM
Theresa Payton
2015 Fall Conference
KEYNOTE SPEAKER
COLLABORATION
GUIDES DATA CENTER DESIGN

2015 FALL CONFERENCE

END-TO-END RELIABILITY: MISSION CRITICAL FACILITIES

COMMITMENT TO EXCELLENCE

CONFERENCE HIGHLIGHTS

The Fall Conference themed **"End-to-End Reliability – Commitment to Excellence"** will be held November 15-18 at the JW Marriott San Antonio Hill Country in San Antonio, TX. The Conference will feature compelling keynotes, high profile speakers, concurrent sessions, an end user only forum, a women's forum, a guest/spouse shopping shuttle, the Marquis Plus+ Partner Showcase, another spectacular sponsored event and more…

Theresa Payton, Former White House CIO, Cybersecurity Authority, Expert on Identity Theft and the Internet of Things will kick off the conference with a keynote address entitled **"Big Data and the Internet of Things – Boon or Bust for Your Cybersecurity Efforts?".** Marketing databases, customer analytics and behavioral patterns are easier to manage with big data – but will these data elements be safe from hackers? And what is the impact of the Internet of Things? Payton will explain how to harness the power of big data and build your big data to achieve business goals while adding in safeguards to fight cybercriminals. She'll also explain how the Internet of Things may be the ultimate driver of global change.

Our second day will open with a Keynote entitled **"Moving Cyber Security to the Strategy Table"** by Fran Dramis, CEO of F. Dramis LLC and Former CIO of BellSouth and Salomon Brothers.

The closing keynote is entitled **"Yahoo! Evaporation Pond Design for Data Center Effectiveness"** and will be delivered by Soechgen Mulia, Construction Manager at Yahoo!.

SESSIONS INCLUDE:

- Oracle's Journey to Data Center Excellence
- The Right Data Center for the Job
- PANEL: Commitment to Sustainability and Efficiency
- Blending the Modular and Traditional Data Center
- Uncovering the Benefits of Modular Chiller Plants
- ASHRAE: Valuable New Information Impacting Decisions
- Project ECHO (CPS) Data Center/Control Room – Challenges & Solutions
- The Impact of IT on Healthcare

MONDAY, NOVEMBER 16th
6:30 P.M. - 9:30 P.M.

MARQUIS PLUS+ PARTNER SHOWCASE

CASINO NIGHT

ABB
ARMSTRONG
CATERPILLAR®
EASTPENN
GE Critical Power
mtu onsite energy
PDI
SIEMENS

7x24 Exchange is proud to present the 3rd Annual Marquis Plus+ Partner Showcase. This premier, one of a kind exposition will allow attendees to network while enjoying cocktails, a variety of food stations, entertainment and more…with the opportunity to view the latest and greatest equipment, products and services available to assist you in your day to day data center operational needs. Special thanks to our Marquis Plus+ Partners as this event would not be possible without their support!

SPONSORED EVENT

A Night at the RODEO

LIVE MUSIC
DANCING
GREAT FOOD

TEJAS ★ RODEO COMPANY©

NOVEMBER 17
6:30 P.M. – 10:00 P.M.

Join 7x24 Exchange and its sponsors for a night at Tejas Rodeo where guests will experience great food along with authentic Texas style entertainment topped off with a professional rodeo.

7X24 Exchange INTERNATIONAL™
The end-to-end reliability forum.™

Special thanks to the partners that made this event possible:

ABB
DRIVEN BY MOTION ACTIVE POWER
ARMSTRONG
ASCO®
CATERPILLAR®
CLUNE Construction Company
ComRent®
dataaire
DPR CONSTRUCTION
EASTPENN
Ehvert
GE Critical Power
GENERAC® INDUSTRIAL POWER
IBM®
IEM™ Industrial Electric Mfg
INFOMART DATA CENTERS™
JACOBS®
KOHLER. Power Systems
MIRATECH
mtu onsite energy
OptiCool® TECHNOLOGIES
Page/
PDI
NECA IBEW POWERING AMERICA
QTS® Data Centers Powered by People
Raritan. Know more. Manage smarter.™
Russelectric Power Control People You Can Rely On
saft
S&C
SIEMENS
STACO ENERGY PRODUCTS CO.
STARLINE
STULZ Air Technology Systems, Inc.
SUNBELT. RENTALS
SYSKA HENNESSY GROUP
marathon™ Thomson Power Systems
WT Whiting-Turner

2015 FALL CONFERENCE

END-TO-END RELIABILITY: MISSION CRITICAL FACILITIES

COMMITMENT TO EXCELLENCE

(at press time)

2015 FALL CONFERENCE CORPORATE LEADERSHIP PROGRAM PARTNERS

MARQUIS PLUS+ PARTNERS

ABB
ARMSTRONG
CATERPILLAR®
EASTPENN
GE Critical Power
mtu onsite energy
PDI
SIEMENS

GOLD PARTNERS

CLUNE Construction Company
dataaire
SYSKA HENNESSY GROUP

SILVER PARTNERS

DRIVEN BY MOTION ACTIVE POWER
ASCO®
ComRent®
DPR CONSTRUCTION
Ehvert
GENERAC® INDUSTRIAL POWER
IBM®
IEM™ Industrial Electric Mfg
INFOMART DATA CENTERS™
JACOBS®
KOHLER. Power Systems
MIRATECH
OptiCool® TECHNOLOGIES
Page/
NECA IBEW POWERING AMERICA
QTS® Data Centers Powered by People
Raritan. Know more. Manage smarter.™
Russelectric Power Control People You Can Rely On
Saft
S&C
STACO ENERGY® PRODUCTS CO.
STARLINE
STULZ Air Technology Systems, Inc.
SUNBELT® RENTALS
marathon™ Thomson Power Systems
WT WHITING-TURNER

BRONZE PARTNERS

ALIGNED DATA CENTERS
AEP AMERICAN® ELECTRIC POWER
ANORD CRITICAL POWER INC.
BTECH®
CELLWATCH POWERING CONFIDENCE®
Dutch Data Ports
GLUMAC engineers for a sustainable future™
IDenticard® ACCESS CONTROL
Intertek
JE DUNN® CONSTRUCTION
Kidde Fire Systems
McKinstry For The Life Of Your Building
PowerShield.
PRINCE WILLIAM COUNTY, VIRGINIA
PURKAY LABS
R monitoring services
SABER Power Services
Server Technology Quality Rack Power Solutions
Tate® AIRFLOW
TOSHIBA Leading Innovation >>>
UMP® Data Center Cooling

MEDIA PARTNERS

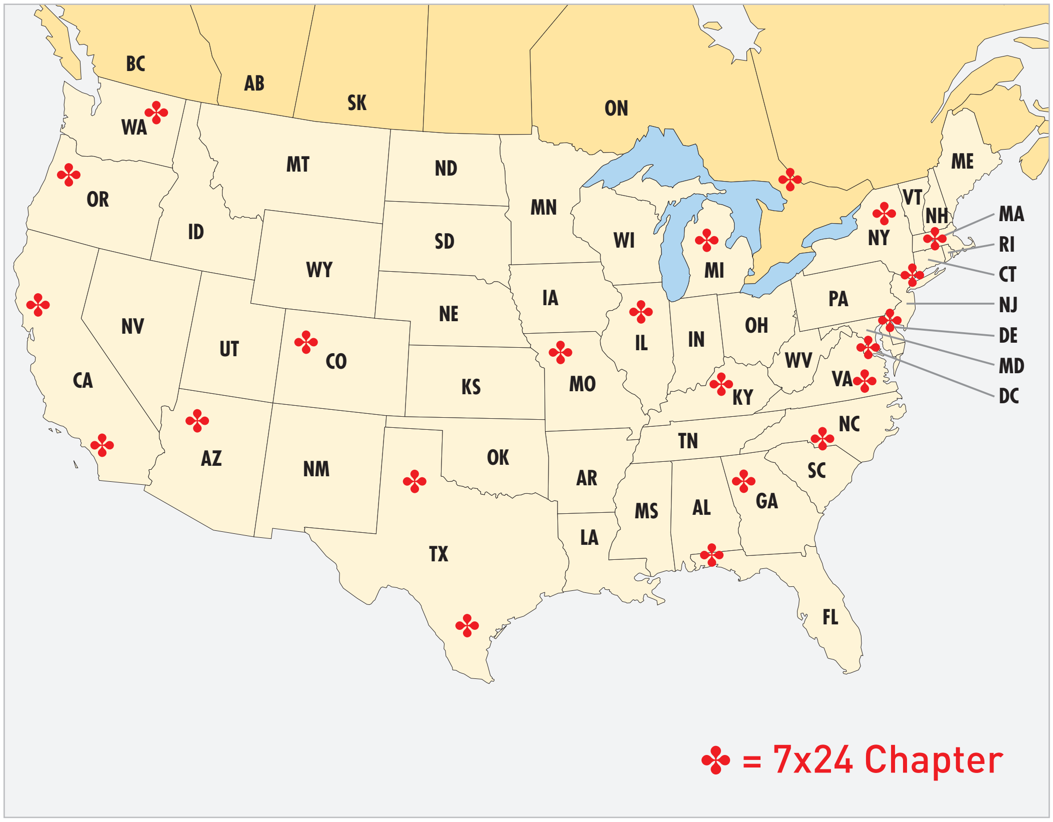
AMERICAN BUILDERS QUARTERLY™
The DATACENTER Journal Where IT, Facilities and Design Meet
Mission CRITICAL Data center and emergency backup solutions

7x24 Exchange INTERNATIONAL

The end-to-end reliability forum.™

BECOME INVOLVED IN YOUR LOCAL 7X24 CHAPTER

INTERNATIONAL CHAPTERS

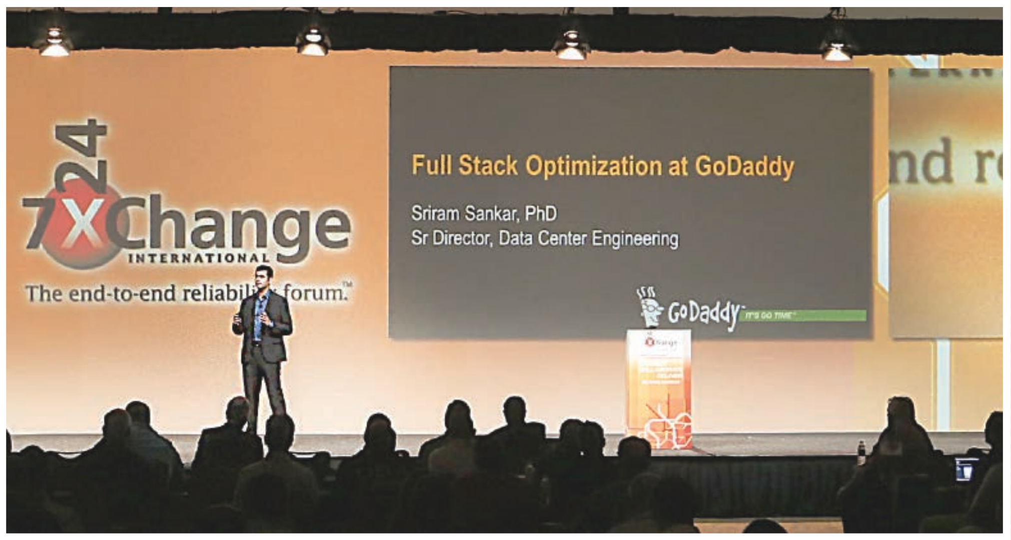


✤ = 7x24 Chapter

- Arizona
- Atlanta
- Bluegrass
- Canada
- The Carolinas
- Central Virginia
- Delaware Valley
- Empire State (Albany)
- Europe
- Greater Florida/Alabama
- Greater Washington DC Area
- Lake Michigan Region
- Lone Star (Dallas)
- Metro New York
- Midwest
- New England Area
- Northern California
- Northwest (Seattle, WA)
- Oregon & SW Washington
- Rocky Mountain
- Southeast Michigan
- Southern California
- Texas South

VISIT WWW.7x24EXCHANGE.ORG TODAY
TO PARTICIPATE IN YOUR LOCAL CHAPTER

2015 SPRING CONFERENCE HIGHLIGHTS


7x24 Exchange INTERNATIONAL
The end-to-end reliability forum.™
Full Stack Optimization at GoDaddy
Sriram Sankar, PhD
Sr Director, Data Center Engineering
GoDaddy

The end-to-
7x24 Exchange INTERNATIONAL
The end-to-end reliability forum.™

the groove

7x24
XChange
INTERNATIONAL
The end-to-end reliability forum.™

CITYWALK
Hot Dog
HALL OF FAME
WORLD'S
Hot Dog

The end-to-

2016 SPRING CONFERENCE

END-TO-END RELIABILITY: MISSION CRITICAL FACILITIES

SAVE THE DATE

JUNE 5-8, 2016
Boca Raton Resort & Club
Boca Raton, FL

7x24 Exchange INTERNATIONAL
The end-to-end reliability forum.™
www.7x24exchange.org

2016 SPRING CONFERENCE
END-TO-END RELIABILITY: MISSION CRITICAL FACILITIES

NAVIGATING THE FUTURE

JUNE 5-8, 2016 Boca Raton Resort & Club, Boca Raton, FL

7x24 Exchange INTERNATIONAL
The end-to-end reliability forum.™

www.7x24exchange.org

DESIGNED FOR UPS APPLICATIONS

Deka®

°fahrenheit™

HEAT TOLERANT VRLA BATTERIES

LASTS 3x LONGER AT HIGH TEMPERATURES*

UPS APPLICATIONS 5-YEAR FULL WARRANTY @ 95°F (35°C)

FEATURING OUR EXCLUSIVE NEW THERMAL MANAGEMENT TECHNOLOGY SYSTEM™

THT™ Plastic – optimizes internal compression
Micro Catalyst – increases recombination and prevents dryout
Helios™ Additive – lowers float current and corrosion
IPF® Technology – optimizes capacity and reliability

EASTPENN

Lyon Station, PA 19536-0147
Phone: 610-682-3263 • Fax: 610-682-0891
www.dekabatteries.com • e-mail: reservepowersales@dekabatteries.com

**Compared to standard VRLA products*