Life Is On | Schneider Electric

Selecting a Building Management System (BMS) for Sites with a Data Center or IT Room

White Paper 233

Revision 0

by Bryan Anderson and Patrick Donovan

Executive summary

A data center or IT room uniquely alters the requirements of a building management system (BMS). This is primarily because of the criticality of IT and its dependence on facility infrastructure. IT's reliance on power and cooling systems makes a BMS an important part of a larger data center infrastructure management (DCIM) solution that brings together Facilities and IT. The cooperation and information sharing better ensures uninterrupted and efficient operation. This paper explains how the requirements for building management are affected by the presence of a mission critical data center or IT room (data rooms) and describes key attributes to look for in an effective BMS system. Common pitfalls of implementing and using a BMS for sites with IT along with advice on how to avoid them are also provided.

Introduction

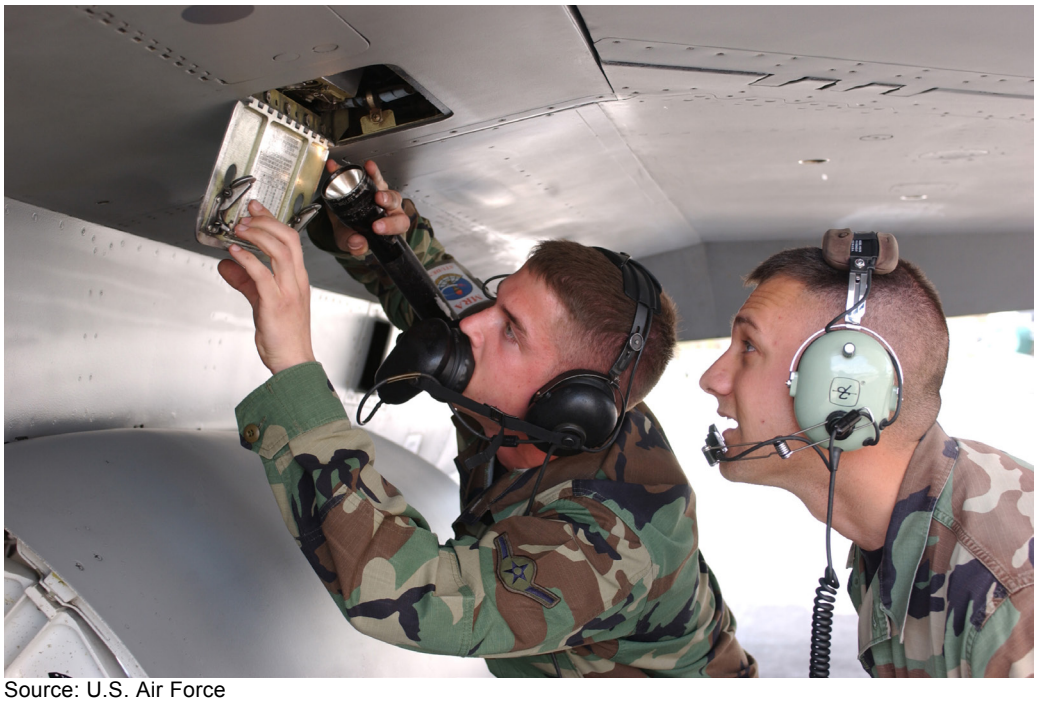
O&M Program

An Operations & Maintenance Program includes the people, processes, procedures, documentation, and tools for operating and maintaining the facility. There are 12 essential elements of the program:

- Environmental health & safety
- Personnel management
- Emergency preparedness & response
- Maintenance management
- Change management
- Documentation management
- Training
- Infrastructure management
- Quality management
- Energy management
- Financial management
- Performance monitoring & review

A facility containing mission critical Information Technology (IT) is substantially different from a typical commercial office building, retail site, or school. For these sites requiring "7x24" continuous operation, failure can shut down the entire enterprise and cause severe, immediate, and often long term financial loss. Some liken the operation and maintenance (O&M) of these to "maintaining an airplane while flying it". Many businesses are often either wholly dependent on their IT or IT IS the business. This is particularly so for web services companies, retailers, cloud/collocation services providers, and financial institutions. Complexity is greater and the pace of change within the data center is faster than in most other types of facilities. The criticality, complexity, and dynamic nature of the IT load dramatically affect the requirements of the facility O&M program (see **sidebar**) as well as for the infrastructure management software tools that support it. This paper is intended to provide guidance for selecting the software tools (i.e., Building Management Systems (BMS) and Electrical Power Monitoring Systems (EPMS)) for managing the power and cooling infrastructure at sites with mission critical IT. The interface and interaction of the BMS and EPMS with a data center information management system is also addressed. The effect of mission-critical IT on the requirements for the overall O&M program is outside the scope of this paper. However, White Paper 196, *Essential Elements of Data Center Facility Operations* and White Paper 197, *Facility Operations Maturity Model for Data Centers* address this topic thoroughly.

In the first section, the paper shows specifically how the presence of a data room affects the requirements of a building management system (BMS); a system that traditionally is designed for occupant comfort and, perhaps, lighting efficiency. The key capabilities of a BMS system designed to support mission-critical IT, available in the market today, are explained. The importance of cooperation, information sharing, and integration with other management systems is emphasized in the second section. The last section describes common pitfalls of evaluating and implementing a management system and how to avoid them.



Source: U.S. Air Force

Figure 1
The extreme criticality and pace of change for IT requiring "7x24" availability has led some to liken the management & monitoring to "maintaining an airplane while flying it".

Key capabilities of a BMS

The presence of mission critical IT equipment fundamentally changes how a site should be operated and maintained by the facilities team. IT relies on the electrical and mechanical systems that power and cool it. Even the briefest of interruptions or misallocations in the supply[1] of power and cooling can result in IT application downtime. And this can have disastrous effects on the business. Complicating this, these critical loads often fluctuate in their demand for power and cooling resources. Loads can be both physically and increasingly virtually moved through the use of automated virtualization and IT container technologies. IT is becoming more "software defined" where networking, storage, and compute resources are virtualized. These virtual machines can be created, moved, and dissolved based on demand at any given moment. White Paper 118, *Virtualization and Cloud Computing: Optimized Power, Cooling, and Management Maximizes Benefits* explains more how electrical and mechanical loads are affected by modern IT. This dynamic environment places new requirements on a BMS system. The following paragraphs explain these key capabilities.

BMS systems serve the purpose of controlling the mechanical infrastructure and providing real time monitoring of facilities equipment and actively managing cooling performance. The BMS system is able to react to changes in the cooling load or failures of equipment automatically by turning on additional equipment, opening valves, or increasing the airflow to maintain cooling. When a failure occurs a BMS must also provide the facilities management team information needed to take actions that keep IT equipment powered and cooled. System dashboards and alarm logs provide local and remote users with real time information about the status of the system. Strategies for reducing energy consumption can be built in to the logic to lower operating costs. **Once a BMS is properly programmed and commissioned** it is the most effective tool to manage the redundant mechanical equipment common in these mission critical environments. The BMS core features of controlling and monitoring equipment make it an ideal platform for consolidating the alarming and system monitoring of the electrical system as well by interfacing it with the EPMS.

Table 1 lists and describes the important key capabilities for a building management system at a site containing a data center or mission-critical IT. These functions are required to continuously monitor system status in real-time, be as proactive as possible, and respond immediately to incidents as they occur with active physical control.

[1] For example, a misallocation could be having enough bulk cooling capacity but being constrained (due to under the floor obstructions, not enough cooling vents etc) at the distribution level which leads to hot spots at some of the IT racks. If hot enough, this can cause these servers to shut down. Another example might be allowing an overload to occur at a branch circuit resulting in a breaker tripping that then causes connected loads to turn off or lose redundancy.

Table 1

Key capabilities for a building management system at a site containing a data center or mission-critical IT

Key capabilities	Why it's important
Physical control and response	Upon failure of a cooling unit, temperatures in a data center rise rapidly in the first 60 seconds[2]. The BMS is programmed to sense equipment failure or rapid temperature rises and automatically turn on redundant cooling equipment. It also senses regular fluctuations in the needs for cooling and adjusts cooling and air flow to maintain consistent temperatures in the space.
Complete visibility of power and cooling system status and performance	System needs to be able to monitor the entire power & cooling trains from the utility connection and head of the mechanical plant down to the IT servers since the load is dependent on them. If subsystems or components are not being monitored, then problems and failures will go unnoticed until it is too late to respond and prevent IT application downtime.
Visibility to dependencies and interconnected nature of infrastructure components	Power, cooling, and IT system failures can be either the cause or symptom of issues. Operators need to quickly assess the root cause and be able to take action to keep all systems on line. This visibility is important to also understand which systems, applications, or customers might be affected or put at risk when performing maintenance or upgrades.
Comprehension and visibility of redundant systems	Mission critical IT often uses redundant power and cooling plants and distribution systems. It is important for the BMS system to be aware of their presence and status since a loss of redundancy is a prelude to IT system and application failure.
Capacity monitoring & planning	Capacity monitoring and planning affects capital expenses, ability to generate revenue, and operational efficiency. Tools that provide accurate real-time status and trend information about spare capacity, stranded capacity, and consumption are vital to maintaining availability and tracking efficiency.
Effective communication tools	Event logging, notification policies, and alarms need to be configured and provide the right context and actionable information to the right people at the right time to ensure swift and appropriate resources are brought to bear as infrastructure status changes or incidents occur.
Shares information with Data Center Infrastructure Management (DCIM) systems	IT managers want to be aware of what is going on with the electrical and mechanical plants since it has such a big impact on their IT gear and applications. They need to be notified of pending maintenance, adds, and changes so they can respond appropriately and be prepared to minimize any potential impact. And vice versa; facility managers should be aware of what is going on in the white space too. Note this capability is discussed in more detail later in the paper.
Network security	Any device that is connected to a network could be a potential attack avenue for cyber attackers. The criticality of IT makes it very important for the BMS system to use the latest cyber security protocols and to be constantly maintained and updated as those protocols change. Note this topic will be discussed further later in the paper.

Additional thoughts on key capabilities

Data centers attract a larger and more intense focus from organizational executives. Attention from CxOs on the BMS for a typical commercial property is primarily limited to energy efficiency and, perhaps in some parts of the world, carbon reporting. The direct impact data centers and IT rooms have on business performance and cost, however, creates a need for greater reporting to a wider variety of stakeholders. The BMS must provide input to the CFO for capital planning, the CMO for

[2] http://www.apc.com/wp?wp=179

EPMS

An electrical power monitoring system provides comprehensive intelligence and detailed power quality data on the electrical distribution network in conjunction with installed power meters. These systems enhance reliability by providing detailed analysis and reporting of input and output power quality. The software also helps optimize energy use by identifying opportunities to reduce electrical power consumption

DCIM

A data center infrastructure management system is a set of software tools used to monitor, plan, and manage infrastructure components within the IT "white space" including UPSs, PDUs, Racks, Rack PDUS, environmental monitoring gear, physical security, and fire detection/suppression systems. Many DCIM systems also integrate directly to IT operations management systems as well. An effective DCIM system can help ensure availability, maintain or improve efficiency, and make capacity planning more accurate.

capacity and performance, and the CIO for system performance. Additionally there are often other demands from compliance officers, Sales, Lines of Business, and Accounting functions within the organization. Some BMS systems are designed to generate highly configurable reports that speak directly in clear and simple terms to each of these stake holders. Basic commercial BMS systems lack the capability of exporting data in formats like Application Programming Interface (API) web services or report that allow for customized web based interfaces. The result is that a basic system can only generate reports and data in its proprietary formats or in technical open protocols that lack tools for customized business information purposes.

Power consumption is a significant cost for both commercial building and data center applications. Both applications can use energy efficiency as a competitive advantage. However, in data center applications the power consumption is a much higher percentage of operating costs. A commercial building with occupancy between 7 am and 6 pm Monday through Friday will need to operate at occupancy conditions approximately 2,860 hours a year. A data center (or any mission critical IT room) operates 8,760 hours a year. Changes in data center equipment efficiency result in approximately three times (3x) the savings of comfort cooling for the organization. The difference is that being too aggressive to gain efficiencies (by eliminating redundancies or reducing capacity safety margins) potentially exposes the enterprise to a greater risk of costly failure that can dwarf the potential energy savings. The need for efficiency must be balanced with the need for the capacity safety margin required to keep the system operational. Working with vendors who have experience balancing the need for efficiency with the need to remain operational can be the difference between savings and considerable loss. And this also emphasizes the need for a BMS that can track and report bulk power capacities and energy consumption in real time and share this information with DCIM systems.

BMS systems need to be able to help mitigate the risk of human error or reduce its impact when it occurs. 70% of data center outages are directly attributable to human error according to the Uptime Institute's analysis of their "abnormal incident" reporting (AIR) database (WP196, *Essential Elements of Data Center Facility Operations*). Human error can occur in two forms. Active error occurs when an operator takes an action that causes loss of cooling or power in the data center. Passive error is a failure to take an action to prevent loss of cooling or power. Both types can occur during normal operation, maintenance, upgrade, or renovation projects. The BMS system needs to react to keep/bring new equipment on line and both alert when a failure or error has occurred and provide timely, accurate, and clear instructions for how to recover from the specific incident. It is a significant benefit when the BMS can assist operators by delivering Method of Procedures (MOPs), Emergency Operating Procedures (EOPs), and equipment/alarm specific instructions, along with the alarm and its raw data. The more context that is provided with an alarm, the faster operators can resolve the problem and determine the root cause. By context, we mean information that explains more of the "where", "how" and "why" vs. the simple "what".

Network security in data centers and mission critical IT rooms is a very high priority for all enterprises. According to Verizon Data Breach Investigations Report 2016 63% of confirmed data breaches involved leveraging weak, default, or stolen passwords and 70% of breaches involving insider misuse took months or years to discover[3]. The BMS that resides in these rooms to control and monitor the equipment must also have robust network security features and policies. Network security, user password protocol, and management of remote connections need to be actively managed in compliance with company's corporate polices and industry best practices. Data rooms are designed for secure communication with controlled

[3] http://www.verizonenterprise.com/resources/reports/rp_dbir-2016-executive-summary_xg_en.pdf

inbound and outbound network traffic via IT security tools. The BMS system and technicians who bring their software tools and hardware in to the space represent risk to the overall cyber security of the system. The set up of the BMS network, cyber security of the BMS, and cyber security practices of the vendor who installs the system represent much higher risk than applications outside of the IT space.

It is clear that the extreme criticality and pace of change of IT drives a need for a secure management system that provides an efficient view of all resources and dependencies from the utility connection to the server, proactive and informative notifications, rapid physical response to incidents, and clear and useful reporting for key stakeholders.

BMS as part of a larger management system

For commercial buildings, facility operators have traditionally operated independently from other departments and functions of the organization. They have been tasked with keeping the lights on, the environment safe and comfortable, and the location secure from fire hazards and other physical threats. As long as there were no incidents or unusual energy bills, facilities would be left alone in their own world. In a data center, this independence and separation should be discouraged. As mentioned before, the IT load's total dependence on the facility's power, cooling and security resources dictates a need for openness and cooperation with their number one customer, the IT department.

Increasingly for more forward-looking organizations where the data center IS the business, this cooperation has gone so far as having the heads of both facilities and IT report into the same senior executive and sharing many of the same organizational goals and objectives. This type of structure is one way to ensure teamwork and achieving the shared goal of keeping the data center available "7x24" as efficiently as possible. Another way is to have Facilities and IT be equal stakeholders and active participants in the planning, design, and commissioning phases of all projects impacting IT. For the longest and costliest phase of the facility's life cycle, the operation phase, the principal means for sharing information and working together is the software management systems (see **sidebar above**); i.e., the BMS, electrical power monitoring system (EPMS), and data center infrastructure management (DCIM).

Modern BMS systems that are optimized for mission critical facilities have the ability to both share and receive status and alarm information with other infrastructure management systems. By supporting common, open protocols such as BACNet IP, MSTP, Modbus IP, and RTU over a standard Ethernet TCP/IP network, today's BMS can send and receive information to and from EPMS and DCIM systems. Some BMS systems also have the ability to transmit data via Application Programming Interfaces (APIs) to host information as databases, web services, and reports. Web services APIs host raw data in formats suitable for stakeholders to create user interfaces customized to their needs. Reports are an extension of APIs that includes some manipulation of the raw data prior to delivery. These API tools allow the data, typically restricted to the BMS and its user interface, to be leveraged throughout a customer enterprise in a wide variety of applications and user interfaces. Engaging a vendor with experience providing these integration services is key to ensuring a successful implementation.

To simplify the effort to make these connections, it is important for Facilities and IT to work together in the evaluation and implementation phase. To properly evaluate software tool options, both sides should meet to define and agree on what the connected systems should do and use that output to compare solutions. The comparison should consider each solution's ability to do what you want, as well as the effort required to make it happen. Determining this means interviewing the

vendor and being specific about your requirements. Note that choosing a vendor who offers and has designed all three tool sets to work together should make the integration simpler and less error prone. For the implementation phase, both groups should agree on alarm notification policies, thresholds, and ensure the requirements from the evaluation phase make it into the actual implementation. And finally during commissioning, both sides (Facilities and IT) should witness the behavior of the system while operating and agree together on a pass or fail of the testing before it goes live.

Common pitfalls and how to avoid them

A BMS as part of a larger data center infrastructure management system has the potential of offering facility managers and other stakeholders a lot of value. A well implemented system provides a clear and concise view of what would otherwise be a complex and diverse ecosystem of disparate facilities and IT components. A BMS that shares and receives information with infrastructure management tools for the servers and network equipment can better ensure resources are efficiently used, planned for, and maintained for high reliability. And they can do so with less human resources than manual monitoring and management. Despite this, we have found that some customers fail to realize this value at all. White Paper 170, *Avoiding Common Pitfalls of Evaluating and Implementing DCIM*, provides a detailed explanation for what can go wrong (for either a BMS or DCIM system) and what steps to take to ensure the full value and promise of an infrastructure management system is realized. We present a summary of the findings in this paper. There are three fundamental pitfalls:

- Choosing an inappropriate solution
- Relying on inadequate or mismatched processes
- Lack of commitment, ownership, and knowledge

Pitfall #1: Choosing an inappropriate solution

At the time of this writing there are dozens of vendors offering various BMS and DCIM software tools. They vary widely in terms of scope and function. There is also overlap in function between tools designed for traditional building facilities and data center “white space” systems. For example, a BMS can monitor and poll information from systems located within the data room. At the same time there are tools designed to monitor, plan, and manage data room infrastructure systems that can also poll information from facility power and mechanical plants. While a software tool might be able to cover multiple domains like this, they tend to be optimized best for one and not the other. When one tool is substituted to do the work of another, the outcome can be a failure due to the inability to execute or due to a lack of use because the interface is too cumbersome to be effective. BMS interfaces are versatile and capable of collecting data from a variety of sources. However, when a

BMS is used to assist operators within the IT space there can be a significant breakdown. The templates for graphics and reports for white space activities are missing. The user interface for the BMS is designed for facilities users with some high level dashboards for reporting based on a limited number of points for mechanical equipment. IT managers, on the other hand, need information specific to the IT gear, network equipment, UPSs, CRACs/CRAHs, racks, rack PDUs, , as well as their dependencies on each other. Therefore a DCIM tool should be used for white space applications and a BMS and EPMS tools should be used for building and electrical applications respectively. To help make sense of this, consult White Paper 104, *Classification of Data Center Infrastructure Management Tools*. This diversity and overlap combined, perhaps, with some overinflated marketing promise, has had

the unintended side effect of causing confusion and missed expectations for some users.

There are a number of key characteristics to look for when selecting BMS and DCIM tools that ensure this pitfall is avoided. **Table 2** summarizes these attributes to look for.

Table 2

Key characteristics to look for when selecting BMS and DCIM tools

Key characteristic	Description	Why it's important
Scalable, modular, flexible system	Ability of system to handle adds, changes, upgrades, as well as flexibility of system to provide the outputs users and stakeholders require	If the software is difficult to update, keep up with change, or cannot be configured to output useful and clear information, then it will not be used.
Open communication architecture	Using open standard communication protocols between equipment such as SNMP, BACNET, and Modbus TCP to connect with all required physical infrastructure systems easily	Effective management systems require a full and accurate picture of power, cooling, space, and IT resources, and their dependencies on each other, ideally in real time.
	Ability to export data in Application Programming Interface (API) for use in databases, web services and reports.	Web services API host data in formats suitable for custom user interfaces. API reports involve manipulating data for delivery to customized database tools.
Standardized, pre-engineered design	Solution is built on previous experience. Pre-engineered indicates much, if not all, of the complex programming work needed to communicate with power, cooling, and IT systems has already been done. A standardized system will likely already come pre-configured to interact with 3rd party systems and management tools making implementation much simpler.	Trying to use highly custom, "one-off" products that aren't designed to work together can make installation, operation, and maintenance of the tools very difficult. Custom solutions tend to result in custom problems.
Active vendor support structure	Vendor's level of expertise, commitment to the BMS/DCIM segment, participation/cooperation with industry organizations, technical support coverage, breadth of services, and their scope of experience with both facilities and IT roles.	Vendors' support capabilities should be evaluated as much as their software tools. Their quality of support can have a big impact on whether the investment in management tools is successful or not.

Note that WP170 provides much more detail on these pitfalls, and specifically, provides a list of questions to ask vendors to help determine if and to what degree their tool sets embody these key characteristics.

Pitfall #2: Relying on inadequate or mismatched processes

Management systems are often separately sold to and sought by both facilities and IT managers as a means to fill gaps in their operational processes. They are a way to simplify and automate monitoring and management, reducing the need for manpower and time. And, indeed, well implemented and effective systems can provide this value. However, the user still has to do their part to make the BMS and DCIM systems work effectively and fulfill its promise. Even the best systems won't eliminate the need for operator processes to implement, operate, and maintain them. Poor process is a common cause of failing to achieve the desired value of a management system.

The amount of operator effort and the number of processes needed to operate a system will vary from vendor to vendor. And this is yet another comparison point for the evaluation phase. Knowing the specific operator requirements of a given offer typically means interviewing the vendor directly. Many vendors will offer training programs on how to operate and maintain the management system. It is important to ensure there will be enough manpower resources (and the on-going discipline to use them) to meet the effort and process required.

Table 3 describes four important and common BMS/DCIM-related processes that, if neglected, will undermine the functioning and benefits of the management system:

Table 3

Critical BMS/DCIM-related processes

Operator process	Description	Implication
Inventory/asset management	Accurately recording and maintaining all monitored assets/systems information including location and interdependencies of assets to each other in real time	Critical management system functions & calculations fail if the software's map of assets and their associated information is incorrect.
System configuration	Once the system is installed and a map of assets and dependencies is created, the system needs to be tailored to meet user requirements and objectives. This includes items such as alarm thresholds, notification policies, defining user access rights, system security settings, device/location labeling within the GUI, report definition/frequency, UPS and cooling unit operating parameters, etc.	If time and care is not taken to configure the system properly, then it will fail to perform properly, perhaps, in ways that could lead to infrastructure down time. Important information won't be conveyed or won't be conveyed to the right people. Alarms may be sent, but clear communication of expectations is required to avoid confusion as to who should respond, what should be done, and where it needs to be done which can result in a crisis situation.
Alarm integration	The process of ensuring that system alarms are noticed, documented, and responded to in the appropriate manner by either incorporating them into an existing issue resolution process or creating a new one (see **sidebar**)	Alarms, if not setup properly and integrated into an issue resolution process, will either go unnoticed or will be intentionally ignored. This could have the obvious effect of a simple incident (e.g., stuck chilled water valve) turning into a major crisis (e.g., servers shutting down due to thermal thresholds).
Reporting for management or other stakeholders	On-going reports generated to clearly communicate important system trends; building/data center KPIs, and overall health/effectiveness of the building infrastructure to management and other key stake-holders	Creating clear and useful reports, sending them to the right people, and acting on their data and analysis is a critical process to making the management system effective. Good reporting can identify trends to proactively mitigate threats, benchmark KPI performance, and make capacity forecasts more accurate.

Focusing on the four key processes above will help ensure the value of the BMS/DCIM system is realized. At a fundamental level, making all of this happen requires:

- Agreement between facilities, IT, and management on operating parameters, metrics, and goals for the data center power and cooling systems and their management.

Alarm integration

Alarms need to be delivered to different users in different formats and with a variety of information. The IT manager needs to know if temperature is out of range in the space. However, the on-call technician needs to know which sensor has registered a high temperature, how quickly the temperature rose, and the MOP (method of procedure) for addressing the problem. When a major piece of electrical equipment fails, it causes subsequent equipment to also go off line. When an electrical failure causes air conditioning equipment to shut off, a substantial quantity of alarms can be generated in a short period of time as associated sensors and parameters are violated. The operations team needs to effectively filter through the alarms to find the root cause. There may be several managers who need to be made aware of the problem but only after a predetermined period of time, if equipment and protocol fails to bring redundant systems back on line. When selecting a product ask the vendor to demonstrate their ability to prioritize and organize alarms to multiple stake holders. Most importantly, ensure that the system is able to directly attach MOPs in multiple document formats like .doc and .pdf, include action items and check lists, and show instructions for specific alarms.

- A review of existing processes and comparison to new management system requirements. (Can processes be incorporated into existing practices or are new practices required?)
- Any new processes be formally defined (who, what, when, where), resources committed, and specific owners assigned.

Pitfall #3: Lack of commitment, ownership, and knowledge

A process without an owner or the resources/knowledge to carry it out almost certainly dooms that process to failure. There is a history of "silo" based organizational structures between facilities and IT staff. Management is too often a third silo. This is a situation where information and objectives aren't always shared or even communicated. Given IT's utter reliance on the underlying electrical and mechanical infrastructure, this isolation and lack of cooperation should be eliminated. The implementation and operation of a broad management system that spans all three silos will be, at least, hindered, if not doomed to failure in such an environment. There is also a natural resistance to changing how things are managed particularly if that change is perceived to come from "outside" of an established silo. Experience has further shown that when management makes a decision to adopt a new system without the participation of those who would operate it there is high risk of incompatibility with existing processes or hardware that adds to the amount of change required. This leads to unforeseen short-comings in the implemented solution or incompatibilities that limit its effectiveness. Or the solution gets chosen and implemented without giving operators time and resources to learn how to use it. All of this can lead to the system being abandoned and ignored. **Table 4** provides a list of tips to help avoid this common pitfall.

Table 4
Tips for avoiding pitfall #3

Involve IT, Facilities, and Management from start of evaluation phase
Obtain "buy-in" from all sides on need for BMS/EPMS/DCIM system
Come to agreement on key requirements and goals
Work with vendor to understand specific operator requirements to achieve goals
Obtain Management commitment to provide necessary resources
Name specific owners for processes and procedures
Leverage vendor to develop required knowledge on how to operate and maintain system

Conclusion

This paper has addressed the unique requirements for managing and operating sites with data centers or IT rooms. The intent was to address both large dedicated data center buildings as well as commercial buildings with smaller IT rooms and/or IT closets. Differences in managing these spaces from other occupancies include significant financial consequences for equipment failure, greater need for reporting and visibility, a critical need to share and communicate with the IT department, and drastically reduced time to respond to critical incidents. Strategies for managing this increased complication and expanded internal oversight include ensuring proper installation and features of the software system selected, using the tools for their intended tasks, and keeping the solution simple. Tips for avoiding common errors in the implementation of systems focus primarily on communication, cooperation, and process.

It is important to communicate with designers and vendors to get systems that will interface with each other for a combined system. It is also important to work with internal stakeholders and set clear expectations and processes. Selecting a vendor that has experience designing and implementing complete solutions with all of the software systems required for a complete solution will reduce risk, time for deployment, and cost of the project.

About the authors

Bryan Anderson is a Data Center Software Sales Manager at Schneider Electric. He has over 15 years of experience in mission critical building management systems including several years as a consultant. He earned a Bachelor of Science degree in Mechanical Engineering and holds a Masters of Business Administration. He has designed a customer product selection and literature tool for Schneider Electric and has spent the last four years providing technical support and design services and solutions for data center owners.

Patrick Donovan is a Senior Research Analyst for the Data Center Science Center at Schneider Electric. He has over 20 years of experience developing and supporting critical power and cooling systems for Schneider Electric's IT Business unit including several award-winning power protection, efficiency, and availability solutions. An author of numerous white papers, industry articles, and technology assessments, Patrick's research on data center operations and physical infrastructure technologies offers guidance and advice on best practices for planning, designing, and operation of data center facilities.

Resources

Essential Elements of Data Center Facility Operations
White Paper 196

Facility Operations Maturity Model for Data Centers
White Paper 197

Virtualization and Cloud Computing: Optimized Power, Cooling, and Management Maximizes Benefits
White Paper 118

Avoiding Common Pitfalls of Evaluating and Implementing DCIM
White Paper 170

Classification of Data Center Infrastructure Management Tools
White Paper 104

Browse all white papers
whitepapers.apc.com

Browse all TradeOff Tools™
tools.apc.com

Contact us

For feedback and comments about the content of this white paper:

Data Center Science Center
dcsc@schneider-electric.com

If you are a customer and have questions specific to your data center project:

Contact your Schneider Electric representative at
www.apc.com/support/contact/index.cfm