Building Management Systems and the Need for High Availability

Protecting Critical Systems from Downtime & Disasters

us.sios.com

Whether a stand-alone skyscraper or a sprawling office campus, modern building design includes sophisticated building management systems (BMS). Facilities managers rely on these computer-based systems to monitor and manage mechanical and electrical plants, including HVAC (heating, ventilation, air conditioning) systems, lighting and power systems, fire systems, elevators, security systems, and more.

With BMS systems, building managers can ensure the safety and comfort of occupants and maximize the overall energy and cost-efficiency of building operations. The systems minimize the need for human intervention by automatically turning equipment on and off, opening or closing valves, and alerting facility staff about issues that could signal imminent building system failures or threats.

BMS solutions are central to the building or campus they manage, so they need to be protected from unscheduled downtime and disaster-related outages. Indeed, given that they control a building's the most vital safety services, a BMS must remain operational and accessible particularly in an emergency. The challenge is, how do you configure a BMS solution to operate at such a high level of availability without adding unnecessary cost and complexity?

## The Ongoing Need for Access to BMS Applications and Data

BMS solutions come in a variety of types and styles – bespoke, hardware-based systems, software-based systems on commodity servers, and cloud-based computer platforms. Fundamentally, all BMS solutions are comprised of software, a server, a database, an IP network, and a set of sensors connected to each of component of the building's or campus's infrastructure that the solution is monitoring and managing. Data from the sensors is captured in the database, where it is analyzed by the BMS software. If the analysis detects conditions that are outside preset parameters (e.g., the temperature in a specific room has suddenly spiked upwards), the BMS software responds with action—sending alerts, triggering alarms, locking doors, or performing any number of similar actions that can be predefined within the solution.

BMS solutions may operate on a standalone basis or they may integrate with other monitoring systems and subsystems. They may run on premises or in the cloud, on an infrastructure built upon a single operating system (OS) or on a complex hardware platform comprised of multiple OSs and protocols. They may rely on any number of popular, high-performance database systems, such as SQL Server, Oracle, SAP HANA, or MaxDB. Large vendors—such as Carrier, Eaton, Honeywell, Johnson Control, Schneider Electric, and Siemens—offer comprehensive BMS solutions. Smaller vendors offer specialized niche solutions for power management, power distribution, cooling, thermal control, and so on.

What all these systems have in common is a need to operate continuously. Building operators need to know that their power and thermal management systems, security systems, and the like are protected from downtime, particularly in the face of disaster that could compromise the safety of the building or campus.

Approaches to Ensuring Availability

Several approaches to ensuring the availability of a BMS, and facilities managers need to evaluate the criticality of their BMS system and balance the cost and complexity of a solution with the overall level of protection they need.
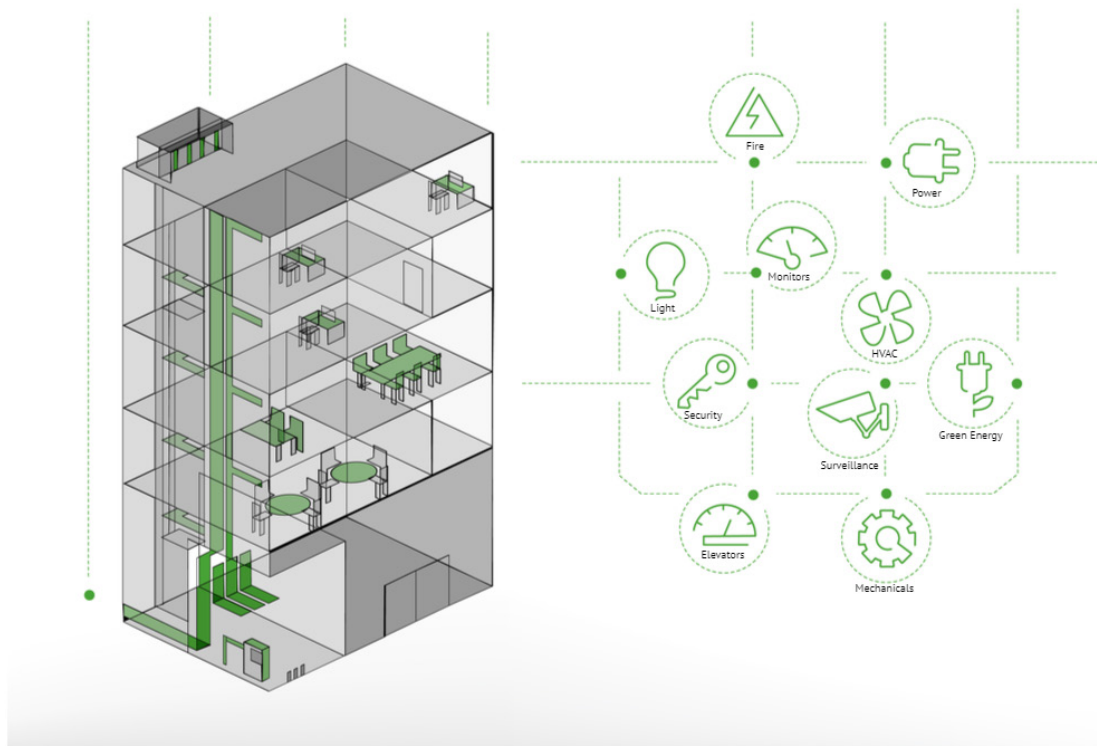
By unifying key functions, such as energy, HVAC, security, and elevator operation, BMS systems enable building managers to ensure the safety and comfort of occupants and maximize the overall energy and cost-efficiency of building operations.

Fault Tolerant Approaches

Fault-tolerant (FT) approaches to BMS availability promise that the servers running the BMS applications and/or database will be available 99.999% of the time (also known as "five nines" of availability). That translates to no more than 5.5 minutes of unscheduled downtime per year. But FT solutions can be extremely expensive to purchase and very complex to configure and manage. They often require an owner to "lock in" to a single vendor for all aspects of the BMS solution. It effectively becomes a bespoke solution, and that can limit the manner in which the solution can evolve over time.

High Availability Approaches

An alternative to the FT approach is an HA approach—where HA stands for "high availability." HA solutions, which can be configured using Linux or Microsoft Windows Server, guarantee that protected infrastructure will be available at least 99.99% of the time ("four nines" of availability).

Four nines of availability translates to no more than 53 minutes of unscheduled downtime per year—and it can translate into a dramatically lower total cost of ownership (TCO) for a still-powerful BMS solution.

Most building owners protect their BMS systems using infrastructure configured for HA–typically several physical or virtual machines (VMs) configured as a failover cluster. This approach provides HA at an attractive price point because the BMS can run on commodity hardware, on-premises or in the cloud, and the infrastructure does not require specialized expertise for maintenance and management. As a consequence, the TCO of a BMS solution configured for HA can be dramatically lower than the TCO of a solution based on non-commodity FT hardware—even though an HA based-approach can effectively provide comparable levels of application availability.

HA for State-of-the Art BMS System at Optus Stadium

Optus Stadium in Perth Australia is a high tech, multi-purpose 60,000 seat arena is the first-ever stadium in Australia to embrace a unified, continuous computing infrastructure platform.

The Environment

The stadium was built with a variety of high tech and future-proofing technology, including face recognition to sophisticated access systems, to thousands of sensors, high megapixel cameras, mission-critical application servers, numerous multi-vendor integrations and dependencies, and ICT (Information Communications Technology) requirements. The amount of data captured and stored on-site required a powerful solution to house, store, and protect it.

The Challenge

The arena's IT systems are unified in a single Hyper-V virtual platform that unifies management of multiple systems, spanning video surveillance management, recording and archival, voice, data, storage, industrial monitoring (SCADA systems), HVAC, building and power management, security systems, video intercoms, irrigation, billboards, lifts, and lighting control. A variety of third-party party vendor applications sit on the integrated platform including Johnson Control, Philips Dynalite, and Schindler.

Each system has stringent requirements for performance and availability. The CCTV management solution alone, include approx- imately 700 cameras provisioned with 1Pb of scalable tiered storage for analytics, facial recognition and database matching,

Stadium designers needed a powerful solution to protect the stadium BMS system from downtime and disaster without impeding application performance or overspending the budget.

They needed a system that could deliver varied levels of availability ranging from 99.999% to 99.9%. They also need to ensure that their HADR solution would enable them to perform routine server maintenance without downtime or data loss.

The Solution
SIOS DataKeeper with Microsoft Windows Server Failover Clustering delivers advanced HADR for the Stadium's BMS platform. This solution protects multiple integrations of devices and data securely, while also guaranteeing high availability protection. With it, the Stadium's BMS system runs on primary server nodes that clustered with secondary nodes. If the clustering software detects an issue, it moves operation to the secondary node(s). SIOS DataKeeper synchronizes local storage on all cluster nodes, eliminating the need for costly SAN storage and enabling efficient, zero-downtime maintenance.

Protecting BMS Systems in a Linux Environment

SIOS provides all the functionality needed to ensure the high availability of a Linux-based BMS solution.

- **SIOS LifeKeeper for Linux** provides automated failover clustering support to ensure that the primary cluster node supporting your BMS system will automatically fail over to a secondary cluster node if the software detects a failure condition. SIOS LifeKeeper also provides full-stack process and application monitoring features that will detect and proactively attempt to fix a wide variety of hardware and software faults that might contribute to infrastructure failure if left unaddressed. And unlike other failover cluster management solutions available in the Open Source world that can be complicated to set up and cumbersome to manage, SIOS LifeKeeper uses intelligent wizards to configure your system for HA. This helps you avoid set-up and management errors that otherwise may not be apparent until the moment a failover fails to occur in the manner you've anticipated.

- **SIOS DataKeeper** is responsible for replicating data stored on the active cluster node to storage attached to the secondary node (or nodes) in the failover cluster. SIOS DataKeeper uses synchronous, block-level replication services, so all the data stored on the primary node will be replicated to secondary storage at very high speeds. This ensures that the instance of the BMS on the secondary infrastructure always has the data it needs to start managing the building's systems if suddenly called into service.

- **Application Recovery Kits (ARKs)** augment the hardware, operating system, and network monitoring and management services present in SIOS LifeKeeper. They bring to your control center application-aware monitoring and management features that can detect and proactively respond to fault conditions in the BMS itself. ARKs also work closely with SIOS LifeKeeper in a failover situation, ensuring that the components of a complex BMS environment are restarted in an orderly manner as defined by established best practices. By monitoring and proactively managing a BMS environment in this way, the ARKs can increase application uptime and availability—while simultaneously optimizing the full failover response for those break-glass moment whose severity truly warrants that strong a response.

Together, SIOS LifeKeeper, SIOS DataKeeper, and the SIOS ARKs work to monitor your entire BMS infrastructure–network, applications, OS, and hardware. In the event of a service failure, SIOS LifeKeeper automatically tries to restart the service. If a restart does not restore operations, SIOS LifeKeeper automatically triggers a failover of application operations to a secondary server node, which can immediately take over and continue BMS operations. The applications also orchestrate the appropriate redirection of services operating across the network. Once the issue behind the failure of the primary node has been resolved, this HA solution can orchestrate fail back of operations to the primary infrastructure. The result? Critical BMS operations continue with no data loss and minimal interruption.

Protecting BMS Systems in a Windows Environment

SIOS also provides all the software you need to configure a BMS solution for HA in a Windows Server environment. Here, many BMS system administers opt to use the Windows Failover Clustering software that is built into Windows Server to create and manage a Windows-based failover cluster.

- To manage the real-time replication of data among server nodes, though, they rely on SIOS DataKeeper Cluster Edition, which integrates with Windows Failover Clustering. As in the Linux environment, SIOS DataKeeper provides synchronous block-level replication services to ensure that secondary storage in the failover cluster has an identical copy of the data in active use on the primary server node. In the event of a failover, SIOS DataKeeper interacts in concert with Windows Failover Clustering to bring the secondary BMS instance online and ensure that the BMS solution has immediate access to exactly the same data that had been active on the primary infrastructure.

- SIOS LifeKeeper for Windows is also available for customers who need to protect applications that are not Windows Failover Cluster aware, who do not use Windows Active Directory, or who have a mixed Windows and Linux environment and want a consistent HA solution across both environments. Like SIOS LifeKeeper for Linux, SIOS LifeKeeper for Windows provides complete HA clustering and failover manage- ment capabilities. It also includes comparable hardware, OS, and network monitoring and management features.

- Additionally, Application Recovery Kits (ARKs) for Windows-based applications are also available, and these operate in the same manner as the ARKs that operate in Linux world.

SANless Clusters

Unlike traditional clusters that rely on a shared storage area network (SAN), SIOS DataKeeper enables what is known as a SANless cluster. Each node in a failover cluster is configured with local storage, and SIOS DataKeeper synchronizes the storage among the nodes by replicating data written to the primary system to the secondary node. Both SIOS DataKeeper for Linux and SIOS DataKeeper Cluster Edition for Windows use synchronous, block-level replication services. The services are application agnostic, so all the data written to a specified storage system—and not just that associated with a specific application, such as SQL Server—is replicated to secondary storage at very high speeds.

With data from the BMS system replicated to one or more secondary storage systems, SIOS DataKeeper eliminates any single point of failure (which a SAN constitutes) and ensures that a complete instance of the BMS is ready to start working from the secondary infrastructure at any instant.

On-Premises or in the Cloud?

All major cloud providers operate multiple data centers (also known as "zones" or "availability zones"), making it easy to distribute your BMS infrastructure within a region for true HA—or to add multi-region support to enable disaster recovery (DR). The same SIOS solutions—on Linux or Windows—supports HA failover among availability zones within a region and DR failover among AZs across multiple regions.

Facilities management team interact with a cloud-based BMS solution in exactly the same way they would interact with an on-premises solution: through PCs in their offices that communicate with the BMS system in a data center. The infrastructure supporting the BMS won't be in your building or on your campus; but your BMS system will perform the same functions and behave in the same predictable way—potentially at significant savings.

By configuring your cloud infrastructure using SIOS HA software for Linux or SIOS HA software for Windows, your BMS solution will always be able to access current data. The SANless clustering approach ensures that storage on all the secondary cluster nodes contains the same data that had been in primary storage. In the event of a failover—even when moving to a separate cloud data center—SIOS HA software ensures that the secondary cluster nodes are always poised to pick up right where the primary node left off.

Cloud Provider High Availability SLAs

All cloud providers offer HA infrastructure solutions with service level agreements (SLAs) that guarantee 99.99% uptime. So why add HA software from SIOS? Cloud provider SLAs guarantee that at least one node in your cluster will be accessible 99.99% of the time, but they do not guarantee application accessibility.

Unless you configure your cloud-based BMS solution to replicate data synchronously from the primary cluster node to one or more secondary nodes, your application may not be accessible even if a secondary node in your cloud-based failover cluster is. SIOS HA solutions for Linux and Windows eliminate this vulnerability, ensuring that your BMS applications and data are as accessible as your HA cloud infrastructure.

SIOS High Availability Solutions for Building Management

By delivering the full range of key HA features—for BMS systems running on-premises or in the cloud—SIOS can help ensure that your critical BMS solution remains operational and accessible. And, SIOS HA solutions for Linux and Windows can ensure that you secure your availability goals in a manner that is far more cost-effective than would be possible using a FT approach.

About SIOS Technology

SIOS Technology Corp. high availability and disaster recovery solutions ensure availability and eliminate data loss for critical Windows and Linux applications operating across physical, virtual, cloud, and hybrid cloud environments. SIOS clustering software is essential for any IT infrastructure with applications requiring a high degree of resilience, ensuring uptime without sacrificing performance or data – protecting businesses from local failures and regional outages, planned and unplanned. Founded in 1999, SIOS Technology Corp. (https://us.sios.com) is headquartered in San Mateo, California, with offices worldwide.

SIOS Technology Corp.
155 Bovet Road, Suite 476
San Mateo, CA 94402
Tel: 650-645-7000

info@us.sios.com
https://us.sios.com