A White Paper from the Experts in Business-Critical Continuity

Managing Critical Systems for Higher Availability and Reliability

Liebert®

EMERSON™
Network Power

Summary

Critical power and cooling systems have a major impact on the performance and availability of IT systems. While the reliability of these systems is high, their value to the business is such that they require an adaptive approach to performance monitoring and management that enables both predictive maintenance and fast response to unexpected events.

It is possible to extend existing network or building management systems to include critical systems, but each of these approaches has limitations that reduce the flexibility and effectiveness of system management.

A more effective approach is Critical Systems Management (CSM). CSM involves establishing a management strategy and technology platform for critical support systems. This platform should encompass all critical support systems across the network, collect and manage trend data and alarm notifications, adapt to changes in equipment and information requirements and be capable of delivering data to any Web-enabled computer system.

In studies conducted by Emerson Network Power, this approach has been demonstrated to increase IT system availability and reduce equipment failures and maintenance costs.

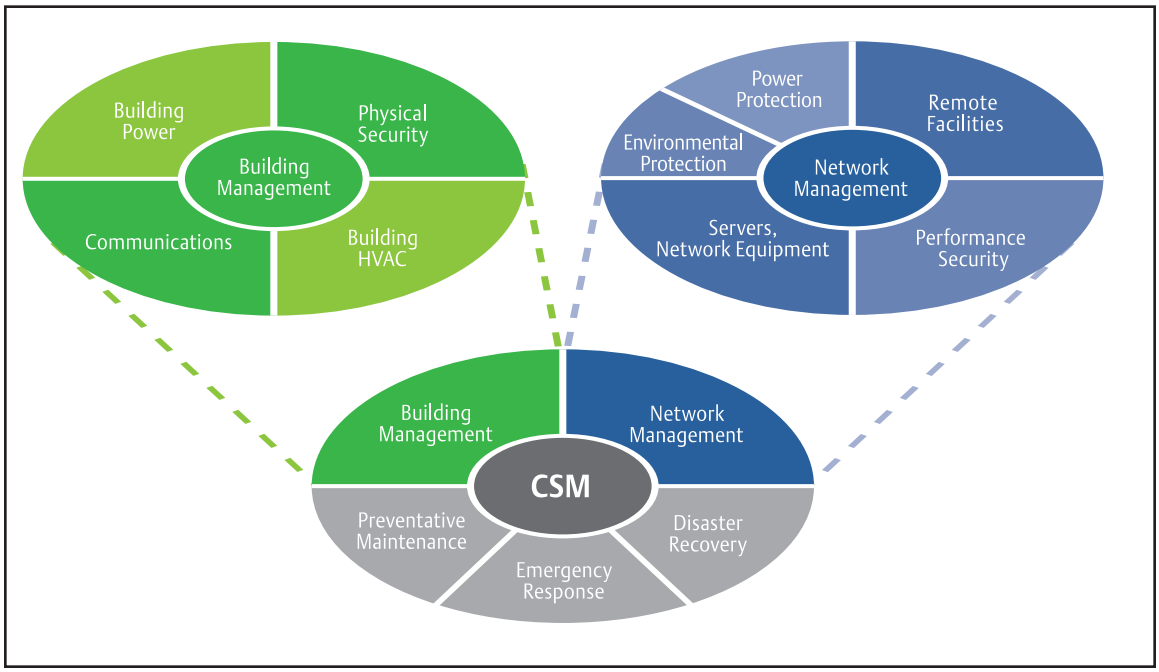

Figure 1. The Critical Systems Management approach supports Network and Building Management Systems but is tailored to the requirements of the power and cooling systems business-critical IT systems depend on.

Introduction

The concept of critical systems management dates to the 1960's when mainframes were changing how businesses processed and used information. Because these systems were critical to business operations, reliability was a major focus. It soon became clear that the reliability of these critical systems improved markedly when the temperature, humidity and voltage inputs were precisely controlled.

Today, critical systems have evolved to include everything from high-density blade server racks operating in a corporate data center to a critical fiber shelf in a broom closet. Yet the reliability of these systems is still dependent on factors such as return air temperature, humidity and power quality.

A number of mechanical and electrical systems are employed specifically to ensure reliable operation of information technology systems, including uninterruptible power supplies (UPS), power switching and distribution systems and specialized cooling systems. Together these systems comprise a critical system infrastructure that has a significant impact on the availability and reliability of IT systems.

This paper describes a dedicated approach to managing critical systems. Like Customer Relationship Management, which combines strategy and technology to improve the effectiveness and efficiency of customer interactions, Critical Systems Management (CSM) combines strategy and technology to improve the efficiency and effectiveness of Critical Systems Management.

Defining Critical Systems Management

Critical Systems Management is a dedicated, centralized approach to monitoring and managing critical infrastructure to improve IT system performance and reliability.

The environmental domain of Critical Systems Management includes any space that is providing an enhanced environment to critical business systems, including the corporate data center, server rooms, wiring closets and remote devices.

The range of power and distribution systems employed to ensure the availability of these systems also varies widely. On the small end, a closet-mounted 700VA UPS may be used to provide localized protection for a VoIP switch. On the other extreme, large data centers may require 1-2 MW of reliable, backed up power, delivered by large multi-module UPS systems supported by backup generators.

Finally, the critical system infrastructure, like the IT systems it supports, is not static. Changes to IT systems force change in the critical system infrastructure.

So a critical system is any system, regardless of its size or location, whose performance, if degraded or interrupted, adversely affects the instantaneous operation of the business. Critical Systems Management is concerned with continuously improving the total uptime and availability metrics for the power, power distribution, surge suppression and cooling systems supporting those systems on which the business depends.

Critical Systems Management must be both comprehensive and adaptive, providing visibility into critical systems across the enterprise and adapting to new systems and business requirements as they arise.

Critical Systems

The following should be considered as part of the critical system infrastructure:

- Engine-generator sets that provide a source of backup power in the event utility power is interrupted
- Automatic transfer switches that detect interruptions in utility power and transfer systems from the primary to the backup power source
- Facility-level surge suppression systems that trap equipment-damaging surges at the service entrance
- Mechanical pumping systems that support the precision air conditioners in server rooms and data centers
- Uninterruptible power supplies (UPS) and their battery systems
- Static transfer switches, control cabinets and load balancing systems that manage redundant UPS systems
- Power distribution units that distribute power within the data center
- Environmental control systems that provide temperature, humidity and air quality control within critical facilities
- Leak detection systems that deliver an early warning of water around critical systems
- Security systems that control physical access to business critical systems

To achieve this objective Critical Systems Management must be both comprehensive and adaptive, providing visibility into critical systems across the enterprise and adapting to new systems and business requirements as they arise.

The Need for Critical Systems Management

Incremental increases in component reliability, more robust designs and product improvements have continually increased the reliability of critical systems. Improvements in the power and distribution domain have been achieved through improved system designs that reduce the number of components and modules in redundant systems, and increased use of dual-bus architectures and dual-corded systems.

Cooling systems have also improved, offering greater reliability and scalability. The emergence of zone- and spot-based cooling has enabled a “right sized” approach to cooling, further contributing to overall availability.

But while system reliability was rising, so too was network criticality and availability requirements. The 24/7 demands of today’s business has eliminated scheduled maintenance downtime in many organizations, while new applications such as supply chain management and IP telephony increase the consequences of downtime for systems outside the data center.

Meeting these new levels of availability and criticality requires that critical systems be proactively managed with a single comprehensive monitor and control system. Gone are the days when a cooling system can operate independently of the power system or the UPS system operates independently from the generator and transfer switch. All of these critical systems interact and their performance can be affected by the performance of other systems.

For example, one common availability-affecting scenario is "power creep," or the steady, gradual addition of power-consuming devices until an internal design limit is exceeded. This can affect IT reliability in any of the following ways.

- If the overall facility power consumption (with startup currents) has exceeded the start capability of the generator system, the voltage will fall back when certain loads start and the generator will be unable to provide backup power when required. A power overload doesn't result in power degradation; it results in a total loss of power.
- If redundancy is achieved through the N + 1 approach (in which N is the specified capacity of the system and "+1" is the inclusion of one extra module to ensure the desired capacity can still be delivered if one module fails), power creep can effectively eliminate redundancy within the system. This reduces reliability since the failure on any module would then result in total power loss. In the case of a well designed 6-module system, reliability is reduced to about 20 percent of its single-module reliability when redundancy is eliminated.
- If an unmonitored branch power circuit is operating at 80 percent or more of full capacity, it is likely that the next load applied will cause the distribution breaker to trip, powering down that entire distribution leg.

Clearly active monitoring and control is required to reach the next level of availability.

Similarly, cooling systems today are subject to widespread "heat creep." Systems that are installed and operating perfectly with three installed blade servers may be impossible to cool adequately when additional servers are added to the rack. As the heat load and densities of critical systems continues to climb, and business demands require more rack space, cooling solutions external to the rack cabinets are required. Therefore accurately tracking consumed power and actual rack temperatures allows system operators to effectively prepare for spot and zone cooling.

The best way to monitor and manage these systems is through a stand-alone CSM system that measures, monitors and predicts these scenarios. With a CSM system tracking the growth in power at the rack point-of-consumption, data center or facility managers have the visibility into individual branch loads to prevent distribution overloads. Plus, the aggregation of branch power consumption measurements not only correlates to real generator and UPS requirements but allows for peak measurement and predictions based upon real, collected statistical data, allowing more accurate facility planning.

Gone are the days when a cooling system can operate independently of the power system or the UPS system operates independently from the generator and transfer switch.

The ability to collect and manage alarms and historical data is key to the success of a CSM strategy.

Requirements of CSM

Critical power and cooling systems represent a unique hybrid of facility and IT systems. Technologically, they are closely related to building power and cooling systems, but functionally they operate in, and support, the IT world. This has resulted in a desire to use existing Building Management or Network Management Systems to manage critical systems.

Unfortunately, each of these systems has serious limitations when it comes to critical systems.

Most Building Management Systems are poor alarm managers because failures in building systems do not represent emergency, immediate-response events. In addition, BMS does not support the long term retention of real-time data (within several seconds) which enables forensic analysis of critical faults. Building Management Systems typically only capture data within a time base of one to two minutes, which may not provide adequate correlation to a critical event.

SNMP-based Network Management Systems, like HP Openview or IBM's Tivoli, are well-suited to alarm management as that is their primary function. However, these systems do not collect real-time data, historic data and long-term telemetry, all of which play an important role in Critical Systems Management.

While many organizations will rightly desire user interface commonality and integration between CSM and Network and Building Management Systems, this can be easily achieved through a CSM system that uses standards-based interfaces. By separating the demands of the CSM from building and network management systems, the capabilities and functionality required are specifically turned for the tasks that are important to a comprehensive CSM strategy. Following are the basic requirements of a CSM system.

Data Collection and Management

The ability to collect and manage alarms and historical data is key to the success of a CSM strategy. CSM systems should have the following basic capabilities:

- Real-time monitoring locally or remotely
- Historical data collection and archiving, including performance tracking
- Alarm notifications
- Event escalation and tracking toward root cause

Performance tracking is a relatively new capability of CSM systems and can have significant benefits. By collecting both short- and long-term performance measurements, preventive measures can be taken before a unit actually fails. This is enabled by very accurate and complete internal monitoring systems now included on best-in-class power, distribution and cooling systems. Performance management has preempted the "break-fix" paradigm traditionally used to maintain critical systems.

It allows organizations to focus on taking actions that prevent failure, rather than responding to failures. Certainly unplanned

failures and damages can still occur in any system, but the ability to track and correlate degradation in performance may eliminate certain classes of failures.

Human Interface

In the case of human interfaces, the dedicated terminal session has all but disappeared. It has been replaced by standard, Web-based CSM portals that enable monitoring through any Web-based computer system. A CSM system should also include immediate alarm notification through phone or email. This allows the CSM system to adapt to the information requirements of a specific organization or business.

System Integration

For the machine-to-machine interface, a CSM system should provide an XML-based interface that allows real-time data, alarms and other information to be communicated to related systems — either NMS or BMS — as required.

Measuring the Impact of CSM

Emerson Network Power has conducted two analyses comparing the results of CSM strategy against that of a "break-fix" service strategy.

The first analysis focused on a large cellular carrier with 470 base stations and five master switch sites that transitioned from alarm only, break-fix monitoring to full telemetric monitoring over several years. The demands for availability, highly modular systems, battery backup and generator operation in the wireless industry are similar to the those of an enterprise IT network.

Table 1 details the results of this project after two years of operation. Notice that availability increased, service-arrive time decreased and overall costs decreased significantly.

The second analysis focused on the time, outages and availability achieved using

Performance management has pre-empted the "break-fix" paradigm traditionally used to maintain critical systems.

Area of CSM	Break-Fix Monitoring (Before)	Telemetry Monitoring (After)	Percent Improvement	Notes
Network Availability	99.44%	99.87%	.43%	Increase in Availability over over 2 years
Major Incident	2	0	100%	
Total Downtime (Hrs/Yr)	49.1	11.4	77%	Power Failures Detected Early
Preventative Maintenance Inspections	36 yr	12 yr	66%	
Service Arrive Time (hr)	2	.5	75%	
Service Engineers	10	5	50%	On Duty, 24 x7

Table 1. Implementing telemetry monitoring increased availability, and reduced service-related costs in this two-year study.

Time System Unavailable – Emergency Managed						
Events	143	144	152	167	184	790
Mean days	3.3	3.3	5	3.2	4.2	19
Mean hours	79.2	79.2	120	76.8	100.8	456
weight	0.18	0.18	0.19	0.21	0.23	
weighted hrs	14.34	14.44	23.09	16.23	23.48	91.57 hrs 3.82 days 8760 hrs/yr
US Utility		99.90%	8.76			0.99 ratio %
Hours Unavailable Prediction		98.95%	91.57			
Time System Unavailable – Emergency Unmanaged						
Events	84	96	103	106	108	497
Mean days	5.2	6.6	6.3	6.2	8.8	33.1
Mean hours	124.8	158.4	151.2	148.8	211.2	794.4
weight	0.11	0.12	0.13	0.13	0.14	
weighted hrs	13.27	19.25	19.71	19.97	28.87	101.07 hr 4.21 days 8760 hrs/yr
US Utility		99.90%	8.76			0.99% ratio
Hours Unavailable		98.85%	101.07	8.66 (Delta hrs)		
Improvement – Managed vs Unmanaged						
Monitoring Availability Gain			**0.11%**	**1.37 (compound hours)**		
Averted downtime $/min			**$41,206.50**			

Table 2. An availability gain of 8.66 hours was achieved in this study.

break-fix paradigm against a CSM strategy that included scheduled preventative maintenance and a spares program. As can be seen from Table 2, an availability gain of 8.66 hours was achieved.

Conclusions

IT system availability and performance can best be optimized through an independent CSM system that connects critical systems into a network and collects, consolidates, manages and archives both long-term historical data and transient alarm data.

An effective CSM system will employ a Web-based architecture to provide access to data from anywhere, can integrate with network or building management systems through XML, and can adapt to changes in the critical system infrastructure or business requirements as they arise.

Liebert Corporation
1050 Dearborn Drive
P.O. Box 29186
Columbus, Ohio 43229
800.877.9222 (U.S. & Canada Only)
614.888.0246 (Outside U.S.)
Fax: 614.841.6022

www.liebert.com

Printed in U.S.A. 0805 WP705