OpenData

CASE STUDY: AVAILABILITY IMPROVEMENTS USING GRANULAR MONITORING

Part of the Measurement Series™, by Modius

In this case study, Modius examines how its OpenData Data Center Infrastructure Management (DCIM) solution allowed its client, a leading technology company, to improve data center reliability by detecting and fixing facility problems before they could cause IT outages.

In three separate instances, the active monitoring provided by OpenData enabled the client to avoid potentially disastrous scenarios, including:

1: overheating in the battery room that would have caused Uninterruptible Power Supply (UPS) failure

2: detecting multiple Computer Room Air Conditioning (CRAC) unit failures and systemic loss in cooling pressure to the data center

3: monitoring the entire facility for problems during a Building Management System (BMS) failure

In each case, OpenData's ability to monitor across multiple sub-systems provided the company with unique visibility across the entirety of their data center site infrastructure. Without this cross-domain visibility, the personnel would not have been able to extract the data they needed to ensure the highest levels of availability in their mission-critical facility. These cases demonstrate the value of implementing N+1 monitoring redundancy across the data center.

TABLE OF CONTENTS

I. CASE INTRODUCTION

This case study consists of three separate sub-cases. Each sub-case lists one event in which the company was able to use Modius' OpenData system to detect and correct an acute problem in its data center before it became an actual outage or interruption in IT service.

RETURN ON INVESTMENT

The company invested in N+1 redundancy in its monitoring capabilities by implementing OpenData across its data center. The resulting return on investment in each of these sub-cases was the avoidance of catastrophic failure across the data center and the potential loss of IT services to the organization.

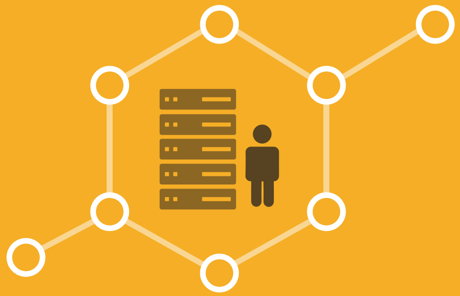
Other management tools that were in place were unable to catch the problems as they occurred. The loss of IT services would have caused a large financial cost to the company many times beyond the cost of deploying the OpenData system. By being alerted in real time to the core failures in the site infrastructure as they occurred, the company's data center personnel were given adequate time to respond to the root causes before the resulting problems became acute. If uncorrected, these failures would have led to a dramatic rise in operating temperature and the potential failure of IT devices.

II. AVAILABILITY SUB-CASE 1: Variable Frequency Drive Malfunction Disables Both Primary and Backup Chillers

CASE DESCRIPTION

A failure of the variable frequency drive (VFD) in the primary chiller at the company's data center resulted in a temporary cooling outage. Whereas the failure of the VFD was significant, the problem was compounded by the failure of the backup chiller to come online because of a quirk in the electrical wiring connections. This cooling outage nearly resulted in a catastrophic overheat condition in the data center battery room.

ABOUT THE MEASUREMENT SERIES



This case study is part of Modius' Measurement Series, which examines the benefits of data center systems that provide detailed monitoring and trending of performance information. This case study was produced with the generous cooperation of our client, whose experience using Modius' OpenData system in its data center has been very valuable. The information in the case study comes from interviews with their data center personnel, and data collected from the OpenData software.

The company's data center houses about 1,800 servers in 16,000 square feet of raised floor area. The data center runs continuously 24 hours a day, 7 days a week, 365 days a year. The data center is part of a much larger office building of approximately 220,000 square feet. The data center space is separately metered for electricity, and it has dedicated chillers serving only the data center and some negligible laboratory area.[1]

[1] Lab space can be very energy intensive, but the company's lab space requires only about 12 tons of cooling from the 240-ton chiller. Therefore, this case study ignores the lab's effect on data center cooling.

EVENT PROFILE	
PROBLEM	Failure of primary cooling and logic controller for backup cooling
THREAT TO DATA CENTER	Overheating in the battery room
MONITORING SOFTWARE DEPLOYED	OpenData, provided by Modius
RESOLUTION	Averted overheat and damage to battery equipment

Table 1. – Event profile for the VFD malfunction

SEQUENCE OF EVENTS

The following steps outline the sequence of events. A schematic is shown in Figure 1, showing steps 1-5.

1: The variable frequency drive on the main chiller (Chiller 2) dies, thereby taking the chiller out of operation (The breaker on the condenser fan had tripped.)

2: The failure causes a cascade, which trips a higher-level circuit breaker, cutting power to other devices, including the pump for the primary chiller.

3: Loss of power to the pump shouldn't matter (since the chiller is out of commission anyway) but the installing electrician had run a power feed from the pump to power the MP581 logic controller used by the data center's Building Management System to operate both the primary and backup chillers. Now this critical logic controller is without power. This electrical connection to the pump was a wiring fault by the electrician which had gone undetected. It was not as designed or as indicated by the building blue prints, and was actually against prevailing electrical codes.

4: The backup chiller (Chiller 1) is on a different and still-operational circuit, ready to start up and provide backup cooling. However, with the logic controller inoperative, the device cannot send a start-up command to the backup chiller.

5: Since Chillers 1 and 2 are not running, the data center's battery room lacks cooling and starts to overheat.

6: The Building Management System does not monitor the health of its devices, so it does not realize that the MP581 logic controller is down. The BMS has the ability to issue alarms and alert data center personnel, but it is unaware that a problem exists.

7: Thankfully, the data center has Modius' OpenData system installed, which is monitoring both the chillers and a temperature sensor in the battery room (as well as other locations throughout the data center).

8: As the battery room begins to overheat, OpenData issues warning messages and alarms to personnel off-site during after-hours. Personnel quickly recognize that both chillers are offline and they must come on-site to intervene.

9: Data center personnel rush to the scene (from off-site) to bring the cooling systems back online.

10: Personnel reset the tripped breakers. Both Chiller 1 and Chiller 2 start momentarily, but the original problem with the VFD causes the breaker to trip again. Both chillers again shut down. Even though Chiller 1 is on a separate circuit and can start successfully, neither chiller can operate without the continuous functioning of the logic controller. Without the controller continuously instructing it to continue running, Chiller 1 simply turns off.

11: Data center personnel restore power to only one side of the Chiller 2 pump, allowing the logic controller to receive power and allowing Chiller 1 to begin cooling the data center.

When data center personnel arrived, the battery room was at 101 °F, just at the "danger threshold" of what the Uninterruptible Power Supply (UPS) in the room could tolerate. According to the manufacturer, the UPS's logic control starts to fail at 100 °F, and the controller is all but guaranteed to fail at 105 °F. A few degrees warmer and the UPS would have become completely unpredictable, possibly blacking out the entire data center.

The company estimates that the total time from the initial failure of the VFD to the resumption of cooling by the backup chiller was about 38 minutes. Quick detection and response was essential.

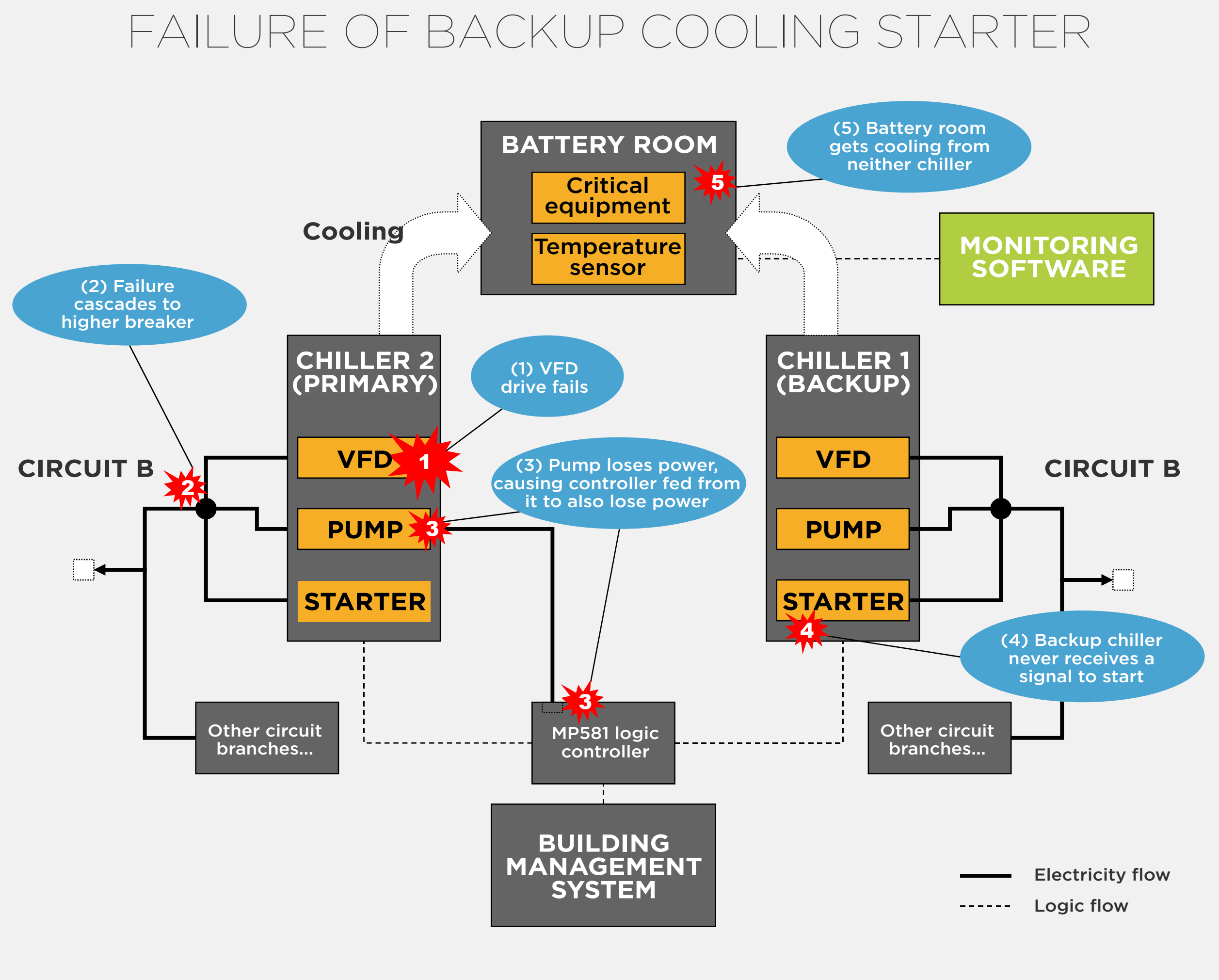

FAILURE OF BACKUP COOLING STARTER
BATTERY ROOM
Critical equipment
Temperature sensor
5
(5) Battery room gets cooling from neither chiller
Cooling
MONITORING SOFTWARE
(2) Failure cascades to higher breaker
CHILLER 2 (PRIMARY)
(1) VFD drive fails
CHILLER 1 (BACKUP)
CIRCUIT B
2
VFD
1
(3) Pump loses power, causing controller fed from it to also lose power
VFD
CIRCUIT B
PUMP
3
PUMP
STARTER
STARTER
4
(4) Backup chiller never receives a signal to start
3
Other circuit branches...
MP581 logic controller
Other circuit branches...
BUILDING MANAGEMENT SYSTEM
Electricity flow
Logic flow

Figure 1 – Schematic of the cooling failure in the data center

HOW DID THE MONITORING SOFTWARE CONTRIBUTE TO THIS "SAVE"?

What role did OpenData play in helping the company avoid a data center overheat? Foremost, it was OpenData, not the equipment itself, which was responsible for polling the temperature sensor in the battery room and issuing an alarm to data center personnel. Without this monitoring overlay, the problem would not have been detected in time.

In addition, this anecdote shows the importance of a system that actively polls the health of the field devices. As mentioned above, the data center's building management system didn't realize that one of its logic controllers was offline. The BMS simply recorded the last status update it received from the devices connected to it. Just before it failed, the logic controller would have reported a healthy operating state. Modius' OpenData system actively polls the health of all connected devices, and it can be set to issue alarms as soon as the connected device stops communicating.

Finally, this anecdote illustrates the importance of N+1 redundancy in monitoring site infrastructure equipment. The loss of the logic controller was a strategic failure of part of the overall Building Management System, which was the first monitoring layer responsible for tracking the health of the data center. Without OpenData as a second or redundant system, the failure would not have been prevented in time.

III. AVAILABILITY SUB-CASE 2: Breaker Trip Causes Power Loss to 7 CRAC Units in the Data Center

CASE DESCRIPTION

Over a year ago, a ground fault tripped a 250 amp breaker in the company's data center, cutting power to 7 of the 20 deployed CRAC units. The building management system failed to notice the problem, but the OpenData system issued an alarm when it detected that it had lost communication with the CRACs.

EVENT PROFILE	
PROBLEM	Breaker trip cuts power to 7 CRAC units
THREAT TO DATA CENTER	Overheating in data center
MONITORING SOFTWARE DEPLOYED	OpenData, provided by Modius
RESOLUTION	Averted overheating

Table 2. – Event profile for the breaker trip

SEQUENCE OF EVENTS

1: A ground fault trips a 250 amp breaker in the data center.

2: The breaker trip causes 7 of the 20 deployed CRAC units to lose power.

3: Under normal circumstances, the 13 remaining CRAC units should provide enough cooling capacity to ensure adequate operating temperature thresholds. However, all 20 of the CRACs are required to maintain enough air pressure to force cooling out of perforated tiles in the floor located near the IT equipment. Unfortunately, each of the 7 CRAC units that was down acted as an unwanted “hole” in the raised floor, through which pressurized cold air was able to escape. This caused a loss of pressure in the plenum, reducing the airflow to the IT equipment via the perforated floor tiles. As a result, cooling to the entire space was threatened, even though the remaining CRAC units could (in theory) handle the load.

4: The building management system is unaware of any problem, since it does not communicate with the CRAC units.

5: The OpenData system is actively polling all 20 CRAC units and stops receiving operational data from them. OpenData issues an alarm when it detects that it’s no longer receiving communication from 7 of the CRAC units.

6: At the same time, environmental sensors attached to OpenData begin reporting a rise in temperature across the data center. Personnel realize that pressurized air is escaping through the stalled CRACs.

7: Data center personnel check OpenData to identify which CRAC units are down. They realize that all 7 of the units share a common breaker, and thus are able to quickly pinpoint the problem.

8: Data center personnel locate and isolate the ground faulted equipment.

9: The tripped breaker is reset, and cooling is restored before the data center overheats.

HOW DID THE MONITORING SOFTWARE CONTRIBUTE TO THIS “SAVE”?

In this case, OpenData was useful because it was set to communicate with many more devices than a typical BMS monitors, including environmental sensors and the CRAC units in question. Also, OpenData reported exactly which CRAC units failed, rather than simply reporting a general cooling problem. This level of granular detail allowed data center personnel to think through common failure points on those CRACs and identify the central breaker.

This advantage of OpenData over a BMS in this case is the range of devices that OpenData actively polls. First, OpenData was collecting information from both the CRAC units and the environmental sensors. There would be many challenges in getting a conventional BMS to provide this level of granular monitoring. First, a BMS is simply not designed to flexibly accommodate real-time communication with many different types of devices. BMS systems typically do not actively poll devices, but instead only receive status updates sent out by the devices. So when a connected device fails and stops sending data, the BMS simply records the last successful update. As can be seen in this case, a system that only captures alerts does not provide adequate monitoring in instances of device failure.

Second, the design of most BMS systems allows very little traffic on the system’s communications loop. The communication loop is intended primarily to send control messages to the logic controllers and is limited in the data it can handle. Therefore, accommodating a large number of CRAC units and other devices is problematic since continuous polling of a broad number of devices can create too much communication traffic and data for the system to handle. Overall, a specially designed multi-device monitoring system such as OpenData clearly boasts an advantage over a typical BMS for measuring and monitoring operational performance data.

IV. AVAILABILITY SUB-CASE 3: Failure of the Building Management System (BMS)

CASE DESCRIPTION

More recently, the company experienced a temporary failure of its building management system during a routine upgrade. OpenData gave personnel another way to keep watch over data center health while the BMS was restored.

EVENT PROFILE	
PROBLEM	Building management system server locks up during routine upgrade
THREAT TO DATA CENTER	No immediate threat, but loss of control and visibility over data center operation
MONITORING SOFTWARE DEPLOYED	OpenData, provided by Modius
RESOLUTION	OpenData provides visibility while BMS server is restored

Table 3. – Event profile for BMS failure

SEQUENCE OF EVENTS

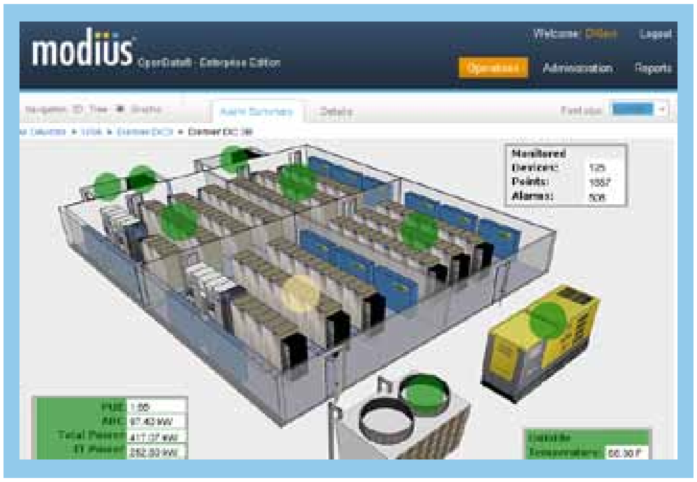
1: The building management system server locks up when the company's IT department attempts to install a routine upgrade patch. IT sent the patch remotely and were unaware that their action had locked up the BMS server.

2: The BMS system cannot be set to issue an alarm when its main server fails (such a setting would be useless anyway, because it is the responsibility of the main server to issue such alarms.)

3: By chance, data center personnel happen to look at the BMS console and notice that the server has failed.

4: The IT department is contacted and informed of the problem.

5: During this outage, data center personnel switch to using OpenData to monitor the health of the data center in real time. With the BMS down, company personnel know that they will need to handle critical data center functions manually. OpenData provides complete visibility into the facility, which allows personnel to make the right adjustments at the right time. For example, the BMS is responsible for telling the backup chiller to start if the primary chiller fails. In this scenario, OpenData would avoid disaster by alerting personnel to make this change manually.



Monitored
Devices: 125
Points: 1557
Alarms: 508

PUE 1.55
AHC 97.42 kW
Total Power 417.07 kW
IT Power 252.93 kW

Outside Temperature 66.30 F

6: After a short time, the BMS server is brought back online.

HOW DID THE MONITORING SOFTWARE CONTRIBUTE IN THIS CASE?

This anecdote again demonstrates the usefulness of N+1 redundancy in data center monitoring. While the BMS is down, data center personnel can still monitor data center health and implement manual control of devices while the automated controls are not functioning.

Is an N+1 system like OpenData really necessary, or could a data center rely on a BMS system with more robust failover capabilities, e.g. primary and failover control systems? In this case, the structural vulnerabilities of a BMS with a single communications loop with limited capacity for device communication traffic make this an unreliable solution. The preferred option is to implement a completely independent communication loop, such as provided by OpenData, which is separate from the logic controllers and thus more reliably ensures against systemic collapse of monitoring capabilities.

V. CONCLUSION

Using Modius' OpenData, the company was able to preserve the reliability of its data center and intercept problems before they became outages. These three cases show how OpenData helped the company avoid a potentially disastrous overheat, catch a CRAC unit failure, and monitor its data center facility for problems even when the building management system was down.

OpenData complements a typical building management system by providing functionality that a BMS does not naturally provide. One of the most important functions is OpenData’s ability to actively monitor the health of devices connected to it, because a broken device often does not report its failed condition to a controller. OpenData also communicates with a wide variety of devices such as CRAC units and critical temperature sensors, and it can support a large number of such connections. If configured correctly, OpenData can give data center operators details on exactly what failed, when, and where. Finally, OpenData allows data centers to extend the idea of N+1 redundancy to their facility monitoring, by providing a backup system if the BMS fails.

TECHNICAL SPECIFICATIONS

Modius OpenData is a software application that can be installed on-premise or hosted in the cloud. Some customers choose to run the application within VMWare ESX. Software platform requirements are as follows:

- **Windows Server -** 2008, 2008 R2, 2012
- **Database -** Express, Workgroup (Up to 2012) and MS SQL Server 2008 - 2016

CONTACT YOUR MODIUS REPRESENTATIVE FOR MORE INFORMATION ABOUT HOW OPENDATA CAN FREE UP TRAPPED CAPACITY IN YOUR DATA CENTER, SIGNIFICANTLY REDUCING OPERATING COSTS.

71 Stevenson Street, Suite 400, San Francisco, CA 94105 USA
sales@modius.com   www.modius.com   (888) 323-0066