Life Is On | Schneider Electric

Essential Guidance on DCIM for Edge Computing Infrastructure

White Paper 281

Revision 0

by Patrick Donovan

Executive summary

The lack of staff or “lights out” nature of many local IT and mobile edge computing (MEC) sites makes operations & maintenance a challenge. This struggle worsens as the number of sites increase. How do you maintain IT resiliency in a cost-effective way under these conditions? It is not practical to staff each location with trained personnel. The answer lies, in large part, on data center infrastructure management (DCIM) software. In this paper we describe essential DCIM functions for small, unmanned edge computing sites and attributes of next-generation DCIM solutions best optimized for that type of environment. We also provide practical advice on how to get started with DCIM to better ensure its value is realized.

RATE THIS PAPER ★★★★★

Introduction

Smaller, local edge computing sites - typically 1 to 4 IT racks in size - are often geographically dispersed, multiple in number, and lacking IT staff. This creates infrastructure management and maintenance challenges (**Figure 1**) that make it difficult to maintain availability of the IT in an efficient manner. Data center infrastructure management (DCIM) software tools are critical to addressing these challenges. Modern, next-generation DCIM apps simplify infrastructure management while improving resiliency. This paper describes:

- Essential DCIM functions for ensuring high resiliency at the edge
- Attributes of next-generation DCIM platforms optimized for use with multiple, highly distributed, and unmanned local edge computing sites
- Tips on how to get started with and use the tools

For a full, detailed explanation of what DCIM is and what all its functions are, see White Paper 104, *Classification of Data Center Infrastructure Management (DCIM) Tools*.

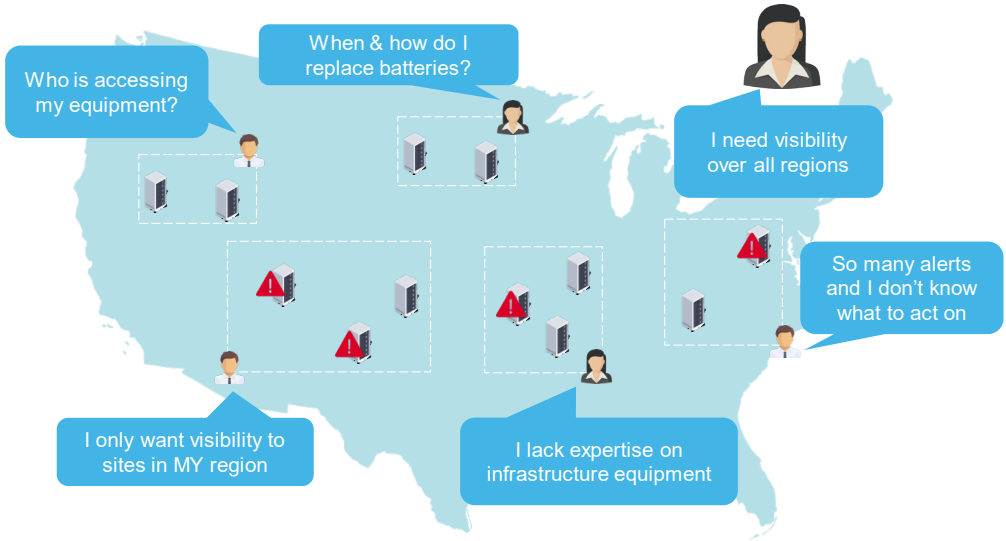

Figure 1
Example challenges that arise when managing infrastructure systems across multiple, geographically-dispersed, unmanned local edge computing sites

Essential DCIM functions for ensuring high resiliency at the edge

White Paper 277, *Solving Edge Computing Infrastructure Challenges*, makes the case for embracing a collaborative ecosystem of partners and vendors, along with adopting integrated micro data center solutions as the best approach for efficiently maintaining IT resiliency at the edge. A critical element of the micro data center solution is the next-generation DCIM system. These software apps remotely monitor and optimize power, cooling, and security infrastructure equipment. Fundamentally, these new cloud-based DCIM tools offer easier management from afar, big data analytics and artificial intelligence technologies, as well as a secure means for trusted partners and vendors to assist with operations and maintenance.

Operation of IT equipment depends on stable electrical power, sufficient ventilation (or active cooling), as well as a secure location that is safe from unauthorized access or exposure to other physical and environmental threats. These dependencies mean that a highly resilient edge IT installation requires remote monitoring of the infrastructure equipment with DCIM software tools. Afterall, you cannot effectively manage something that cannot be seen. **DCIM provides that remote visibility**.

White Paper 280, *Practical Guide to Ensuring Availability at Edge Computing Sites*, goes beyond the DCIM system and describes specific actions to take to improve reliability of the power and cooling systems that support the IT.

While traditional DCIM suites offer a wide variety of functions and capabilities, a smaller subset of core essential functions is needed for local edge environments. These are summarized in **Table 1** below. **When you are in the process of selecting a DCIM solution, focus on these functions and compare each vendor's approach and performance in delivering them.** Most, if not all, vendors will offer these functions in some form. But they will differ in terms of the platform architecture used to deliver the functions. As the next section will show, **the platform's architecture drives how effective the DCIM tools will be for local edge environments**.

Table 1
Essential DCIM functions for managing multiple, distributed local edge environments

Function	Description	Why important
Device & environmental monitoring	Provides a "read only" connection to all critical infrastructure devices (e.g. UPS, rack PDU, cooling, etc.) – regardless of vendor – to monitor status, access & alarms in real time.	Awareness of status changes, trends, and alarms, prevents issues from becoming critical incidents that could lead to IT service interruptions.
Device management	Provides a means by which infrastructure devices can be configured and their firmware updated.	Configuration & updates ensures equipment performs as expected and helps secure the overall system from cyber security threats.
Asset tracking	Provides a holistic view of all assets; their location, name, status, resource dependencies, etc.	IT resiliency requires having an asset inventory and knowing their dependencies.
Data analytics & visualization	Presents useful and actionable information on device status, alarms, and the health of the infrastructure systems and their environment.	Raw device data, frequent status change notifications, and "alarm storms" can overwhelm users; analytics and clear visualization of data makes DCIM use simpler and more effective.
3rd party platform integration	Allows DCIM data to be shared with a remote monitoring and management (RMM) tool or building management system (BMS) using application programming interfaces (APIs) or an SNMP management information base (MIB).	Managed service providers (MSPs) commonly manage edge computing IT and use their own management platforms; sharing DCIM data with these tools solves "lack of staff" challenge by enabling trusted partners to manage it for you.

We believe next-generation DCIM platforms are most capable of providing these functions for local edge applications.

Attributes of effective next-generation DCIM platforms

A next-generation DCIM platform is defined by 5 key attributes. These items are what differentiate these modern suites from traditional or legacy DCIM systems that were designed for large single-site data centers.

1. Relies on **cloud technologies** for ease of implementation, scalability, analytics, and maintenance
2. Connects to a **data lake** enabling insight and event prediction with **artificial intelligence (AI)**
3. Uses **mobile and web technologies** and integrates with 3rd party platforms
4. Prioritizes **simplicity** and **intuitive** user experiences in its design
5. Serves as a **compliance tool** to identify and eliminate potential cyber security risks

Relies on cloud technologies for ease of implementation, scalability, analytics, and maintenance

By hosting the DCIM server in the cloud, **deployment is simpler and faster** by eliminating the need to go through the procurement process for a new server for every site. Next-generation DCIM typically installs as a simple gateway app on an existing server (physical or virtual). This avoids the often-lengthy security and validation reviews that can take weeks or months. Since each site would require a DCIM server, this time savings can be significant when there are dozens or hundreds of small remote sites. This also makes the tool **highly scalable** in that it can handle an unlimited number of monitored devices across any number of sites. Cloud technologies also facilitates further value as described in the attributes below.

Connects to a data lake that enables insights and event prediction with AI

The cloud-based architecture of next-generation DCIM also provides the opportunity for vendors to offer a "data lake", a secure repository of massive amounts of anonymized device data. **"Big data" analytics and machine learning algorithms** can be developed and trained on this data to **yield insights and make predictions** that improve reliability, improve efficiency, and/or reduce operating expenses. Early examples of "big data" analytics and artificial intelligence applied to data center physical infrastructure include:

- Predicting when UPS batteries will fail – allows for early planning and budgeting for service replacements
- Real-time optimization of cooling system controls based on changing climate and load conditions – reduces operating expenses
- UPS health scorecard sorting the inventory of UPSs based on a determination of the device's age and health – simplifies management by first focusing user on what needs attention most

While this functionality is still in its infancy (at the time of this writing), edge computing **owners and operators considering DCIM solutions today can put themselves on the right future path by adopting a next-generation DCIM architecture that includes a data lake.**

Uses mobile and web technologies and integrates with 3rd party platforms

End users, trusted service partners, and vendors can **all access the same data at the same time from any browser** or mobile device. **Open APIs** enables DCIM data to be shared to MSP RMM tools for easier 3rd party management. Being browser based and encrypted, the need for VPN and unique login credentials for every single site is eliminated. This gives **real-time visibility to all assets and sites from one login**. These attributes serve to mitigate the challenge of having many, unmanned sites. For example, mobile access could help remote IT staff guide untrained, on-site personnel to troubleshoot and resolve issues without dispatching service. And integration into your **MSPs** RMM tool means that they **can now manage and service your physical infrastructure equipment for you**, just as they might be doing for your IT applications.

Prioritizes simplicity and intuitive user experiences in its design

Next-generation DCIM tools tend to perform better than legacy DCIM suites in terms of ease of installing, configuring, and using the software. Some of the common improvements include things like:

- Installations use easy-to-follow wizard-based routines
- Device alarm thresholds come with useful default settings
- Device health scorecards sort devices in need of attention or action first
- Performance benchmarking provides context on how you are performing relative to peers
- Alarms and status changes are grouped based on common causes to eliminate alarm "storms"
- Device setting and policy changes can be mass applied to many devices at once
- DCIM app gateway and device firmware can be set to auto-update to roll out bug fixes, feature enhancements, and security patches as soon as they are available; no longer a vendor-provided server that must be maintained by the end user

Serves as a compliance tool to identify and eliminate potential cyber security risks

Given that DCIM systems are made up of software apps, servers, gateways, and critical infrastructure devices, all inter-connected over mobile and IT networks, it is important to ensure cyber security best practices are continuously followed by both the vendor and end user. Next-generation DCIM should simplify this for the end user by **automating the detection and reporting of DCIM gateway and device vulnerabilities**. Some DCIM solutions do this using a threat assessment tool. Users are notified if device configurations (e.g., set to use SSH or Telnet) put the device at risk of attack. Devices with outdated firmware is also identified. This greatly simplifies management and automates a critical function of the DCIM system.

Tips & guidance for getting started with DCIM at the edge

Like any enterprise grade software suite, successful DCIM implementations require organizational buy-in and on-going cooperation and participation amongst key stakeholders. While DCIM ultimately aims to simplify and, to some degree, automate management of data center infrastructure, the users of the system must do their part to ensure the value of the software is realized. For example, the operations and maintenance (O&M) of the software system must be built in to the organization's O&M program. The facility O&M program's change management processes must be adapted to account for the DCIM system. This takes commitment and continuous effort by management and operations teams. If this is not done, the implementation and use of DCIM can fail. Note that next-generation DCIM O&M requirements are less burdensome than legacy DCIM. Some of the key DCIM-related processes that need to be accounted for in the existing IT or facility O&M program include:

- configuring device network settings for equipment that is added or replaced, and confirming that network communication is established
- reviewing status of device firmware periodically and updating when available
- ensuring device alarm thresholds and notification policies are set properly
- reviewing DCIM alarms and status changes regularly

- maintaining DCIM software, server and/or gateway with updates, bug fixes, and security patches (**NOTE:** most next-generation DCIM solutions can automate this process and there's no server to maintain)

White paper 196, *Essential Elements of Data Center Facility Operations*, describes the importance of change management process and DCIM in operating a data center efficiently and effectively. White paper 170, *Avoiding Common Pitfalls of Evaluating and Implementing DCIM Solutions*, goes into much more detail on the subject of integrating DCIM processes into your existing operations program.

Table 2 provides a summary list of tips to help make your deployment and operations of DCIM a success.

Table 2
Advice on how to better ensure the value of DCIM at edge compute sites is realized

Tips for ensuring DCIM success at the edge	Description
Obtain buy-in and commitment from key stakeholders before purchase and implementation	Without the full support of everyone involved, the system can fall out of use. Be sure to include the operations team and/or the MSP to assist in selecting and implementing the tools. (See next section for more information about role of MSP)
Select a next-generation solution	Cloud-based DCIM platforms are better architected for managing highly distributed, unmanned infrastructure, and puts you on the right path to more predictive, automated management.
Focus on monitoring first	The most critical function is being aware of alarms and status changes with the physical infrastructure. Once this is in place and the processes to use and maintain it are mature, then other functions and features of DCIM can be considered. (See next sub-section below)
Integrate processes to operate and maintain DCIM with your existing O&M program(s)	Operating and maintaining a DCIM solution takes effort and discipline. It must be an official, documented part of the existing O&M program to minimize the risk that the tools fall out of use.

Avoid the "information problem" by using next-generation DCIM

Regardless of who is doing the day to day management, it is important to choose software management tools that clarify and prioritize status notifications and alarms. Traditional tools might leave operators spending a lot of time trying to evaluate each one. What does it mean? Do I need to do something? Instead of providing raw data about the IT environment and supporting infrastructure, modern tools draw conclusions to either provide a root cause for the problem or to make clear which alarms or devices are most critical and require attention. For example, a retail store chain may have thousands of UPS units deployed across the country. The manager could see hundreds of thousands of data points and status change notices from that population. It would be easy for critical alarms to go unnoticed or for a storm of alarms to occur with no understanding of what is driving them. Effective software tools focus the operations manager on only the UPS units that need attention first or on the one alarm that started a cascade of further alarms. One way to do this is through a device health score card system that ranks devices based on their health. For a UPS, the health would be determined by the age of the unit, battery charge capacity, temperature, and so on. **Figure 2** shows an example "health" score card for a fleet of UPSs.

This capability saves time and reduces trial and error efforts to understand what is happening with the equipment. It reduces the need to send out service personnel to investigate problems. It reduces cases where equipment thought to be faulty is prematurely replaced with new. We often hear of cases where service people are dispatched to replace a "bad" UPS only to find it was being overloaded by store employees who found the unused outlets useful for powering space heaters, vacuums, or coffee makers. Effective software tools would've clearly alerted management that the UPS had shut down because they had been overloaded, not because they had failed.

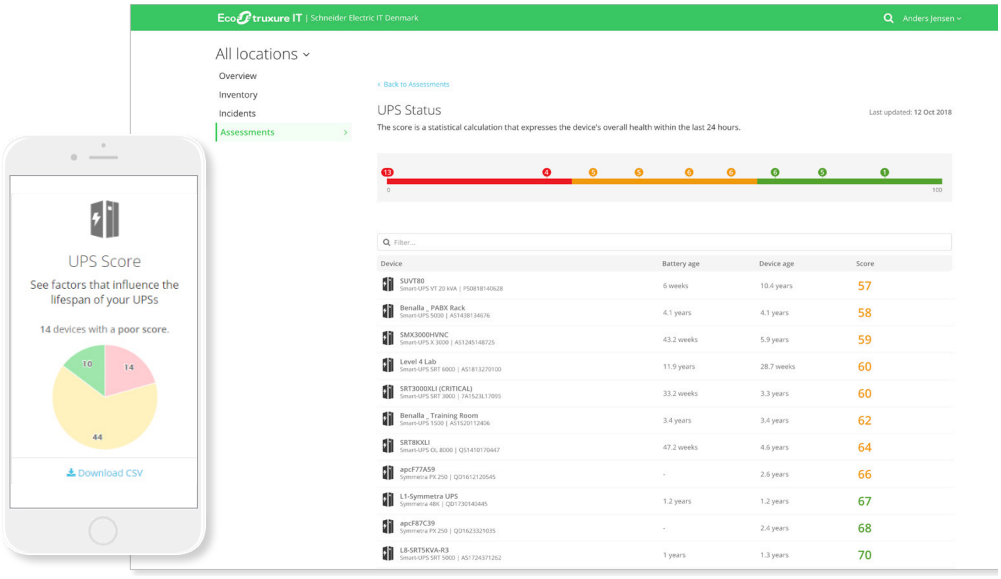

Figure 2
An example screenshot showing a health scorecard for a fleet of managed UPSs; units needing the most attention are sorted to the top of the list.

To monitor yourself or rely on partners and/or vendors

DCIM was originally designed to be self-managed and monitored by the owner of the tools. You buy a lifetime license and operate and maintain the system yourself. Vendors typically offered implementation and startup services as well as training programs to ensure your operations team could handle it for the long term. Remote monitoring services by the DCIM vendor or other 3rd party service providers have existed, but they tend to be very basic and reactive in nature. Essentially the infrastructure devices are configured to send alarms to the vendor who react if something goes wrong.

Next-generation DCIM provides a platform that makes it easier for 3rd parties to manage and monitor for you or together with you. The end user, the MSP, and the DCIM vendor can all have access to the same data at the same time. Under this new digital services model, servicing and replacing components could be carried out even before the local site knows there's an issue. Enabling full use of the DCIM system by 3rd parties mitigates the key edge computing challenge of having unmanned sites. Your service providers and DCIM vendor can, in effect, become your virtual staff. Connecting your MSP to the system can happen either by giving them access to the DCIM software itself or by using application programming interfaces (APIs) so that MSPs can bring DCIM information in to their RMM software tools.

However, as explained in previous sections, Modern DCIM tools are making it easier to use the software yourself if that is the preferred operating model. Using a simple gateway app instead of having to source and implement a 3rd party server simplifies getting started. Simple wizard-based setup and configuration tools with suggested default settings makes implementation easier. And a move towards providing more

intuitive, insightful analytics vs. raw data also contributes to making next-generation DCIM tools simpler to do yourself. Mobile apps also help simplify management by giving managers and operators visibility from anywhere, at any time.

Ultimately, you have 3 basic choices in terms of who manages the DCIM system:

- Do it all yourself
- Let the DCIM vendor remotely monitor in collaboration with you
- Leverage an MSP who is managing the IT (Note, the MSP might also benefit from having the DCIM vendor remotely monitor as well in this case.)

The service of having the DCIM vendor remotely monitor the infrastructure devices is commonly called digital remote monitoring. The benefit of using this type of service is two-fold:

- **Expertise** –The vendor's operators are experts on the equipment being monitored
- **Time** – Time to detect and troubleshoot problems is significantly reduced, and the need for the end user to have to call vendor's tech support and navigate to the right person is eliminated; Time to recover is faster in that the vendor can immediately dispatch field service

To determine the right choice, you should ask yourself the following questions:

- How critical is the IT infrastructure?
- Do you already have or plan to use an MSP to manage the IT?
- Does your operations team have the expertise and bandwidth to monitor and manage the physical infrastructure?
- Do you require less than 24hr resolution of problems and replacement of failed devices?
- What service contracts exist for the infrastructure hardware already?

Conclusion

Power, cooling, and environmental/security monitoring equipment is critical to the continued operation of the IT at edge computing sites. Particularly since these are often geographically dispersed and unmanned, next-generation DCIM software that relies on cloud, mobile, and AI technologies should be used to effectively monitor this infrastructure from afar. Compared to legacy DCIM solutions, modern DCIM tools are easier to scale, use, maintain, and provide a way for MSPs to remotely manage for you. Newer DCIM platforms are also beginning to take advantage of AI technologies that will make management more predictive and automated.

We believe well-maintained and operated DCIM systems make data centers more reliable and efficient. This means having buy-in from all stakeholders, integrating DCIM processes with the existing O&M program, and either having the discipline to regularly monitor the system yourself or choosing to have your trusted partner or vendor manage it all for you.

About the author

Patrick Donovan is a Senior Research Analyst for the Data Center Science Center at Schneider Electric. He has over 25 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 physical infrastructure technologies and markets offers guidance and advice on best practices for planning, designing, and operation of data center facilities.

RATE THIS PAPER

Resources

Classification of Data Center Infrastructure Management (DCIM) Tools
White Paper 104

Solving Edge Computing Infrastructure Challenges
White Paper 277

Practical Guide to Ensuring Availability at Edge Computing Sites
White Paper 280

Essential Elements of Data Center Facility Operations
White Paper 196

Avoiding Common Pitfalls of Evaluating and Implementing DCIM Solutions
White Paper 170

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