Life Is On Schneider Electric

How Modern DCIM Helps Multi-Tenant Colocation Data Centers Be More Competitive

White Paper 290

Version 1

Energy Management Research Center

by Patrick Donovan

Executive summary

The data center retail colocation market is highly competitive and growing. Providers are under continuous pressure to be resource efficient while being ready to scale and meet tenants' evolving demands. In addition to this increasingly complex and challenging environment, tenants are demanding transparency on billing, SLA performance, and environmental sustainability metrics. Modern data center infrastructure management (DCIM) software can be an effective tool to help address these needs. This paper will show with practical examples how modern commercial DCIM software makes colocation data center operations more competitive by improving resiliency, security, environmental sustainability, transparency, and operational efficiency.

RATE THIS PAPER ★★★★★

Introduction

Multi-tenant data center (MTDC) colocation providers are always under pressure to remain competitive. Although demand for their services continues to grow, their tenants have ample choices of where to source their IT services: on premise, public cloud, and other data center colocation providers. Armed with other places to turn, increasingly discerning tenants expect providers to be more transparent in terms of SLA performance, billing, and environmental sustainability metrics.

Within the domain of data center operations, being competitive in the past had largely just meant maintaining availability and being resource efficient through effective capacity management. To those ends, Data Center Infrastructure Management (DCIM) software is widely used today as a critical operations tool for maintaining resiliency and managing IT space, power, and cooling resources more efficiently. And while these fundamental DCIM functions are still very much relevant, tenants today are also focused on security, sustainability, and transparency. While traditional DCIM tools have lacked the capabilities to address all these needs, improved, modern DCIM ("DCIM 3.0") solutions do include these capabilities. Figure 1 shows how DCIM has evolved, adding capabilities over time as supporting technologies have improved and tenant needs have grown.

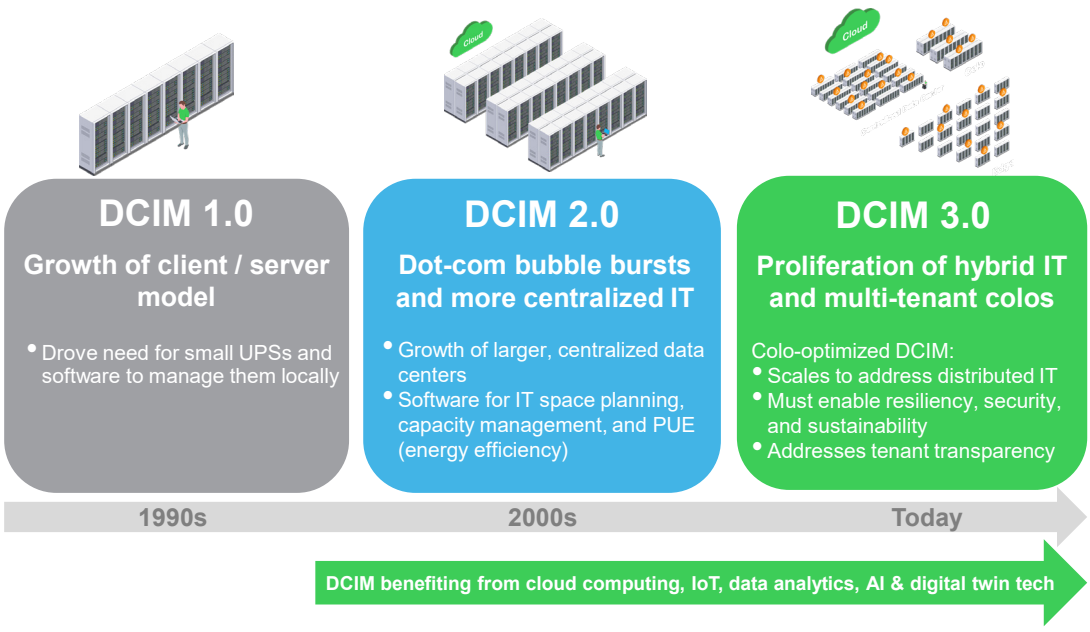

Figure 1

Evolution of DCIM as the data center market has evolved over time. DCIM 3.0 is the trend representing the need for a modernized DCIM to overcome the new infrastructure challenge of managing across a highly distributed environment with the continuous pressure of being efficient and sustainable while maintaining resiliency, security, and being transparent to tenants.

Multi-tenant colocation providers who can meet or exceed tenant requirements and expectations at a lower cost will be best positioned to win in the market. This paper shows, with practical examples, how DCIM can make your data center more resilient, secure, sustainable, transparent, and operationally efficient. Attributes of more effective DCIM solutions and how to avoid common pitfalls are also shared. We show that modern "DCIM 3.0" solutions, when well implemented and maintained, help make colocation providers more competitive and responsive to the needs of their customers.

Improving resiliency

Although customer availability requirements may vary by tenant, workload, or application, providing a high level of availability is largely considered "table stakes" for colocation vendors and is typically a defined metric in the SLA. A power or sustained cooling outage can wreck a provider's reputation and business. Therefore, it

is imperative for providers to continuously monitor their infrastructure and work to reduce the risk of human error that might lead to a system outage.

Data Center Infrastructure Management (DCIM) software monitors and collects real-time data from power, cooling, environmental monitoring devices, as well as with other facility and IT management software. Well-implemented, DCIM improves the availability and resiliency of physical infrastructure systems and the IT workloads they support. Most DCIM software suites offer 2 core functions:

- Monitoring & device management – awareness of device/environmental health and security status changes, trends, and alarms
- Planning & modeling – simulating adds, moves, and changes; performing risk analysis, and optimizing capacity

Both functions work to improve and sustain resiliency of the provider's power and cooling infrastructure, and thereby, the tenants' IT. Monitoring & device management functions do it primarily by making sure you're aware of conditions that, if left alone long enough, will lead to system downtime. And planning & modeling functions do it by reducing the risk of human error occurring during adds, moves, and changes. The next two subsections explain this in more detail.

How monitoring & device management improves resiliency

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 IT installation requires monitoring and management of the infrastructure equipment with DCIM software tools. This is particularly so in the case when managing a portfolio of geographically dispersed sites and/or when IT operations staffing is constrained. You cannot effectively manage something that cannot be seen, after all. Waiting too long to discover there's a problem with the supporting power and cooling infrastructure will lead to business interruption. DCIM software provides that remote visibility and early warning in conjunction with device and environmental sensors and cameras. These are summarized in Table 1.

Table 1

Resiliency benefits of DCIM monitoring and device management functions

Function	Description	Resiliency impact
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. Monitoring for unauthorized access to equipment reduces physical security risks.
Device management	Provides a means by which infrastructure devices can be configured (e.g., alarm thresholds, communication settings) 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, including their location, name, status, etc.	IT resiliency requires having an asset inventory and understanding their attributes and resource dependencies, particularly when conducting maintenance activities.
Data analytics & visualization	Presents useful and actionable information on device status, alarms, and the health of the infrastructure systems and their environment through dashboards and reports.	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 to ensure critical alerts do not go unnoticed. Predict battery failures ahead of time to avoid unplanned outages.

Function	Description	Resiliency impact
3rd party ticketing system integration	Allows device alarm data to be shared with ticketing system in use by provider, using application programming interfaces (APIs) or an SNMP management information base (MIB).	By working with established workflows, this better ensures power, cooling, and environmental monitoring unit status changes and alarms are detected and responded to more quickly, thereby, preventing an outage and/or reducing mean time to repair (MTR).

Particularly with highly distributed IT portfolios, resiliency depends first on using DCIM to monitor critical power and cooling systems and the environmental monitoring sensors that support the IT. Next, we show how DCIM planning and modeling functions improve resiliency to sustain business operations.

How planning & modeling improves resiliency

Multi-tenant colocation data centers make for a challenging operations environment given their criticality to their customers' business operations. Careful coordination and planning are required between facilities and IT when it comes to power and cooling system maintenance or IT adds, moves, and changes. The potential impact on system availability can be so severe that each operational task must be carefully evaluated in terms of its net effect on availability. DCIM planning and modeling modules provide the means to do this careful evaluation.

This function begins with creating and maintaining an accurate map of all infrastructure assets and IT equipment along with their interdependencies with each other. Once set up, the software will map a given virtual machine (VM) to a specific:

- Physical host server and network port
- U space
- IT rack
- Power path(s) (i.e., path A and/or B showing Rack PDU, UPS, PDU, switchgear)
- Cooling units

In 2D and 3D views, DCIM planning & modeling modules show real-time capacities of all resources (e.g., power, cooling, rack space, network switches, and cabling). Policies can be set down to the workload level by tenants to ensure workloads receive the required level of criticality (e.g., the VM can only reside on a host with 2N power redundancy or a UPS with xx minutes of runtime).

By creating, in effect, a "digital twin" (in both 2D and 3D, typically) of your portfolio of data centers, this DCIM function simulates adds, moves, and changes so that operators understand the potential impacts *before* real action is taken. By first performing actions virtually, the risk of an unplanned interruption in IT service, as maintenance is conducted, is minimized. Particularly if onsite IT staff availability is limited, having this digital visualization of all assets and their interdependencies is important. Note, with all assets fully documented (type, serial number, rack location, network port, power path, etc.) and mapped to each other, this information could also serve as a basis for a disaster recovery (DR) plan.

Imagine needing to "swap and replace" all your UPSs. With DCIM planning and modeling functionality, you would understand – without being on site - which tenant racks were dependent on each of the UPSs. Turning the UPS off and switching to a redundant power path could be simulated to understand what the impact would be on connected workloads and applications. This information and the ability to run

simulations makes it easier to plan and execute the actual transition while reducing the chances of an unexpected outage caused by human error.

The following bullets summarize some example ways that DCIM planning and modeling functions can improve resiliency of the IT:

- Prevent VMs or physical servers from being moved or added to locations with insufficient power and cooling capacities that could otherwise result in system downtime.
- Be alerted to an unexpected change in power capacity to avoid a sudden outage when the circuit becomes overloaded and trips a breaker.
- Reduce risk of human error during maintenance activities through fault simulations.
- Integrate with virtual machine management software to initiate VM migration once the UPS reaches a low battery state or fault condition to avoid an unintended loss of service.
- Use work order management/ticketing system tools to better ensure critical maintenance is properly scheduled, assigned, defined, and carried through before a failure occurs.
- Simulate a replacement of a UPS to understand potential impacts before physically making the replacement.

Improving security

Security and compliance are frequently described as a top concern for MTDC providers[1] and as a top consideration for tenants when selecting a provider[2]. And the reason is, perhaps, obvious given the potential high costs[3,4] associated with a security breach, be it physical or cyber oriented. Heightened concern over security is also unsurprising since colocation, by definition, means space shared with the information from other firms, and IT assets being outside the enterprise's direct control. Like resiliency, implementing and maintaining an effective multi-layered security strategy is "table stakes" for any provider trying to remain competitive in their market. Modern DCIM can be used to reduce both physical and cyber security risks.

Cyber security

Devices monitored by DCIM – i.e., Rack PDUs, UPSs, cooling units, and environmental monitoring appliances, etc. – all have built-in network management cards that enable the device to communicate on the network. All these devices, as well as DCIM servers and gateways must always be kept up to date with the latest firmware or software patches. Note that a network-connected infrastructure device contains both device firmware and network management card firmware and/or software. It is important that both are kept up to date. Cyber criminals are constantly working to find vulnerabilities in existing code to hijack devices and steal data, control devices, cause outages, etc. New firmware and software patches not only fix bugs and provide additional performance enhancements, but they often address known security vulnerabilities. These code updates should be installed or applied as soon

[1] https://www.sphomerun.com/data-center-sales-and-marketing-blog/top-10-data-center-colocation-challenges-faced-by-ceos

[2] https://community.fs.com/blog/seven-essential-factors-to-consider-while-choosing-your-colocation-provider.html

[3] https://www.statista.com/statistics/273575/us-average-cost-incurred-by-a-data-breach/

[4] https://www.ibm.com/reports/data-breach?utm_content=SRCWW&p1=Search&p4=43700072379268784&p5=e&gclid=Cj0KCQjwyLGjBhDKARIsAFRNgWm6Lnn-kiy2F0CHf_rChxvhIDJZDEbGmODBnPFKyfNaW8RIabefUsaAo2REALw_wcB&gclsrc=aw.ds

as they become available from the vendor. This requires on-going discipline from the operations team.

The security features and settings that were enabled and configured during the initial setup and installation, also need to be maintained throughout the life of the infrastructure device, network appliance, or management server/gateway. By minimizing the number of users with the ability to change these settings, you reduce the chances of unintended or non-permitted changes being made. Beyond that, these settings should be checked regularly to ensure they remain set properly over time.

Some modern DCIM software offer a **security assessment feature**, as shown in **Figure 2**, that can simplify the work described above, at least, for power and cooling infrastructure devices. These assessments will scan all connected devices across the entire IT portfolio to provide a report highlighting out of date firmware and compromised security settings.

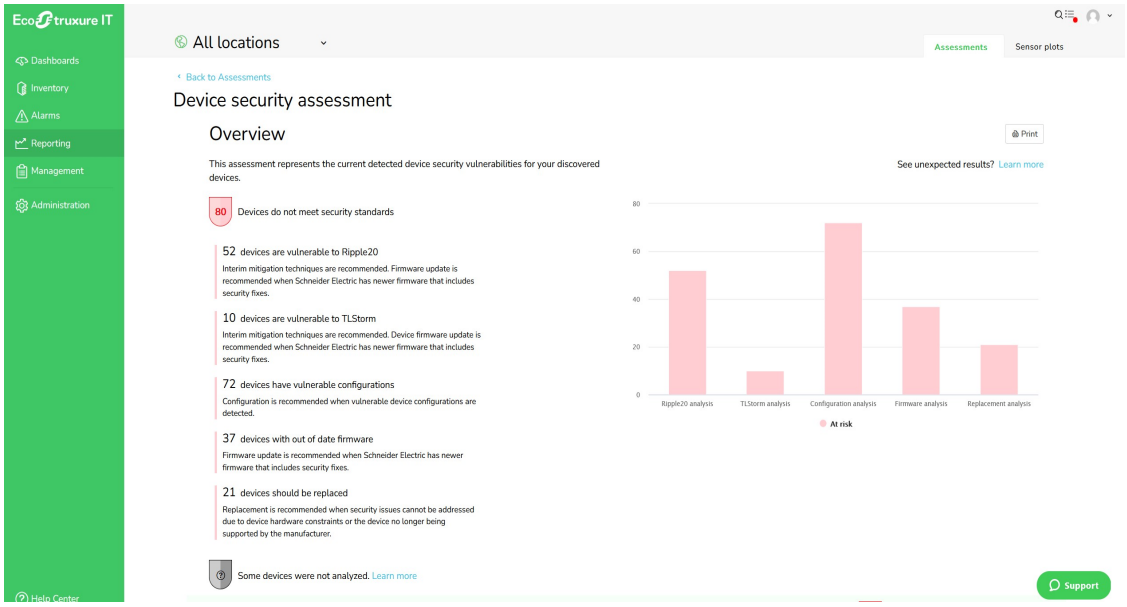

Figure 2

Example of a DCIM security assessment function from Schneider Electric's EcoStruxure Data Center IT Expert software tool. It assesses which devices are not meeting security standards in terms of firmware being up to date and whether there any vulnerable configurations.

Some DCIM tools will also automate the updating of firmware and provide a means to perform mass configurations of security settings across multiple devices at once to greatly simplify the process. The more DCIM can simplify and automate these security processes, the more secure the physical infrastructure systems will be as it reduces the opportunity for human error.

Physical security

Modern DCIM software not only communicates with power and cooling devices, but they also will communicate with environmental monitoring appliances. These can be used to not just detect/track temperature, humidity, fluid leaks, smoke, and vibration, but they also typically integrate with security cameras, door sensors, and access cards. Monitored and controlled through DCIM software, these appliances help operations teams monitor and track human activity around critical IT as well as environmental conditions that could equally threaten the resiliency of business operations. **Figure 3** shows an example environmental monitoring appliance and camera system interface as part of an overall DCIM implementation.

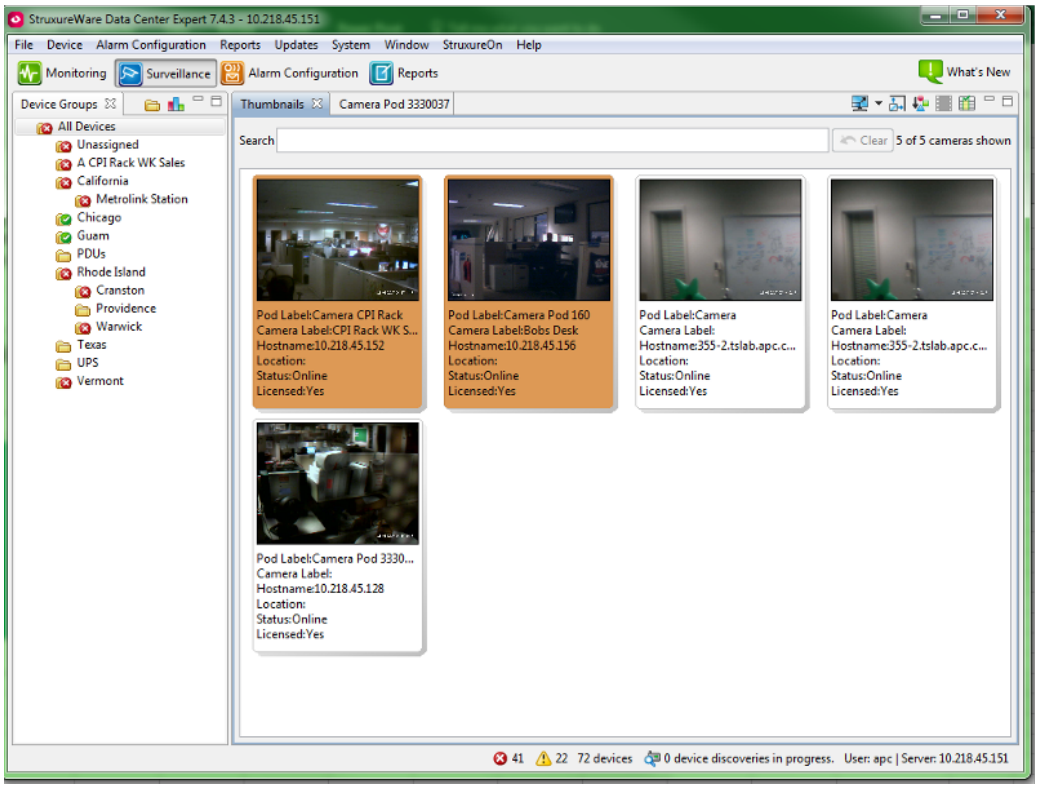

Figure 3

Example of Netbotz camera systems appearing within Schneider Electric's on premise DCIM monitoring software.

Improving environmental sustainability

As MTDC owners work to maintain resiliency, security, and other performance metrics of their SLAs, there is growing pressure to track, measure, report, and ultimately decarbonize their IT operations. This pressure is coming from tenants, governments, investors, and internally, perhaps, out of a sense of having a shared responsibility to address climate change. Consistently showing up in RFPs now[5], tenants expect their providers to address the environmental impact of their operations and to be transparent about it. Schneider Electric White Paper 64, *Why Data Centers Must Prioritize Environmental Sustainability: Four Key Drivers*, explains in detail why data center owners will have to focus much more on this in the future.

Modern DCIM software offers are beginning to address this need. They help achieve environmental sustainability goals in two fundamental ways: metrics & reporting, and by reducing Scope 2 carbon emissions.

Metrics & reporting

Once sustainability goals and objectives have been set, reducing the MTDC provider's own environmental impact and addressing the sustainability needs of their tenants begins with collecting data for metrics and tracking progress on them through regular reporting. While at the time of this writing, DCIM is in the early phase of its evolution towards becoming an environmental sustainability reporting management tool for colocation data centers, some modern DCIM offers available today will "out of the box" collect data and report fundamental sustainability metrics for individual tenants, single data center sites, and in aggregate across the entire portfolio of sites owned by the provider. Reported metrics may include:

- Power usage effectiveness (PUE): current and historical

[5] https://datacenterfrontier.com/the-state-of-the-colocation-data-center-industry/

- Energy consumption: usage at sub-system level to show in both real-time and historical trends of total consumption, IT consumption, and power losses
- Carbon footprint (scope 2 emissions) based on local carbon emissions factors in total and by subsystem including IT, power, and cooling.
- Carbon and water usage effectiveness (i.e., CUE and WUE)
- Waste

In the case of Schneider Electric's EcoStruxure™ IT DCIM offer, our approach has been to give users the ability to set goals for each metric, select metrics to view, design/choose a report template, and then publish that report on a defined schedule for selected stakeholders. Figure's 4 and 5 show example screenshots of this approach.

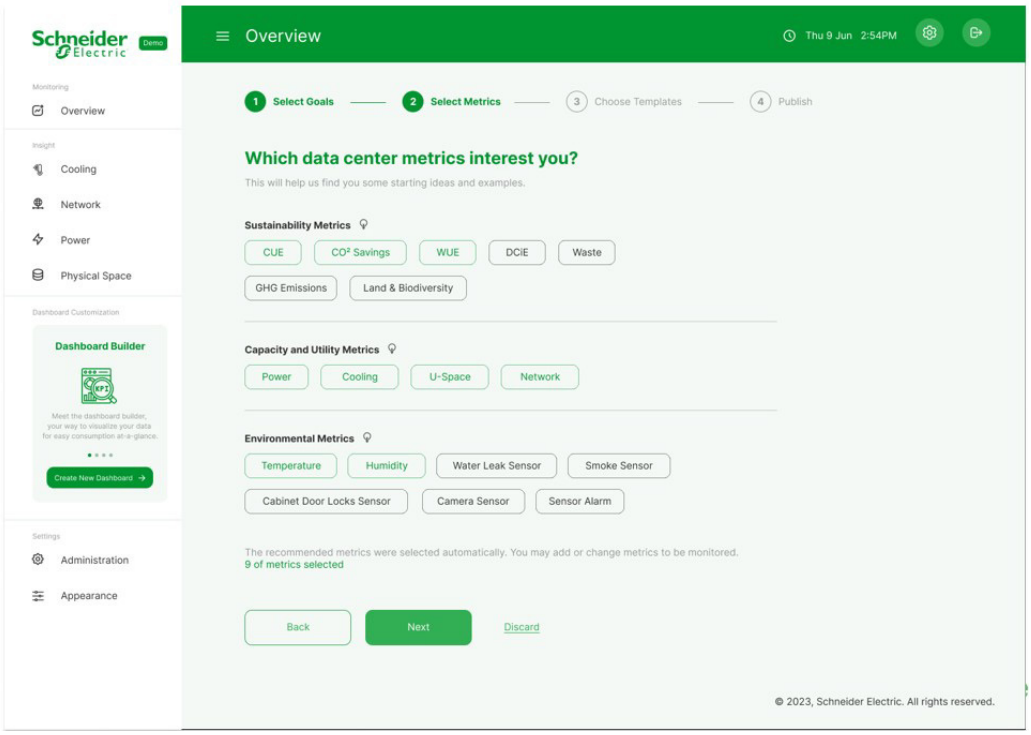

Figure 4

This screenshot shows how Schneider Electric's EcoStruxure IT Advisor DCIM software provides users with the ability to setup and publish environmental sustainability metric tracking reports

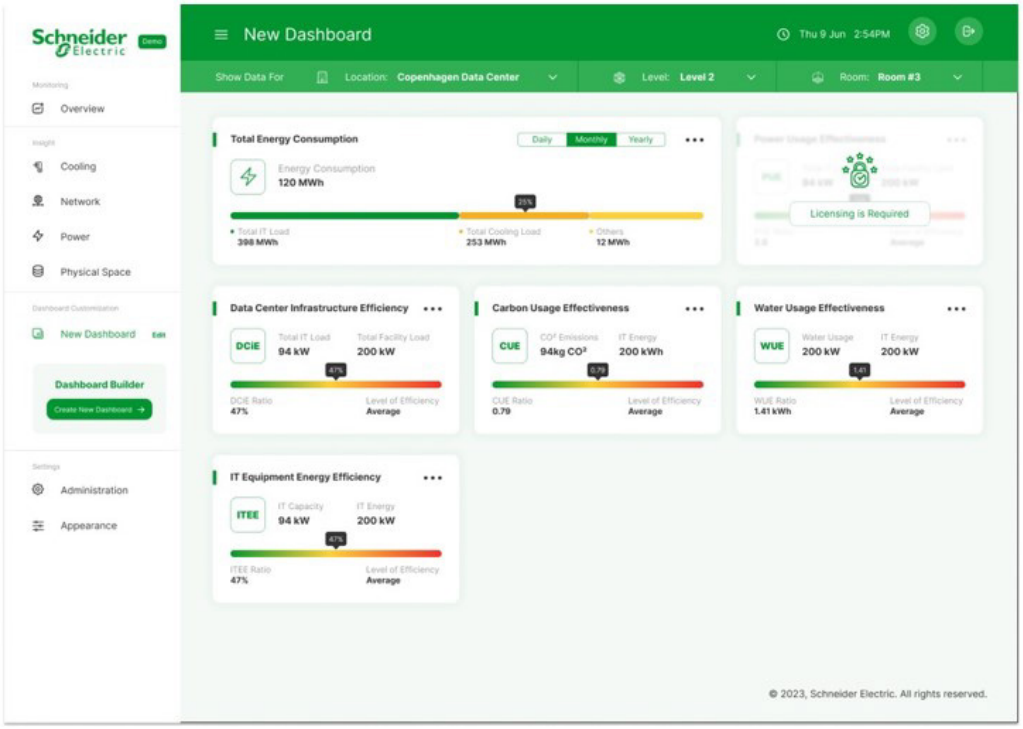

Figure 5

Example environmental sustainability dashboard created by a user at Schneider Electric's Copenhagen data center using our EcoStruxure IT Advisor DCIM software; the dashboard shows current values in the context of performance.

For these metrics to be meaningful, of course, it is important that the DCIM software be able to communicate with and normalize data from all power and cooling infrastructure devices, regardless of make or model. This ensures a complete picture of environmental impact. So DCIM tools and infrastructure devices that embrace common, open protocols (e.g., SNMPv3) and that accommodate the use of APIs/web services should be used.

While standard offers are limited today, some vendors offer engineering services to customize the output of a DCIM system and/or integrate the DCIM software with other data sources (e.g., emissions factor libraries) or platforms (e.g., IT asset management or ITAM, configuration management database or CMDB software) to address a provider's specific environmental sustainability reporting needs.

For providers who are tracking their Scope 3 emissions, which is largely the embodied carbon in the IT and supporting infrastructure, DCIM can also help. The first step is to take inventory of what is installed at all sites. DCIM's asset management functionality can be used to map out all devices in data centers or edge IT installations including the IT, networking, storage, power distribution, and cooling infrastructure. Embodied carbon data obtained from device manufacturers can be stored as attributes of the devices in DCIM asset management tools. DCIM can be used to track equipment age to differentiate between new equipment and existing to assist with Scope 3 emissions accounting, as well. Note, some DCIM tools can integrate with IT discovery and inventory software tools (ITAM, CMDB) systems which potentially could be used in a similar way to track embodied carbon of all physical assets, including those devices monitored by DCIM.

Reducing Scope 2 carbon emissions

Optimally managing and balancing a site's space, power, and cooling resources has always been a critical function of DCIM for MTDCs. Using up one resource's capacity before the others' results in stranding the capacity of those other resources making them, in effect, unusable. Stranded power and cooling capacity is under scrutiny not only for lost revenue opportunities, but increasingly for its

sustainability impact. IT footprint optimization and capacity management not only yields more sellable space, but it also reduces overprovisioning and energy losses that would otherwise increase the site's carbon emissions. DCIM will give providers a clearer link between tenant IT footprint optimization and carbon emissions. Note, Schneider Electric also offers a free TradeOff™ Tool called the, *Data Center Lifecycle CO2e Calculator*, that estimates a data center's total carbon footprint as seen through the lens of the owner. The results can be broken down by Scope. It helps MTDCs quickly understand what their largest emission sources are, where to focus carbon reduction efforts, how rack power density affects the numbers, and so on. It's a good companion tool to use with DCIM.

The use of DCIM in your day-to-day operations can directly serve to reduce energy consumption and, thereby, lower your carbon emissions today. The following bullets list some of the ways this can be done. Note, not all DCIM offers can perform these actions.

- Design energy-efficient floor layouts for expansion/consolidation projects that optimize airflows and ventilation pathways to minimize cooling energy.
- Use built-in computational fluid dynamics (CFD) analysis tools to reduce cooling energy by modeling increased temperature set points, enabling economizer mode, and changing other cooling parameters.
- Use built-in CRAC/CRAH AI-based optimization tools in DCIM to automatically regulate unit airflow speeds or turn off cooling units when cooling energy is overprovisioned.
- Use DCIM energy consumption data (via rack PDUs) as a mechanism to drive more energy efficient behavior from tenants.

Put more simply, DCIM functions can be used to better match power consumption to the IT load by turning down or turning off idle infrastructure resources. Providers could also reduce both IT energy consumption and power losses from the supporting infrastructure, by encouraging or even requiring tenants to consolidate their IT loads or decommission zombie servers. All of these reduce Scope 2 emissions.

Improving transparency

As mentioned in the introduction, tenants expect transparency from their providers. This is fundamentally because:

- customers have valuable assets not under their direct control (i.e., "I really need to know what's going on over there").
- enterprise tenants are pressured to understand and account for the environmental impact of their use of cloud and colocation services.
- tenants are under constant pressure to reduce cost and/or to show value for the IT spend; creates need to evaluate and validate provider performance against SLA.

As a result, the "tenant digital experience" has become a key differentiator for providers. This digital experience is the vehicle for having transparency between supplier and tenant. And this is an essential step towards building a relationship of trust. Without this trust, the provider will likely lose out to the competition. Optimized for colocation data centers, modern DCIM software is now an important part of this digital experience by providing a portal for tenants to view and monitor their assets and the resources they consume. Figures 6a and 6b show two examples of tenant portal dashboards.

Providers can enable their customers to have a current and historical view of the IT load, power, cooling, and space capacities, as well as energy consumption.

Tenants can view all their monitored devices with the capability to search and drill down into rooms, cages, and racks; while also being able to view environmental data (i.e., temp and humidity) and security cameras. Tenants can edit and track changes to their rack inventories by adding, moving, editing, or deleting equipment in racks. DCIM vendors offering tenant portals give the provider full control over whether a tenant has access and what they have access to.

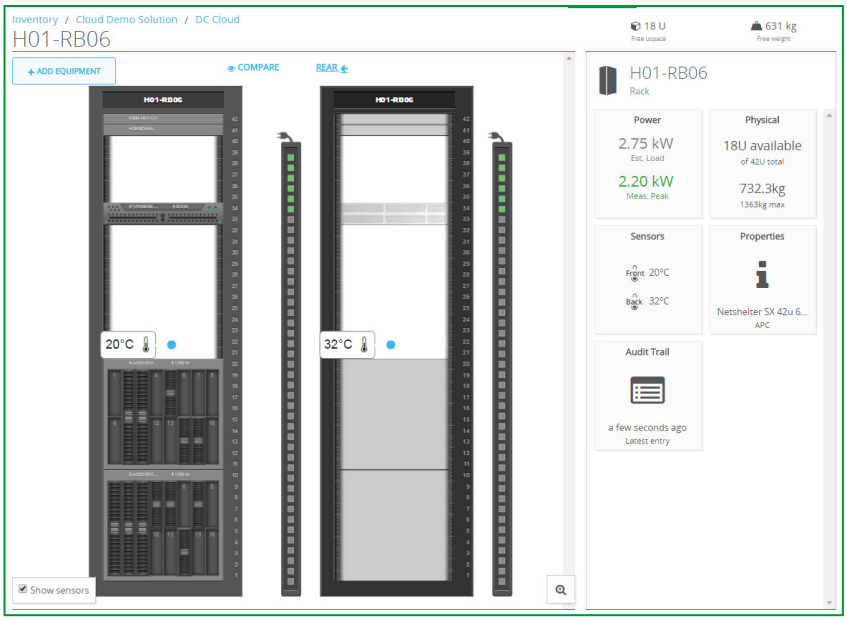

Figure 6a

Example screenshot of a tenant portal dashboard showing IT rack elevation details.

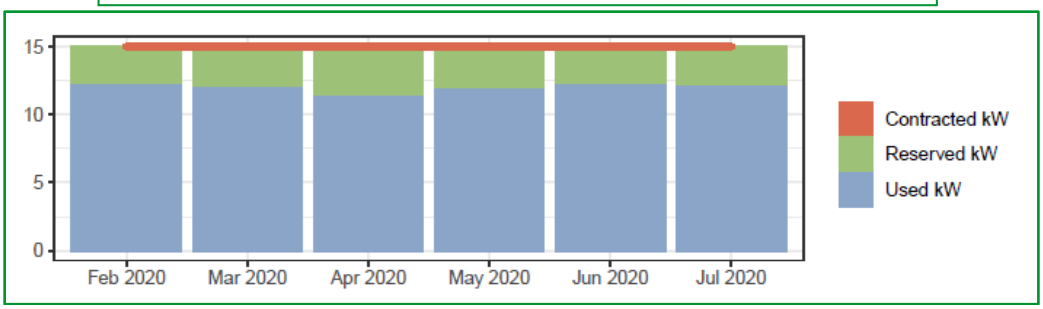

Figure 6b

Example screenshot of a tenant portal dashboard showing a tenant's power capacity report.

In Schneider Electric's experience, some colocation data center providers charge their tenants for this functionality, and some do not. Regardless, this "digital experience" functionality of modern DCIM increases the value that MTDC providers bring to their customers. Some have also been able to use tenant portals to create additional revenue streams and managed service opportunities. These opportunities can include things like provisioning KPI dashboards and trend analysis reporting, to managing access and permissions, or providing active hands as a virtual extension of DCIM to supplant customer in-house IT capability for moves, adds, and upgrades. The use of DCIM by both the provider and the tenant, facilitates having the provider add on additional services to manage their tenant's environment with "remote" or "smart hands" services.

Improving operational efficiency

Perhaps obvious to any IT operations professional who uses software (ITIM, ITAM, ITSM, Ticketing, etc.) to track, manage, and automate their daily workflows, using DCIM improves operational efficiency. Reducing the time, effort, and knowledge needed to manage data center infrastructure can free up staff to focus on other business critical activities. These labor efficiency gains can translate to a competitive advantage.

The following bullets are a few examples of how modern DCIM software improves provider and/or tenant operational efficiency:

- Know where to place or move a physical server without having to physically check for open U-spaces with available network ports, sufficient power and cooling capacity, and required redundancy levels.
- Perform mass device configurations and firmware/security updates at once versus having to log into each device and perform the update tasks manually.
- Understand all device dependencies (on power, cooling, network, physical host) without having to physically be on site and tracing everything manually.
- Integrate DCIM device alarms with Ticketing system to automate ticket generation with required device information
- Receive device alarms anywhere at any time through your mobile device or browser without needing separate login credentials for each location.
- Automate the data collection and generation of customizable reports on topics such as energy consumption, carbon emissions, capacity trending, and sellable space status and trend.

DCIM planning and modeling software optimized for MTDCs will have a digital overlay for the 2D map of data center assets that shows the commercial status of racks and floor space. Schneider Electric's default options (see Figure 7) are "open" (for sale), "closed" (in use), "reserved" (kept for customer), and "internal" (booked for internal use). DCIM solutions typically allow customizing the status labels.

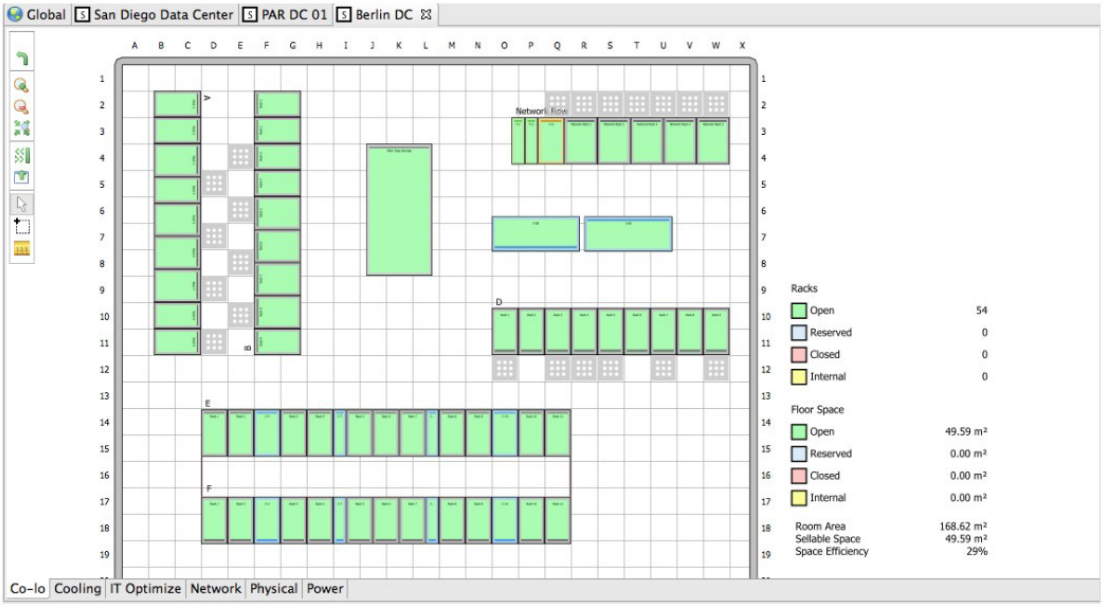

Figure 7

Example digital floor overlay within DCIM that shows the commercial status of racks and floor space.

This overlay map of the IT space shows a breakdown by tenant, what space is reserved for future tenants, what is available to sell to new tenants now (as well as showing power/cooling capacity, network ports for a given zone, etc.) This gives the provider improved visibility to data center assets and capacity in real time yielding sales enablement and change management efficiency benefits.

It should be noted that like with any enterprise-level operations software tool, efficiency improvements might take time to develop to their full potential. Software management tools take time to implement, setup and configure, train operations staff, and integrate into current workflows. This aspect of the solution is another comparison point to consider when evaluating DCIM solutions. Some vendors offer

services to do the implementation and setup and configuration for the provider, as well as offer in person and/or virtual staff training on how to operate the DCIM software. Well executed, these types of services can make it easier to begin realizing the potential value of DCIM faster than you would otherwise.

The next and final section of the paper discusses how to avoid common pitfalls that can negatively impact the potential value of DCIM.

Avoiding common pitfalls to ensure DCIM success

As with any major operations software platform, realizing the potential value of DCIM depends in large part on whether you select the appropriate tool for your needs and on how well it is implemented and maintained over time. The remaining sub-sections briefly describe common pitfalls we have seen and explains how to avoid them.

Selection

Taking on more than you are prepared to manage
Work closely with the DCIM vendor to understand the training, staffing, and implementation needs to integrate the new functionality into your daily operations workflows. It may be advisable to start with mastering DCIM monitoring and alarming first before tackling planning and modeling functions, for example.

Not realizing the degree to which the DCIM software supports 3rd party device and app integration
DCIM tools that support common open communications protocols (SNMP, BACnet, etc.), mobile, and web technologies (e.g., APIs) should be favored. Ask vendors if they support all the devices, you will be monitoring and whether (and how) the tool integrates with your existing operation tools such as the BMS, EPMS, ITAM, ticketing systems, and so on. Embedding DCIM data and functions into your already established workflows increases the likelihood of success.

Selecting a solution based solely or mostly on price and features offered
Most DCIM platforms offer, or at least claim to offer, the same general feature sets. It is important to understand how suitable the solution is for your specific situation and needs by interviewing the vendor or testing the solution. How easy and flexible is it to deploy, setup, use, maintain and scale? What does it take to customize the software? The vendor's execution in these areas is where you are likely to see the most differences in one solution from another. And it is in these areas where DCIM success most likely lies.

Not validating security capabilities and certifications of vendor
The degree to which a vendor prioritizes security in the design, development, and support of their products should be a key decision factor in which solutions you choose. Always choose to work with security-conscious vendors who are proactive, open, and transparent. Doing so will make it less likely for a breach to occur since there should be less vulnerabilities by design and any that do emerge should be detected and addressed sooner than they would otherwise.

Implementation

No implementation with existing workflows and tools
Successfully introducing new software tools that bring with them new workflows and processes can be a challenge. It is human nature to resist change and continue to rely on "the way things have always been done". This mentality can lead to the newly installed DCIM not being used or not taking advantage of its data. The extent to which you are able to integrate DCIM functions and data with existing tools (e.g.,

building management system or BMS, ITAM, ticketing systems), the greater the likelihood that DCIM's value will be fully realized. Otherwise, it is imperative for data center management to ensure new processes are developed (to account for DCIM functions) and followed by IT operations staff. This is why DCIM solution criteria should focus on how intuitive the software is to operate and maintain and how easy it is to integrate and share data with existing management tools.

Poor setup and configuration of users, alarms, and notification policies

The pitfall is that alarms go unnoticed or are simply ignored. There are two basic reasons why this happens. The first is because DCIM alarms and messages are not included in existing issue resolution processes or a new process to accommodate the alarms has not been implemented. The operations team needs to identify and agree on what constitutes an alarm, who should be notified, how (and how often) they are notified, who should act, and how is it confirmed the alarm condition has been resolved. These notification policies will need to be setup and configured within the DCIM system. Using default settings can simplify this process.

The second reason has to do with the sheer volume of data and a lack of context. Increasing device intelligence and decreasing sensor costs means a typical data center today can feed many tens of thousands of data points into a DCIM server. If thresholds and notification policies are too broad, this reported data could be overwhelming and, perhaps, even largely irrelevant. This then leads to the data being ignored while critical information (such as a UPS fault) goes unnoticed. Therefore, it is important that alarm policies and thresholds be designed to only broadcast an alarm when it is truly important or critical. And only those who really need to know should be notified. If you are unsure of what constitutes an important or critical alarm, choose the system default, or contact the vendor. Some vendors offer a setup and configuration service and online operator training to help with this important step.

Operations and maintenance

Failing to maintain an accurate map of assets in the DCIM software

For DCIM planning and modeling functions to work properly, IT and facility infrastructure asset information, including their location and interdependencies on each other, must be accurately recorded, and continuously maintained over time as adds, moves, and changes take place. The output of any modeling function would be flawed if the inputs into the model were wrong or inaccurate. To help ensure DCIM's value, it is important that the process of updating and keeping the map of assets current in the DCIM software is continuously kept up. There should be a commitment from management to ensure there are resources and focus to perform this function.

Note, success here also assumes that DCIM software is communicating with all critical power and cooling infrastructure devices so that the software output represents an accurate picture of the built environment. Environmental sustainability metrics will be flawed, for example, if the DCIM software is not collecting power or energy data from all cooling units, including any extra units installed for redundancy. Energy and emissions data would be underreported.

Lack of commitment, ownership, and knowledge

Sometimes the familiarity and habitual use of existing tools and workflows combined with a "well-its-worked-fine-before" mindset has meant that DCIM did not get fully implemented or used. It is important, therefore, for Facilities, IT, and Management to work together early on and come to agreement on the adoption and use of DCIM tools in conjunction with their existing tools. It's a mistake for management to decide to use a DCIM system without the buy-in from those who will be required to

implement and operate it. All sides should be involved in the early evaluation phase to ensure everyone's needs and expectations are met. Each group should come to see and understand the value of the proposed solution upfront. There also needs to be agreement and management support for committing the necessary resources to implement and operate the management system. All this upfront discussion and buy-in ensures on-going cooperation and participation well beyond the implementation phase.

Conclusion

Multi-tenant colocation providers who can meet or exceed tenant requirements and expectations at a lower cost will be best positioned to win in the market. This paper showed with practical examples how DCIM can make MTDCs more resilient, secure, sustainable, transparent, and operationally efficient. Achieving this value, however, depends on selecting the appropriate tool for your needs, effectively implementing and setting up the solution, and continuously maintaining its map of assets over time. We explained how modern "DCIM 3.0" solutions, when well implemented and maintained, help make colocation providers be more competitive, transparent, and responsive to the needs of their customers.

About the author

Patrick Donovan is a Senior Research Analyst for the Energy Management Research Center at Schneider Electric. He has over 27 years of experience developing and supporting critical power and cooling systems for Schneider Electric's Secure Power 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

Why Data Centers Must Prioritize Environmental Sustainability: Four Key Drivers
White Paper 64

Browse all
white papers
whitepapers.apc.com

Data Center Lifecycle CO2e Calculator
TradeOff Tool 33

Browse all
TradeOff Tools™
tools.apc.com

Learn more about the next evolution of DCIM
se.com/dcim

Note: Internet links can become obsolete over time. The referenced links were available at the time this paper was written but may no longer be available now.

Contact us

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

Schneider Electric Energy Management Research 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