

Peter M. Curtis is the president of Power Management Concepts, LLC, in Bethpage, NY, and an associate professor at New York Institute of Technology. Read this article online at www.missioncriticalmagazine.com/petermcurtis.



By Peter M. Curtis

Optimal Reliability Strategies For Your Critical Facility

Marrying operational tactics and predictive analytics with data center infrastructure management.

The repository of data collected by the critical facility industry contains zetabytes. This is an inordinate amount of information and, certainly, difficult to wrap your mind around. Plus, the pot keeps growing and growing. The emergence of advanced, automated data center infrastructure management (DCIM) tools has allowed data center operators to aggregate, analyze, and integrate the massive amounts of data collected from the multiple, disparate platforms which monitor servers, cooling, power, and other ancillary systems. The process of identifying the specific factors most likely to influence the value of a discrete body of data, especially one that you actually care about, can feel unworkable. Most data center facility professionals focus on the design, implementation, system control, and monitoring of infrastructure causing data overload and a dearth of actionable ideas. Our industry is poorly served by overemphasizing the “I” in DCIM. This terminology fosters a “break-fix” mindset; in reality, infrastructure is only as good as the people managing it.

As professionals, we need a renewed focus on data center operations management, or DCOM. DCOM involves strategies related to the people, processes, documentation, maintenance, testing, training, lifecycle, change management, and risk mitigation measures employed to ensure long-term reliability.

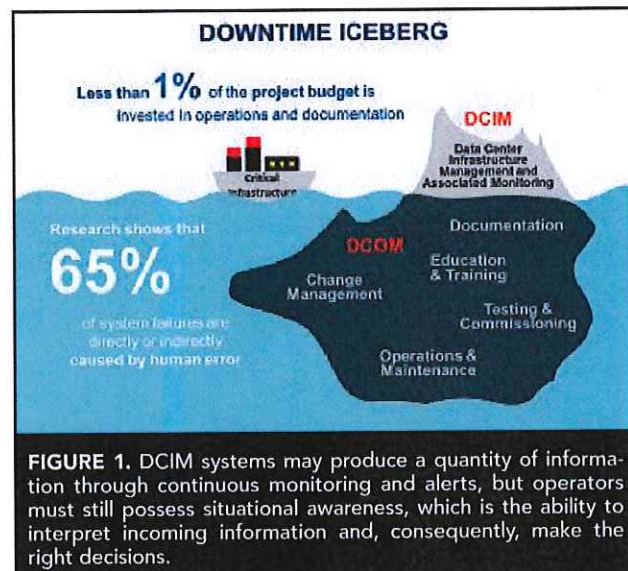


FIGURE 1. DCIM systems may produce a quantity of information through continuous monitoring and alerts, but operators must still possess situational awareness, which is the ability to interpret incoming information and, consequently, make the right decisions.

Consider that on average, 65% of downtime in critical facilities is the result of human error. Is this really the only reliability strategy for your critical facility considering all the advanced technologies that are available today for reducing human error?

As professionals, we need a renewed focus on data center operations management, or DCOM. DCOM involves strategies related to the people, processes, documentation, maintenance, testing, training, lifecycle, change management, and risk mitigation measures employed to ensure long-term reliability. Marrying DCOM with more traditional DCIM tactics, in conjunction with predictive and prescriptive analytics and algorithms, as well as industry intelligence and external data sources, or “influence information,” is the more strategic path toward the Holy Grail of the critical facility industry, the perfect standard of 100% uptime or unity.

Ultimately, data is only beneficial when you know what is

meaningful for your critical facility and what is just noise.

WHAT THE CRITICAL FACILITY INDUSTRY CAN LEARN FROM ALGORITHMIC TRADING AND IBM WATSON

Increased precision is the common denominator among enterprises that have successfully adopted a more systematic approach to decision making. The application of predictive analytics in other industries, for example, the financial industry's use of algorithmic trading and the commercial market's increasing reliance on data visualization and analysis tools, such as IBM Watson Analytics, is revealing. This tells us that those invisible lines surrounding a value, the limitations and boundaries that an asymptotic equation is

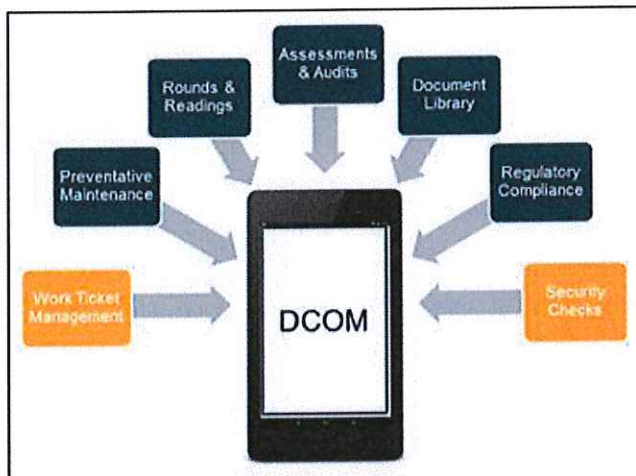


FIGURE 2. Data center operations management (DCOM) involves strategies related to the people, processes, documentation, maintenance, testing, training, lifecycle, change management, and risk mitigation measures employed to ensure long-term reliability.

always approaching but can never actually attain, are proving less and less elusive.

Diversification is at the heart of most investment strategies; risk attributes and investment opportunities vary widely among investment styles. With an increased number of scenarios to consider, whether based on the occurrence of desirable trends or price differentials, having some help is, well, helpful. Algorithmic trading offers an appealing alternative to relying on intuition and instinct, as is the capacity to quickly consider multiple decision parameters at the exact same time. Similarly, critical facility operators have positively responded to the inherent opportunities in translating a specific strategy into a computerized process with implementation capabilities. But, can pre-programmed instructions/rules-based environment ever be enough, especially, in environments that demand real-time situational awareness, often under evolving circumstances, as is the case with critical facilities?

Removing human error from the equation remains an effective

strategy. Reliance on defined sets of rules based on decision parameters, such as timing and quantity, allows for simultaneous automated checks on multiple conditions, in addition to reducing chances for manual errors or emotional decision making. However, the move toward predictive analysis is ultimately about precision and identifying exactly what factors are most important in predicting a positive outcome. We can see similar challenges affecting the critical facility industry as those facing the trader equipped with a powerful data aggregator tool. An algorithm must be continuously back-tested based on historical and incoming data, and the more complex the algorithm the more back-testing and ongoing analysis required.

Our industry's devotion to DCIM tools has perpetuated the idea that infrastructure — typically encompassing the plant, property, and equipment (PP&E) — is the key to predicting the reliability of a facility. The operation of the PP&E and the utilization of the information produced by a myriad of systems, including the building management system, the computerized maintenance management system, the energy management system, and the security access system, etc., also deserve some consideration.

DCOM can encompass some of the most difficult reliability strategies to standardize and to control, for implementing them involves processes and procedures affecting the entire enterprise with standards instituted by industry experts. But, the resulting documentation (information) has a distinct advantage. In contrast to DCIM, DCOM informs decisions about predictive maintenance and proactive management of the facility in holistic terms. This is the ideal to work toward, as well as the model currently employed by more sophisticated predictive and prescriptive analytics.

DCIM systems may produce a quantity of information through continuous monitoring and alerts, but operators must still possess situational awareness, which is the ability to interpret incoming information and, consequently, make the right decisions. DCIM is what we physically see in a critical facility, but DCOM is what goes on below the surface to bolster what we see.

COMPUTER-AIDED AUTOMATION'S POTENTIAL: THE NEXT GENERATION OF ADVANCED RISK MITIGATION

Computer-aided automation is hardly the end-all/be-all solution. A true read of an algorithm's performance requires both qualitative and quantitative analysis. This continuous stream of information comes from internal and external sources. Returning once again to algorithmic trading for illustrative purposes, recognize that the trader relies on both the infrastructure to back-test and numerous market data feeds to identify arbitrage opportunities. Critical infrastructure operators also benefit from a geographic overview of their facilities, such as real-time site conditions and weather. In both scenarios, the capacity to effectively read incoming data, convert this data into actionable ideas, and then execute a solution can all come down to milliseconds. If executed as designed, you are good to go, as demonstrated by a profitable trade or an averted equipment failure.

However, when the timing — the precision — is off, the results can be serious, leading to significant financial loss, infrastructure damage, and potentially lost lives.

Although DCIM can effectively map IT resources and facility assets, it is still necessary to analyze real-time operating data within the context of IT service management data. DCIM tools are efficient data aggregators for managing critical facilities more effectively, but they are not an end-to-end solution; rather, the relationships between applications and the IT resources that support them must also be accounted for. In the case of equipment failure, truly comprehending interdependent relationships in a holistic manner is the difference between alerting the operator of the abnormal system status vs. providing insight into the root cause of the problem or, better, suggesting the best way to correct it. The critical facility industry also needs advanced, automated DCOM strategies to remain viable and to evolve to the next generation of advanced risk mitigation.

The public entry of IBM's Watson Analytics is evidence of how analytics are driving fundamental changes in how business is conducted from isolated data collection to frontline adoption. The critical facility industry needs a "Watson" to help break down the barriers between siloed functions within a critical infrastructure environment, for example, between inspections, preventive maintenance, predictive maintenance, and testing. All of these forms of maintenance are necessary to reduce the risk of downtime because they give operators the best chance to predict equipment issues before a failure. Since a trend analysis must start with a baseline, it is important to have a repository of data and documented readings to provide operators with information while they are performing maintenance — not afterwards, when they return to the office. Similarly, data from initial validation and commissioning contributes to the robust nature and accuracy of this repository.

Ideally, operators have data from inception at their fingertips. A holistic solution means having the capacity to ask pertinent

questions that result in actionable items for immediate investigation.

THE ROSETTA STONE OF CRITICAL FACILITY ANALYTICAL TOOLS

Unity is the Holy Grail for the critical facility industry. Although potentially unobtainable, it is the ideal sought for its great significance and universal relevance to people's daily lives: data is the lifeblood of our modern society.

The intricacy of critical infrastructure designed to buttress society has evolved in concert with the growing complexity of the human and technical systems (man and machine) that comprise it. The exponential proliferation of data generated by and collected from myriad, non-compatible components, like cutting-edge sensors, servers, generators, and smart HVAC systems, taxes the capacity of critical infrastructure and the current tools used to control and monitor it. It is symbolic that the instruments contributing to this intricacy, to data overload, may also hold the keys to unlocking the solution for the perfect standard of 100% uptime.

The solution is not so much about what data we should pull and when, but rather about what we do with the data once we collect it. An onslaught of data can feel like unintelligible hieroglyphics to a facility operator who requires clues to understand what would otherwise appear undecipherable. The critical facilities industry needs a Rosetta Stone, a DCOM tool that can create meaning from data where there was previously just noise. Such digital companions would enhance, not replace, humans in all the operational and emergency tasks integral to operating a critical facility environment. This is an appealing solution to our quest for 100% uptime — it translates information into actionable ideas. The Rosetta Stone solution is about aggregating divergent data sources and creating algorithms capable of mining those zetabytes. And, all of this would be accomplished in pursuit of the most invaluable knowledge: the nugget that will approach uptime unity. ■

SECURITY CHIMNEYS SECURE SEAL

SINGLE, DOUBLE WALL
AND DOUBLE WALL
INSULATED

STRINGENT STANDARDS FOR QUALITY ASSURANCE

A perfect fit every time. Viton® pressure gasket ensures a leak free system.

INSTALLER FRIENDLY

Secure Latch system allows for a fast and tool-free installation.

AVAILABLE UP TO 36" DIAMETER



For more information scan QR Code, follow us on social media or visit securitychimneys.com



security

securitychimneys.com
800-361-4909 US
800-667-3387 Canada
Security Chimneys © 2016