Life Is On | Schneider Electric

Attributes of an Effective Maintenance Program for Data Center Physical Infrastructure

White Paper 264

Version 1

Authors

Ken Belanger
Eric Brun
Prasanna Kanchikere
James Martinec
Wendy Torell

Executive summary

Data center maintenance is in the midst of a gradual evolution toward condition-based and eventually risk-informed maintenance. However, many data center operators today rely on calendar-based maintenance. In this paper, we discuss what key attributes to look for in a maintenance service provider. We also describe how data analytics, digital services, and connected systems are enabling the evolution from calendar-based maintenance to condition-based maintenance.

RATE THIS PAPER ★★★★★

Introduction

Critical data center information technology (IT) loads depend on the reliability and availability of the physical infrastructure systems that support them. This includes uninterruptible power supplies (UPSs), electrical distribution equipment like switchgear and power distribution units (PDUs), and cooling systems like computer room air conditioners (CRACs)/ computer room air handlers (CRAHs), direct expansion (DX) condensers, chillers, etc. Maintenance programs are an essential part of keeping these systems operational. In addition to minimizing downtime, these programs help the systems run efficiently and maximize their life expectancy, ultimately reducing the operating expense of the data center over time.

There are two core functions of infrastructure maintenance programs, as described in **Figure 1** below. Preventive maintenance (PM) is intended to eliminate preventable failures from occurring, while also optimizing system upgrades, parts procurement and manpower resources. The more robust the program, the more likely it is that the activity does what it is intended to do. Remedial maintenance (sometimes referred to as break/fix or unplanned maintenance), the other part of the equation, is necessary for when an unforeseen failure occurs. Some programs do a better job than others at performing the remedial repairs timely and effectively.

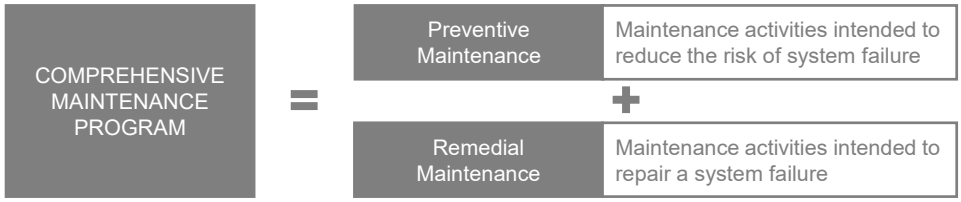

Figure 1
Two parts of a comprehensive field-based maintenance program

White Paper 124, *Preventive Maintenance Strategy for Data Centers*, discusses the history of PM visits for data center systems like UPSs and the progress the industry has made in evolving from component level maintenance plans to more holistic maintenance.

In *this* paper, we describe both preventive and remedial maintenance in greater detail, describe the approaches to each, and provide examples. We then present five key attributes that are critical to look for when selecting a maintenance service provider. Lastly, we will describe how data analytics and the adoption of digital services and connected systems will lead to an evolution from calendar-based maintenance to condition-based maintenance.

Preventive maintenance

Preventive maintenance (aka preventative maintenance), when executed effectively, reduces downtime and its associated costs, reduces operating costs, and defers capital costs. Today, data center preventive maintenance programs most often fall under the category of **calendar-based maintenance**. Calendar-based maintenance means the activities are performed on a regular occurring, pre-determined schedule – quarterly, semi-annually, or annually. During those visits, specific sets of tasks are performed. Later, in the section titled, **Evolution of maintenance**, we discuss how we are seeing a shift towards hybrid models that include condition-based maintenance as technologies like data analytics and artificial intelligence (AI) become more widely adopted, and data center systems continue to evolve into highly connected, smart, and remotely manageable systems.

The following major activities should be completed as part of a preventive maintenance visit:

- **Perform comprehensive onsite inspection**. This includes a visual inspection of all physical infrastructure systems, an environmental (and thermal) inspection, and an electrical/mechanical inspection. These onsite inspections can be crucial for determining the type of maintenance work to perform on the systems. In the "Elements of effective maintenance" section, we discuss this in greater detail and describe what attributes to look for in a service provider's approach to inspection.
- **Replace consumable components**. Most physical infrastructure systems have parts that are consumable, meaning they have a limited life expectancy. Common examples of these are batteries, capacitors[1], filters, and humidifier cylinders. It is important to replace these components before they present a downtime risk to the data center. Timely intervention also minimizes capital costs by deferring the parts replacements until necessary ("just-in-time"). Life expectancy of key components is a variable that should be considered when designing your data center, as it impacts the frequency of maintenance needed. One way to prepare for the evolution towards condition-based maintenance is to retrofit older equipment with modular equipment that has replaceable or upgradeable components.
- **Functional verification** – In this step, the technician confirms the system is (or will) perform as needed. For a UPS, this may be a system self-test, self-load test, runtime test, or a transfer to and from static bypass. For a CRAC/CRAH, this includes testing the fans, heaters, humidifiers, compressors, condensate pumps, and checking the refrigerant level or chilled water flow. Some of these parts related to condensate management and humidification are used seasonally, and sediment can accumulate due to water impurities which can inhibit proper operation; performing the test ensures it will turn on when needed. Functional verification can involve state changes, and state changes always introduce a potential risk. Data centers designed with redundancy present a lower risk in performing this verification. Ultimately, the end user must decide if they are comfortable with the risk introduced. It's a tradeoff between a potential event during a scheduled maintenance window, vs. an unexpected event during business hours. For example, knowing if a UPS battery supports the critical load due to a power event.
- **Updates/revisions** – Vendors periodically update firmware or implement circuit board revisions. During a preventive maintenance visit, the technician should update the systems with the latest available updates.
- **Communication of status** – It is important the service technician provides communication on their findings. A report is generally provided digitally to the operator/owner, so they know what tasks were completed, what components were changed, what software was updated, and any other further recommendations.

There are standards available that guide the preventive maintenance work that should be done for the systems within a data center. For example, **Table 1** is the checklist recommended for external VRLA batteries, according to IEEE Standard 1184-2006.

The objective of preventive maintenance is to avoid failure and ultimately avoid the need for remedial maintenance. But sometimes unexpected problems occur. In the next section, remedial maintenance is discussed.

[1] Most newer UPSs don't require this because they are designed with capacitors that have an equal lifetime to the UPS. See White Paper 116, Standardization and Modularity in Data Center Physical Infrastructure, for further discussion on the benefits.

Table 1
Preventive maintenance check list, according to IEEE Standard 1184-2006

Description	Quarterly	Annually
Visual inspection of battery	✓	✓
Environmental inspection	✓	✓
Ambient temperature	✓	✓
String float voltage	✓	✓
String float current	✓	✓
Unit float voltage	✓	✓
Individual cell float voltage	✓	✓
Individual battery temperature	✓	✓
Terminal connection verification		✓
AC ripple current and voltage	✓	✓
System load testing		✓

Remedial maintenance

In the event of an unexpected problem, remedial maintenance, sometimes referred to as “break/fix” or unplanned maintenance is necessary to provide repairs. The goal of this unplanned maintenance should always be to get the failed system(s) up and running as quickly as possible while ensuring the system will not pose any further risk to safety or the environment, to prevent impending downtime or, if downtime occurs, reduce downtime expense to the business. Redundancy in the data center design reduces the negative impact of a single system or component failure. The most common system failures are shown in **Figure 2**.

Several variables impact how quickly a service provider can complete the remedial maintenance:

- **Ability to identify problem** – Troubleshooting the problem is the first crucial step. Being remotely connected generally reduces the time it takes to identify the problem. A correct diagnosis prior to dispatching a technician, means that the technician arrives with the right parts and an immediate plan to resolve the problem.
- **Service level agreements (SLAs)** – Some vendors offer SLAs that determine how fast the technician will arrive at the site. A response time of 4 hours is common for highly critical systems.
- **Competency and skill level of service technicians** – Trial and error approach often results in longer-than-necessary downtime and resolution time. This is why product expertise, genuine replacement parts, and accessibility to technical documents are so important.
- **Parts availability** – The ability to get the needed parts onsite is crucial to resolving the problem. Some vendors stock critical components in regional warehouses to improve the speed of dispatching necessary parts.

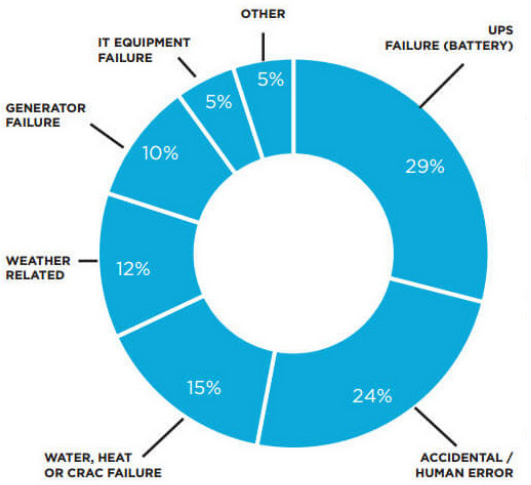

Figure 2
Uptime Institute summary of data center outage root causes
https://journal.uptimeinstitute.com/data-center-outages-incidents-industry-transparency/

Elements of effective maintenance programs

When selecting a provider for your maintenance programs, there are five key attributes to consider. These will determine the effectiveness of the maintenance activities, whether they are indeed "preventive" and help to reduce downtime risk as intended, or whether they do the opposite – introduce human error and downtime risk into the data center. These five attributes are:

- Expertise of the maintenance personnel
- Quality assurance
- Onsite response time
- Remote monitoring capability
- Comprehensive onsite inspection

Expertise

Human error is a significant source of downtime in the data center. Maintenance activities are not immune to that. In fact, there are many potential ways to introduce defects during maintenance interventions. Some test procedures expose the equipment to atypical hazards, unusual stresses, or accelerated wear. Configuring the equipment for testing often involves operating several different controls, each of which must be restored to the proper position, generally in the proper order, when the equipment is returned to service. This is why detailed procedures must be used and the **maintenance personnel must be well trained** in all processes/procedures that are within their statement of work.

Service personnel that are dispatched to the site for maintenance work should:

- be subject matter experts on the systems they will maintain.
- be certified to perform work (e.g. OSHA certified, refrigerant handling certification by EPA, local state licensure)
- have effective communication skills – discussing work to be done, expectations, answering questions, etc.
- receive on-going training/professional development to stay up to date on skills.
- have access to vendor tools/software that enable better diagnostics.
- have access to latest field service bulletins created by system vendor(s) that alert them to trending issues.

- have access to sustaining engineers, application engineers, and design technical support teams for escalating problems.
- know and follow all safety guidelines, including wearing appropriate PPE.
- be knowledgeable on the latest technology and systems available in the market and make recommendations for replacements when systems reach end-of-life.

When evaluating maintenance program options, this level of expertise and knowledge will ensure the maintenance activity will enhance the performance of the data center and/or resolve unanticipated break/fix maintenance in an effective manner to get the system back up and running as fast as possible. In White Paper 196, *Essential Elements of Data Center Facility Operations*, we discuss the importance of well documented procedures and well trained personnel further.

While cost of maintenance certainly comes into play, it is important not to "cut corners" here, as it can have direct impact on the availability of your data center. Service providers pose a greater risk if they don't have the skills and expertise described above. Vendor technicians go through a series of in-depth trainings, product-specific trainings, exam certifications, and on-the-job supervised trainings with a locally qualified field service representative who assesses their competencies. However, third-party , non-vendor-specific providers often go through multiple learning curves on multiple vendor's systems; this may lead them to be generalists on all, but experts on few or none. Not working day in and day out on the same systems can lead to multiple issues. Below are **examples of poor maintenance practices** that can occur when the provider isn't fully knowledgeable on the systems being maintained:

- Technician swaps out parts that were not in need of replacement, which increases risks of downtime.
- Technician replaces part of a battery string rather than the entire string, which can impact the integrity of the entire string.
- Technician swaps out one capacitor in a capacitor bank, which can lead to an imbalance since the internal impedance is different on the new one vs the existing ones in the bank; this can decrease the capacitor bank life significantly.
- Technician installs a spare part that is not compatible with the software and leads to a malfunction.
- Technician misses a problem because the system showed the "green light".
- Technician doesn't know of or have access to, and therefore doesn't update to latest version of firmware (which are important as they address minor bug fixes, add support for new features, and provide updates for cyber-security risks).

Quality assurance

Effective service partners have well-documented, and well-established processes and procedures. White Paper 178, *A Framework for Developing and Evaluating Data Center Maintenance Programs*, goes in depth on the implications of having inadequate maintenance and risk mitigation processes, and suggests a framework to align maintenance activities with a facility's operational and performance requirements. It also provides a list of criteria and documentation to look for when evaluating a maintenance program, including:

- operational procedures (i.e. standard operating procedures, methods of procedure)

- operational processes (i.e. change management process)
- training program (i.e. program description, personnel training records)
- controlled firmware and software

A service provider that can demonstrate these processes and procedures is more likely to assure you the service needs are met, and downtime is minimized.

Onsite response time

When remediation is necessary, it is important to get your systems back up as quick as possible. Some companies are able to offer service level agreements (SLAs) that guarantee response times as short as 4 hours. These providers are able to do this because of their global field service coverage. Smaller 3rd party providers may not be able to make guarantees like this. It is important to understand the criticality of your loads and associated costs of downtime when selecting a vendor and an SLA. The shorter the guaranteed response time, the greater the cost.

But it is also important to note, these SLAs are guaranteeing when a service technician will arrive on site to begin addressing the problem. It does not guarantee when the system will be fixed, because that depends on the diagnosis and access to spare parts. Service technicians that are part of the vendor's organization generally have improved access to spare parts. They also often have the ability to get the parts on site quicker and get the problem resolved quicker. After diagnosis, obtaining the parts (if necessary), and making the repair, the system should be tested to ensure it is fully functioning to specifications.

Look for a vendor that has a tiered support staff, one that can leverage and escalate challenging scenarios to engineering resources beyond the field service techs to diagnose and resolve problems quickly. Some third-party vendors may end up with a trial and error approach, which leads to lengthy resolution time, and potentially making the situation worse before better.

Remote monitoring capability

Digital monitoring enables more effective preventive maintenance. Algorithms can predict when failures will occur and notify responsible parties. If you have a lot of assets, having a 3rd party remotely monitor can be a significant time saving benefit and removes the burden for your staff. White Paper 237, *Digital Remote Monitoring and Dispatch Services' Impact on Edge Computing and Data Centers*, explains how seven trends are re-defining remote monitoring and field service dispatch service requirements and how this will lead to improvements in operations and maintenance of IT installations.

Not only does remote monitoring of assets enable the shift towards condition-based maintenance instead of calendar-based (discussed in the next section), but it also enables timely identification of problems, that are sometimes remotely diagnosed and resolved completely. When field technicians are necessary, they come armed with critical background information and the necessary spare parts to resolve the problem faster. Without a remote monitoring capability, the timeline looks very different. The problem is described by the onsite staff, the field technician goes on site, and may then realize they need spare parts, which causes a delay while awaiting spare parts to arrive.

Comprehensive onsite inspection

Onsite inspections are important because they provide a global view of the system. The technician sees the system operating in their environment and can identify

problems not identified through reported data. For example, dirty components, blanking panels that were removed, or a panel removed and not remounted on machines, creates a potential risk. During a PM onsite visit, there are three types of inspections that should be performed to ensure the system(s) are operating as efficiently and reliably as possible. These activities are not necessarily completed sequentially, as each inspection may lead to actions that are necessary to ensure optimal performance.

1. Visual inspection
2. Environmental inspection
3. Mechanical/electrical inspection

Perform a visual inspection. For example, dust can accumulate on fans which may reduce airflow; An outdoor condenser may be covered in debris, dust, tree pollen, leaves, insects, etc. Dirty condenser coils result in higher system pressure and higher current draw, ultimately leading to greater energy expense. The same is true for dirty air filters. Batteries can show signs of irregularities in appearance, and doing a visual inspection is important to identify potential damage such as cracks, deformation, leakage of electrolytes, excess thermal activity or corrosion. Based on the visual inspection, systems should be safely cleaned (and if necessary, replaced). Visual inspection also includes refrigeration level and oil levels in DX systems.

Perform an environmental inspection. The surrounding space can have an impact on the function and life of the systems in the data center and its support rooms like the electrical and mechanical rooms, and in the case of cooling, outdoor spaces as well. Geographies near the ocean may have to contend with corrosion on the aluminum fins of outdoor units; northern climates may have to contend with snow and ice. Diesel generators will have accelerated corrosion and oxide formations if located near sulfur-based exhaust such as airports. In addition to the environmental outdoor conditions, water quality is another variable that should be considered. Systems like humidifiers can require additional maintenance if the water is hard and leaves deposits that could clog the system assembly.

Perform an electrical/mechanical inspection. An inspection of the components ensures they are performing according to the defined technical specifications. This may include tasks like a runtime test of a UPS battery, UPS self-testing and loading, checking fans, and correcting any faults. This inspection may include tightening electrical terminations in electrical panels, checking things like temperature sensors, humidity sensors, pressure sensors – components that are crucial to control of the systems; for chilled water systems, checking the controller valves that regulate the chilled water through the units to make sure movement is smooth, there's no obstructions, it's not leaking, or showing any signs of impending failure. The more that can be done in a non-invasive way, the better. Infrared cameras should be used to check the temperature of a busbar or cable terminations, for example, which can indicate increased resistance that may be caused from loose connections. See White Paper 268, *Using Infrared Thermography to Improve Electrical Preventive Maintenance Programs*, for more about how infrared can be used to improve maintenance while decreasing the likelihood of human error.

Onsite inspection is also crucial when a system failure is identified. Remote monitoring allows the vendor to have information about the system but having a field technician onsite allows them to see the system in the context of the environment, to see the global view of the system. For instance, is there an airflow problem because a panel was removed and not remounted on the system being maintained? There are many things you can see in person that you cannot see through the information digitally communicated to a remote service bureau.

Just like we have seen the automobile industry evolve towards less frequent, less intensive maintenance as a result of consumer demand, we are seeing a similar shift in the data center industry. A focus on less invasive approaches to maintenance, such as thermography, is enabling diagnostics with a decreased risk of human error.

Evolution of maintenance

Preventive maintenance interventions can be classified by the strategy used to schedule them. These classes are calendar-based maintenance, condition-based maintenance, and risk-informed maintenance. **Figure 3** describes these three maintenance strategies along a maturity scale. While today, most PM is calendar-based, we believe there is a natural progression towards condition-based, as systems become smarter and more connected for monitoring.

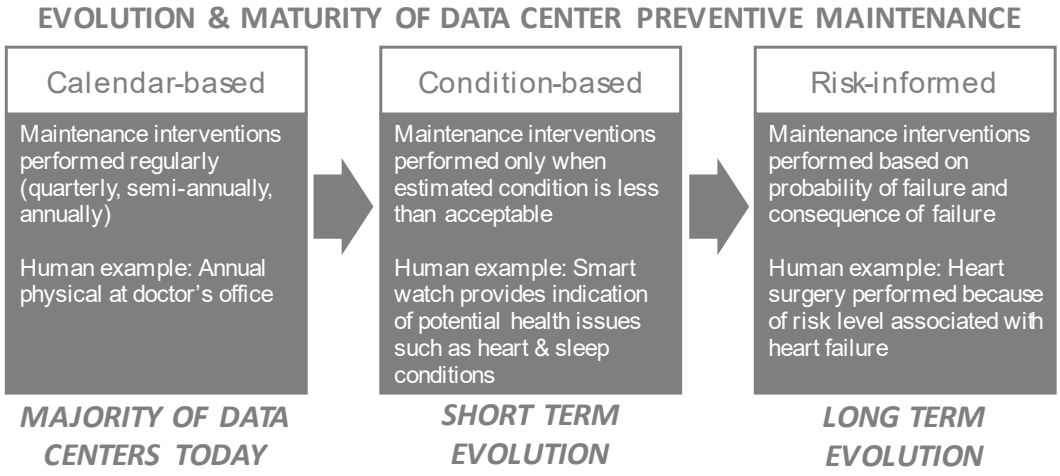

Figure 3
Industry evolution in preventive maintenance, with human medical examples

Condition-based maintenance

Through condition-based maintenance (sometimes referred to as predictive maintenance), technicians are only onsite when the system is considered in a "less than acceptable" or approaching a "less than acceptable" state, when the maintenance is most beneficial, which means some measurement of the specific device falls outside the thresholds set. Common metrics for making this assessment are variables such as temperature, voltage, current, cycles. This avoids unnecessary maintenance being performed on systems that are still in working acceptable condition. Without the condition-based maintenance visit, the system may operate in a degraded state or have an increased risk of failure.

Condition-based maintenance is achieved by continuously or periodically computing an estimate of a system or component's condition and scheduling a maintenance intervention *only when the estimated condition is less than acceptable*. Generally, the system or component remains in operation even after the estimated condition has deteriorated. In other words, the computations take into consideration an adequate margin to ensure the system remains in operation until the maintenance activity can occur. The "check engine light" on modern car dashboards is an example of condition-based maintenance. The driver is often unaware that anything is amiss, but the engine and vehicle systems management computers detect sensor readings that are out of expected range, off trend, or otherwise indicative of deteriorating condition. Another example is a smart watch monitoring your heart rate, blood pressure, and sleep and alerting you if it exceeds an acceptable range.

Big data analytics has enabled more sophisticated battery life expectancy algorithms, which are already in place in some UPS systems today. Digital twin technology, which refers to a digital replica of potential and actual physical assets[2], are being applied throughout buildings, including data centers. This allows the operator to observe differences in performance between the actual system and the digital system, which could identify degraded states, premature aging, etc.

Risk-informed maintenance

If we look out further into the future, there's an even more mature form of preventive maintenance, whereby the maintenance processes are planned based on failure risks, effects, and calculated costs. Risk-informed maintenance requires more sophistication on the part of the data center facility owner / operator. This maintenance strategy attempts to balance the Probability of Failure (PoF) and Consequences of Failure (CoF) of each asset.[3] Risk is the product of probability and consequences.

Predicting the consequences of failure in a mission critical facility is difficult. A complete failure of the data center supporting trading floor operations for a major financial firm might result in billions of dollars in damages if it occurs during normal market hours. The same failure, if it occurs at 2 AM on a Saturday, may be little more than a major nuisance so long as recovery can be completed before the next market opening. System design is certainly the most important aspect of designing and managing to reach a certain availability goal.

Risk-informed maintenance can also help prioritize maintenance based on limited maintenance resources. In the human example of **Figure 3**, if the patient had varying conditions identified, the one(s) with the greatest risk, i.e. risk of heart failure leading to death, would be prioritized to be addressed first.

Constructing a risk-informed maintenance program requires operators to know the probability of failure of the system for a variety of conditions. Therefore, a fully risk-informed maintenance program is probably beyond the means of most mission critical facility owner / operators today and for the near future. As technologies like big data, AI and machine learning continue to advance, and high quality, low cost sensors/controllers continue to expand, this evolution will take place.

Conclusion

Maintenance programs are an important aspect of data center operations. It is important to select programs that are comprehensive with experienced staff; and that have capabilities to gradually move up the maturity scale as the industry continues to evolve towards less invasive, more condition-based and risk-based activities.

In this paper, we presented five key attributes to look for in a service provider – (1) expertise of the maintenance personnel, (2) quality assurance (3) onsite response time that meets your needs, (4) remote monitoring capability which makes maintenance more effective, less invasive, and (5) comprehensive inspections during preventive maintenance that focus on ensuring the systems are operating as efficiently and reliably as possible.

A vendor should be your trusted advisor, one you feel confident will ensure your systems operate as expected, one that has the foresight and capabilities to provide hybrid service models (calendar-based and condition-based) and continue to evolve as technologies enable more sophisticated, lower risk maintenance.

[2] https://en.wikipedia.org/wiki/Digital_twin

[3] https://www.assetinsights.net/Glossary/G_Risk-Based_Maintenance_(RBM).html

About the authors

Ken Belanger is a Senior Level Field Service Representative based in South Florida, USA. He started his career with APC in 2002 with the NAM cooling technical support team and helped support sales, certified partners, field service, and 3rd party vendors. He transitioned to the Cooling Sustaining Engineering team and was responsible for managing quality of installed cooling products, customer escalations, and new product development projects. Ken became a member of the Global Service Team in 2010 as Service Lead for development of new cooling products. Under this role he acted as an advisor to global engineering teams to improve product serviceability, drive the spare parts creation process, assist with development of service trainings, engaged with global product marketing, and created service offers for start-up and maintenance of cooling products. Ken graduated from New England Institute of Technology in Rhode Island in 1993.

Eric Brun is a Power Conversion, Distinguished Architect. In this role he researches the best available technologies and architectures related to power quality and energy efficiency, to improve the development of future products and data center power systems. He also has leading positions in several international standard committees linked to UPS and power conversion systems, where he contributes to the writing of new standards with the aim of improving the safety, the performance and the integration of new constraints linked to the use of renewable energies and direct current for future power converter products and applications. He received his bachelor's degree in Electronics from CNAM of Grenoble, France, his master's degree in applied sciences from CESI of Grenoble/Lyon, France and his MBA from IAE/ESA from University of Grenoble France.

Prasanna Kanchikere is a Senior Manager in India Field Services Level 2 Technical Support for Schneider Electric's secure power products. In this role, he provides technical expertise for field service engineers and customers when issues are escalated. He also helps internal stakeholders (sales, quality, business development) with his technical knowledge. He is a certified trainer from Global Field Services Academy and conducts customer trainings on various products available within the secure power line of business, He has been with Schneider for over 14 years in positions involving manufacturing, and customer satisfaction & quality.

James Martinec is a technical expert supporting Level 3 escalations as well as platform engineering related support and projects, primarily for UPS and associated products. He supports NAM, Taiwan, South America, and Central America for critical escalations, assessment analysis on returned products, quality review and execution, site Method of Procedure (MOP) creation, visits to customer sites and technical support. His 35 years with EPE, MGE and Schneider Electric included power equipment test specialist, all Industrialization and engineering phases from start to finished goods, R&D for EPS UPS products, PCBA design and testing, platform engineering duties, quality engineering, lab expert analysis, technical support and troubleshooting. He is continuously involved in resolving customer issues, site repairs, training and customer satisfaction.

Wendy Torell is a Senior Research Analyst at Schneider Electric's Data Center Science Center. In this role, she researches best practices in data center design and operation, publishes white papers & articles, and develops TradeOff Tools to help clients optimize the availability, efficiency, and cost of their data center environments. She also consults with clients on availability science approaches and design practices to help them meet their data center performance objectives. She received her bachelor's degree in Mechanical Engineering from Union College in Schenectady, NY and her MBA from University of Rhode Island. Wendy is an ASQ Certified Reliability Engineer.

Acknowledgements

Special thanks to **Stephen Fairfax of MTechnology, Inc** for subject matter expertise and contributions to the condition-based and risk-informed sections of this paper.

Resources

A Framework for Developing and Evaluating Data Center Maintenance Programs
White Paper 178

Preventive Maintenance Strategy for Data Centers
White Paper 124

Using Infrared Thermography to Improve Electrical Preventive Maintenance Programs
White Paper 268

Digital Remote Monitoring and Dispatch Services' Impact on Edge Computing and Data Centers
White Paper 237

Browse all white papers
whitepapers.apc.com

Edge UPS Fleet Management Comparison Calculator
TradeOff Tool 27

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

RATE THIS PAPER ★★★★★