Life Is On | Schneider Electric

Practical Guide to Ensuring Availability at Edge Computing Sites

White Paper 280

Revision 0

by Victor Avelar

Executive summary

IT stakeholders recognize the need for computing at distributed sites, where part or all of their business operations take place. Assessing the criticality of these edge sites should reveal which sites are in greater need of availability improvement. Schneider's experience with edge computing environment assessments reveals a list of practical actions that improve the availability of IT operations by improving the physical infrastructure systems supporting the IT. This paper provides specific availability improvements broken down by eight key systems including power, cooling, physical security, environment, and management.

RATE THIS PAPER ★★★★★

Introduction

Deployments for distributed IT are typically relegated to small confined rooms, closets, or even on the office floor. However, as businesses grow and rely more on edge computing applications, IT downtime has a greater impact on the business. An interview with a small food distributor exemplifies this sensitivity. As this food distributor gained more customers, they realized it wasn't possible to fulfill orders accurately and on time without their IT systems. Downtime of these systems would not only interrupt their distribution schedules, but would cause restaurants to place last minute orders. Restaurants need only a few missed deliveries to have a good reason to seek a new distributor. The following are some example causes of downtime that were uncovered in this research:

- The wrong server was unplugged. The IT admin thought he had traced the correct power cord to the tower server. The "rat's nest" of power and network cabling significantly increased the likelihood of this error. Dual-power supplies later became a standard specification for critical IT gear to avoid this type of human error.
- A server error for high temperature forced a shutdown of the system.
- A few pieces of IT gear turned off during a brief power outage. It was later discovered that the equipment was never plugged into the installed UPS. This was most likely due to the disorganized cabling behind the rack.
- A cleaning person unplugged a server to plug in the vacuum cleaner.
- A power outage caused all the systems in a branch office IT rack to go down. The IT admin arrived later to discover that the UPS had been signaling for some time that it had a bad battery that required replacement.

As with many businesses, especially small businesses, it takes a downtime event or a series of close calls to finally invest in improving the availability of IT operations. In many cases, this spurs new IT upgrade projects. An upgrade project is the optimum opportunity to assess the physical infrastructure required to support IT, however, **our research suggests that IT managers often lack the time to research and specify an appropriate solution** and **the plan for deploying it**. We addressed these two needs in two papers. This white paper provides practical guidance on how to **improve the IT availability** at these sites, while White Paper 174, *Practical Options for Deploying Small Server Rooms and Micro Data Centers*, describes a practical plan for **deploying a micro data center** at one or more locations. Furthermore, you should perform a health assessment to ensure old equipment is modernized as discussed in White Paper 272, *A Framework for How to Modernize Data Center Facility Infrastructure*.

Practical availability improvements at edge sites

Before improving your site availability, you first need to know which site to focus on. White Paper 256, *Why Cloud Computing is Requiring us to Rethink Resiliency at the Edge*, provides this guidance to help you identify which site is most in need of availability improvement. Once you've identified the site, you need to choose the availability improvements that make the most sense. Schneider's experience with edge computing environment assessments reveals a list of practical actions to improve the availability of IT operations. This paper provides these improvements in a series of convenient checklists.

These improvements apply to small server rooms and micro data centers with up to 10kW of IT load. **We recommend that you print the checklist in each section and check off all the improvements that you think make sense, while assessing the actual edge site.** When your done going through each checklist, you

should review your choices to make sure they're consistent. For example, it's unwise to spend money on dual power feeds and dual-corded servers, if the cooling system only runs from 9am to 5pm on weekdays. The cooling system becomes the "weakest link" and will likely cause downtime due to thermal shutdown, despite having high-availability power to the servers.

Note that there are plenty of science-based mathematical tools and services available to quantify the availability impact of different practices. If your cost of downtime is high relative to the cost of these types of services, it may make sense to invest in the rigor of a quantitative analysis to inform the design of your edge site.

Improvements are qualitatively ranked in order of highest priority. What does this mean exactly? It means that, relative to a baseline, we think the items towards the top of the list provide more availability for your money. In this paper, the baseline is a stack of IT equipment, sitting on the floor of an open room, powered directly from utility, with only comfort cooling. For example, in the Power category, we think a small rack-mount UPS (without bypass) will greatly improve your availability for a relatively small amount of money. If you had a choice to add a UPS bypass or install a generator, we think you will get more availability for your money by adding a UPS bypass. This is the logic we used for all categories of improvements.

The improvements are organized by the following systems:

- Power
- Cooling
- Rack
- Physical security
- Fire protection
- Environment
- Network connectivity
- Management

Power

This subsystem is arguably the most critical because it powers everything including IT and cooling. **Table 1** provides UPS and generator availability considerations.

Power checklist (Ranked in order of highest priority)

☐ **Connect critical IT loads to UPS (N, N+1, or 2N)** - Li-ion batteries are preferable because of longer lifetime and higher energy density compared to lead-acid batteries. Supply the UPS from a dedicated electrical circuit to prevent other loads from tripping the breaker. White Paper 48, *Comparing Availability of Various Rack Power Redundancy Configurations* quantifies the differences in redundancy options. 2N UPS and power distribution is ideal when used with dual corded loads like servers and domain controller(s). **Figure 1** shows an example of a prefabricated integrated solution in a single 42U enclosure with redundant UPSs.

☐ **Ensure UPS bypass function** - Prevents dropping critical load in the event of an overload or UPS fault. If UPS has no integrated bypass (typically the case for single-phase UPSs), you can add an external bypass module (**Figure 2**), but note that this type of added solution doesn't switch to bypass during UPS overload.

☐ **Connect critical IT and cooling to standby generator** - A generator can provide a significant availability increase, especially in locations with poor power quality. For guidance on this topic, see White Paper 52, *Four Steps to Determine When a Standby Generator is Needed for Small Data Centers*. Note that a UPS is still required to ensure uninterrupted power to the critical loads in the event of a power outage.

☐ **Include a minimum of two maintenance receptacles** - For example 20A (North America) and 16A (Europe) wall-mounted in the IT room to allow easy access to power. Not having available outlets in a room increases the likelihood that people will plug unauthorized equipment into critical IT power receptacles. For example, plugging in a vacuum cleaner could overload the UPS and drop the load.

☐ **Connect maintenance receptacles to generator (if available)** - Allows you to plug in a spot cooler during long power outage. Label it as the generator receptacle, typically with a red color.

☐ **Use remotely switched rack PDUs** - Remotely switch individual outlets on/off to reboot hung servers or keep unused outlets off to prevent powering unauthorized devices.

☐ **Switch to lockable IEC cables for IT loads** - Most IT equipment have detachable power cords, prevents accidental downtime when someone is making changes inside the rack (see **Figure 3**).

☐ **Use locking input connector for rack PDU** - Prevents accidental unplugging of the rack PDU which will drop all loads on it. Plastic zip ties (tie wraps) are a good alternative for non-locking connectors.

☐ **Color code redundant power feeds** - When using dual-corded UPS and IT equipment, color code A and B feed cables and rack PDUs with different colors to avoid human error, e.g. plugging both cords into a single feed (e.g. blue and red or blue and orange can be seen by those that are color blind).

☐ **Bond all rack enclosure doors and panels** - This is about safety, in case any portion of the rack becomes energized, you want the breaker to trip open.

Table 1
UPS runtime and generator considerations for availability

Power improvement	Baseline	Higher availability
UPS redundancy	1N	N+1 or 2N
UPS runtime (with standby power)[1]	<10 min	15 min
UPS runtime (without standby power)[1]	<10 min	30 minutes - 2 hours depending on utility quality

[1] Generator, fuel cell, or other technology to provide power during utility outage

Life Is On Schneider Electric

Figure 1
Example of a 1-rack micro data center with redundancy built in

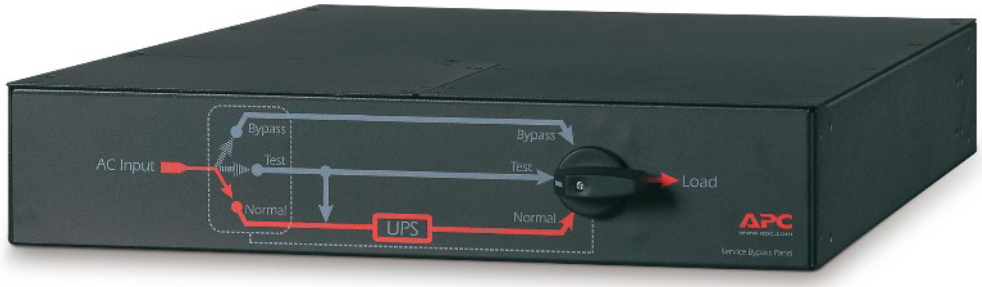

Figure 2
Two examples of bypass switches by Schneider Electric

Figure 3
Lockable IEC C13 and C19 power cords

Building comfort cooling system

Ideally the building's comfort cooling system would cool the IT equipment all year round, but this is not the case in colder climates when the heating system is turned on and the air conditioning is turned off.

Cooling

The primary decision regarding cooling, is to figure out which kind of cooling system best meets your needs. White Paper 68, *Cooling Strategies for IT Wiring Closets and Smalls Rooms* provides a general guideline for cooling strategies based on IT equipment power and target room temperature. In many cases, no dedicated cooling exists to support the IT rooms, resulting in over-heated equipment. Typically, these IT rooms depend on comfort cooling systems (see **sidebar**). With comfort cooling, the IT temperature is rarely controlled by its own thermostat, so lowering the zone temperature to help cool IT gear, would adversely affect people in the surrounding area. The improvements below help to improve the cooling availability.

Cooling checklist (Ranked in order of highest priority)

- ☐ **Use cooling system designed for 7x24x365 operation** - IT equipment runs continuously throughout the year; therefore, your cooling system must be designed to do the same. Set IT inlet temperatures to within ASHRAE's recommended 2015 Thermal Guidelines operating temperature range of 18-27°C (64.4-80.6°F).
- ☐ **Use blanking panels in empty rack U-spaces** - Without these panels, hot exhaust air (from the back of the rack) returns to the air intake, causing hot spots for IT. This practice also helps prevent thermal shutdown events and reduces the need to overcool the space with oversized air conditioners. Not placing IT equipment in a rack, often allows the hot exhaust air of one chassis to blow into the intake of another.
- ☐ **Include a condensate pump** - in cases where the cooling system produces condensate, a pump is required to remove the water from the IT space.
- ☐ **Use redundant fans** - Fan-assisted ventilation systems should have more than one fan for fault tolerance.
- ☐ **Use a UPS to power cooling fans** - Fans draw a small amount of power, in the event of a power outage, fan-assisted ventilation systems will continue to cool the IT equipment. Another option is to place the cooling system on a generator if available.
- ☐ **Use dual power inputs for cooling system** - Some air-conditioning systems come with two power cords for a high-availability. It's best to use this feature with separate dedicated circuits from the distribution panel.

Rack

A rack is the fundamental structure for IT gear that facilitates cooling and enables organization that can decrease human error when troubleshooting problems.

Rack checklist (Ranked in order of highest priority)

- ☐ **Bolt racks in seismic zones** - Either bolted to seismic stand or directly to slab.
- ☐ **Use racks with lockable doors and side panels** - One of the best ways to avoid downtime is to keep unauthorized people away from IT gear.
- ☐ **Use racks with tool-less doors and side-panels** - This feature saves time and reduces accidents associated with dropping things like screws into IT equipment. Removable side panels simplify cable management.
- ☐ **Use racks hinged for either left or right operation** - Sometimes rack location is constrained by things like building columns, which may limit the rack doors to open to the right or left, increasing likelihood of human error.
- ☐ **Ensure wall-mount enclosures can support up to 90 kg (200 lbs)** - IT equipment and UPS(s) add a considerable amount of weight to an IT rack. A properly designed wall-mount enclosure won't fail under this weight.
- ☐ **Use snap-in blanking panels** - Snap-in (no tools required) blanking panels prevent hot exhaust air from recirculating to the front of IT equipment.

Physical security

People are directly responsible for much of the downtime that occurs through accidents and mistakes – improper procedures, mislabeled equipment, things dropped or spilled, and other unforeseen mishaps. If the cost of downtime is significant, then physical security is important even for a small business or branch office. Moreover, physical security is tightly linked to cyber security. If someone gains physical access to IT equipment, cyber security is significantly compromised.

Physical security checklist (Ranked in order of highest priority)

- ☐ **Use locks on IT room and IT racks** - This is a vital method of preventing human error. Keys should only be issued to personnel responsible for IT operations or public safety.
- ☐ **Use sensors on doors** - Whether a door to an IT room or IT rack door, sensor should alert when a door is open.
- ☐ **Place physical security devices on UPS** - This practice ensures security during power outages. For security devices not located within the IT rack, a separate UPS may be required.
- ☐ **Set alert for doors propped open** - If someone props the door open, the management system should alert after a pre-programmed period of time. The longer doors stay open, the higher the chance of unauthorized entry.
- ☐ **Use video surveillance system with DCIM** - The surveillance system should send alarms to the data center infrastructure management (DCIM) system.
- ☐ **Use motion activated cameras** - Recording and storing video when prompted by motion or an alert saves storage space and bandwidth. This allows a visual record to be paired with an access or environmental alert, which speeds up root cause analysis (**Figure 4**). For example, an IT admin can be alerted via SMS or email upon access by unauthorized personnel via door switch or motion detection. Cameras should allow access via smart phone to view images and environmental data.
- ☐ **Use network-based digital recordings** - Using color camera technology with network-based recording protects video footage from tampering.
- ☐ **Integrate video surveillance system with building's CCTV (closed-circuit television) system** - this ensures that critical IT areas are also monitored by building security personnel.
- ☐ **Use biometric access locks** - This prevents someone from lending a key or access card to someone else to open the IT room or IT rack.

Figure 4
Example of single security camera with integrated 2-way audio, door contact, and motion sensor

Fire protection checklist (Ranked in order of highest priority)

- ☐ **Remove flammable materials from IT space** - Things like printer paper, hand towels, paint thinner, etc. are oftentimes stored in the same space as IT equipment (e.g. IDF closets). These items increase the likelihood of downtime due to fire.
- ☐ **Use smoke detection system** - This is typically the same type used in the rest of the building.
- ☐ **Configure sprinkler heads** - When no suspended (drop) ceiling exists, sprinklers should be configured upright. However, when a suspended ceiling is present, use concealed-type sprinkler heads to prevent accidental discharge due to human error (e.g. hitting the head with a broom handle).
- ☐ **Locate fire sprinklers at least 46 cm (18 inches) from the top of equipment** - Fire codes typically require sprinkler heads to be a certain distance from the tops of equipment to allow sufficient water coverage in case of a fire.
- ☐ **Use a pre-action sprinkler system** - In a typical sprinkler system, if the glass bulb is accidently broken, water is discharged immediately. However, pre-action systems prevent water from entering the pipe, unless triggered by a smoke alarm.
- ☐ **Use cross-zone smoke detectors** - This consists of using two different types of smoke detectors. This prevents a false alarm and accidental suppression discharge. A discharge only occurs when both detectors alarm.
- ☐ **Uses addressable fire alarm panel** - Addressable fire alarm panels allow each detector to have a unique identifier, making it easier to identify the physical location of the alarm, thereby decreasing the response time.
- ☐ **Use a clean-agent fire-extinguishing system** - These systems can extinguish flames without the use of water which can damage IT equipment. See White Paper 83, *Mitigating Fire Risks in Mission Critical Facilities*, for more information.

Network connectivity checklist (Ranked in order of highest priority)

- ☐ **Organize network cables** - Human error is more likely when cables are disorganized. Network cable management devices (raceways, routing systems, ties, etc.) make it easier to track cables and also improve airflow through the IT rack. Cable chaos in the networking closets also breeds human error.
- ☐ **Label and color-code network lines** - Oftentimes the wrong cable is pulled because they look like all the other cables in a rack. Cables should be labeled on both ends and color-coded by their use to avoid human error. For example, WAN, LAN, redundancy, out-of-band management, etc.
- ☐ **Add a second network provider** - This can be an expensive improvement but may be required for business continuity at select sites.
- ☐ **Locate redundant network connections at opposite ends of the facility** - Sometimes redundant network lines come into a facility through the same conduit. This significantly reduces the availability gains of redundant network feeds. Routing the feeds far apart (ideally opposite ends of the facility) greatly reduces the likelihood of a common cause network failure (e.g. a backhoe cutting both cables).

Environment checklist (Ranked in order of highest priority)

- ☐ **Dedicate the room for the telecom / IT / network equipment** - Reduces likelihood of human error. For example, using the room as storage space may require access to non-IT personnel.
- ☐ **Guard against harsh environments** - For harsh environments, secure equipment in an enclosure that protects against fire, flood, humidity, vandalism, and EMF effects. For more information, see White Paper 278, *The Three Types of Edge Computing Environments*.
- ☐ **Use steel sleeves to protect cabling** - For cabling that penetrates walls, floors, or ceilings, not installed in conduit, steel sleeves protect the wiring from damage. Use plastic bushings on both ends of the steel sleeve to prevent chaffing the cables.
- ☐ **Seal concrete floors** - Concrete floors should be sealed or painted with at least one coat of a paint, for dust control.
- ☐ **Avoid exterior windows and doors in IT space** - Exterior windows and doors represent a security risk and should be avoided, unless they're required by safety codes.
- ☐ **Avoid access through this room to other rooms** - This isn't always possible (e.g. micro data center in an open office environment). However, where possible, limiting human contact with an IT rack reduces likelihood for human error.
- ☐ **Use self-closing doors** - This prevents others from gaining access to the IT room.
- ☐ **Use fire-rated doors** - Use fire-rated doors consistent with insurance company and lease agreement requirements.
- ☐ **Locate the room above average grade** - This reduces the risk of flooding.
- ☐ **Seal off floor drains** - Existing room floor drains should be sealed off to prevent sewer gases from entering the room.
- ☐ **Ensure drainage of condensate from cooling system** - The condensate drain piping should be gravity fed or, if not possible, use a condensate pump.
- ☐ **Oversize condensate pipes** - Oversizing pipes by one size above design requirements decreases the likelihood of water damage due to clogs.
- ☐ **Install bleed / snake access fitting** - Where condensate pipe layouts have 90-degree turns, installing a snake fitting simplifies clearing clogs that tend to occur at bends.
- ☐ **Locate the room away from water sources** - Don't locate the room below lavatories, washrooms, break room areas, etc. to avoid the risk of water damage.
- ☐ **Divert plumbing and piping away from IT room** - When IT relocation is not possible, piping that is separate from the cooling or fire suppression systems should be diverted away from inside, overhead, and perimeter of the room.

Management

Given that edge computing installations are typically remote and lack IT personnel, remote management is a critical component to maintaining uptime. Monitoring is accomplished through a data center infrastructure management (DCIM) system. For more information on this topic see White Paper 281, *Essential Elements of Effective Edge Computing Infrastructure Management*. **Figure 5** shows an example of management devices for remote sites.

Management checklist (Ranked in order of highest priority)

- ☐ **Use a remote monitoring platform** - This is especially valuable for organizations with many distributed remote sites such as retail, oil fields, or large automotive manufacturing facilities. See White Paper 237, Digital Remote Monitoring and How it Changes Data Center Operations and Maintenance, for more information on how remote monitoring can help reduce downtime.
- ☐ **Monitor at least one temperature sensor at the front of the rack** - Typically at the top, but ideally you would use three (top, middle, and bottom of rack). If temperatures are trending upward over time, there may be something wrong with the cooling system that requires inspection.
- ☐ **Monitor UPS** - UPS systems with integrated management capability allow critical remote UPS monitoring such as low battery, bad battery, on battery, overload, low runtime, etc. For example, if UPS load is trending upward over time, and no new loads have been added, this could be a sign that a particular load (e.g. server, fan) is malfunctioning or nearing failure.
- ☐ **Monitor dry contact sensors** - These sensors are typically used to detect when a rack door or room door is open.
- ☐ **Monitor leak detectors** - This is important when condensate pumps are used for cooling systems. These should also be used in cases where the IT racks are in close proximity to a water source such as a water pipe, or when below grade.
- ☐ **Monitor at least one humidity sensor at the front of the rack** - Typically at the top. If humidity is trending upward over time, there may be something wrong with the cooling system or a source of moisture entering the room.
- ☐ **Monitor motion sensor** - These sensors help to alert management when someone is in the IT room. A good security camera automatically detects motion and begins capturing video.
- ☐ **Monitor vibration sensors** - Excessive vibration can damage circuit boards and other components over time. Monitoring vibration trends can alert management of an otherwise “invisible” threat to IT availability.

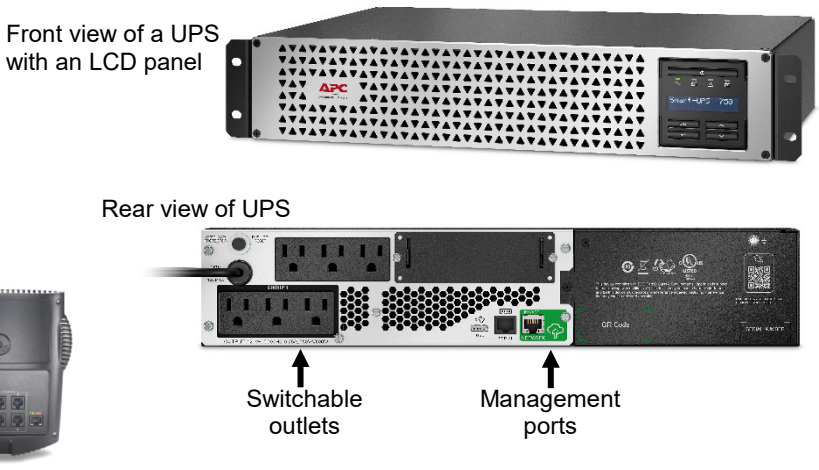

Figure 5
Example of a management-enabled UPS with li-ion batteries and switchable outlets.

Example of camera with integrated temperature, humidity, airflow, dewpoint, and camera motion sensors.

General practices

In addition to improving the availability of the systems discussed above, it's also important to follow these general practices, to improve the availability at edge sites.

General practices checklist (Ranked in order of highest priority)

- ☐ **Provide electronic and printed user manuals** - this simplifies the maintenance of all physical infrastructure equipment. As augmented reality tools (e.g. smart glasses) become more prevalent, they may replace manuals as a maintenance tool.

- ☐ **Ask manufacturers to provide a spare parts inventory list** - Having spare parts of critical systems on hand (preferably close to critical sites) significantly decreases mean time to repair (MTTR). If parts can't be stored close by, contract with a shipping logistics company for rapid delivery. The spare parts inventory should include components whose procurement lead times exceed the maximum acceptable downtime period for the associated system.

- ☐ **Train onsite personnel to reduce IT downtime** - Training should bring onsite personnel (e.g. factory workers, cashiers, managers, etc.) to a minimum level of competency regarding the criticality of IT systems and what to do in case of IT downtime. If any work is to be performed on critical IT systems, it should be authorized by the IT department. The training should also cover the process for assuring that outside contractors are aware of infrastructure that support critical IT systems, to avoid downtime.

- ☐ **Label all support systems directly connected to edge IT loads** - Remote IT sites are usually a small part of a larger group of systems, depending on the industry. As such, work that occurs on these non-IT systems may inadvertently cause IT system downtime. Therefore, labeling electrical circuits, piping, video wiring, etc. helps to avoid potential IT downtime. Labeling should clearly communicate that the breaker, wire, feed, etc. are part of the critical IT system, and may even instruct someone to call the IT department before performing any work.

Conclusion

Edge computing typically involves many distributed IT sites. Making simultaneous availability improvements to all sites quickly escalates capital expenses. Therefore, before improving availability of any edge computing site, you first need to know which site to focus on. White Paper 256, *Why Cloud Computing is Requiring us to Rethink Resiliency at the Edge*, provides this guidance to help you identify which site is most in need of availability improvement. Once you've identified the site, this paper provides a list of availability improvements in a series of convenient check-lists. We recommend that you print the checklist in each section and check off all the practices that you think make sense, while assessing the actual edge site. This process can save a significant amount of time to research and specify individual practices.

About the author

Victor Avelar is the Director and Senior Research Analyst at Schneider Electric's Data Center Science Center. He is responsible for data center design and operations research, and consults with clients on risk assessment and design practices to optimize the availability and efficiency of their data center environments. Victor holds a bachelor's degree in mechanical engineering from Rensselaer Polytechnic Institute and an MBA from Babson College. He is a member of AFCOM.

RATE THIS PAPER

Resources

Comparing Availability of Various Rack Power Redundancy Configurations
White Paper 48

Four Steps to Determine When a Standby Generator is Needed for Small Data Centers
White Paper 52

Cooling Strategies for IT Wiring Closets and Smalls Rooms
White Paper 68

Physical Security in Mission Critical Facilities
White Paper 82

Mitigating Fire Risks in Mission Critical Facilities
White Paper 83

Monitoring Physical Threats in the Data Center
White Paper 102

How Monitoring Solutions Reduce Human Error in Distributed Server Rooms and Remote Wiring Closets
White Paper 103

Guidelines for Specifying Data Center Criticality / Tier Levels
White Paper 122

Practical Options for Deploying Small Server Rooms and Micro Data Centers
White Paper 174

Why Cloud Computing is Requiring us to Rethink Resiliency at the Edge
White Paper 256

Essential Elements of Effective Edge Computing Infrastructure Management
White Paper 281

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

© 2019 Schneider Electric. All rights reserved.