How to Build Maximum Availability into Edge Data Center Infrastructure

Easy-to-follow checklists and deployment guide

apc.com/partnerlocator

Life Is On Schneider Electric

INTRODUCTION

How to Build Maximum Availability into Edge Data Center Infrastructure

Edge computing is growing in popularity thanks to its ability to reduce latency and save on the cost of upgrading or building new large, traditional data centers. These edge deployments are often housed in small, confined rooms, IT closets, or in other environments that weren't really built to house IT equipment. Edge data centers like these require a supportive infrastructure to protect them from expensive downtime caused by both the unique hazards of these environments and human error.

A couple examples of real-world obstacles edge data center deployments have encountered are:

- Accidentally unplugging the incorrect server cord. Disorganized clumps of cords increase the chance of this, but the cause could also be as simple as cleaning personnel unplugging a server so they can plug in cleaning gear. Dual-power supplies for critical IT gear can help avoid this mishap.
- Gear that hasn't been plugged into the installed UPS affected by power outages. Again, disorganized clumps of cords increase the chance of this.

Today's IT managers don't often have the time to research and specify a physical data center infrastructure solution and deployment plan. This eBook includes all the information you need to quickly and easily put together a sound plan for your edge data center upgrade or deployment. Our health assessment can help you ensure that your older equipment is modernized. Plus, our easy-to-follow checklists and deployment guide will save you a lot of time researching and specifying choices for specific pieces of your data center infrastructure.

Assess the Health of Your Data Center Infrastructure

When physical data center infrastructure systems approach the end of their useful life and programs become outdated, your risk of significant downtime increases. To minimize this risk, you should modernize those systems or have them outsourced to the cloud/colocation service providers. Modernization will also make managing your data centers simpler, more efficient, and more cost effective.

In just a couple of steps, you can assess the health of your data center infrastructure to see what's performing well and what could use an upgrade.

Step One: Identify Performance Standards

Business and IT objectives should drive your data center infrastructure requirements. The requirements for an existing site may have changed since its original deployment, so it's important to re-evaluate each site regularly for today's evolving needs. Energy efficiency or carbon emission standards and mandates are a good example of recently evolving needs.

As you begin defining your performance standards, think about these key drivers:

- Cost/risk of downtime to the business, both tangible and intangible costs
- CapEx and OpEx budgets and/or cost reduction initiatives
- Sustainability initiatives like carbon reduction or PUE targets
- Industry expectations (what are your peers doing?)

There are often trade-offs to be made between highly available systems, highly efficient systems, and cost. The budget is usually a constraint, but methodically charting this iterative process can help justify larger budgets and align project scope.

If you have multiple sites serving a variety of business functions at varying levels of criticality, you can approach developing standards in different levels or tiers for a more tailored approach.

Step Two: Benchmark Performance & Identify Health Risks

Now that your performance standards are identified, you can begin comparing your edge deployments to find areas where the new standards aren't met. This step involves:

- Physically investigating infrastructure equipment
- Collecting device data
- Verifying interconnections
- Tracing electrical circuits
- Piping mechanical connections
- Reviewing methods of procedure and training documentations for operations and maintenance teams.

These steps help you identify exactly what loads are plugged in where, current redundancy levels, runtime availability, and more. Drawings and written reports often become outdated as changes are implemented in the data center, and should be updated as soon as they are identified. The DCIM should also be checked against your new benchmarks.

Next, perform a basic health check to identify systems at risk. A basic table comparing as-is to the desired performance standard, with risk scores for each row. Here's what to evaluate:

- Age of devices and warranty status
- Maintenance history and service contract status
- Current load vs. capacity

If loads have grown since the last upgrade, systems may become overloaded. Conversely, if loads have become virtualized or outsourced over time, your system may be oversized and it may save you money to reduce some operations.

DCIM monitoring tools can be helpful in identifying health risks. You can run reports to identify units out of warranty, units that fail a self-test, etc.

Checklists for Specifying and Deploying Your Data Center Infrastructure

Now that you have an idea of which areas to focus on for upgrades, it's time to start forming a holistic plan. Even if you are planning for a brand new deployment, you can use the following checklists to start from scratch. Checklist items are ranked qualitatively in order of highest priority — items toward the top of the list provide the most availability improvement for your money. These checklists are edge-specific and apply to small server rooms and micro data center infrastructure with up to 10kW of IT load. The baseline is a stack of IT equipment, sitting on the floor of an open room, powered directly from utility with only comfort cooling.

Power

This is the most critical aspect because it powers everything, including IT and cooling.

Power for small server rooms consists of a UPS and power distribution. UPS systems greater than approximately 6kVA are typically hardwired from an electrical panel. Installing a new receptacle or hardwiring requires an electrical contractor. If this is not a possibility, an alternative approach is to use multiple lower-capacity UPS systems.

There are two basic power distribution methods:

- Plug IT gear into the receptacles on the back of the UPS
- Plug IT gear into a rack power distribution unit (rack PDU) which is plugged into the UPS (requires IT gear to be mounted in a rack)

Redundant UPS systems are recommended for critical dual-corded gear, like servers and domain controllers. They should be plugged into a separate UPS or rack PDU. We recommend UPS systems with an integrated network management web card because they allow for critical remote UPS monitoring like low battery, bad battery, overload, low runtime, etc.

For more information on UPS topology, see our white paper 1, The Different Types of UPS Systems. Following is the checklist to use when specifying your power systems.

Power Checklist

- ☐ **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. Our white paper 48, Comparing Availability of Various Rack Power Redundancy Configurations quantifies the differences in redundancy options.

- ☐ **UPS has no integrated bypass (typically the case for single-phase UPSs), you can add an external bypass module, but note that this type of added solution doesn't switch to bypass during UPS overload.** Connect critical IT and cooling to a standby generator. A generator can provide a significant availability increase, especially in locations with poor power quality. For guidance on this topic, see 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 a generator (if available).** Allows you to plug in a spot cooler during a 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 which prevent accidental downtime when someone is making changes inside the rack.

- ☐ **Use a locking input connector for the 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 who 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.

Cooling Checklist

Our white paper, Cooling Strategies for IT Wiring Closets and Small 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. These rooms depend on comfort cooling systems, and IT temp is rarely controlled by its own thermostat. Lowering the zone temp to help cool IT gear adversely affects the people in the surrounding area, which is especially a problem in areas with colder climates where the AC may be off and heating is on. Here is the checklist to use when specifying your cooling systems.

- ☐ **Use a 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 the cooling system.** Some air-conditioning systems come with two power cords for high availability. It's best to use this feature with separate dedicated circuits from the distribution panel.

Rack Checklist

The rack is the fundamental structure for IT gear that facilitates cooling and enables greater organization to decrease human error during troubleshooting. It's difficult for small businesses to justify the extra cost of an enclosure, but when the decision is part of an overall upgrade project, it becomes easier to do it right.

Objectives like availability, organization, cable management, physical security, cooling effectiveness, ease of power distribution, and professionalism are all offered by a well-designed rack enclosure. A rack is the fundamental structure for IT gear that enables organization, which can decrease the instances of human error when troubleshooting a problem. For example, cable management becomes easier with integrated accessories so wiring doesn't turn into a rat's nest. Removable side panels also improve the ease of cable management.

Rack enclosures are recommended with loads greater than 2kW because they help isolate the hot and cold air streams which means the IT equipment is breathing in cooler air (blanking panels are also key to improved air flow). Without the side panels or doors, enclosures become a 4-post rack, which does nothing to separate the air streams. However, if 4-post racks are used, blanking panels are recommended as well. An enclosure's locking doors also provide physical security — critical in open office areas or unlocked server rooms. This is a big problem in cases where the door is purposely left open to cool the room. Here is the checklist to use when specifying your rack setup.

- ☐ **Bolt racks in seismic zones.** Bolt to either a seismic stand or directly to the 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 UPSs 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 Checklist

Physical security breaches are responsible for much of the downtime that happens through accidents or mistakes — improper procedures, mislabeled equipment, things dropped or spilled, etc. If the cost of downtime is high, then physical security is important even for small businesses or branch offices because it is also tightly linked to cyber security — if someone gets physical access to equipment, cybersecurity is compromised. Here is the checklist to use when specifying physical security options.

- ☐ **Use locks on the 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, sensors 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 a 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. 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.

Fire Protection Checklist

Here is the checklist to use when specifying options to protect your IT equipment from fire hazards.

- ☐ **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 a 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 accidentally 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 send an alarm.
- ☐ **Use an 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 our white paper 83, Mitigating Fire Risks in Mission Critical Facilities, for more information.

Infrastructure Environment Checklist

Here is the checklist to use when specifying options to protect the infrastructure environment of your IT equipment.

- ☐ **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 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 chafing the cables.
- ☐ **Seal concrete floors.** Concrete floors should be sealed or painted with at least one coat of 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 the 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 the IT room.** When IT relocation is not possible, piping that is separate from the cooling or fire suppression systems should be diverted away from the inside, overhead, and perimeter of the room.

Network Connectivity Checklist

Here is the checklist to use when specifying options for optimal network connectivity.

- ☐ **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).

Management Checklist

Since edge computing deployments are typically remote and lack IT personnel, remote management is critical for maintaining uptime. Monitoring happens through a DCIM system — for more information on this topic, see Essential Elements of Effective Edge Computing Infrastructure Management.

- ☐ **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. Read 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.

General Practices Checklist

- ☐ **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 also needs to 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 must 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.

Expert Guidance in Edge Data Center Infrastructure

Our experience with thousands of data rooms of small businesses and branch offices reveals that most of them are unorganized, unsecure, hot, unmonitored, and space constrained. It is also clear that these situations often result in avoidable downtime and inconvenience. IT managers in these environments have little time to research physical infrastructure best practices -- that's why we're here to help.

Schneider Electric's proven industry leadership, combined with our large community of IT partners, has resulted in collaborative technology that delivers connectivity, reliability, and accessibility through simplified delivery and expert services. We can serve as your trusted partner, helping you reap all the benefits of on-premise edge micro data center solutions to the fullest. Our EcoStruxure Micro Data Center solutions offers a complete IT infrastructure within a stand-alone, secure enclosure for protection of critical business applications, and includes power distribution, UPS, and environmental monitoring. It's fast to deploy, secure, standardized for reliability, and cost effective.

Contact us today to learn more. We can schedule a discovery meeting to develop a comprehensive solution-based proposal that supplies your business with exactly what it needs.

Contact Schneider Electric

Shop Our Micro Data Center Solutions

Life Is On | Schneider Electric

We can help you tackle anything, from basic preventive services all the way to redesigning your permanent IT backbone.

Call us at 1 (877) 800-4272 to get started, or check out our partner selector tool to find a partner ready to support you.

apc.com/partnerlocator

APC by Schneider Electric

Boston One Campus
800 Federal Street
Andover, MA. 01810 USA
Phone: + 1 976 794 0600

www.apc.com