

Three Types of Edge Computing Environments and their Impact on Physical Infrastructure Selection

White Paper 278

Version 1

by Wendy Torell

Executive summary

Edge computing deployments are on the rise, as more and more use cases are conceived for local compute, storage, and networking. Although there are fundamental needs of all edge compute sites to ensure availability, environmental differences can be significant which impact the specific attributes of the systems you deploy. It's important to understand characteristics like ambient temperature & humidity conditions, security / access of the space, and purpose of the space, as these parameters drive your choice of physical infrastructure. Sites with greater business risks warrant more robust infrastructure. In this paper, we define three types of environments for micro data centers: (1) IT environments (2) commercial & office environments, and (3) industrial & harsh environments. We discuss the challenges of each and share best practices for physical infrastructure deployments for each environment.

RATE THIS PAPER



Introduction

With growing use cases for real-time processing, businesses today must depend on the local edge for compute, data, and storage close to or at the point of consumption. In White Paper 256, [Why Cloud Computing is Requiring us to Rethink Resiliency at the Edge](#), we discuss the hybrid data center architectures that exist now, and the importance of ensuring these edge sites are designed in a resilient way. There are fundamental physical infrastructure needs that all local edge sites require, to ensure the availability of the business processes. These include:

- **Physical security** – a secure space to avoid malicious or accidental downtime incidents of the IT equipment
- **IT rack enclosure(s)** – to house the IT equipment (servers, storage, networking, and any other systems/controls that serve a critical function)
- **Environmental separation** – protection from fire, water, and other environmental risks in the space (i.e. contaminants)
- **Power infrastructure** – a reliable power source (i.e. UPS, generator), and power distribution to the IT equipment
- **Cooling infrastructure** – temperature/humidity control to ensure IT equipment operates within expected range
- **Management** – a means of monitoring/maintaining the physical infrastructure assets at the site

White Paper 280, [Practical Guide to Ensuring Availability at Edge Computing Sites](#), provides specific improvement recommendations and considerations. While the above needs are applicable across all edge sites, the business risks vary significantly from one type of environment to the next. Greater risks warrant more robust solutions. We classify the risks in two ways:

1. **IT downtime risks** – downtime of the IT equipment resulting from security gaps, environmental conditions being out of tolerance for the IT equipment, or failures of physical infrastructure systems.
2. **Non-IT risks** – adverse impact on employee productivity and/or customer experience, when the IT equipment resides in a shared space due to factors like noise, aesthetics, space constraints, and other factors that could impact business outcomes.

In this paper, we define three categories of edge environments (**Figure 1**) – IT, commercial & office, and industrial & harsh, which have distinct challenges and needs based on the above two risk types. The figure shows them in order of growing risk factors from left to right.

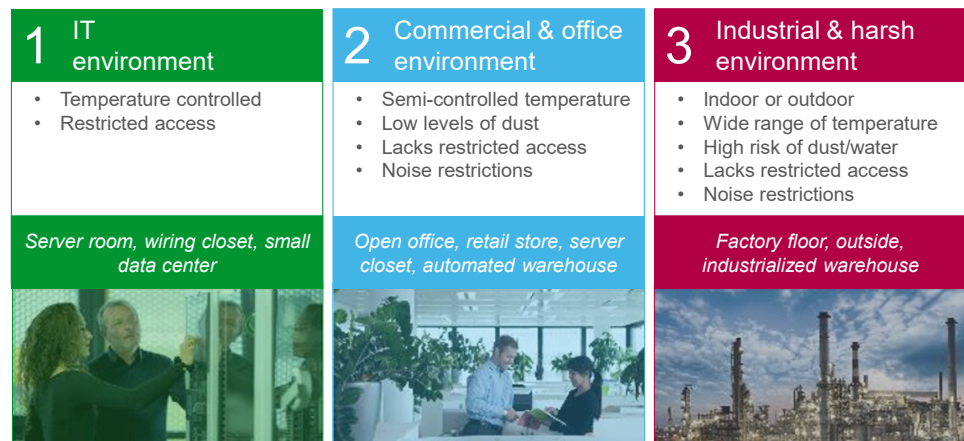


Figure 1
Three types of edge environments with distinct challenges and needs

Note, these environments are independent of both the industry deploying the infrastructure as well as the edge computing application being deployed. Most industries have edge computing applications that cross all three types of environments. **Table 1** illustrates some examples.

Table 1
Examples of industries that span all three edge environments

Industry	IT	Commercial / Office	Industrial / harsh
Automotive	R&D centers	Dealerships	Manufacturing plants, Industrial IoT
Retail	Regional offices	Retail stores	Warehouses, distribution centers
Oil & gas	Research parks	Gas stations	Refineries, oil-fields
Defense	Permanent military bases, military academies	Recruiting offices	Battlefields
Telco	Central offices, headend facilities	Telco retail outlets	Cell tower base stations
Transportation	Regional centers	Train ticket offices	Train signaling control

In the following sections, each of the three environments is described in detail, along with unique needs and recommended attributes to look for in physical infrastructure systems to support your edge compute applications. The first environment is considered the “baseline” environment, since it’s the most protected and controlled environment for IT devices to reside. The other two environments build from that baseline, meaning they have the same fundamental needs but have added challenges, risks and constraints. The term “micro data center” is used throughout the paper, and refers to a self-contained, secure computing environment at the local edge, that is typically a single rack.

1 - IT environment

The first environment is the IT environment. An IT environment at the edge is defined as a **temperature-controlled location** that is **secure with restricted access**. It is a **dedicated space, designed for the purpose of securely housing the edge IT/networking equipment**. This is often a single rack of equipment but may be multiple racks. Think of traditional network closets, wiring closets, or a small computer room in buildings; except these spaces are now often housing greater compute power and more business-critical equipment which require a high level of resiliency and provides connectivity/interaction with a broader data center architecture (it is not operating as an island).

Because this environment is designed to house business-critical IT equipment, the staff allowed in this space are generally limited to a small number of authorized employees. If the site is a regional corporate office or a university campus, the onsite staff may be IT-trained, but for commercial and industrial applications, there is often no knowledgeable IT staff on-premise. In those situations, a general facility employee or a manager may have access to the space in order to be the liaison in addressing equipment failures or maintenance needs that arise.

Key considerations

Physical security – In White Paper 82, [Physical Security in Mission Critical Facilities](#), we discuss important considerations in mapping out your physical security plan for a site. The more controlled levels of access that exist (i.e. perimeter, building, room, rack), the lower the risk of a physical breach. For an IT environment at the

edge, it is recommended that the IT room access is limited to a minimal number of authorized personnel. These should be the people that are managing/working on the IT and physical infrastructure equipment within the room. Note, insufficient physical security can lead to cyber security risks as well, but these are not covered in this paper.

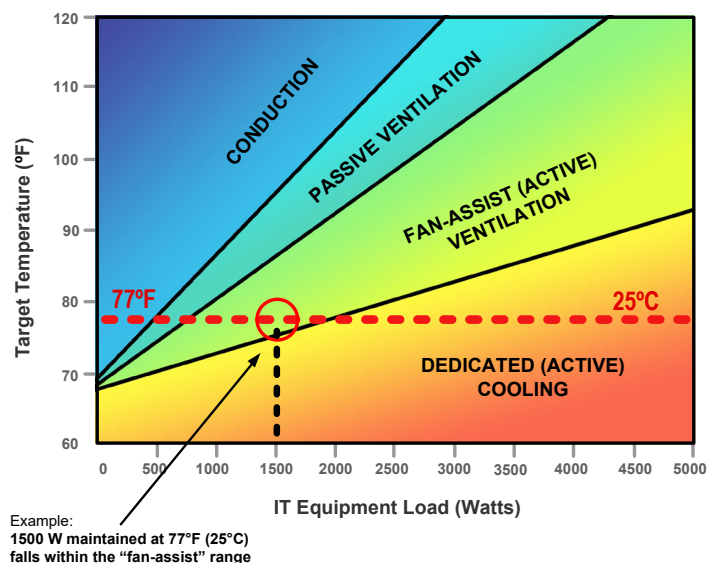
IT rack enclosure(s) – Although the room has controlled access, it is also a best practice to limit the IT access to those who need to get into a particular rack(s) of equipment. For this reason, a rack with doors and a lock, vs an open rack, is advised. Racks come in a wide range of sizes – different widths and heights based on the size and number of IT devices being placed within it. No special environmental ratings should be required since the space is designed to be protective of the IT equipment. White Paper 201, [How to Choose an IT Rack](#), discusses key size and feature options for IT racks and criteria for selection.

Environmental separation – Sensors are key to detecting potential environmental problems in a space. Fire detection and suppression is necessary. See White Paper 83, [Mitigating Fire Risks in Mission Critical Facilities](#), for best practices. Water leaks are less likely in this type of environment, but still a possibility, so a water sensor at the bottom of the rack(s) can be helpful in early detection of a problem, particularly in cases where active cooling is present. A security camera to monitor the space is also a best practice, even though the space is secured.

Power infrastructure – A UPS is an important element to ensure resiliency of local edge IT installations, especially sites with poor utility power quality. UPSs using lithium-ion batteries are of growing interest because of their longer life expectancy (> 10 years) compared to traditional valve-regulated, lead-acid (VRLA) batteries. Although there may be trained staff at an IT environment, li-ion batteries still offer the benefit of reduced maintenance needs which can be costly and disruptive. White Paper 266, [Battery Technology for Single Phase UPS Systems: VRLA vs. Li-ion](#), provides a comparison and TCO analysis of the two battery approaches.

Cooling infrastructure – Having temperature control does not necessarily mean having a dedicated active cooling system. In White Paper 68, [Cooling Strategies for IT Wiring Closets and Small Rooms](#), we present a guide to selecting the right type of cooling (see **Figure 2**) for small IT spaces. The paper describes the various ways to cool, including conduction, passive-ventilation, active-ventilation, and dedicated cooling.

Figure 2
Cooling method guide
based on power load and
target room temperature



Many edge compute sites are still low enough density where fan-assisted (active) ventilation can be used to ensure the temperature remains within tolerance. For example, if the goal is to maintain the IT environment at 25°C (77°F), then a load exceeding approximately 2 kW/rack would require dedicated or active cooling, like a DX system or chilled water system (if available in building). Keep in mind this is meant for directional guidance. Actual points will vary based on specific room attributes. It is also important to understand the operating schedule of the building's comfort cooling system; some run 24x7, while others are turned off when staff leave at the end of the work day and/or certain times of the year. Confirming set points of the comfort cooling throughout days/weeks/year will determine if a dedicated system for the IT room is needed as the density climbs.

Management – Monitoring the IT environment is important to ensuring resiliency. Even in a secure IT environment, breaches are possible, equipment fails, IT devices need a reboot, maintenance is needed, and so on; White Paper 281, [Essential Guidance on DCIM for Edge Computing Infrastructure](#), provides guidance on management systems for the local edge.

2 - Commercial & office space environment

The second environment is a commercial and office space environment. This is defined as one that has **semi-controlled temperature and low levels of dust**. The space likely **lacks restricted access** since **the space has another primary function**. Employees and even customers may be in the space where the equipment resides. Simply put, this is not a dedicated IT space, so the primary function of the space needs to be factored in. Two examples – a medical care room, and a business' conference room – are illustrated in **Figure 3**. There are many other examples, however, such as an automobile dealer showroom or a retailer break-room.



Figure 3

Examples of commercial and office space environments

Note, the practices discussed in the previous section apply to this environment, unless otherwise noted. Here we discuss the **additional challenges, risks and constraints** that must be considered since the IT equipment resides in a shared space that has another primary function. Both IT risks and non-IT risks (as described in the introduction) exist here.

Five constraints in commercial & office environments

There are five key constraints that come into play when the IT equipment is placed in a commercial and office environment. The first four, aesthetics, noise restrictions, thermal comfort, and space constraints are what we define as “non-IT risks” as they could impact customer and/or employee satisfaction; and the last, physical security, is an “IT risk” since it impacts likelihood of downtime.

Aesthetics – Although hard to quantify the importance of aesthetics, when equipment is co-located with employees and even customers or patients, the appearance of the equipment is an important design criterion. No one wants an eye sore in a

public space. Businesses want the appearance of being professional, organized, and to be visually appealing. Obviously, a rat’s-nest of cables hanging out of a stack of visible IT equipment in a metal frame is not likely to give that impression. There are enclosures designed to address this need, and blend discretely into an office environment as office furniture, such as the examples illustrated in **Figure 3**.

Noise restrictions – Generally, if you have an aesthetics need because the space is open to employees and customers, you also have a need to limit the noise coming from the IT equipment. But *even if* a site is ok with poor aesthetics, there still may be a need to manage the noise level if employees work close to the IT equipment, since the fan noise can be disruptive.

We often hear of acoustic requirements or human tolerance to sound levels in terms of decibels (dBA). Average background noise of an office is approximately 50dBA. Normal conversation is around 60dBA. The IT fans of 4-8 low form factor servers (1-2U) with average CPU loads fall in the range of 65-68dBA. Add in cooling fans and the noise level is even higher.

In a commercial or office space, these levels can be very frustrating, distracting, and annoying to employees or customers. It is therefore best practice to house equipment in an enclosure with acoustic material lining for noise dampening (**Figure 4**).



Figure 4
Example of an enclosure with noise dampening material inside

As **Figure 5** illustrates, such an enclosure can reduce the noise level of IT equipment to below that of average background office noise, allowing the equipment to be placed in an open populated space.

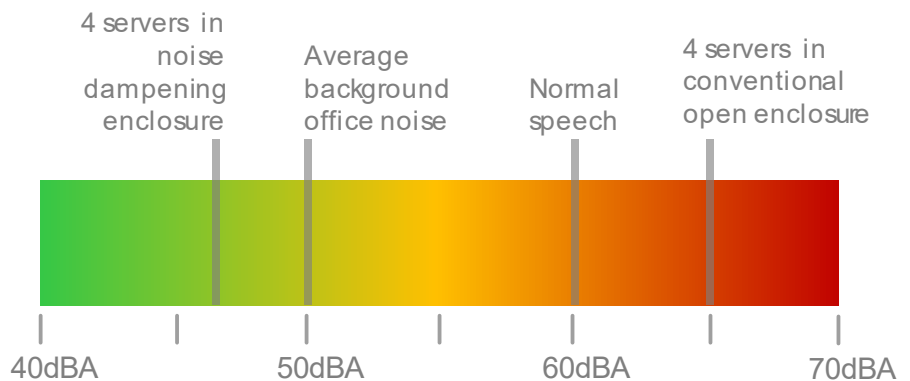


Figure 5
Reduction of IT equipment noise level (4 servers) with noise dampening enclosure, (based on [study of Schneider Electric Netshelter CX enclosure](#))

Thermal comfort – Just like noise, heat output impacts human comfort. According to [ASHRAE 55-2017](#), a comfortable work environment ranges between 19°C (67°F) and 28°C (82°F). A narrower range for a particular work space is further determined based on a model that factors in relative humidity, season, type of clothing worn, type and level of activity, and other factors.

Most comfort cooling systems are designed to provide on the order of 54 watts/m² (5 watts/ft²) of cooling, which equates to 150 watts / rack (assuming 2.8m²/rack or 30ft²/rack). Room size has a big impact on this, meaning for example that a small office would heat up much faster than a large call center floor or retail store front.

For micro data centers deployed in a space with comfort cooling, power density becomes the critical variable. Enclosures exist that provide active ventilation of the IT equipment (**Figure 6a**), but this is only effective up to a certain density (our testing concludes a limit of 3.6kW per enclosure). Beyond this, some form of supplemental heat rejection (i.e. a split system air conditioner) is likely necessary to keep the IT equipment operating within ASHRAE limits and while keeping the ambient occupied space within desired limits (**Figure 6b**).

(a)



(b)



Figure 6

(a) Example of IT enclosure with ventilation fans in rear door

(b) Example of IT enclosure with integrated rackmount cooling unit

Space constraints – For many businesses, real estate within a building is a sparse resource. Companies generally want to maximize use of their space to serve their primary business function, while minimizing space used for support functions and systems. In the case of retail, for example, store fronts try to maximize the footprint of sellable products. It's not uncommon to find small multi-purpose rooms to serve a range of support functions – so in the case of the retail example, a small back room may be the break room, the office supply closet, the safe room, and the IT room, all in one.

With floor space coming at a premium, wall-mount rack options should be considered for the IT equipment, when feasible. A growing number of wall-mount options exist to get the IT equipment off the floor and mount them to minimize protrusion from the wall. Not only do you benefit from consuming zero-footprint, but you also reduce the likelihood of human error or security breaches because the equipment is not as reachable. In addition, the heat output from the enclosure is further away from people. **Figure 7** is an example of a wall-mount micro data center.

Figure 7

Example of 6U wall-mount micro data center



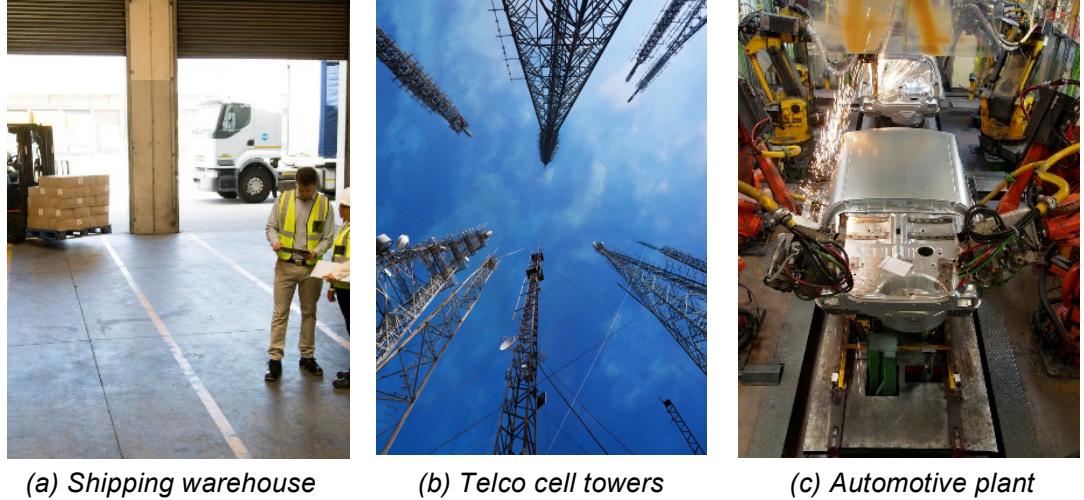
Physical security – When the IT equipment is in an occupied “common” space, you lose the concentric circles of protection that you have when the IT equipment is in a dedicated secure room. People can now walk up to it, touch it, leading to malicious or accidental downtime. It is therefore crucial that the IT enclosure housing the equipment be locked, with limited access.

Placement should be in an inconspicuous location, with security camera coverage, even in the case of locked enclosures. Since the rack is now in a foreign environment, it is also advisable to configure the enclosure with dry contacts, so you get alerted whenever the doors open. A wall-mounted enclosure placed high on the wall adds a level of protection because a person with malicious intent would have to get on a stool or ladder to reach it.

3 - Industrial & harsh environment

The third environment is an Industrial & harsh environment. This is an **indoor or outdoor location with less controlled ambient conditions**, such as a wide range of temperature and humidity, a high degree of dust or other contaminants, and the potential for water. As with the office and commercial environment, this type of environment will likely **lack restricted access**. It’s important to note that not all harsh environments are the same. There are degrees of harshness, so we can’t paint with a broad brush when talking about challenges or solutions here. **Figure 8** illustrates examples of industrial/harsh environments, across the spectrum.

In this section, we describe the common risks associated with placing micro data centers in harsh environments, and considerations for addressing them. Not all will likely apply to your environment, so it’s important to identify those that are, as to not specify a more robust solution than necessary.

**Figure 8**

Examples of industrial / harsh environments



Potential risk factors in industrial & harsh environments

When evaluating each of these risk factors, the goal is to isolate the IT equipment from the environment. In other words, it is necessary to create a new micro-environment that is suitable based on the specs and tolerances of the IT equipment. Oftentimes this is standard, non-hardened IT equipment that would otherwise be placed in a controlled IT room.

Temperature/Humidity – There are two considerations when it comes to temperature and humidity: extreme highs or lows; and rapid changes, both which can impact the reliability and life of the IT equipment. Think about an open warehouse, where the variable outdoor conditions are in direct contact with equipment within the space; or think about an arc furnace in a metal casting factory turning on and heating up equipment located in close proximity. In cases like these, you may need a dedicated air conditioner to keep the micro data center temperature and humidity regulated. There are micro data center solutions that have a self-contained air conditioners that are either self-contained or exhaust to the building HVAC system. An example of a ruggedized enclosure with self-contained DX cooling is shown in **Figure 9**.

Figure 9

Ruggedized micro data center with self-contained air conditioner



Water/Leaks – Water and standard IT equipment don’t mix. It’s important to consider the likelihood and severity of water impacting the function of your micro data center. If it’s placed in a warehouse or factory near or under a water main line, or with water pipes overhead, you may want to ensure some sort of umbrella or “hood” to protect it. If your micro data center is outdoors (like a pole-mounted rack), a more robust enclosure would be necessary – since it would now be subjected to rain.

IEC standard 60529, also called the Ingress Protection or the IP code, classifies and rates the level of protection against water (and solids/dust, which will be discussed with the next risk factor). **Figure 10** is a reference guide to these IP ratings¹. The second number in the IP rating syntax tells you how protective the system (in this case a micro data center enclosure) is from water. We discuss the first number in the next section as it relates to dust. A rating of “0” means no protection from water; a rating of “5” protects against water jets in all directions; and the highest rating of “8” is protective for a submerged system. Industrial applications often request IP ratings of IP54 or IP55, meaning a water protection rating of “4” or “5”.

Note, an alternative rating system for defining the level of protection of enclosures is the **NEMA rating**, used primarily in North America. This standard serves the same purpose as the IEC standard.

Make sure you know the risks and implement the appropriate IP rating for that environment. An over-specified solution will come at a cost premium. There are often-times more basic lower cost solutions that can eliminate the risks (like a hood for an enclosure if the water risk is strictly from potential leaks overhead).

Also note that not all enclosures have been tested against the IP code, but that doesn’t mean it isn’t protective against some of these conditions. Look for enclosures that are designed with a sealed roof design to keep water from leaking/pooling.

¹ https://www.schneider-electric.com/resources/sites/SCHNEIDER_ELECTRIC/content/live/FAQS/176000/FA176928/en_US/Degrees%20of%20protection%20IP,IK,%20NEMA.pdf





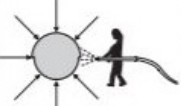
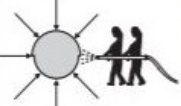
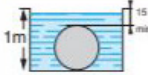

SOLIDS			WATER		
0	Non-protected		0	Non-protected	
1	Ø 50 mm	Protected against the penetration of solid objects having a diameter greater than or equal to 50 mm	1		Protected against vertical dripping water, (condensation).
2	Ø 12,5 mm	Protected against the penetration of solid objects having a diameter greater than or equal to 12.5 mm.	2		Protected against dripping water at an angle of up to 15°.
3	Ø 2,5 mm	Protected against the penetration of solid objects having a diameter greater than or equal to 2.5 mm.	3		Protected against rain at an angle of up to 60°.
4	Ø 1 mm	Protected against the penetration of solid objects having a diameter greater than or equal to 1 mm.	4		Protected against splashing water in all directions.
5		Dust protected (no harmful deposits).	5		Protected against water jets in all directions.
6		Dust tight.	6		Protected against powerful jets of water and waves.
			7		Protected against the effects of temporary immersion.
			8		Protected against the effects of prolonged immersion under specified conditions.

Figure 10

IEC Standard 60529
guidelines for ingress protection

Particles/Dust – Dust and other particles can impact the reliability and life expectancy of IT equipment. In harsh environments where airborne contaminants exist, this is an important design consideration. A self-contained design, sealed from the environment, ensures those contaminants are not getting to the IT equipment. If not sealed and the IT is intaking air from the surroundings, an air filter can offer a level of protection for the equipment. It's important to keep in mind, however, that if an air filter is used, it must be cleaned or replaced as needed to maintain its effectiveness.

Just like water, the level of protection needed depends on the severity of the risk. Referencing back to **Figure 10**, IP ratings verify the level of protection a system provides. The first number represents the level of protection against dust/solids. A rating of “0” means no protection, a rating of “4” is protection from the penetration of solid objects having a diameter greater than or equal to 1mm, a rating of “5” is dust protected meaning no harmful deposits, and the most robust protection is a rating of “6” which means it is dust tight. A rating of “5” is often requested in industrial surroundings, and a rating of “6” is often requested for outdoor protection.

Vibration - Large industrial machinery might produce significant vibration, which could impact the longevity of any IT equipment located too closely and cause hard drives to fail early. It is important to understand the threshold for the IT equipment being installed in the environment. There are mitigation techniques to ensure vibration doesn't exceed operating limits. One common technique is to place the enclosure on isolated spring mounts to reduce the transfer of vibration. Another solution is the use of rubber vibration isolation pads which absorb noise and high frequency vibration from machinery. It is similar to the rubber feet we may use in our homes to absorb or deaden the vibration of our washing machines/dryers. The right approach will depend on the magnitude of the vibration.

Collision – In industrial settings, forklifts and other heavy mobile machinery can present collision and ultimately downtime risks for micro data centers. For this reason, it is best practice to position the micro data center out of main traffic areas when possible. Additional protection is advised by placement of concrete bollards to prevent these vehicles and machines from getting close to the critical IT. White Paper 82, [Physical Security in Mission Critical Facilities](#), discusses these solutions in greater detail. Wall-mounted micro data centers can be a solution here as well, although it's important to ensure it's not protruding into a space with equipment traffic. Motion sensors and security cameras are also advised. Similar to the IP rating discussed above, there is a rating that specifies the level of protection an enclosure has against external mechanical impacts. It is called the IK rating and is specified in the IEC 62262 standard. For example, a rating of IK01 protects against 0.14 joules of impact, a rating of IK05 protects against 0.7 joules of impact, and a rating of IK10 (the highest rating) protects against 20 joules of impact.

Nuisance events – The less controlled the environment, the more likely we are to see nuisance events. Outdoor micro data centers are the most likely candidates. Think about annoyances like rats chewing on electrical lines/insulation or someone vandalizing your equipment. Tactics to mitigate these risks include site selection to minimize visibility and reach of the micro data center, implementing proper security measures, and designing the system with protective liquid-tight conduit or rigid conduit. There are a number of standards that exist to address nuisance events. For example, EN 1627 is the European Standard for burglar resistant classifications; and IEC 61439-5 is an international standard for anti-vandalism resistance from shock, impact, torsion, and so on.

Corrosion – In harsh environments, hard disk drives, servers, and printed circuit boards are susceptible to corrosion which can impact equipment reliability. Factories with heavy machinery using chemicals in their manufacturing processes release gaseous contaminants. Fresh air exposure presents an additional corrosion risk. Consider a micro data center placed outdoors or in a warehouse exposed to the outdoor conditions; or a site that deployed fresh air (direct air) cooling to improve operational efficiencies. These sites can experience corrosion and a higher failure rate for the IT due to high humidity levels or proximity to salt water.

Different enclosure materials, i.e. stainless steel vs. aluminum vs. plastics offer different corrosive properties. There are also coatings or paints that offer levels of protection. ISO 12944 is an international standard for corrosion protection of steel structures by protective paint systems. It provides different classifications based on the type of environment the enclosure is exposed to. It's important to understand the corrosive risks for your specific environment to ensure the appropriate enclosure materials/coatings are used. Enclosures also exist that use gasketing, thermal insulation, double wall panels, and robust cable fittings (such as Roxtec) to help ensure the environment is isolated.

Addressing the risks with ruggedized IT

Up until now, we've talked about protecting standard IT systems in harsh environments by fortifying or hardening the environment. In this section, we briefly cover an alternative to that approach: hardened or ruggedized **IT equipment**. IT equipment can be designed to be temperature/humidity tolerant, water proof, dust proof, seismic rated, and so on. They can be built "military grade", like a tank. But there are trade-offs in taking this approach vs. designing a ruggedized environment.

Price premium – Ruggedized IT (such as the one in **Figure 11**) comes at a premium over standard IT. The amount of that premium depends largely on the standard or specs it is built to. NEBS-compliance is what telco equipment is built for, which is designed to a higher standard for vibration, shock, temp range, etc. The degree with which the system must be ruggedized depends on what conditions it is going to be exposed to. For instance, you need a much more tolerant system if it's going to sit outside on a pole vs. if it's in a warehouse where the temperature may fluctuate, and you want a 10-degree wider operating tolerance. The latter is easier and less costly to achieve. In general, when components have higher ratings and tolerances, they cost more. There's also a price premium because volumes are much lower, since its more specialized equipment.



Figure 11

Example of ruggedized servers for harsh environments

Limited performance – Ruggedized IT equipment is often completely sealed and fan-less. This means components are relying on convection and radiation for cooling the components. Therefore, the power envelope is greatly reduced, and you are constrained on how much compute power you can get. You may only have a need for one device at the edge, and the compute is sufficient. But when multiple devices become necessary, the economics will often favor a single ruggedized enclosure.

Supplier base – Not every server manufacturer makes ruggedized IT equipment. This limits your supplier base. You're likely to be purchasing your equipment from a boutique specialist server manufacturer that makes equipment for military/harsh environments, or a division of a large global server vendor. Since the low-end server vendors are likely not at play here, the solutions are likely to be of higher quality.

Service life & TCO – The IT refresh cycle may have a big impact on the decision of whether to ruggedize the environment or the IT equipment itself. If IT is refreshed every 3-4 years (which it often is), you are paying the premium for ruggedized IT every 3-4 years. You'll also need ruggedized support infrastructure, like UPSs and rack PDUs that can handle the same conditions as the IT equipment. With a ruggedized enclosure, depending on the level of protection it provides, these systems can be standard. Ruggedized enclosures do need some basic maintenance (i.e. filter changes, CRAC maintenance, gasketing materials), but generally has an overall

useful life of at least 10 years. That means you can amortize the premium for the ruggedized environment over a longer period of time.

Sensitive business processes

We've covered extensively the risks and challenges with protecting the IT equipment from the harsh environment. But sometimes the opposite is necessary... where we need to protect the sensitive business process from the micro data center. **Figure 12** are two examples of such business processes – a chip fabrication plant and a carbon-fiber-based aircraft manufacturing plant, both which must be in a highly controlled environment.

(a)



(b)



Figure 12

*Examples of a sensitive business processes –
(a) A chip fabrication plant or clean room, and
(b) Carbon fiber-based aircraft manufacturing plant*

It is important that the micro data center, including the IT equipment don't contaminate the space. Fans (both IT and CRAC) are a concern here, as they can introduce dust and particles into the business process.

Liquid cooling provides an alternative approach in harsh environments. Immersive liquid cooling isolates servers from the environment. Removing the fans from the IT equipment provides protection against airborne contaminants in harsh environments such as heavy industrial manufacturing plants or in environments with sensitive processes. White Paper 279, [Five Reasons to Adopt Liquid Cooling](#), explains the benefits of this approach in more detail.

Vibration from the micro data center may also be a concern. For example, a hospital building may house powerful microscopes and other equipment that are very susceptible to relatively low levels of noise and vibration. The same strategies listed above for dampening the vibration are recommended for the micro data center, in these situations.

These environments should be highly instrumented with extensive sensors (like particle, vibration, temperature), to ensure the sensitive environment is not breached and the business process not impacted.

Conclusion

As the proliferation of edge computing continues, micro data centers will be deployed in great numbers across a spectrum of industries and applications. The design requirements for a micro data center, however, are highly dependent on the environment they will reside. In this paper, we define three types of environments: (1) IT environments, (2) commercial & office space environments, and (3) industrial & harsh environments.

While there are fundamental needs of all micro data centers in terms of physical infrastructure (i.e. security, power, cooling, management, safety), the business risks grow as you go from an IT environment to a commercial/office environment, and finally to an industrial or harsh environment. As the business risks grow, the solution must become more robust. This includes protection from both IT downtime risks and the risks associated with the business process, employee productivity, customer satisfaction, or other primary function of the space.

Before starting a new micro data center project for your edge computing needs, we recommend classifying your site(s) by one of the three categories defined in this paper, and then following the guidelines/best practices presented to ensure all risks are mitigated and the right attributes are included in your design.


About the author


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 of Mechanical Engineering degree from Union College in Schenectady, NY and her MBA from University of Rhode Island. Wendy is an ASQ Certified Reliability Engineer.

RATE THIS PAPER





 [Why Cloud Computing is Requiring us to Rethink Resiliency at the Edge](#)
White Paper 256

 [Practical Guide to Ensuring Availability at Edge Computing Sites](#)
White Paper 280

 [Physical Security in Mission Critical Facilities](#)
White Paper 82


 [How to Choose an IT Rack](#)
White Paper 201


 [Battery Technology for Single Phase UPS Systems: VRLA vs. Li-ion](#)
White Paper 266

 [Cooling Strategies for IT Wiring Closets and Small Rooms](#)
White Paper 68

 [Essential Guidance on DCIM for Edge Computing Infrastructure](#)
White Paper 281

 [Solving Edge Computing Infrastructure Challenges](#)
White Paper 277

 [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