Maximizing Uptime of Critical Systems in Commercial and Industrial Applications

White Paper 7

Revision 1

by Dan McGinn

Executive summary

As technology and information reach into every corner of our world, the availability of critical systems in industrial process and facility management is more important than ever. Uptime and the availability of critical process information is no longer a lofty goal, but is a necessity to remain competitive. Much has been made of uptime with respect to data centers. However, applications exist within industrial and commercial facilities that also merit “mission critical” treatment even if the larger facility as a whole is not viewed as such. Maintaining productivity and overall equipment effectiveness (OEE) requires design and operational practices that maximize uptime. This paper describes those key practices in the context of the facility life cycle.

Introduction

According to the Department of Energy, utility power loss events have almost tripled in the US since the mid-80s contributing to more than $150 billion in losses per year[1]. There are also more and more issues and events associated with delivering and distributing clean uninterrupted power within modern industrial and commercial facilities. Remaining competitive requires that business, industrial, and machine processes and systems support continued operation with very high availability. In most cases, practical investment trade-offs require that the more critical systems and applications be identified for special treatment rather than the whole facility. That said, as we adopt the Internet of Things and rely on more connected and intelligent systems, the communication and "brains" that provide data important to effective operation often warrant treatment as mission-critical across all applications.

What constitutes a "mission critical" application?

It is important to determine which systems or elements of the enterprise most warrant treatment as mission critical and therefore warrant investment in high availability power solutions. Of course, precedence should be given to any equipment whose operation is important to life safety. Beyond that, most investments will be driven by investment return, risk avoidance, and protecting critical data. Mission critical applications will most likely fall into one of the following categories:

Emergency systems - Treatment of backup power for emergency systems is governed by NFPA 110 Chapter 4. However, which applications constitute emergency systems is largely undefined beyond emergency lighting. Instead the code refers to performing risk analysis and the governance of the authority having jurisdiction (AHJ). Emergency applications and those affecting life safety are identified through such a process.

Critical process equipment - Continuous operation of some equipment or systems is more critical based on critical path, recovery time, idle labor costs, maintenance intervention, as well as the potential equipment and service losses. Design and analysis of the process should help identify the most critical applications.

Problematic equipment - Some systems may operate in areas more prone to power-related issues and interruptions. Some systems may be more susceptible to such issues. Analyses of productivity data (MES, 6σ, etc.) and power monitoring information can identify the most critical applications with respect to these issues.

Monitoring and control equipment - The cost of providing critical power systems for some equipment is often prohibitive. However, many systems that provide intelligence, control and communication for processes can be protected separately from the main power at more reasonable costs. In modern systems, there is often much to be gained from ongoing connectivity and data collection.

Security systems - Modern access control systems and security-related digital video recording (DVR) equipment are generally mission critical in that loss of operation during power related events is not acceptable. Likewise, the proliferation of security cameras (esp. IP cameras) and the networks supporting them often warrant critical application treatment.

[1] http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/DOE_SG_Book_Single_Pages%281%29.pdf

Operations centers - Dedicated centers for managing operations are often treated as mission critical applications: control rooms, command centers, and security offices, for example.

IT/Telecom edge compute environments - While “edge” is often a reference to on premises elements of a distributed datacenter enterprise, many instances of compute and network infrastructure exist further down into the enterprise in industrial and commercial spaces. More and more, these systems should be treated as managed assets with mission critical treatment since they are often instrumental in keeping site operations up and running, as well as the monitoring and control functions.

Planning

Begin with the end in mind. Whether it’s new construction, upgrading or operating, it is important to carefully identify and prioritize applications in terms of mission criticality. In new construction and upgrades this should be considered in terms of design and involve input from consulting engineering and/or process integration partners. For systems already in operation, data from production systems and enterprise systems can reveal the more critical applications.

In addition to determining what the most mission critical applications are, it is valuable to look at the power distribution architecture and either:

- Consider grouping mission critical loads to support more centralized UPS systems for high availability power (new construction, upgrades)
- See what opportunities already exist to serve multiple mission critical loads together for central systems (existing applications)

Selecting a design concept that meets criticality needs

High-availability power solutions can take on a number of forms, use varied system elements, include system redundancy and provide a layered defense against power related issues.

At the utility level, some improvements in power quality and availability can often be accomplished in consultation with the utility itself. For some facilities, a secondary source of utility power may be incorporated to provide redundancy. This is more typical of the most critical facilities like hospitals, datacenters and large industrial facilities. Of course, redundant utility feeds are still vulnerable to larger scale regional utility interruptions. And, it is important to note that most power related issues originate further down the power path than the utility feed; everything from transients to tripped circuits.

In addition to the typical utility feed, micro-grid solutions are becoming more viable options for certain facilities. These systems connect intelligently to alternative and more locally generated power grids that have electrical energy storage capacity. A micro-grid can “island” the facility from the larger utility grid to reduce energy costs and isolate itself from utility disturbances that would threaten system availability.

At many larger facilities with critical applications, generator systems often exist to provide longer periods of backup power in the event of a sustained utility outage. Generator systems can be paralleled and bused together to enhance redundancy and increase capacity. A limitation of generator systems is that they take several seconds to start up when a blackout occurs. In some applications that interruption on power can cause equipment and systems to suddenly shutdown and become unavailable.

Within a facility, uninterruptable power supplies (UPSs) can be incorporated to provide nearly instantaneous backup power for sensitive equipment. These battery backup systems will bridge the gap in power between an outage and when the generator starts up. A UPS will ensure even the most sensitive equipment stays up and running without interruption when the power goes out. Smaller UPS systems can be distributed around the facility as needed to provide local protection or be centralized in a larger solution hardwired into the building electrical distribution network to provide protection for devices connected downstream. UPSs not only protect against power outages, but also provide protection against several other types of power transients (e.g., impulse transients and voltage sags) that can damage hardware, lockup micro-processors, and/or cause a loss of network communication.

In most applications, outside of entire facilities deemed "mission critical" (e.g. datacenters), a UPS by itself is considered sufficiently redundant to the utility feed for critical applications. However, the available battery runtime for a typical UPS is measured in minutes with full load runtimes in the 4 to 5 minute range. Many UPS systems have the option to add additional battery modules to increase the runtime into the few hours range. In cases where there is a need for backup power that lasts for several hours or days, however, backup generator systems are required.

In the most critical applications, redundant UPS systems are often deployed to ensure a higher degree of availability. Traditionally, this has been achieved by paralleling multiple UPSs for a given load. Some of the newer UPS systems are internally redundant where a single UPS frame is supported by multiple modules configured in an "N+1" arrangement. There are cost, speed of deployment, and reliability tradeoffs between these two approaches. White Paper 234, *Cost, Speed, and Reliability Tradeoffs between N+1 UPS Configurations*, goes into this in detail in the context of a data center mission critical facility. **Figure 1** shows UPSs being deployed for industrial process machines.

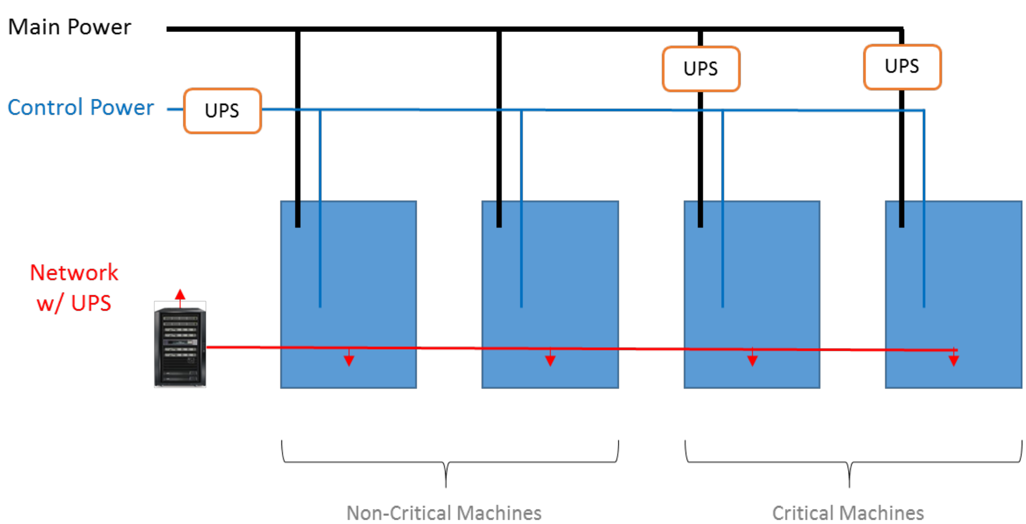

Figure 1
Example of UPS deployment for industrial process machines

The graphic shows two main power UPSs for critical machines but, as the distribution architecture allows, several loads could be grouped into a single UPS. Also, the graphic shows a single central UPS for control power but that could take the form of small, individual UPSs integrated into the machines or control cabinets at the machines. UPSs could be deployed in both ways for additional protection. Local machine networks and connected devices are powered by the control power feed while the upstream network is powered from the UPS in the network panel.

Equipment selection and integration

Selecting the right equipment vendors for the project helps ensure its successful completion. It is crucial to ensure that the equipment vendor meets the engineering specifications. Beyond the equipment-side however, the vendor's ability to support the equipment is an equally important consideration. This includes delivery times, installation support, start-up services and the availability of spare parts and authorized maintenance personnel. For complex systems and fast-track projects, consider using an equipment integrator. Complex systems rely on the operation of multiple systems and platforms. Therefore, it is essential to have the support of an organization focused on the overall connectivity and interaction of multiple systems. A qualified integrator can help eliminate the confusion that multiple Request for Information (RFIs) from various installing contractors can cause. Integrators provide the customer with a single point- of-contact, reducing the projects' completion times, and ensuring that all systems are properly installed and interconnected. When selecting equipment for your mission-critical facilities, work with an Integrator can verify that all of the equipment complies with the project specifications. Listed below are some equipment options to consider for a mission-critical facility.

Generators

When selecting the generator, review the technical specifications to ensure that your project needs are met. Consider the interaction of the generator equipment with other systems in place for power continuity such as UPS systems. The generator is there to provide power in the case of an outage. Consideration should be given to the criticality of various systems and whether they should have provisions for generator power, UPS power or both.

UPS systems

There are as many different types of UPS systems as there are topologies. Your requirements may be best suited for a double conversion, line interactive or delta conversion. Double conversion UPS is most common UP in mission critical applications because it provides true power source isolated from upstream disturbances. In many mission critical applications, the UPS invertor needs to be sized adequately for instantaneous in-rush loads. Regardless of the type of system that fits the application, make sure the appropriate internal and external maintenance bypasses are installed. A maintenance bypass should be sized to support 100% load on external maintenance bypass while providing enough capacity to perform 100% load tests.

Energy storage

The most common energy storage option for UPS systems are Valve Regulated Lead Acid (VRLA) batteries. When using VRLAs, specify multiple battery strings that can be independently isolated by opening a breaker. With an independently isolated VRLA battery string, maintenance can be performed while keeping the critical load on the UPS system. Note that lithium-ion batteries are becoming a viable energy storage option for mission critical applications and UPSs. Although their cost is higher, they are much lighter, small, and have a much longer life vs. VRLA batteries. White Paper 229, "Battery Technology for Data Centers: VRLA vs. Li-ion" provides a detailed comparison.

In some mission critical applications with UPS systems providing bridge power for short durations, mechanical storage is an alternative consideration in the form of rotary flywheels. There are advantages, disadvantages and cost tradeoffs but the most common application is in hospital systems where system real estate is very premium and the possibility battery gassing is a strong concern. As newer battery technologies such as Li-Ion emerge, similar size and cost tradeoffs are likely to be realized

Monitoring

In mission critical facilities, UPS systems along with the IT equipment they service often have a dedicated monitoring solution. In the non-IT world, UPS system information may have a number of interested consumers and in our "Internet of Things" world, there may be different monitoring systems looking for information from the same device.

- IT manager may want to monitor remote UPS systems using the software managing datacenter assets.
- A department or production manager may want to see basic UPS system data in the SCADA
- A facility manager may want to see the same type of information in the BMS system

All possibilities exist but it is key that there be some point of asset responsibility to take action in response to various states and alarms. Trends and notification can provide not only alarm notification, but also important historical data that can be used to predict and prevent failures. It is, of course, essential that the monitoring system itself continues to operate when the systems that are being monitored fail. Proper setup of monitoring system alarm points is crucial to preventing failures.

Installation / Construction

For smaller UPS systems installed in proximity to individual equipment, installation is fairly straight forward and can be done by qualified people based on the manufacturer's instructions. This is especially true for pluggable single phase loads. For larger systems applied local to loads, an electrical contractor might be involved. This is especially true for hard-wired and three phase systems.

The key discussion is for larger systems integrated with the power distribution architecture. These systems are typically monitored, maintained and provide the highest availability as a more permanent part of the infrastructure. Well-planned and meticulously implemented construction is the key. The owner should take an active role in selecting and working with the team throughout the construction process. A team approach from system design through installation and commissioning with a project plan and project oversight, will help to ensure that your final implementation will meet your specifications.

Safety first - Insist on vendors providing safety plans before any work begins. Review the plans to ensure their current and appropriate to your project. Injury and fatalities can affect the reputation of your organization, along with the potential for OSHA fines and other litigation costs.

Construction inspections - The owner, or the owner's representative, should conduct regular inspections of the jobsite during the construction process to document and photograph the installation process. Any items of concern should be addressed immediately rather than waiting until after the installation is completed.

Project meetings - Conduct regular project construction meetings that are professional and productive. Building a fast-track project for mission critical applications requires a team approach, good facilitation and mediation skills can be tremendous assets.

Project documentation - Keep a full and detailed project file with construction log, relevant documentation, submittals, approvals and even digital pictures. After the installation, be sure to secure the project's as-built drawings. Invest the time to verify the accuracy of the drawings. Then institute a practice that ensures that all applicable drawings are undated as upgrades occur at the facilities.

Commissioning

Commissioning is the systematic process of verifying and documenting the performance of the equipment. Commissioning an installation has many benefits providing direct and indirect paybacks. Prior to starting the commissioning program, take the time to define the key purpose of the program. For example, systems can be setup to achieve higher energy efficiency, but this may affect the system reliability. Trade-offs between energy efficiency and system reliability must be carefully weighed. This is ultimately a priority-based decision for the owner. Benefits to commissioning, include:

- Improved system performance and reliability,
- Hands-on training for operations and maintenance personnel,
- Early identification of outstanding issues,
- Verification of operating parameters and procedures,
- Establishing an operating baseline,
- Extended equipment life

Commissioning procedures

All operating procedures should be tested for functionality during the Commissioning process. This includes start-up and shutdown of equipment, equipment bypass and failure-recovery procedures. Equipment should be exercised through all of the modes of operation. To avoid future problems, it is essential to verify all operational modes and procedure methods.

Systems may warrant re-commissioning if changes are made to the installation or to the loads served by the installation. Re-commissioning should follow similar procedures using the original commissioning documents and incorporating all changes into updated system documentation.

Operations and maintenance

Once the system is operational you will need to decide who will monitor and maintain the systems. Depending on the nature of your operation this could be inside or outside staff responsible for facility maintenance or for trades/engineering within the department. It is important that the depth of knowledge meets the requirements of the application

Operation, maintenance, and recovery procedures need to be defined and communicated. This is especially true for a procedure to transfer the UPS system, to maintenance bypass. Maintenance windows should be defined and allowances made for bypass or operational downtime. Systems without the appropriate maintenance allowances may require the use of temporary equipment or the installation of additional systems if continuous uptime is an absolute requirement.

All maintenance documentation should be detailed, and provide methods for predicting and anticipating potential trouble spots and weaknesses. Have specific procedures in place for start-up, shutdown, bypass, lock-out tag-out, maintenance and disaster recovery.

Training

It is also important to have a comprehensive training for the operation and maintenance staff. Training should start with the equipment manufacturer/installer. Start-ups and commissioning offer ideal opportunities for training operation and maintenance staff. Once the site is operational, it is wise to have periodic follow up training to keep operational and maintenance staff current.

Conclusion

Protecting your most critical applications from power disturbances ultimately leads to an overall operation that mitigates risk and provides greater business continuity. Maximum uptime depends on technology, trust, and teamwork. For your equipment it pays to invest the time to select a company you can trust. And, for your design and construction partners, it pays to invest in those with the experience and resources to assure timeliness and quality of work.

About the author

Daniel McGinn is the Director of Secure Power Systems at Schneider Electric. In his role, Dan is responsible for business development strategies and execution in the area of UPS and IT related technologies in the Industry and Infrastructure spaces. Dan works across multiple business units within Schneider Electric to address the Secure Power needs of varied market segments. Dan has over twenty years of experience as a business and technology professional in the arena of Process Automation, Energy Management and Manufacturing IT systems with extensive experience in the application of UPS technology including 3-phase systems and redundant power generation. Daniel has a Bachelor of Science degree in Electrical Engineering from the University of Michigan at Ann Arbor.

Resources

Battery Technology for Data Centers: VRLA vs. Li-ion
White Paper 229

Cost, Speed, and Reliability Tradeoffs between N+1 UPS Configurations
White Paper 234

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