A Practical Guide to Disaster Avoidance in Mission-Critical Facilities

White Paper 5

Revision 0

> Executive summary

A disaster preparedness plan is crucial to organizations operating in 24/7/365 environments. With zero disruption the goal, management must carefully evaluate and mitigate risks to the physical infrastructure that supports the mission-critical facility. While business continuity planning typically addresses Information Technology, this paper reviews and discusses the requirements of the facility's infrastructure as part of a comprehensive business continuity disaster plan. Without a proper disaster mitigation plan for the facility's infrastructure, the overall business continuity plan is built on a risky foundation. If a natural, human, or technological disaster strikes your facility, are you and your infrastructure prepared? Does your organization have procedures in place to prepare for severe winter storms, earthquakes, tornados, hurricanes, or other disasters? Surviving tomorrow's disaster requires planning today.

Contents

Click on a section to jump to it

APC white papers are now part of the Schneider Electric white paper library produced by Schneider Electric's **Data Center Science Center**
DCSC@Schneider-Electric.com

Schneider Electric

Introduction

Link to resource
White Paper 7
Maximizing Uptime in Mission-Critical Facilities

What is a disaster?

A disaster is an event that can unexpectedly affect the continuity of a business by damaging or injuring its employees, business systems, information, environment or the facility. Disasters can take the form of emergencies or accidents. Fires, floods, tornadoes or terrorism, hurricanes, HAZMAT spills or human error, earthquakes, equipment failures, utility outages, winter storms and virtually any other event that may injure people, property, information, or the eironment. In many cases, small avoidable problems may cascade to create a major disaster. See also White Paper 7, *Maximizing Uptime in Mission-Critical Facilities*.

Failures

Disasters can start from various types of failures. To facilitate effective planning it is crucial to understand the types of failures that may be experienced. Equipment downtime in a mission-critical facility can be attributed to four (4) major types of failures:

- Design Failures
- Catastrophic Failures
- Compounding Failures
- Human Error Failures

Each type of failure requires a different approach to prevention. Attacking a potential failure at its root cause may avert a much larger disaster

Design failures
To help prevent design failures, start with a comprehensive design intent. Select design firms with experience in your specific application and be an active member of the design process. Use component vendors and review, check and recheck the work. Begin with the end in mind.

Catastrophic failure
To help prevent catastrophic failures, develop a comprehensive maintenance program that uses Predictive Analysis. Evaluate the potential for failure, its consequences, and examine the steps to prevent its failure. In addition, implement a formal "Lessons Learned" program to prevent history from repeating itself.

Human Error failure
Use detailed "Switch Level" Methods of Procedure (MOPs).Verify the accuracy of the MOPs before implementation through the use of a pilot/co-pilot approach during switching operations. Thorough training of internal staff and vendors is fundamental to minimizing the risk of human error.

Disaster planning

Planning and preparedness, in the broadest context, means any and all measures taken to prevent, prepare for, respond, mitigate and recover from a crisis. Preparedness consists of four critical aspects:

1. Preparation and Prevention: Any set of activities that prevent a crisis, reduce the chance of a crisis happening, or reduce the damaging effects of a crisis.
2. Detection and Incident Classification: Actions taken to identify, assess and classify the severity of a crisis.

3. Response and Mitigation: Actions taken to save lives, prevent further damage and reduce the effects of the crisis.
4. Reentry and Recovery: Actions taken to return to a normal or an even safer situation following the crisis.

Information

Access to the essential information is critical during a crisis. This information should be continuously backed-up, and stored at multiple locations. Many companies lost 100% of their assets, including their recovery plans, in the collapse of the World Trade Center. Many of those companies do not exist today.

Emergency contact list
An up-to-date emergency contact list of employees and vendors should be continuously updated and readily accessible during a disaster.

Facility access list
Make sure your Facility Access List is up-to-date. During emergencies your staff will need access to locations such as back-up sites where they may not be known. Access denials or delays can result in the loss of valuable recovery time.

Verify recovery capacity

With the rapid growth of data and applications, make sure your disaster recovery sites have the required resources to house your data. The focus on keeping primary sites up to speed with the pace of technology often results in the secondary sites falling behind.

Do not under-estimate recovery time

Few planners accurately anticipate the delays that are part of a massive disaster, such as the time required to complete the life-safety phase, damage assessment phase, and to reach the hot site and establish remote operations.

Coping with stress

The massiveness of a disaster can paralyze an organization. A key to performance under stress is preparation and continuous practice. During a disaster, your employees will need to make contact with their families before they are able to focus clearly on your recovery plan. You also need to evaluate factors such as the number of continuous hours your responders can work before being relieved, and the amount of time required to ascertain the status of injured personnel. Most plans today do not realistically anticipate the time needed to recover from a disaster.

Beware of evacuation flaws

Another common miscalculation is the complications caused by mass evacuations. Your plans should assess evacuation related concerns such as how soon after a disaster should your personnel evacuate, as well as primary and alternative evacuation routes. An Alternate Emergency Operation Center (EOC), a reasonable distance from your primary site, should also be designated.

Eliminate communication bottlenecks

Multiple communications failures occur due to "single point of failure" situations. Many companies' plans are based on the public network performing as normal. Unfortunately, in a major disaster, the public network can become overwhelmed. Organizations need alternate forms of communication in place.

Seek coverage

Review your insurance coverage. Be sure you have the adequate coverage to provide the resources needed for the continuity of your business operations.

Assessing the situation

In personal healthcare, the practice of routine physical exams for the early detection of disease is a highly successful method for the prevention of catastrophic illness. The same is also true for the prevention of a catastrophic loss when a physical risk assessment is applied to a building or facility on behalf of a building owner or insurer.

Hazards assessment

Hazard Assessment is the process of defining hazard-prone areas. These hazards can include wild fires, mudslides, tornadoes, hurricanes, railroads, gas lines, floods, etc. The Hazard Assessment estimates the probability and severity of the hazard risks and evaluates existing mitigation efforts. The Hazard Assessment should address the location and boundaries of the hazard, the potential magnitude of an event, and the likelihood of each event.

Vulnerability assessment

Vulnerability Assessment is the process of estimating disaster potential in terms of susceptibility to damage. A thorough Vulnerability Assessment should evaluate such crucial issues as the number of people at risk, the value of property, the number and function of the exposed critical systems, and the dangers of secondary hazards.

Risk assessment

The Risk Assessment is a measure that combines the likelihood of a hazard event with the probable degree of damage that would result. It should also account for secondary damage.

Disaster recovery assessment

Disaster Recovery addresses the adequacy of backups, equipment replacement prioritization, vendor lists, emergency response planning, plan exercising and additional procedures that will expedite recovery from a disaster event.

Fire safety assessment

The most frequent cause of declared disasters is fire. Building fire codes are designed to ensure that structures are safe from fires for the occupants, and based on safe evacuation. However, an objective limited only to compliance to code is inappropriate. The various codes are a minimum standard and depending on risk and exposure, additional measures should be used. The key category in "learning before burning," the Fire Safety Assessment focuses on

fire safety systems (e.g., detector spacing and appropriate usage), hazards (e.g., paper and flammables storage), evacuation procedures, fire suppression, and fire department relationships (e.g., response time, access and, familiarity with the facility).

Security & alarm assessment

The Security and Alarm Assessment evaluates the adequacy of both security and equipment alarming, facility accessibility, security breach rates, alarm center routing, and alarm response procedure issues.

Environment assessment

The Environment Assessment evaluates settled and airborne contamination, air filtration, environmental impact on equipment, occupant comfort level and overall facility cleanliness, as well as the outdoor air source and ventilation rate, and the vulnerability of support systems such as the HVAC (Heating, Ventilating and Air-Conditioning).

Power assessment

Determines the adequacy of back-up power systems, surge suppression, primary power source reliability, power routing diversity, connector systems and many other energy reliability factors.

Testing your disaster plan

Once the plan has been developed, it must be subjected to rigorous testing. The testing process itself must be properly planned and should be carried-out in an environment that realistically simulates authentic conditions, by the actual individuals who will undertake those activities in the event of emergency. Testing disaster recovery plans, alarms and procedures, conducting building inspections and reviewing building incident reports are some sources of effectiveness measurements. Whichever measurements are chosen, it is crucial that management realistically assess the results. There is a temptation to downplay poor results and offer sympathetic assessments of efforts. However, the time to take corrective actions is now. Every step taken now can save time, money and lives in the future. For example, in fire scenarios, preventive action calls for periodic inspection of all electric appliances in the facility. What if management decides to do this inspection less often than prescribed, such as only once a year? A review of the building incident reports could disclose that two other appliances caused minor fires in the last three months. An annual review may prove too late to recognize "a gathering storm." Once the plan has been tested and updated, the test procedures and results should be documented. All personnel required to implement the plan must undergo formal and ongoing training.

Disaster mitigation

Disaster mitigation is the cornerstone of emergency management. It's the ongoing effort to lessen the impact disasters have on people and property. For example, mitigation involves keeping homes away from floodplains, engineering bridges to withstand earthquakes, and creating and enforcing effective building codes to protect property from hurricanes. Disaster mitigation is defined as "sustained action that reduces or eliminates long-term risk to people and property from natural hazards and their effects." It describes the ongoing effort at the Federal, State, local, and individual levels to lessen the impact of disasters upon our families, homes, communities and economy.

Updating your disaster plan

It is important that feedback is obtained for fine-tuning the plan after testing. It is a living document that must always be up-to-date and applicable to current business circumstances. It is crucial to have an individual responsible for ensuring that the plan is maintained and regularly updated. Any changes or amendments made to the plan must be fully tested. Personnel should be kept abreast of how such changes affect their duties and responsibilities.

The 9 R's of a successful recovery plan

Reason for planning

List the reasons your organization has for disaster planning. Some common reasons include: protect human life; recover critical operations; protect competitive position; preserve customer confidence and good will; and protect against litigation.

Recognition

Personnel must be trained to recognize warning signs.What happens if someone spots water coming under the door to your equipment room at 3 a.m.? Do the security guards, cleaning crews and other contractors know who to call and how to report trouble? These are the kinds of concerns to address in the Recognition phase: initial reaction procedures to a disaster report; notification procedures for police, fire, medical; and notification procedures for management.

Reaction

What happens after an alarm is sounded? Who handles security? Who talks to the media? How do you distinguish authorized personnel from opportunists and trespassers? Careful planning addresses these questions. Mobilizing the Executive Management Team (EMT); filing of initial damage assessment reports to the EMT; assisting the EMT in preparation of statements; and opening a critical events log for audit purposes, are just a few of the many actions taken during the Reaction phase.

Response

The response to a disaster will greatly affect the impact that it has on your business operation. Having the proper notification system in place will expedite recovery. Establish a designated Emergency Operation Center (EOC) or "war room" to allow you to focus on the recovery efforts rather than locating and setting up the required resources.When conducting damage assessment it is important that you protect your human and equipment resources. Safety should be your first priority.

Recovery

Establish procedures for operations during the Recovery phase. Concerns include modified signing authority for equipment purchases, procedures for obtaining cash, procedures for maintaining physical security, procedures for arranging security at the damaged site and at the recovery center, in addition to procedures for finding and getting to the recovery center.

Restoration

The Restoration phase involves coordinating restoration of the original site, restoration of electronic equipment; reloading of software; restoration of power, UPS, and common building systems; replacement of fire suppression systems; rewiring of the building; restoring the LAN; and restoring the WAN connections.

Return to normal

During the Return to Normal phase established testing procedures for new hardware and software will be implemented; operation personnel and other employees will be trained or retrained; and a systematic migration back to the original site will be scheduled and implemented.

Rest and relax

Be sure to schedule compensatory time off to provide personnel energy and clarity to focus on the future. Be sure to build-in scheduled visits to any employees undergoing rehabilitation.

Re-evaluate and re-document

Having survived a disaster, it's time to analyze your recovery efforts and take steps to mitigate future risks and expedite future recovery efforts. Review your critical events log, evaluate vendor performance, recognize extraordinary achievements, prepare a final review and activity report, and aid in liability assessments.

Data center design factors

Link to resource
White Paper 145
The Top 9 Mistakes in Data Center Planning

Begin with the End in Mind. Too often the design intent is either vague or not fully developed. A comprehensive design intent is crucial for all involved parties to succeed in achieving maximum uptime in a mission-critical facility. There is no ideal facility design configuration. Depending on your goals, each type has advantages and disadvantages. Work with experts with the experience to design in the functionality, flexibility and affordability to meet your organization's goals. See also White Paper 145, *The Top 9 Mistakes in Data Center Planning*.

Site selection

Link to resource
White Paper 81
Site Selection for Mission Critical Facilities

There are many factors that influence the location of your facility. In addition to business factors, beware of how local hazards (Flood Zones/Flood Plans, easements and building setbacks) will affect you. Will there be the desired resources available for you when a disaster strikes? Make sure that the utilities will support your needs as you grow, and that there will be enough capacity and redundancy. For more information on site selection, see White Paper 81, *Site Selection for Mission Critical Facilities*.

Shell building design

One of the most important factors that affects the shell building design is the local environment. Your hazard assessment will define all local hazards. Incorporate protection against these hazards when designing the shell building. These hazards can include wild fires, mudslides, tornadoes, hurricanes, railroads, gas lines, terrorist risk, floods and many others.

For example, reduce the risk of fire by having fire resistant roofing materials, proper setbacks and keeping property clear of flammable vegetation. Trees and tall bushes should be pruned so that it will not interfere with electrical lines. Keep other critical systems (such as generator exhaust, cooling towers, transformers and condenser units) clear of trees and brush. If you are located in a Seismic zone; prepare your facility to withstand the shaking force of an earthquake.

Roofs and walls should be designed to provide a high degree of security and protection from local hazards. Floor and roof loading should be considered in order to handle the weight of the expected equipment, while allowing for future expansion. Weight of batteries for UPS systems sometimes requires special bracing or floor plating to displace the weight. The data center should be placed in the center of the facility and not against the perimeter walls. Blast Proofing with the increased threat from terrorist activities, make sure you provide the proper protection for your facility. Blast proofing measures include controlling building access, creating large setbacks, and specialized construction of the shell building and windows. For example, the use of glass as a construction material has grown dramatically. Glass is often the first line of impact, yet it is often overlooked in vulnerability assessments. The use of security film, a highly sophisticated, laminated film of polyester and metalized coatings, can drastically reduce damage and injury due to natural and manmade disasters.

Equipment selection

When selecting equipment for the mission-critical facility, make sure that the equipment specifications from the manufacturer match the specifications provided by your design engineer. In addition, most equipment will have an assortment of available accessories and options.Work with your design engineer to determine the value of these options, and the likelihood of needing them in the future.

While you may not need a specific option initially, growth might necessitate adding it in the field in the future.This may require equipment downtime and cost much more than if you ordered it at the time of the original purchase.A specialized systems integrator can help plan for the future, recognize and avoid potential equipment shortcomings, and maximize your return on investment.

Utilities

Prepare for the next utility outage today.While power is often the first concern, the loss of utilities such as water, natural gas, sewer service or telecommunications can also severely affect you mission-critical facility. Examples of utility considerations follow.

Electric
Burying utility lines helps preserve service and protect critical connections, particularly during high winds and ice storms. However, buried utilities are at higher risk to underground construction and flooding. Redundant feeds from separate substations provide the greatest level of protection, but cost often outweighs the assurance.

Water
If your facility uses chillers with a cooling tower you are dependent upon the continuous supply of water to keep your cooling system online. The advantages and disadvantages of using water-cooled chillers versus air-cooled units, and the ability to secure reliable backup water, need to be carefully evaluated.

Sewer
If you have a high demand on your sewer system, evaluate how its loss will affect operations, and evaluate provisions for providing backup facilities in the event of lost sewer services.

Natural gas
If you require natural gas for your chillers, boilers or generators, make provisions for a redundant fuel source, or install redundant equipment that uses another fuel type.

Telecommunications
Design your facility to use redundant communication services that enter your facility from diverse routes.

Diesel fuel
In the event of a widespread power outage, like the one which occurred in the Northeast in August 2003, diesel fuel stocks can become limited. Determining the proper amount of fuel needed is a challenge. Under normal conditions diesel fuel is available with a few hours notice. However, your supplier may not even have the ability to pump fuel from his tanks during a power outage.

On the other hand storing large amounts of fuel has its on concerns, from environment constraints to the limited "shelf life" of stored fuel. Over time fuel begins to break down. Gum and varnish form and certain algae can grow. Fuel additives extend the useful storage period. During generator maintenance it is important that your service provider performs a fuel analysis. A filtering system and a planned program of fuel cycling will mitigate these risks.

Electrical design considerations

Power is fundamental to the operation of mission-critical facility. And while we often take it for granted, electrical service is quite vulnerable to a number of hazards, and outages are common. Following are a number Electrical Design Considerations which can help minimize the risk posed by power outages.

Generators
Generators provide backup power when electrical utilities fail. From a simple single generator and Automatic Transfer Switch (ATS) to a complex multi-generator plant, the care and maintenance of your generator is crucial to the survival of your facility. Starting an emergency generator with no load during a weekly test provides reassurance that the generator is operation. However, weekly tests may also lead to "Wet Stacking." Wet Stacking occurs when a generator is run repeatedly with no load or a light load. When the generator is asked to come online to power a full equipment load, deposits that build up during no-load tests prevent it from developing full power under load. The generator should be tested under loaded conditions when possible to allow these deposits to be blown-out of the system. Scheduled 2- to 4-hour full load tests should be performed regularly. Consult your generator manufacturer or infrastructure specialist for recommendations of frequency and length of load testing. Generators consume crankcase oil during extended runs. Know your generator's crankcase oil consumption rate and add oil well before the engine grinds to a screeching halt. Some generators require the installation of oil lube systems to allow oil to be added while running. Consult with your generator manufacturer or service provider to determine your lube oil consumption rate. In addition, most generators have low-coolant alarms and shutdowns that prevent the generator from starting when the coolant is low. (Outages at mission-critical facilities caused by generator low-coolant levels are surprisingly common.) Periodic maintenance is key to avoiding major problems caused by minor oversights. Have enough coolant and oil on hand to get your facility through a minimum of one week of constant duty. If possible, install external crankcase and coolant reservoirs to eliminate the need to stop the generator and check the oil and coolant levels. Engine block heaters allow generators to start and come online quickly. However, the constantly heated water and generator vibration causes stress on the hoses and fittings. Isolation valves installed between the engine block and block heaters allow hoses and heaters to be replaced without taking the generator out of service.

Automatic transfer switches

Automatic transfer switches (ATS) are used to automatically provide emergency power during the loss of utility power. An ATS senses when utility power fails, starts the generator, and brings it online. When utility power is restored, most transfer switches wait a prudent amount of time and automatically switch back. These transfer switches contain parts and connections that can and will fail, therefore ongoing maintenance is critical. When possible, wraparound feeders, or the use of isolation bypass, will allow you to maintain power to your facility when your ATS is out of service.

Uninterruptible power supplies

Uninterruptible power supplies (UPS) are essential equipment at mission-critical facilities. From a small UPS plugged into an outlet at a personal computer, to large parallel systems that power large computer centers, UPSs all have one thing in common - batteries. UPS batteries have a finite life span and must be tested regularly. There are many different types of UPS systems (double conversion, Ferro-resonant or delta conversion) and many configurations (e.g., single module, parallel modules, isolated redundant, catcher systems, system plus). Each system and configuration has strengths and weaknesses. Work with your design engineers, manufacturers and infrastructure specialist to determine the right solution for your facility. There are two basic types of UPS batteries, Electrolytic (Flooded wet cell) and Vented (VRLA), each with advantages and disadvantages. Flooded batteries have a higher initial cost, but are more reliable and will last longer than VRLAs. (The typical life of a flooded battery will be 15 to 20 years. A VRLA only lasts 3 to 5 years.) When using VRLAs, have your UPS manufacturer configure your batteries into separate battery strings with their own dc breakers and cabinets. This will allow for one string to be isolated from the UPS system, keeping the UPS system online during maintenance and replacement. As with any new technology, UPS systems, and battery monitors, are getting better and cheaper. The battery is the heart of the UPS system, and battery monitors help extend the life of batteries while increasing the reliability of the battery plant. Don't overlook maintenance of other batteries in your facility. From generator-starting batteries, Program Logic Controllers (PLCs), monitoring and control systems, to breakers and trip units, a $2.00 watch battery may prevent your generator from coming online. Even UPS systems are not immune to failure. Consider designing in the appropriate redundancy to ensure that your critical load remains operational in case of a UPS failure. Once again, a proactive maintenance program is essential to minimizing the risk of a failure. Some maintenance tasks necessitate taking the UPS system offline. This requires you to have a completely redundant system, such as a System-plus-System design or external wrap around maintenance bypass. These systems are crucial when performing maintenance without affecting the critical load.

Power distribution

Once you have determined the proper UPS configuration you need to now distribute that power to the floor. This is done through Power Distribution Units (PDUs), Remote Power Panels (RPPs), distribution panels and an assortment of power cable and power strips. Many facilities are designed with state-of-the-art technology such dual utility feeds, large generator plants and redundant systemplus-system UPS plants. However, all that technology is wasted if the final connection hinges on inadequate cabling, breakers and distribution methods. The 20 amp breaker supporting your server should be a tested bolt-in breaker. Snap-in breakers used in residential applications are cheaper and easier to use and install, but are also less secure, untested, and far less reliable. (Failure rates of 20% to 50% are not unheard of.) An inexpensive breaker can negate all the redundancy built-in to the lines preceding it. Once past that breaker, don't leave millions of dollars in infrastructure at the mercy of a a $4 powerstrip with a 10¢ push-out circuit breaker and 20¢ switch.

Load banks

Load Banks are an essential tool in the maintenance of your mission-critical facility. Load Banks are used to test your standby power system to ensure it can handle the necessary load during an emergency. You can install permanent Load Banks or have your service

provider bring temporary units for maintenance. Either way, be sure you make the provisions in your switchgear to connect the Load Bank to the UPS system and Generators. This extra Load Bank breaker will save you a great deal of grief later.

Mechanical design considerations

People and equipment can crash when overheated. Clean, cool, dry, and pollution-free air in generous quantities is critical for your mission-critical facility. However, if you occupy a high-rise, you may not have your own air system. Many building systems have no air-handling backup and less than reliable maintenance support. Your best protection is to get the exact terms for air conditioning nailed down in your lease. You may wish to consider adding your own backup system - a costly but essential strategy if your building air supply is unreliable or without backup.

As with UPS systems and configurations, there are many choices for your primary and backup air-handling systems. There are large central plants with water-cooled chillers or air-cooled chillers, or Direct Expansion (DX) units at the point of use that are air-cooled, glycol-cooled or cooled by other means.

When selecting air-cooled or water-cooled chillers make sure that you have the required resources to support the system, from redundant power to redundant water supplies. In addition, rental companies specializing in emergency portable air conditioning offer pre-arranged contracts for emergency Heating Ventilating and Air Conditioning (HVAC) that can be invoked with a phone call. This could save you hours or even days of downtime. Remember, plan for your next disaster today. Make sure you know who to call, what equipment you will need, and that you have the provisions to connect it.

Control system design

The brain of your mission-critical facility is the multiple systems controlling the generators, switchgear, UPS systems, chillers, fire alarms, security and other mechanical and electrical systems. Make sure these systems are designed fault tolerant and redundant, and that loadable (including passwords) copies of the software are secure and available. In times of an emergency, you need to be able to reload and restore key systems independent of outside sources.

Temporary system provisioning

When disaster strikes, temporary equipment may be needed to support your facility. Without prior planning, connecting temporary equipment could require a total shutdown of your facility, and take a long time to complete. The use of temporary generators, fuel storage, UPS systems, batteries, load banks, chillers and even water could all be required at some point. Inspect your facility today to identify the breakers, fittings, access doors, temporary power provisions, space and access, and isolation valves that may be required to accommodate the temporary equipment.

Security design

When designing a security system for your facility it is important that you use multiple security measures to cope with security threats as well as to prevent unauthorized access to the building and the various rooms throughout the facility. There are three basic elements of physical security: Mechanical, Organizational and Natural.

Mechanical security
Mechanical (electronic systems) Security covers the use of security hardware, including access control, Closed Circuit Television (CCTV), door locks, monitoring systems, emergency call boxes and intrusion alarms.

- Access control systems – Access control systems regulate who is able to enter a building through devices such as electronic card readers and electronic locks on doors.
- Intrusion detectors – Intrusion detectors use sensors to detect either the open or closed status of protected points of entry. They can also determine the presence of a person in an area and the place where the alarm terminates.
- Surveillance systems – Surveillance systems use video cameras and monitors to alert people to events. Surveillance equipment is generally comprised of television cameras and monitors, video amplifiers, video switches, video recorders, audio recorders, and related cables, fittings and attachments.
- Traffic control – Vehicle traffic and parking should be controlled to prevent unauthorized vehicles from entering the property. The use of fences, gates, concrete barriers and bollards can be used to prevent and control access.

Organizational security
Organizational (security staff and procedures) Security covers the involvement in the security programs by management, security staff, tenants and employees.

Natural security
Natural (architectural elements) Security covers basic security philosophies involving property definition, natural surveillance and access control. It is important to note that while the data center is the brains of the mission-critical facility, the heart of the system is in the machine and equipment room. Too often, the data center is well protected, but the equipment rooms that power and protect the data center are left completely vulnerable. Access to the electrical and mechanical rooms should be protected and critical systems should monitored by CCTV.

EPO switches
Various Safety, Fire and Electrical codes require facilities to have an Emergency Power Off (EPO) system that powers down the facility in an emergency. These systems are required, but often too little thought is put into their design. The design of the EPO system should allow the system to work when needed, but should provide assurance that the system will not accidentally activate during upgrades and maintenance. The EPO system should require a dual method of activation, such as an alarmed button-cover that activates cameras, or other security devices when lifted.

Monitoring system design

Technology now allows monitoring of virtually any type of infrastructure equipment and environmental condition, on-site or remotely. Using this information, trending information can be gathered that can help predict equipment failure and inform you when a piece of equipment changes modes of operation or goes into alarm.

The ability to trend data from multiple points allows management to gather data sufficient for predictive analysis. With this data you can determine when to replace pump bearings, service batteries or rotate equipment. From generator vibration to chiller performance, monitoring the right data saves time and money while increasing system reliability.

Safety considerations

Safety goes hand-in-hand with reliability, saving time, money and possibly lives. A facility that is unsafe, cannot be reliable. Human costs aside, injuries and fatalities can cause equipment downtime. This downtime can be greatly extended for rescue and investigation efforts. Insist that your safety plans are up-to-date and are being followed. Before outside vendors work in your facility, demand a copy of their safety plan, and make sure it is current and adhered to. Develop a proper safety plan for the work that you perform in your facility, then train your staff on the safety plan. This should include the use and care of Personal Protection Equipment (PPE), Lock-out/Tag-out procedures, and the safety requirements for performing hot work. Ensure that employee safety is maintained prior to, during and after a disaster event. Prior to asking employees to evacuate the building, to re-enter a damaged building, or to respond to an affected location, the employer should make sure that they are not putting the employees in danger.

Site operation

Site Operation is an important part of the reliability of your mission-critical facility. A significant percentage of failures can be attributed to human error. Increasing reliability starts with knowing how your equipment operates, and how its failure will affect the facility. It is vital to post and use detailed operational, maintenance and recovery procedures. The development of detailed switch-level Methods of Procedure (MOPs) for every aspect of the mission-critical facility's infrastructure is essential. Test them, trust them, use them. The MOPs should be strictly adhered to using a Pilot/Co-Pilot approach. No matter how you decide to operate your facility, ensure that the staff is well trained. Schedule regular exercises that incorporate all of the operations and communications that will be required to maintain and recover your facility should disaster strike. Pay particular attention to what may need to be changed due to congested or ineffective communication or information. Revise your plans after each test. Record keeping is an important part of operations. You should have a system in place that will maintain your records and make them available to review.

Site maintenance

Proper maintenance is crucial to operating the highest level of reliability. Failure to perform proper maintenance, inevitably leads to failure of the system. During maintenance, it is important that detailed records be kept on the problems that were discovered and the action taken to correct them.

Predictive maintenance

A comprehensive Predictive Maintenance program can improve your facility's safety and reliability through early detection of equipment problems. The benefits of a successful Predictive Maintenance inspection program are tremendous. Predictive Maintenance anticipates trouble spots before a potential problem manifests itself. Some forethought and a solid foundation in managing the data of what is tested and what isn't, what problems were found and whether they were fixed, will provide the expected return on investment over time. Keeping it simple and remembering that it all boils down to increasing the reliability of your facility's equipment will be your guide to a world class Predictive Maintenance program.

Site commissioning

Plans on paper are essential, but infrastructure combines both the virtual world and the realm of the mechanical and environmental. It is bits and bytes as well as nuts and bolts. Commissioning is where designer's dreams and manufacturer's claims meet the real world. Commis-

sioning is the systematic process of verifying and documenting the performance of the facility's equipment by performing realistic testing.

Your facility's infrastructure is comprised of mechanical, electrical and control components and systems from numerous manufacturers, installed by a variety of specialized firms.The Commissioning process systematically tests and balances each system to ensure that it is installed properly and operates as specified.

Site Commissioning Services must ensure that your systems perform at the highest levels, right from the start. The best commissioning experts adhere to a thorough quality management process that validates and documents your facility and its systems. Commissioning methodologies cover a wide variety of procedures to verify the integrity and performance of your mission-critical facility's infrastructure, including:

- Commissioning Plan Preparation
- Pre-start-up and Start-up Procedures
- Integrated System Testing (IST)
- Operational Training and Turnover, including Development of Standard Operating Procedures (SOPs) and Methods of Procedure (MOPs)
- System (as built) Documentation

Training

A comprehensive Training program should be developed for all mission-critical faculties. It is important for the facility's reliability that you train the staff early and regularly. The construction phase and commissioning phase is an ideal time to get your operations staff up-to-speed on the equipment. Once your facility is operational, it is important that you have continuous training on safety, as well as the operation and maintenance of your equipment. The cost of training, in time and money, will be pay dividends in the future.

Conclusion

Keeping good company is key. Ultimately, mission-critical facilities run on technology, trust and teamwork. A highly-available infrastructure is the result of the concerted efforts of electricians and engineers, planners and plumbers, CIOs and cleaning crews, technicians, managers and maintenance teams. Your infrastructure provider works to orchestrate and coordinate the efforts of this diverse team to ensure your mission-critical facility delivers the performance and availability you require. For an asset as crucial as your mission-critical facility's infrastructure, it pays to invest the time to select a company you can trust, with the experience and resources to maximize uptime and mitigate risk. Ideally, your mission-critical infrastructure specialist will offer you all of the products, people, services and strategies needed to design, integrate, commission, staff, maintain, service and monitor your facility. Acquiring these crucial services from a single source can greatly reduce headaches and finger-pointing in the future. Of course, not every disaster can be avoided, but many would-be disasters can be prevented with proper planning and maintenance. And for unavoidable disasters, such as hurricanes, strategic disaster planning can minimize the disasters impact and provide the fastest recovery time possible. With each lesson learned, we are better prepared to deal with the next challenge. As Henry Ford once said, "Failure is only the opportunity to begin again more intelligently."

Resources

Click on icon to link to resource

Maximizing Uptime in Mission-Critical Facilities
White Paper 7

Site Selection for Mission Critical Facilities
White Paper 81

The Top 9 Mistakes in Data Center Planning
White Paper 145

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