energycentral

HOME

MORE

Login

EVENTS

Add Event

Edit Event

Home

An Overview of Business Resiliency in Today's Mission Critical Building

Peter Curtis | Aug 09, 2006

Continuous and uninterrupted power and cooling comprise the lifeblood of any data center, especially those that operate 24 hours a day, 7 days a week. Critical enterprise power is the power without which an organization would quickly be unable to achieve its business objectives. Today enterprises of all types and sizes are demanding 24-hour IT system availability. This means enterprises must have 24-hour power and cooling day after day, year after year. One example is the banking and financial services industry. Business practices mandate continuous uptime for all computer and network equipment to facilitate round-the-clock trading and banking activities everywhere in the world. Financial service firms are completely intolerant of unscheduled downtime, given the guaranteed loss of business that results. However, providing the best equipment is not enough to ensure 24-hour operation throughout the year. The goal is to achieve reliable 24-hour power and cooling supply at all times, regardless of the technological sophistication of the equipment or the demands placed upon that equipment by the end user, be it business or municipality.

It is also necessary for critical industries to constantly and systematically evaluate their mission critical support systems, assess their level of risk tolerance versus cost of downtime, and plan for future upgrades in equipment and services designed to ensure uninterrupted power and cooling supply. Simply put, minimizing unplanned downtime, and reducing or eliminating planned downtime reduces risk. The interconnectedness of robust software applications, coupled with a growing global digital economy continues to drive the requirements for business resiliency, thereby increasing the levels of complexity of the critical infrastructure. Providing continuous operation under all foreseeable risks of failure such as power outages, equipment breakdown, internal fires, etc., requires use of modern design techniques and an appropriate critical infrastructure to enhance reliability. These include redundant systems and components, standby power generation, fuel systems, automatic transfer and static switches, UPS systems, cooling systems, raised access floors, fire protection, as well as the use of Probability Risk Analysis modeling software, used to predict potential future outages, develop maintenance programs and upgrade emergency action plans for all major systems.

Also vital to the facility's lifecycle is clear communication between upper management, facilities and IT departments. Only when all parties fully understand the three mainstays of power and cooling reliability: design, maintenance and operation of the critical infrastructure, can they properly fund and implement a resilient plan.

Risk Assessment

Critical industries require an extraordinary degree of planning and evaluation. In order to design a critical business function with the appropriate level of reliability, the cost of downtime and the associated risks need to be identified. Planning for success creates considerable pressure to design an infrastructure that will change over time in order to support continuous growth. Routine maintenance and upgrading equipment alone does not ensure business resiliency. Employing new methods of delivering critical electrical and mechanical support, understanding capital cost constraints and developing processes that minimize human error are key factors in improving recovery time in the event critical systems are impacted by internal failures or external disasters. A program known as Probability Risk Assessment (PRA) addresses the hazards affecting data center uptime. PRA looks at the probability of failure of each type of critical component. It can be used to predict availability, average number of failures per year and average annual downtime. PRA is also a facilitating agent when assessing each step listed in the Facilities Resiliency Process below.

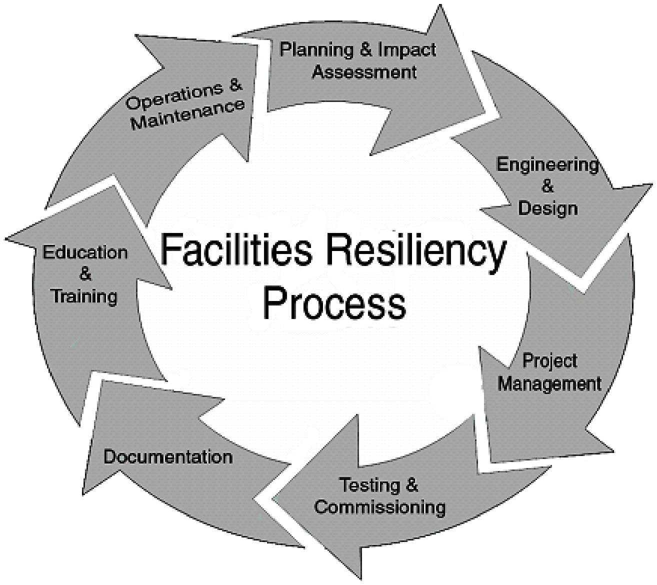


Fig 1 – Facilities Resiliency Process

These processes are so important in today's world that the industry has established regulations and policies, such as Basel II, to protect infrastructure. Basel II recommends "three pillars" to bring stability to critical industries – risk appraisal and control, supervision of assets and the monitoring of financial markets. Basel II involves identifying operational risk and then allocating adequate capital to cover potential loss. A survey concerning human error and its effects on downtime was conducted by Liebert Corporation in 2004, 500 IT and Facilities professionals were interviewed. It showed that 79% considered downtime from human error to be possible or highly probable. Considering that the mission critical industry requires a 99.9 to 99.999 availability, this survey shows that it is imperative to give more attention to the above Facilities Resiliency Process, particularly to Documentation, Education/Training and Operational Maintenance. Up to date documentation, refreshed employee training and ongoing equipment maintenance results in improved emergency preparedness and awareness during critical events. This is the lowest cost method that a company can invest in to increase business resiliency. The goal is to retain all facets of intellectual assets while business continues to undergo constant changes and employee turnover/attrition. The National Institute of Standards and Technology estimates an annual loss of $15.8 billion, or $.18 per SF, due to time spent locating, verifying and recreating facility data. In order for information to be implemented properly, it must be transitioned from storage rooms to an electronic secure browser application, as illustrated below by using the intellectual capital data structure tree. Essentially, there needs to be a transition from unavailable and inefficient data, to data that is easily accessible to enhance a business enterprise.

Fig 2 – Data Transition

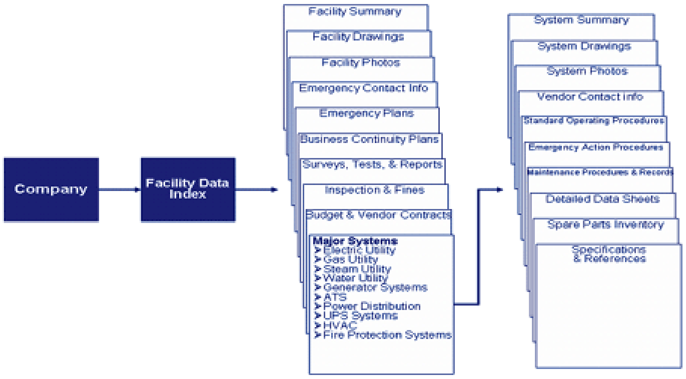


Fig 3 - Intellectual Capital Data Structure Tree

The constant dilemma of meeting the challenges of an already constrained budget can become a limiting factor in achieving optimum reliability. Today IT and Facilities professionals are being asked to do more with less, thus increasing operational risk. The leveraging of intellectual assets is one way to combat this problem.

Aligning Business Strategy with Expenditures

Business losses due to downtime alone total billions of dollars a year globally. Capital project spending must be aligned with the organization's business strategy as well as how their critical infrastructure can be shutdown (or remain operating) during annual routine maintenance.

Many organizations associate disaster recovery and business continuity only with IT and communication functions and miss other areas that seriously impact their business. A strategy that guarantees recovery has an impact on employees, facilities, power, critical infrastructure, customer service, billing and customer relations. All areas require a clear approach based on recovery time objectives, cost and profitability impact. At minimum, the decision is based on the following factors:

- The minimum computer and communication equipment required for the most critical applications
- The maximum allowable delay time prior to the initiation of the recovery process
- The time frame required to execute the recovery process once it begins
- The minimum space requirements for essential staff members and equipment
- The total cost involved in the recovery process and the total loss as a result of downtime

Capital projects and operating budgets require consideration of these factors. Developing strategies with implementation steps means no time is wasted in a recovery scenario. The right strategy will quickly and effectively mitigate damages and minimize the cost of downtime.

Change Management

The Mission Critical Industry today has an infrastructure primarily composed of silicon and information. Business resiliency rests at the mercy of the mission critical facilities sustaining them. In some cases the backup power fails, power generation is not initiated, there is a mechanical failure or the fuel supply is exhausted. A thorough problem-tracking system and a strong change management system is essential to an Emergency Preparedness plan.

Change management crosses many departments and must be coordinated and used by all participants to work effectively. Management needs to plan for the future, to make decisions on how to support the anticipated needs of the organization, especially under emergency situations.

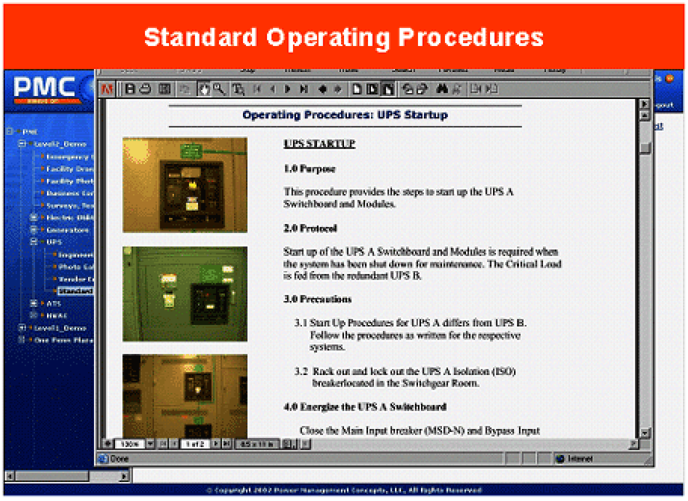
Testing and Commissioning

Facilities engineers must work with A&E firms, contractors, vendor field engineers and independent test consultants to coordinate testing and commissioning activities. Many decisions regarding how and when to service a facility's mission critical power, fire/life safety equipment and cooling equipment are going to be subjective. The objective is clear: a high level of safety and availability from the equipment, components and systems. Common practice is for personnel to perform maintenance without reviewing prior records. Maintenance programs should be continuously improved so that previous report knowledge can facilitate ongoing maintenance.

Twenty-five years ago the Mission Critical Facility Engineering Industry was in its infancy and technology was simple. There was little sophistication in the electrical load profile and equipment was forgiving of cooling failure. As more computer hardware occupied the data center, the design of systems supporting the electrical load became more complicated, as did business applications. With businesses relying on this infrastructure, more capital went toward improving the uptime of business lines. The mission critical industry can no longer manage theses critical systems as it did 25 years ago. Today the sophistication of the data center infrastructure necessitates perpetual documentation refreshing. Surprisingly, human factors are the most poorly understood aspect of process safety and reliability management.

Balancing system design and training staff in a cost effective manner is essential to critical infrastructure planning. When designing a mission critical facility, the level of complexity contrasted with ease of maintainability is a major concern. A recipe for human error exists when systems are complex and customized, especially if key system operators and effective documentation of Emergency Action Procedures

(EAP) and Standard Operating Procedures (SOP) are not immediately available. A simplistic electrical system design will allow for quicker and easier troubleshooting during critical times.



Standard Operating Procedures

Operating Procedures: UPS Startup

UPS STARTUP

1.0 Purpose

This procedure provides the steps to start up the UPS A Switchboard and Modules.

2.0 Protocol

Start up of the UPS A Switchboard and Modules is required when the system has been shut down for maintenance. The Critical Load is fed from the redundant UPS B.

3.0 Precautions

3.1 Start Up Procedures for UPS A differs from UPS B. Follow the procedures as written for the respective systems.

3.2 Rack out and lock out the UPS A Isolation (ISO) breakerlocated in the Switchgear Room.

4.0 Energize the UPS A Switchboard

Close the Main Input breaker (MSD-N) and Bypass Input

When designing a mission critical facility, a budgeting and auditing plan should be established. The importance of testing and commissioning, especially in mission critical facilities, cannot be stressed enough. If not, the next opportunity will come at a much higher price: downtime, lost business and clients, not to mention safety issues. So do it correctly ahead of time, and avoid shortcuts. Plug and play is not an option when critical systems are deployed.

Education/ Training and Documentation

Despite attaining high levels of technological standards in the mission critical industry, most of today's financial resources remain allocated for planning, equipment procurement, construction and continued research/development. The diversity among mission critical systems severely hinders the ability to master all necessary equipment and relevant information.

Today millions of dollars are invested into the critical environment that supports a 24/7 business application. To sustain the highest levels of reliability we also now must add budget dollars for testing/commissioning, documentation (MOP'S, SOP'S, EAP's) and education/training. Just as we train our airline pilots; a formal training program is imperative to the successful operation of critical environments. Would you step aboard a commercial airline jet if you had reason to believe that the pilot was not formally trained? The level of sophistication built into the data center that maintains our digital society can carry a price tag between $20,000,000 and $200,000,000, and can be compared to the dashboard of a high performance aircraft.

A growing concern within the Mission Critical Industry is how businesses can manage and safeguard intellectual assets. According to NIST, 71 percent of design and engineering documentation maintained by facility executives is still recorded on paper. Intellectual assets are often in the form of pictures, drawings and other images not easily stored in databases. A survey of 200 business executives found that more than half rely on imaging databases and spreadsheets to manage intellectual assets. This means that spreadsheets and images are scattered about employee's desktops which makes assets more susceptible to loss or theft. This leads to the need for an electronic, centrally managed data base system. 54% cite that with an efficient electronic system there is improved protection from theft, increased accountability, and improved ability to share information companywide internally and externally with partners.

Operations and Maintenance

An effective maintenance and testing program for your mission critical loads is imperative to protecting your investment. Maintenance procedures and schedules must be developed, staff properly trained, spare parts provisioned and mission critical equipment evaluated regularly. Predictive maintenance, preventive maintenance and Reliability Centered Maintenance (RCM) programs play a critical role in the reliability of mission critical systems.

How often should maintenance be performed? Part of the answer lies in what level of reliability your company can live with. What are your expectations in terms of risk tolerance or goals with regard to uptime? If your company can live with 99% reliability, or 87.6 hours of downtime per year, then the answer would be to run a maintenance program every 3 to 5 years. However, if 99.999% reliability, or 5.25 minutes of downtime per year is mandatory, then you need to perform an aggressive preventive maintenance program every 6 months.

There are several excellent resources available for developing a testing and maintenance program. One is the InterNational Electric Testing Association (NETA), which publishes the Maintenance Testing Specifications that recommends frequencies of maintenance tests. Another is the National Fire Protection Association's (NFPA) 70B Recommended Practice for Electrical Equipment Maintenance. These publications, along with manufacturer's recommendations, give guidance for maintenance tasks and schedules to incorporate in your maintenance program.

Traditionally, the goal of a maintenance program has been to reduce and avoid equipment failures. RCM was developed to shift the focus to understanding the failure effect upon the process it protects. The effects of each failure are analyzed and ranked according to their impact on safety, environment, business mission and cost. Failures with a significant impact are further analyzed to determine their root causes. Finally, preventive or predictive maintenance is assigned based on the analysis, with emphasis on condition-based procedures to ensure optimal performance.

Employee Certification – Standards & Benchmarking

Technology is driving itself faster than ever. Large investments are made in new technologies to keep up to date with advancements, yet industries are still faced with operational challenges. One possible reason is the limited training provided to employees operating the mission critical support equipment. Employee certification is crucial not only to keeping up with changing technology, but also to promote quick emergency response when called upon. In the last few years, technologies have been developed to solve the technical problem of linkage and interaction of equipment but there remains a lack of well-trained personnel. How can we validate that the workforce meets the complex requirements of the facility to insure high levels of reliability?

The answer is to internally identify core business resiliency needs, then partner with an organization that can assist in the process. Great care should be taken to ensure critical functions that will minimize down time. As mentioned previously, preventive maintenance and testing are crucial. The most important aspect of benchmarking is that it is driven by the participants whose goal is to improve their organization. It is a process through which organizations learn about the successful practices of others, and then draw on those cases to develop solutions most suitable for themselves. True process benchmarking identifies the “hows” and “whys” for performance gaps and helps organizations to perform with higher standards of practice. Remember, if you can’t find the time to do it right the first time… when will you find the time to do it over?

Related Topics

- Information Technology

Comments

No Comments