Chapter 1

An Overview of Reliability and Resilience in Today's Mission Critical Facilities

COPYRIGHTED MATERIAL

1.1 INTRODUCTION

Continuous, clean, and uninterrupted power is the lifeblood of any data center, especially one that operates 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 more than ever, enterprises of all types and sizes are demanding 24-hour system availability. This means that enterprises must have 24-hour power day after day, year after year. One such 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 anywhere and everywhere in the world. Banking and financial service firms are completely intolerant of unscheduled downtime, given the guaranteed loss of business that invariably 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 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.

The banking and financial services industry is constantly expanding to meet the needs of the growing global digital economy. The industry as a whole has been innovative in the design and use of the latest technologies, driving its businesses to become increasingly digitized in this highly competitive business environment. The industry is progressively more dependent on continuous operation of its data centers in reaction to the competitive realities of a world economy. To achieve

Maintaining Mission Critical Systems in a 24/7 Environment By Peter M. Curtis
Copyright © 2007 The Institute of Electrical and Electronics Engineers, Inc.

optimum reliability when the supply and availability of power are becoming less certain is challenging to say the least. The data center of the past required only the installation of stand-alone protective electrical and mechanical equipment mainly for computer rooms. Data centers today operate on a much larger scale—that is, 24/7. The proliferation of distributed systems using hundreds of desktop PCs and workstations connected through LANs and WANs that simultaneously use dozens of software business applications and reporting tools makes each building a "computer room." If we were to multiply the total amount of locations utilized by each bank and financial service firm that are tied together all over the would through the internet, then we would see the necessity of uninterrupted power supply, uptime, and reliability.

The face of Corporate America was severely scarred in the last few years by a number of historically significant events: the collapse of the dot.com bubble and high-profile corporate scandals like Enron and WorldCom. These events have taken a significant toll on financial markets and have served to deflate the faith and confidence of investors. In response, governments and other global organizations enacted new or revised existing laws, policies, and regulations. In the United States, laws such as the Sarbanes–Oxley Act of 2002 (SOX), Basel II, and the U.S. Patriot Act were created. In addition to management accountability, another embedded component of SOX makes it imperative that companies not risk losing data or even risk downtime that could jeopardize accessing information in a timely fashion. Basel II recognizes that infrastructure implementation involves identifying operational risk and emphasizes the allocation of adequate capital to cover potential loss. These laws can actually improve business productivity and processes.

Many companies thoughtlessly fail to consider installing backup equipment or the proper redundancy based on their risk profile. Then when the lights go out due to a major power outage, these same companies suddenly wake up, and they end up taking a huge hit operationally and financially. During the months following the Blackout of 2003, there was a marked increase in the installation of UPS systems and standby generators. Small and large businesses alike learned how susceptible they are to power disturbances and the associated costs of not being prepared. Some businesses that were not typically considered mission critical learned that they could not afford to be unprotected during a power outage. The Blackout of 2003 emphasized the interdependencies across the critical infrastructure, as well as the cascading impacts that occur when one component falters. Most ATMs in the affected areas stopped working, although many had backup systems that enabled them to function for a short period. Soon after the power went out, the Comptroller of the Currency signed an order authorizing national banks to close at their discretion. Governors in a number of affected states made similar proclamations for state-chartered depository institutions. The end result was a loss of revenue and profits and almost the loss of confidence in our financial system. More prudent planning and the proper level of investment in mission critical infrastructure for electric, water, and telecommunications utilities coupled with proactive building infrastructure preparation could have saved the banking and financial services industry millions.

At the present time, the risks associated with cascading power supply interruptions from the public electrical grid in the United States have increased due to the ever-increasing reliance on computer and related technologies. As the number of computers and related technologies continue to multiply in this ever-increasing digital world, the demand for reliable quality power increases as well. Businesses not only compete in the marketplace to deliver whatever goods and services are produced for consumption, but now must compete to hire the best engineers from a dwindling pool of talent who can design the best infrastructures needed to obtain and deliver reliable power to keep mission critical manufacturing and technology centers up and running to produce the very goods and services that are up for sale. The idea that businesses today must compete for the best talent to obtain reliable power is not new, as are the consequences of failing to meet this competition. Without reliable power, there are no goods and services for sale, no revenues, and no profits—only losses while the power is out. Hiring and keeping the best-trained engineers employing the very best analyses, making the best strategic choices, and following the best operational plans to keep ahead of the power supply curve are essential for any technologically sophisticated business to thrive and prosper. A key to success is to provide proper training and educational resources to engineers so they may increase their knowledge and keep current on the latest mission critical technologies available the world over. In addition, all companies need to develop a farm system of young mission critical engineers to help combat the continuing diluted work force for the growing mission critical industry.

It is also necessary for critical industries to constantly and systematically evaluate their mission critical systems, assess and reassess their level of risk tolerance versus the cost of downtime, and plan for future upgrades in equipment and services designed to ensure uninterrupted power supply in the years ahead. Simply put, minimizing unplanned downtime reduces risk. Unfortunately, the most common approach is reactive—that is, spending time and resources to repair a faulty piece of equipment after it fails as opposed to identifying when the equipment is likely to fail and repairing or replacing it without power interruption. If the utility goes down, install a generator. If a ground-fault trips critical loads, redesign the distribution system. If a lightning strike burns power supplies, install a new lightning protection system. Such measures certainly make sense, because they address real risks associated with the critical infrastructure; however, they are always performed after the harm has occurred. Strategic planning can identify internal risks and provide a prioritized plan for reliability improvements that identify the root causes of failure before they occur.

In the world of high-powered business, owners of real estate have come to learn that they, too, must meet the demands for reliable power supply to their tenants. As more and more buildings are required to deliver service guarantees, management must decide what performance is required from each facility in the building. Availability levels of 99.999% (5.25 minutes of downtime per year) allow virtually no facility downtime for maintenance or for other planned or unplanned events. Moving toward high reliability is imperative. Moreover, avoiding the landmines that can cause outages and unscheduled downtime never ends. Even planning

and impact assessments are tasks that are never completed; they should be viewed afresh at least once every budget cycle.

The evolution of data center design and function has been driven by the need for uninterrupted power. Data centers now employ many unique designs developed specifically to achieve the goal of uninterrupted power within defined project constraints based on technological need, budget limitations, and the specific tasks each center must achieve to function usefully and efficiently. Providing continuous operation under all foreseeable risks of failure such as power outages, equipment breakdown, internal fires, and so on, requires use of modern design techniques to enhance reliability. These include redundant systems and components, standby power generation, fuel systems, automatic transfer and static switches, pure power quality, UPS systems, cooling systems, raised access floors, and fire protection, as well as the use of Probability Risk Analysis modeling software (each will be discussed in detail later in this book) to predict potential future outages and develop maintenance and upgrade action plans for all major systems.

Also vital to the facilities life cycle is two-way communication between upper management and facilities management. Only when both ends fully understand the three pillars of power reliability—design, maintenance, and operation of the critical infrastructure (including the potential risk of downtime and recovery time)—can they fund and implement an effective plan. Because the costs associated with reliability enhancements are significant, sound decisions can only be made by quantifying performance benefits against downtime cost estimates for each upgrade option to determine the best course of action. Planning and careful implementation will minimize disruptions while making the business case to fund necessary capital improvements and implement comprehensive maintenance strategies. When the business case for additional redundancy, specialized consultants, documentation, and ongoing training reaches the boardroom, the entire organization can be galvanized to prevent catastrophic data losses, damage to capital equipment, and danger to life and limb.

1.2 RISK ASSESSMENT

Critical industries require an extraordinary degree of planning and assessing. It is important to identify the best strategies to reach the targeted level of reliability. In order to design a critical building with the appropriate level of reliability, the cost of downtime and the associated risks need to be assessed. It is important to understand that downtime occurs due to more than one type of failure: design failure, catastrophic failures, compounding failures, or human error failures. Each type of failure will require a different approach on prevention. A solid and realistic approach to disaster recovery must be a priority, especially because the present critical area is inevitably designed with all the eggs located in one basket.

Planning the critical area in scope of banking and financial services places considerable pressure to design an infrastructure that will change over time in an effort to support the continuous business growth. Routine maintenance and upgrading equipment alone does not ensure continuous power. The 24/7 operations

of such service mean an absence of scheduled interruptions for any reason including routine maintenance, modification, or upgrades. The main question is how and why infrastructure failures occur. Employing new methods of distributing critical power, understanding capital constraints, and developing processes that minimize human error are some key factors in improving recovery time in the event critical systems are impacted by base-building failures.

The infrastructure reliability can be enhanced by conducting a formal Risk Management Assessment (RMA) and a gap analysis and by following the guidelines of the Critical Area Program (CAP). The RMA and the CAP are used in other industries and customized specifically for needs of Data Center environments. The RMA is an exercise that produces a system of detailed, documented processes, procedures, checks, and balances designed to minimize operator and service provider errors. The practice CAP ensures that only trained and qualified people are associated and authorized to have access to critical sites. These programs coupled with Probability Risk Assessment (PRA) address the hazards of data center uptime. The PRA looks at the probability of failure of each type of electrical power equipment. Performing a PRA can be used to predict availability, number of failures per year, and annual downtime. The PRA, RMA, and CAP are facilitating agents when assessing each step listed below.

- Engineering and design
- Project management
- Testing and commissioning
- Documentation
- Education and training
- Operation and maintenance
- Employee certification
- Risk indicators related to ignoring the Facility Life Cycle Process
- Standard and benchmarking

Industry regulations and policies are more stringent than ever. They are heavily influenced by Basel II, Sarbanes–Oxley Act (SOX), NFPA 1600, and U.S. Securities and Exchange Commission (SEC). Basel II recommends “three pillars”—risk appraisal and control, supervision of the assets, and monitoring of the financial market—to bring stability to the financial system and other critical industries. Basel II implementation involves identifying operational risk and then allocating adequate capital to cover potential loss. As a response to corporate scandals such as Enron and WorldCom, SOX came into force in 2002 and passed the following act: The financial statement published by issuers is required to be accurate (Sec 401); issuers are required to publish information in their annual reports (Sec 404); and issuers are required to disclose to the public, on an urgent basis, information on material changes in their financial condition or operations (Sec 409) and impose penalties of fines and/or imprisonment for not complying (Sec 802).

The purpose of the NFPA 1600 Standard is to help the disaster management, emergency management, and business continuity communities to cope with disasters and emergencies. Keeping up with the rapid changes in technology has been a long-standing priority. The constant dilemma of meeting the required changes within an already constrained budget can become a limiting factor in achieving optimum reliability.

1.3 CAPITAL COSTS VERSUS OPERATION COSTS

Businesses rest at the mercy of the mission critical facilities sustaining them. Each year, $20.6 billion is spent on the electrical and mechanical infrastructure that supports IT in the United States. Business losses due to downtime alone total $46 billion per year globally. An estimated 94% of all businesses that suffer a large data loss go out of business within two years regardless of the size of the business. The daily operations of our economic system depend on the critical infrastructure of the banking and finance services.

Critical industries are operating continuously, 365 days. Because conducting daily operations necessitate the use of new technology, more and more servers are being packed into a single rack. The growing numbers of servers operating 24/7 increases the need for power, cooling, and airflow. When a disaster causes the facility to experience lengthy downtime, a prepared organization is able to quickly resume normal business operations by using a predetermined recovery strategy. Strategy selection involves focusing on key risk areas and selecting a strategy for each one. Also, in an effort to boost reliability and security, the potential impacts and probabilities of these risks as well as the costs to prevent or mitigate damages and the time to recover should be established.

Many organizations associate disaster recovery and business continuity only with IT and communications functions and miss other critical areas that can seriously impact their business. One major area that necessitates strategy development is the banking and financial service industry. The absence of strategy that guarantees recovery has an impact on employees, facilities, power, customer service, billing, and customer and public relations. All areas require a clear, well-thought-out strategy based on recovery time objectives, cost, and profitability impact. The strategic decision is based on the following factors:

- 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 computer configuration required to process critical applications
- The minimum communication device and backup circuits required for critical applications
- 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.

Developing strategies with implementation steps means that no time is wasted in a recovery scenario. The focus is to implement the plan quickly and successfully. The right strategies implemented will effectively mitigate damages and minimize the disruption and cost of downtime.

1.4 CHANGE MANAGEMENT

To provide an uncompromising level of reliability and knowledge of the critical operations contributing to the success of maintaining 100% uptime of the U.S. critical infrastructure, it is crucial to define Mission Critical based on today's industry. The Mission Critical Industry today has an infrastructure primarily composed of silicon and information. Business continuity relies on the mission critical facilities sustaining them.

The Blackout of 2003 resulted in an economic loss estimated at between $700 million and $1 billion to New York City alone. Many city offices and private sector functions did not have sufficient backup power in place, including key agencies such as the Department of Health and Mental Hygiene, Department of Sanitation, and Department of Transportation, and certain priority areas of hospitals. In some cases the backup power failed to operate, failed to initiate power generation, and experienced mechanical failure or exhaustion of fuel supply. Whatever the nature of the problem, it is important to understand the underlying process by which an organization should handle problems and changes. A thorough problem tracking system and a strong change management system is essential to an Emergency Preparedness plan.

Change management crosses departments and must be coordinated and used by all participants to work effectively. Management needs to plan for the future and to make decisions on how to support the anticipated needs of the organization, especially under emergency situations. It is also imperative to understand that we cannot manage today's critical infrastructure the way we did in the early 1980s. Our digital-society needs are very different today.

1.5 TESTING AND COMMISSIONING

Before the facility goes on-line, it is crucial to resolve all potential equipment problems. This is the construction team's sole opportunity to integrate and commission all the systems, due to the facility's 24/7 mission critical status. At this point in the project, all systems installed were tested at the factory and witnessed by a competent independent test engineer familiar with the equipment.

Once the equipment is delivered, set in place, and wired, it is time for the second phase of certified testing and integration. The importance of this phase is to verify and certify that all components work together and to fine-tune, calibrate, and integrate the systems. There is a tremendous amount of preparation in this phase. The facilities engineer must work with the factory, field engineers, and independent test consultants to coordinate testing and calibration. Critical circuit breakers must be tested and calibrated prior to placing any critical electrical load on them. When all the tests are completed, the facilities engineer must compile the certified test

reports, which will establish a benchmark for all-future testing. The last phase is to train the staff on each major piece of equipment. This phase is an ongoing process and actually begins during construction.

Many decisions regarding how and when to service a facility's mission critical electrical power distribution equipment are going to be subjective. The objective is easy: a high level of safety and reliability from the equipment, components, and systems. But discovering the most cost-effective and practical methods required to accomplish this can be challenging. Network with colleagues, consult knowledgeable sources, and review industry and professional standards before choosing the approach best suited to your maintenance goals. Also, keep in mind that the individuals performing the testing and service should have the best education, skills, training, and experience available. You depend on their conscientiousness and decision-making ability to avoid potential problems with perhaps the most crucial equipment in your building. Most importantly, learn from your experiences, and those of others. Maintenance programs should be continuously improving. If a task has historically not identified a problem at the scheduled interval, consider adjusting the schedule respectively. Examine your maintenance programs on a regular basis and make appropriate adjustments.

Acceptance and maintenance testing are pointless unless the test results are evaluated and compared to standards, as well as to previous test reports that have established benchmarks. It is imperative to recognize failing equipment and to take appropriate action as soon as possible. Common practice in this industry is for maintenance personnel to perform maintenance without reviewing prior maintenance records. This approach defeats the value of benchmarking and trending and must be avoided. The mission critical facilities engineer can then keep objectives in perspective and depend upon his options when faced with a real emergency.

The importance of taking every opportunity to perform preventive maintenance thoroughly and completely—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 lost potential clients, not to mention the safety issues that arise when technicians rush to fix a maintenance problem. So do it correctly ahead of time, and avoid shortcuts.

1.6 DOCUMENTATION AND HUMAN FACTOR

The mission critical industry's focus on physical enhancements descends from the early stages of the trade, when all efforts were placed solely in design and construction techniques to enhance mission critical equipment. At the time, technology was primordial and there was a significant need to refine and perfect mission critical electrical and mechanical systems.

Twenty-five years ago the technology supporting mission critical loads was simple. There was little sophistication in the electrical load profile; at that time the Mission Critical Facility Engineering Industry was in its infancy. Over time the data centers have grown from a few mainframes supporting minimal software applications to LAN farms that can occupy 25,000 SF or more.

As more computer hardware occupied the data center, the design of the electrical and mechanical systems supporting the electrical load became more complicated as did the business applications. With businesses relying on this infrastructure, more capital dollars were invested to improve the uptime of the business's lines. Today billions of dollars are invested on an enterprise level into the infrastructure that supports the business 24/7 applications; the major investments are normally in design, equipment procurement, and project management. Few capital dollars are invested in documentation, a significant step in achieving optimum level of reliability.

Years ago, most organizations heavily relied on their workforce to retain much of the information regarding the mission critical systems. A large body of personnel had a similar level of expertise. They remained with their company for decades. Therefore, little emphasis was placed on maintaining a living document for a critical infrastructure.

The mission critical industry can no longer manage their critical system as they did 25 years ago. Today the sophistication of the data center infrastructure necessitates perpetual documentation refreshing. One way to achieve this is to include a living document system that provides the level of granularity necessary to operate a mission critical infrastructure into a capital project. This will assist in keeping the living document current each time a project is completed or milestone is reached. Accurate information is the first level of support that provides first responders the intelligence they need to make informed decisions during critical events. It also acts like a succession plan as employees retire and new employees are hired thus reducing risk and improving their learning curve.

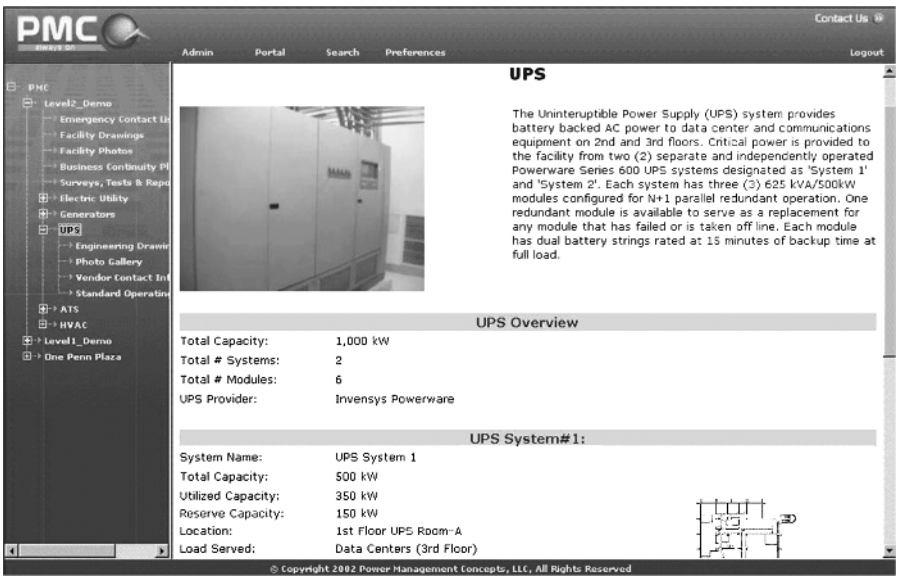

Figure 1.1 Typical screenshot of M. C. Access. (Courtesy of Power Management Concepts, LLC.)

Figure 1.2 M. C. Access. (Courtesy of Power Management Concepts, LLC.)

Human error as a cause of hazard scenarios must be identified, and the factors that influence human errors must be considered. Human error is a given and will arise in all stages of the process. It is vital that the factors influencing the likelihood of errors be identified and assessed to determine if improvements in the human factors design of a process are needed. Surprisingly, human factors are perhaps the most poorly understood aspect of process safety and reliability management.

Balancing system design and training operating staff in a cost-effective manner is essential to critical infrastructure planning. When designing a mission critical facility, the level of complexity and ease of maintainability is a major concern. When there is a problem, the Facilities Manager (FM) is under enormous amounts of pressure to isolate the faulty system while maintaining data center loads and other critical loads. The FM does not have the time to go through complex switching procedures during a critical event. A recipe for human error exists when systems are complex, especially if key system operators and documentation of Emergency Action Procedures (EAP) and Standard Operating Procedures (SOP) are not immediately available. A rather simplistic electrical system design will allow for quicker and easier troubleshooting during this critical time.

To further complicate the problem, equipment manufacturers and service providers are challenged to find and retain the industry's top technicians within their own company. As 24/7 operations become more prevalent, the talent pool available will continue to diminish. Imagine an FM responsible for 20 mission critical facilities around the globe. This would indicate that response times could increase from the current standard of four hours to a much higher and less tolerable timeframe. The need for a simplified, easily accessible, and well-documented design is only

further substantiated by the growing imbalance of supply and demand of highly qualified mission critical technicians.

When designing a mission critical facility, a budgeting and auditing plan should be established. Over 60% of downtime is due to human error. Each year, substantial amounts of money are spent on building infrastructure, but inadequate capital is allocated to sustain that critical environment through the use of proper documentation, education and training.

1.7 EDUCATION AND TRAINING

Technology has been progressing faster than Moore's Law. Despite attaining high levels of technological standards in the mission critical industry, most of today's financial resources remain allocated for planning, engineering, equipment procurement, project management, and continued research and development. Unfortunately, little attention is given to the actual management of these systems. As equipment reliability increases, a larger percentage of downtime results from actions by personnel that were not properly trained or do not have access to accurate data during crisis events. Currently, there is a great need to educate and train facility engineers and operators in a swift manner, allowing a more efficient employee learning curve and in the process reducing risk because the employee can respond with situational awareness. Informed decision-making comes with familiar emergency action and standard operating procedures. The diversity among mission critical systems severely hinders people's ability to fully understand and master all necessary equipment and relevant information.

1.8 OPERATION AND MAINTENANCE

What can facility managers do to ensure that their electrical system is as reliable as possible? The seven steps to improved reliability and maintainability are:

- Planning and impact assessment
- Engineering and design
- Project management
- Testing and commissioning
- Documentation
- Education and training
- Operations and maintenance

Hire competent professionals to advise each step of the way. When building a data processing center in an existing building, you do not have the luxury of designing the electrical system from scratch. A competent electrical engineer will design a system that makes the most of the existing electrical system. Use electrical

contractors who are experienced in data processing installations. Do not attempt to save money using the full 40% capacity for a conduit, because as quickly as new, state-of-the-art equipment is installed, it is de-installed. Those same number 12 wires will need to come out of the conduit without disturbing the working computer hardware.

Have an experienced electrical testing firm inspect the electrical system, perform tests on circuit breakers, and use thermal-scan equipment to find "hot spots" due to improper connections or faulty equipment. Finally, you should plan for routine shutdowns of your facility so that you can perform preventive maintenance on electrical equipment. Facility managers as well as senior management must not underestimate the cost-effectiveness of a thorough preventive maintenance program. Electrical maintenance is not a luxury; it is a necessity. Again, do you want electrical outages to be scheduled or unscheduled?

Integrating the ideal infrastructure is just about impossible. Therefore, seek out the best possible industry authorities to solve your problems. Competent consultants will have the knowledge, tools, testing equipment, training, and experience necessary to understand the risk tolerance of your company, as well as recommend and implement the proper and most-advanced proven designs.

Whichever firms you choose, always ask for sample reports, testing procedures, and references. Your decisions will determine the system's ultimate reliability, as well as the ease of system maintenance. Seek experienced professionals from within and without your own company: information systems, property, and operations managers, space planners, and the best consultants in the industry for all engineering disciplines. The bottom line is to have proven organizations working on your project.

1.9 EMPLOYEE CERTIFICATION

Empowering employees to function as communication allies can be achieved through a well-planned certification program. Employees have a vested interest in working with management to prevail over the crisis, and many are eager to actively promote the company's positions internally as well as externally. Empowering employees to take charge in times of crisis creates valuable communication allies who not only reinforce core messages internally, but also carry them into the community. The internal crisis communication should be conducted using established communication channels and venues in addition to those that may have been developed to manage specific crisis scenarios. Whichever method of internal crisis communication a company may choose, the more upfront management is about what is happening, the better-informed and more confident employees feel.

In this way, security can be placed on an operation or a task requiring that an employee be certified to perform that action. Certification terms should be defined by the factory and should include training or even periodic recertification as desired. Another way of evaluating certified behavior is to examine employee performance

including times and yields. Should these evaluations fall too far below standard over a period of time, the system could recommend decertification.

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 equipments. Employee certification is crucial not only to keep up with advanced technology, but also to promote quick emergency response. In the last few years, technologies have been developed to solve the technical problem of linkage and interaction of equipment, but without well-trained personnel. How can we confirm that the employee meets the complex requirements of the facility to ensure high levels of reliability?

1.10 STANDARD AND BENCHMARKING

The past decade has seen wrenching change for many organizations. As firms and institutions have looked for ways to survive and remain profitable, a simple but powerful change strategy called "benchmarking" has become popular. The underlying rationale for the benchmarking process is that learning by example and from best-practice cases is the most effective means of understanding the principles and the specifics of effective practices. Recovery and redundancy together cannot provide sufficient resiliency if they can be disrupted by a single unpredictable event. A mission critical data center designed and developed as mentioned above must be able to endure hazards of nature, such as earthquakes, tornados, floods, and other natural disasters, as well as human made hazards. Great care should be taken to ensure critical functions that will minimize downtime. Standards should be established with guidelines and mandatory requirements for power continuity. Procedures should be developed for the systematic sharing of safety- and performance-related material, best practices, and standards. Supervisory control and data acquisition for networks should be engineered for secure exchange of information between public and private grids.

Preventive maintenance and testing are crucial. The key is to benchmark the facility on a routine basis with the goal of identifying performance deviations from the original design specifications. Done properly, this will provide an early warning mechanism to allow potential failure to be addressed and corrected before it occurs. Once deficiencies are identified, and before any corrective action can be taken, a Method of Operation (MOP) must be written. The MOP will clearly stipulate step-by-step procedures and conditions, including who is to be present, the documentation required, phasing of work, and the state in which the system is to be placed after the work is completed. The MOP will greatly minimize errors and potential system downtime by identifying responsibility of vendors, contractors, the owner, the testing entity, and anyone else involved. In addition, a program of ongoing operational staff training and procedures is important to deal with emergencies outside of the regular maintenance program.

The most important aspect of benchmarking is that it is a process driven by the participants whose goal is to improve their organization. It is a process through

which participants learn about successful practices in other organizations and then draw on those cases to develop solutions most suitable for their own organizations. True process benchmarking identifies the "hows" and "whys" for performance gaps and helps organizations learn and understand how to perform with higher standards of practice.