1

AN OVERVIEW OF RELIABILITY AND RESILIENCY IN TODAY'S MISSION CRITICAL ENVIRONMENT

1.1 INTRODUCTION

Continuous, clean, and uninterrupted power and cooling 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 enterprises must have 24-hour power and cooling 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 and cooling at all times, regardless of the technological sophistication of the equipment or the demands placed upon that equipment by the end user, be it a business or municipality.

Today, all industries are constantly expanding to meet the needs of the growing global digital economy. Industry as a whole has been innovative in the design and use of the latest technologies, driving its businesses to become increasingly digitized in

Maintaining Mission Critical Systems in a 24/7 Environment, Second Edition. Peter M. Curtis

this highly competitive business environment. Industry is progressively more dependent on continuous operation of its data centers in reaction to the competitive realities of a global economy. To achieve 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, 24/7. The proliferation of distributed systems using hundreds of desktop PCs and workstations connected through LANs and WANs, simultaneously using dozens of software business applications and reporting tools, makes each building a computer room. As we add the total number of locations utilized by each bank all over the world utilizing the Internet, we now realize the necessity of a critical infrastructure and the associated benefits of uptime and reliability.

The face of corporate America was severely scarred in the last decade by a number of historically significant events: the collapse of the dot.com bubble and the high-profile corporate scandals. 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 imbedded 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. 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, with the outcome of taking a huge hit operationally and financially. During the months following the Northeast blackout of 2003, there was a marked increase in the installation of uninterruptible power supply (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 Northeast blackout of 2003 emphasized the interdependencies across the critical infrastructure and the cascading impacts that occur when one component falters. Most automated teller machines (ATMs) in the affected areas stopped working, although several 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-charted depository institutions. The end result was a loss of revenue, 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 and operations, could have saved the banking and financial services industry millions of dollars.

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 in-

creasing reliance on computer and related technologies. Today, there are close to one trillion devices and one billion people connected to the Worldwide Web. As the number of computers and related technologies continue to multiply in this increasingly digital world, the demand for reliable quality power increases as well. Businesses are not only competing in the marketplace to deliver whatever goods and services are produced for consumption, but now they 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 and cooling. This keeps the mission critical manufacturing and technology centers up and running with the ability to produce the very goods and services that sustain them. The idea that businesses today must compete for the best talent to obtain reliable power is not new, and neither are the consequences of failing to meet this challenge. Without reliable power, there are no goods and services for sale, no revenues, and no profits—only losses. 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 is 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 all over the world, which is one of the purposes of this book. In addition, all companies need to develop an educational system and certification programs for young mission critical engineers to help combat the decreasing workforce necessary to sustain the growing mission critical industry.

It is also essential 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 that are designed to meet business needs and ensure uninterrupted power and cooling supplies 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 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, as 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 other planned or unplanned events. Moving toward high reliability is imperative. Moreover, avoiding the problems that can cause outages and unscheduled downtime never ends. Even planning and impact assessments are tasks that are never completed; they should be reviewed 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 and modeling 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) to predict potential future outages, 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 infrastructure reliability—design, maintenance, and operation of critical environments (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 failures, catastrophic failures, equipment failures, or failures due to human error. Each type of failure will require a different approach to prevention. A solid and realistic approach to business resiliency must be a priority, especially because the present critical infrastructure is inevitably designed with all the eggs located in one basket.

Within the banking and financial services industries, planning the critical area places considerable pressure on designing an infrastructure that evolves in an effort to support continuous business growth. Routine maintenance and upgrading of equipment alone does not ensure continuous availability. The 24/7 operation of such services means an absence of scheduled interruptions for any reason, including routine maintenance, modifications, and upgrades. The main question is how and why infrastructure failures occur. Employing new methods of distributing critical power, under-

standing 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), 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, and checks and balances designed to minimize operator and service-provider errors. The CAP ensures that only trained and qualified people are associated with 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 facility life cycle process
- Standard and benchmarking

Industry regulations and policies are more stringent than ever. They are heavily influenced by Basel II, the Sarbanes–Oxley Act (SOX), NFPA 1600, and the U.S. Securities and Exchange Commission (SEC). Basel II recommends "three pillars"—risk appraisal and control, supervision of assets, and monitoring of financial markets—to bring stability to the financial system and other critical industries. Basel II implementation involves identifying operational risk, then allocating adequate capital to cover potential loss. As a response to corporate scandals in the last decade, SOX came into force in 2002 and contains the following sections:

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)

Issuers are required to disclose to the public, on an urgent basis, information on material changes in their financial condition or operations (Sec 409)

Penalties of fines and/or imprisonment are imposed 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 critical events.

Keeping up with the rapid changes in technology has been a longstanding priority. The constant dilemma of meeting the required changes within an already constrained budget can become a limiting factor in achieving optimum reliability.

1.2.1 Levels of Risk

Risk can be described as the worst possible scenario that might occur while performing a task within a facility. Risk assesses how much we know or can predict about unforeseen circumstances. As we review risk, it is essential that the facility IT team has the proper change management processes and procedures in place for planned events, so that downtime can be minimized. Reducing the frequency of these events and understanding their impact is the key to proper critical environment management. Table 1.1 shows the three typical levels of impact—high, medium, and low—that result from event occurrence.

1.3 CAPITAL COSTS VERSUS OPERATION COSTS

Businesses are at the mercy of the mission critical facilities sustaining them. Each year, billions of capital dollars are spent on the electrical and mechanical infrastruc-

Table 1.1. Levels of risk impact on facilities

Risk impact	Effects of system failure
High	It will cause an immediate interruption to the clients' critical operations such as: • Activity requiring a planned major utility service outage, or temporary elimination of system redundancy in the critical environment • Activity that would disrupt critical production operations • Activity that would likely result in an unplanned outage or disruption of operations if unsuccessful
Medium	There is time to recover without impacting the clients' critical operations, including any: • Activity requiring a planned service outage that does not affect systems but may impact noncritical operations • Activity that involves a significant reduction in system redundancy • Activity that is not likely to result in an unplanned outage in the critical environment or disruption of operations if unsuccessful
Low	It will not interrupt operations and will have minimum potential of affecting the clients' critical operations including: • Activity involving systems directly supporting operations but the execution of which will be transparent to operations • Activity that cannot result in an unplanned outage of the critical environment or impact operations if unsuccessful
None	Activity not associated with the critical environment

ture that supports IT around the globe. It is important to keep in mind that downtime can cost companies millions of dollars per hour or more. 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 and our way of life depend on critical infrastructure being available 100% of the time with no exceptions.

Critical industries are operating continuously, 365 days a year. Because conducting daily operations necessitates the use of new technology, more and more servers are being packed into a single rack. The growing number 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 needed to recover, should be established.

Many organizations associate disaster recovery and business continuity only with IT and communication functions and miss other critical areas that can seriously impact their business. Within these areas may be a multitude of critical systems that require maintenance, the development of procedures, and appropriate documentation. Some of these systems are listed later in Table 1.3.

One major area that necessitates strategy development is the banking and financial services 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, profitability impact, and safety. The strategic decision is based on some of 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 configurations 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 no time is wasted in a recovery scenario. The focus is to implement the plan quickly and successfully, and in order to accomplish this people must be properly trained. Is the person you hired 3 months ago up to this task? The right strategies implemented will effectively mitigate damages, minimize disruptions, reduce the cost of downtime, and remove the threat to life and safety.

1.4 CRITICAL ENVIRONMENT WORKFLOW AND CHANGE MANAGEMENT

To assure reliable operation, a critical environment workflow and change management process must be established and followed. Commensurate roles and responsibilities of the engineering, technology, and security groups must be developed, implemented, and adhered to in order to manage both planned and unplanned events and associated risks.

The critical environment (CE) is defined as the physical space and the systems within a facility that are uniquely configured, sized and dedicated to supporting specific critical business operations as defined by the user. There are many specific rooms and areas within facilities in today's ever-changing environment. Some are located within the buildings structure whereas others are located outside. Regardless of where a CE may be located, these locations have immediate impact on the client's ability to maintain business operations and continuity. Examples of some of these CE areas can be seen in Table 1.2.

Table 1.2. Critical Areas

Data centers
Operations center
Electrical switchgear rooms
Network equipment rooms (NER)
Intermediate distribution frames (IDF)
Main distribution frames (MDF)
Main equipment rooms (MER)
Telecom rooms (TR)
Switching and hub rooms
Voice telephone and data closets
Server rooms
Business continuity and technology recovery rooms
Tape silo and storagetek rooms
Local area network (LAN) rooms
Business operations control rooms
Uninterruptible power supply (UPS) rooms
Command centers
Chiller rooms and thermal energy storage spaces
Building management, monitoring, and automation centers
Mechanical equipment rooms
Standby emergency power (SEP) generator and switchgear rooms

Critical infrastructure systems are prevalent throughout a facility. Depending on the facility size, there could be many redundant systems supporting the same critical environment. Knowing which systems could impact the clients' critical functions and operations is paramount. Some of these systems are listed in Table 1.3.

1.4.1 Change Management

Change management is a process for managing and communicating change across relevant functions and business units to ensure and deliver integration of procedures and processes. Note that during emergency situations, established emergency response and escalation procedures must be followed.

When work is must be done within the critical environment, ranging from certain simple or routine cleaning and inspection tasks to very complex and detailed preventive maintenance, corrective maintenance, or construction efforts, it is essential that an orderly and thorough approach to work planning and execution be undertaken. In every instance where work is planned in the critical environment, all departments must ensure that risk to company operations is thoroughly assessed and that appropriate risk mitigation is in place while the work is performed.

The level of detail required in a method of procedure (MOP) must be correlated to the complexity of the work and magnitude of the potential risk. Relatively complex or high-risk work must be meticulously detailed in the MOP. The detail required for less complex work would not necessarily be as extensive. The bottom line is that a proper-

Table 1.3. Critical systems

Compressed air systems
Utility power feeder systems
Diesel engine fuel systems
Fire and life safety systems
Natural gas supply systems
Electrical distribution and grounding systems
Condenser water systems
Telephone and fiber optic communications systems
Standby emergency power (SEP) systems
Glycol systems
Environmental control systems (chillers, CRACs, etc.)
Water service systems
Building management systems (BMS)
Boilers
Uninterruptible power supply (UPS) systems

ly developed, reviewed, and approved MOP will result in reduced risk to business operations. Required change request information includes:

- Who is doing the work?
- What systems will be affected?
- Which areas of the building will be affected?
- Is there redundancy for the system being disrupted?
- Are there detailed procedures for the proposed task
- Is assistance needed from other lines of business?
- What hardware will be moved, added, or changed?
- How long will the task last?

If an outage is required:

- How long will power be out?
- Are there any critical points during the process (high risk) that can be identified?
- Will those systems be protected by UPS, generators, or other redundancy?
- What kind of backup systems are available if a problem arises?
- Will utility power be taken down?
- Are other feeds to the building affected?
- If redundancy is to be reduced, what redundancy will be lost and for how long?

1.4.2 Escalation Procedures

The purpose of the critical escalation procedures is to allow for the successful response to a critical site event. Following the escalation process assures proper notification and timely response. By assessing the event first, critical information will be available early on. It is important that a chain of command be followed because when events arise, teams need to ensure that communication and reactions are escalated in the proper fashion.

1.5 TESTING AND COMMISSIONING

The definition of commissioning (Cx) has developed over the past 12 years from being nothing more than vendor start-up to the full quality-control process it is today. Some still cling to the idea that commissioning is something that starts at the end of construction or after the design is complete. In some circles, they talk about levels of commissioning and level one starts after the design is complete at factory acceptance testing (FAT). The use of levels of commissioning goes out the window as soon as leadership in energy-efficient design (LEED) certification is injected into the mix, as LEED requires design reviews and other requirements that start earlier in the project. The best

definition of commissioning can be found in ASHRAE's Guideline 0.* ASHRAE's Commissioning Guideline 0-2005 is a recognized model and good resource that explains commissioning as a quality-control process in detail and can be applied to critical facilities with some embellishment when it comes to verifying critical system performance. The quality-control process given by ASHRAE is in phases, starting with the predesign phase and continuing through the occupancy and operations phase.

A summary of the phases given in the ASHRAE Guideline are given below, with some additions for mission critical facilities, and these phases should be included in all mission critical facility projects.

- Predesign phase
  —Document owner's project requirements and basis of design
- Design phase
  —Commission-focused design review
  —Writing Cx specifications
- Construction phase
  —Factory acceptance testing (FAT)
  —Construction-check listing
  —Start-up (prefunctional) testing
- Acceptance phase
  —Site acceptance (functional)
  —Acceptance testing to verify performance of critical equipment
  —Integrated testing
  —O&M document review
  —Staff training oversight
  —Develop and prove out EOPs, SOPs, and MOPs
- Occupancy and operations phase
  —Continual review and updating of materials
  —Continual training of O&M staff
  —Reliability assurance testing (continual commissioning)

A quality-control process would never be overlooked in any valuable production project. Why would we neglect quality control for critical facility projects? In the case of critical facility projects, quality control or commissioning starts at the predesign phase so we can make sure the owner's project requirements (OPRs) are fully developed and track all relevant documents such as the basis of design (BOD). We do this so that during value engineering we can evaluate any impact to the BOD and OPR, and if the proposed change does not meet the documented requirements, then the team must sign off on it. It should be clear that these documents are the foundation of any

*www.wbdg.org/pdfs/comm_def.pdf

project and part of the quality control process required for the commissioning of a critical facility.

In the design phase, we have a commissioning-focused design review that should not be confused with a peer review. In a commissioning-focused design review, the commissioning authority (CxA) should provide input on making the building and systems easier to commission and comment on equipment layout as it pertains to operational symmetry to help prevent operational staff from making errors during crisis situations. The CxA should also verify that bid documents adequately specify building commissioning as this will help reduce vendor change orders. It many cases, it is better to have the CxA provide commissioning specifications and have them included in the prepurchase and other bid sets. The focused review also needs to verify that there are adequate monitoring and control points specified to facilitate commissioning and O&M (trending capabilities, test ports, control points, gages, and thermometers). A review needs to include a review of design as it pertains to the reliability and redundancy standards of the owner and industry standards and verify that building O&M plan and documentation requirements specified are adequate.

During the construction phase, much of the rudimentary testing is accomplished. During this time, the factory acceptance testing is being conducted and it is important to have the CxA involved to verify that the controls and interlocks will work with the complete system. During this time, equipment is being delivered and installed. During this installation, the vendors and GC should be verifying the installation using construction checklists provided be the CxA. These checklists basically track the construction process and verify that the vendor delivered what was paid for in good condition, and that it was installed properly and has the proper clearance. The vendor start-up will follow and, if performed in accordance with the agreed procedures, all the functions including all the alarms will be verified. It is important to track all these documents and have them signed off by the vendors as proof of proper start-up. In some cases, the vendors will sign off the documents and not perform all the requirements, and that will slow down the acceptance and integrated testing. In this case of improper start-up, the delays can be back charged to the responsible vendor.

In the acceptance phase, the CxA will first operate all the equipment in all configurations and verify proper start-up by the vendors. Once this is completed, the CxA should verify performance of certain equipment without using vendor-provided test gear. This is done to keep the quality control process in the hands of the CxA and make sure that only calibrated equipment is used and the calculations are performed without bias. The equipment listed below is recommended to be subjected to this extra acceptance test phase:

1. Emergency power systems and controls
2. Uninterruptible power supply (UPS) systems and batteries
3. Flywheel energy storage systems
4. Static transfer switches (STS) and all associated controls

If the acceptance testing is done properly, it as a minimum will verify that the equipment is worthy of critical load. In some cases, deficiencies found during this

process have forced the vendors to meet their own specifications and improve product quality.

We are now ready for integrated testing, and the intent of this test is to verify that the building and all the systems work together to meet the client's design requirements. Some hints for having a successful integrated test that proves proper operation and no unwanted system interaction are:

1. Perform a full data center heat-load test, including any enclosed cooling systems
2. Perform integrated testing at 25%, 50%, 75%, and 100% of the design load
3. Use data loggers on the data center floor to verify measured data and BMS controls
4. Check all operating modes, including maintenance configurations

Staff training and operations documents need to be provided before we can start operations. Proper training must be given to the staff for systems and integrated operations. I would suggest that the vendors provide system training and the CxA provide overall operations documents. The operations documents should include maintenance operation procedures (MOP), emergency operation procedures (EOP), standard operation procedures (SOP), and alarm response procedures (ARP). With properly trained staff and proper operations documents, the human error faults can be minimized.

As we stated earlier, the commissioning process continues into the occupancy phase to maintain operational continuity. A yearly review and update of training as required due to system upgrade or operational requirements maintains staff and procedural quality. For mission critical facilities, a yearly verification of performance for critical electrical systems prevents loss of productivity due to system degradation; this is referred to as reliability assurance testing. These tests should be similar to those performed in the system acceptance-test procedures used during the acceptance phase and should use the original data for trending any changes in the system. The reliability assurance testing should be performed after the vendor has provided preventive maintenance (PM). The reason we perform these tests after the vendor preventive maintenance routine is that the vendor will have interacted with a commissioned system and disassembled some portions. In some cases, they provide updated software or control boards. The system now needs to be certified through reliability assurance testing to be worthy of critical load. Remember that the vendor-provided PM does not measure performance or track system degradation, so without a reliability assurance testing program the quality control process will have been compromised.

Before the facility goes online, it is crucial to resolve all potential equipment problems (technology, operations, etc.). 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 have been tested at the factory and witnessed by a competent commissioning authority (CxA) familiar with the equipment processes and procedures.

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 for 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 and prepare for the transition to operations.

Many decisions regarding how and when to service a facility's mission critical electrical and mechanical 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 and best practices 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 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 scheduled procedure has not previously identified a problem, consider adjusting the schedule respectively. Examine your maintenance programs on a regular basis and make appropriate adjustments to constantly improve.

Acceptance and maintenance testing are pointless unless the test results are evaluated and compared to standards and 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 technicians to perform maintenance without reviewing prior work tickets and records. This approach defeats the value of benchmarking and trending, and must be improved. The mission critical facility engineers can then keep objectives in perspective and depend upon their 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 because it will be very difficult to do it again.

1.6 DOCUMENTATION AND THE HUMAN FACTOR

The mission critical industry's focus on physical infrastructure enhancements descends from the early stages of the trade, when all efforts were directed solely toward design and construction techniques to enhance mission critical equipment.

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 indus-

try was in its infancy. Over time, the data centers have grown from a few mainframes supporting minimal software applications to server farms that can occupy 100,000 ft^2 or more, with Google and Microsoft being prime examples.

As more processing power is required to sustain our global economy, the electrical and mechanical systems supporting the critical load became increasingly complex. 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 in 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, change management, education and training, or operations and maintenance. The initial capital investment was just the tip of the iceberg (Figure 1.1).

Years ago, most organizations relied heavily 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. Tables 1.4 to 1.6 identify questions with regard to managing loss of personnel, documentation, and managing during a critical event.

The mission critical industry can no longer manage critical systems as they did 25 years ago. The requirements are very different today in that the sophisticated nature of the data center infrastructure requires the constant refreshing and updating of documentation. 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 in a capital project. This will assist in keeping the living document current each time a project is completed or a milestone is reached. Accurate information is the first level of

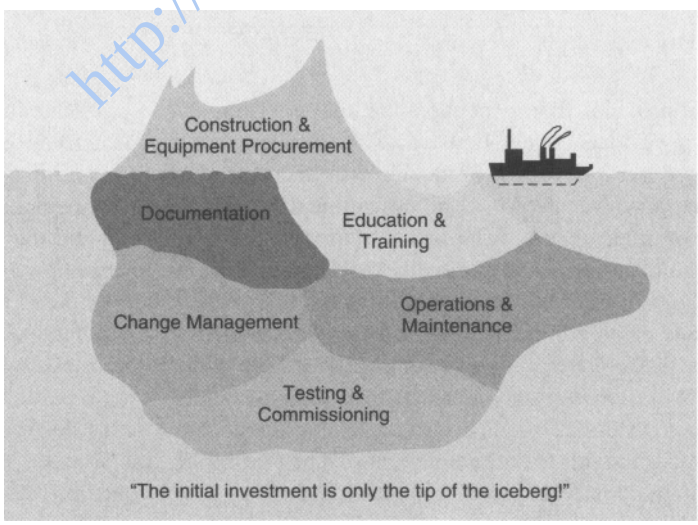

Figure 1.1 Hidden costs of operations.

Table 1.4 Managing loss of critical personnel

The issues: employee turnover, retirement, sick leave, or vacation
Was knowledge lost?
Where is the existing documentation?
How are new employees trained?
What risks are faced during the transition?

Table 1.5 Documentation issues

The issue: traditional documentation systems are inconsistent, inaccessible, and unstructured.
How is information shared?
Is system data readily available?
Where is the documentation?
How are revisions approved and made available to all users?

Table 1.6 Managing during critical events

The threats: fires, natural disasters, blackouts, and intentional disruption
Who should be contacted?
Is your critical system data defined?
Where are the procedures?
Will you be able to respond in time?

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. Remember that greater than 50% of all downtime can be tracked to human error.

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 (Figures 1.2 and 1.3). When there is a problem, the facilities manager (FM) is under enormous pressure to isolate the faulty system while maintaining data center loads and other critical loads.

Figure 1.2 Typical screenshot of mission critical access. (Courtesy of Power Management Concepts, LLC.)

Figure 1.3 Mission critical access screenshot. (Courtesy of Power Management Concepts, LLC.)

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 or have not been reviewed or updated periodically. 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. 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. 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 who were not properly trained or did not have access to accurate data during crisis events. The diversity among mission critical systems severely hinders people's ability to fully understand and master all necessary equipment and relevant information.

In the past, a greater percentage of people were hands-on, and it was natural for many families to make their own home and auto repairs just out of necessity. In doing so, they became mechanically inclined and attained an understanding of how systems operate. This experience gave a number of today's mission critical professionals a set of skills to build upon.

Today's "Nintendo generation" is gaining a slightly different set of skills through computers, software, and video games. They are gaining valuable experience with IT systems, and will have a solid foundation to continue to develop more advanced IT skills. The next step is to create a strong succession plan that teaches them how critical infrastructure operates and connects their already abundant IT knowledge to engineering. Then, existing professionals can show them how to apply that knowledge in the field.

The best strategy may be to start training successors as early as possible so, upon retirement of current staff, someone is trained with the necessary experience to take on operational responsibilities. Such training may be online (Figure 1.4). New college programs that include internships should be developed and made attractive for young

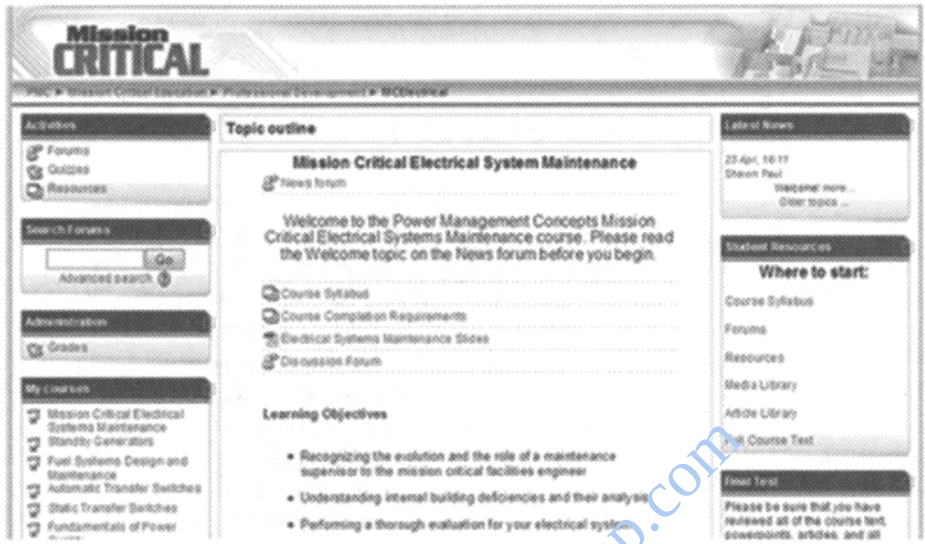

Figure 1.4 Screenshot of an online training program. (Courtesy of Power Management Concepts, LLC, and *Mission Critical Magazine*.)

engineers. These programs need to show real career path options and align with corporate needs.

It is time to invest in our future, so that the people who will be running the critical infrastructure of our country will have the necessary skill sets needed to meet and exceed our current standards. We need to constantly evolve and improve as professionals or risk becoming extinct. If not addressed in a timely and proper manor, we jeopardize the foundation of how our everyday business is run and our e-commerce generated. Imagine what would happen if, due to inadequate training, no one fully understands how to operate and maintain our critical infrastructure before all the experience-hardened experts retire.

With that being said, certified training programs should be developed by industry and instituted so there are established standards and best practices. It is only through education and training that we can guarantee facility employees are knowledgeable about all equipment and processes.

1.8 OPERATION AND MAINTENANCE

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

1. Planning and impact assessment
2. Engineering and design

3. Project management
4. Testing and commissioning
5. Documentation
6. Continuing education and training programs
7. Operations and maintenance

Hire competent professionals to advise at 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 and mechanical systems from scratch. A competent engineer will design a system that makes the most of the existing building design. However, before investing precious capital be sure you understand your business requirements for the next 3–5 years, as well as the reliability levels you must sustain. Use contractors who are experienced in data processing installations. Have an experienced firm inspect all systems, such as performing tests on circuit breakers and using thermal-scan equipment to find hot spots due to high-resistance connections or faulty equipment. Finally, you should plan for routine shutdowns of your facility so that you can perform preventive maintenance on critical equipment. Facility managers as well as senior management must not underestimate the cost-effectiveness of a thorough preventive maintenance program. Maintenance is not a luxury; it is a necessity. Do you want electrical outages to be scheduled or unscheduled? Or better yet, can you afford to deal with the consequences of an unscheduled outage?

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 your own company as well as outside professionals: 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 effectively and efficiently can be achieved through a well-planned certification program. Employees have a vested interest in working with management to reduce risk. 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 daily operations. 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 industry best practices. Furthermore, the company's risk profile should include training and periodic recertification. Should these evaluations fall 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 for this is the limited training provided to employees operating the mission critical equipment. Employee certification is crucial not only to keep up with advanced technology, but also to promote quick emergency response and situational awareness. 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 insure high levels of reliability?

1.10 STANDARDS 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 must be able to endure hazards of nature, such as earthquakes, tornados, floods, and other natural disasters, as well as human-made events. Great care should be taken to ensure those critical functions that will minimize downtime. Standards should be established with guidelines and mandatory requirements for continuity of business applications. Procedures should be developed for the systematic sharing of safety- and performance-related material, best practices, and standards.

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 a 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. Keep in mind that you cannot improve if you do not measure and benchmark.

1.11 CONCLUSION

Everyday industries are becoming increasingly dependent on continuous business operations. As a result, companies need to understand the level of reliability that they can supply to their customers and evaluate how this can either be improved or maintained. The following chapters will reinforce the concept that reliability and resiliency is dependent on an array of variables such as education and training, operation and maintenance, documentation, and testing and commissioning. It is the responsibility of employees at all levels of a hierarchy to communicate and develop best practices that will strengthen their business.

1.12 RISK ANALYSIS AND IMPROVEMENT

Below is a list of questions that you may wish to ask yourself about the needs analysis and risk assessment of the mission critical infrastructure you are supporting with regard to reliability and resiliency. Your answers to these questions should help to shed some light on areas where you can improve your operations.

1. How much does each minute, hour, or day of operational downtime cost your company if a specific facility is lost?
2. Have you determined your recovery time objectives for each of your business processes?
3. Does your financial institution conduct comprehensive business impact analyses (BIAs) and risk assessments?
4. Have you considered disruption scenarios and the likelihood of disruption affecting information services, technology, personnel, facilities, and service providers in your risk assessments?
5. Have your disruption scenarios included both internal and external sources, such as natural events (e.g., fires, floods, severe weather), technical events (e.g., communication failure, power outages, equipment and software failure), and malicious activity (e.g., network security attacks, fraud, terrorism)?

6. Does this BIA identify and prioritize business functions and state the maximum allowable downtime for critical business functions?
7. Does the BIA estimate data loss and transaction backlog that may result from critical business function downtime?
8. Have you prepared a list of "critical facilities" to include any location where a critical operation is performed, including all work area environments such as branch backroom operations facilities, headquarters, or data centers?
9. Have you classified each critical facility using a critical facility ranking/rating system such as the Tier I, II, III, and IV rating categories?
10. Has a condition assessment been performed on each critical facility?
11. Has a facility risk assessment been conducted for each of your key critical facilities?
12. Do you know the critical, essential, and discretionary loads in each critical facility?
13. Must you comply with the regulatory requirements and guidelines discussed in this chapter?
14. Are any internal corporate risk and compliance policies applicable?
15. Have you identified business continuity requirements and expectations?
16. Has a gap analysis been performed between the capabilities of each company facility and the corresponding business process recovery time objectives residing in that facility?
17. Based on the gap analysis, have you determined the infrastructure needs for your critical facilities?
18. Have you considered fault tolerance and maintainability in your facility infrastructure requirements?
19. Given your new design requirements, have you applied reliability modeling to optimize a cost-effective solution?
20. Have you planned for rapid recovery and timely resumption of critical operations following a wide-scale disruption?
21. Following the loss of accessibility of staff in at least one major operating location, how will you recover in a timely manor and resume critical operations?
22. Are you highly confident, through ongoing use or robust testing, that critical internal and external continuity arrangements are effective and compatible?
23. Have you identified clearing and settlement activities in support of critical financial markets?
24. Do you employ and maintain sufficient geographically dispersed resources to meet recovery and resumption activities?
25. Is your organization sure that there is diversity in the labor pool of the primary and backup sites, such that a wide-scale event would not simultaneously affect the labor pool of both sites?

26. Do you routinely use or test recovery and resumption arrangements?
27. Are you familiar with National Fire Protection Association (NFPA) 1600—Standard on Disaster/Emergency Management and Business Continuity Programs, which provides a standardized basis for disaster/emergency management planning and business continuity programs in private and public sectors by providing common program elements, techniques, and processes?