

in this ISSUE:

**THE IMPORTANCE OF BACKUP**

**MISSION CRITICAL OFFICE  
REQUIREMENTS**

**TRENDS IN STATIC TRANSFER SWITCH  
IMPROVEMENTS**

design PLUS





www.feace.com

design PLUS

## Winter 2003

The Winter 2003 designPLUS Newsletter marks the publication of our sixth quarterly newsletter. During the past year and a half we have tried to present technical and non-technical articles with differing themes for the mission critical facilities manager, and hope that you found them timely and informative. We recently conducted a survey regarding this newsletter and received many favorable responses. We also began distributing the designPLUS newsletter electronically by emailing a link to the newsletter on our web site at FEACE.COM. We are always interested in your comments and feedback so feel free to contact me at [lsoucy@feace.com](mailto:lsoucy@feace.com).

## THE IMPORTANCE OF BACKUP

*By William H. Flaherty, Jr., P.E. - FEA*

Users have many opinions as to what constitutes a proper backup for a data center. Some feel that duplicate files stored either on site or off site will suffice. These users have no protection when considering the potential problems that could arise with power, equipment or weather related failures. When their systems go down they must rebuild their infrastructure and databases before they can continue with their mission, which may be acceptable to some users. Other organizations feel they are adequately protected once they build a 7 x 24 facility and provide redundant UPS, STS, cooling and generator power systems

It is possible to build a facility with N+N redundant systems but many users do not go that far and assume that N+1 will protect their operations but these local systems are still at the mercy of major catastrophic occurrences such as fire, seismic events or weather. The best solution to total redundancy still remains having geographical remoteness between sites.

Site mirroring has been implemented by some users but is limited to about 20 or 30 miles with weather or seismic events still being potential troublesome factors.

The events of September 11 brought into sharp focus how important remote backup facilities can be to data centers. The traditional contingencies were planned for in New York City but an intentional catastrophic terrorist action was not considered. The pre September 11 thinking was that it was prudent to have a backup facility somewhere in the New York City area. As a result of the September 11 event, many data centers located in Manhattan were severely damaged or totally destroyed. Copper, fiber and satellite links were lost for weeks. The resulting air quality problems and damage to transportation routes and infrastructure made it impossible for many employees to report to work. Some firms took days or even weeks to get back into operation. As a result, federal regulators are reassessing their guidelines for financial institutions concerning backup facilities. Hard and fast rules have not been issued but they are considering a 200 to 300 mile requirement for the distance between primary and backup facilities. This type of geographical remoteness would insulate each facility from local catastrophic events whether they are due to terrorist activities, weather, seismic events, or fire. Such drastic measures do have a high cost and must be weighed against the benefits derived. In the quest for reliable backup, it is always prudent to consider geographical remoteness as one component.

# MISSION CRITICAL OFFICE REQUIREMENTS

By Leo P. Soucy, Jr., P.E. - **FEA**

Today's office buildings house many functions that are crucial to the business. While the main data processing function may be located in a hardened environment, the actual business operations and many times the main interface with the market are in general office buildings. The connections between the business operations and the data center are via communication links. These connections are normally fiber with local area networks interconnecting the PCs.

It is common for fiber networks to be hardened by providing separate paths into the building. When this is proposed it is important to review the actual routing of the fiber links between the office building and the data center to insure that there are no single points of failure (common duct bank, manhole, central office, etc.) This review is especially important if a single service provider is supplying the diverse fiber. Even if there are two independent service providers, there is a possibility that at some point they contract with the same network carrier which could result in total loss of communication if the carrier's system should fail or have a problem.

With regard to the office building itself, we are seeing an increase in the implementation of dual power cord topology for the servers that connect

the office functions to the data center, but many times the building utility systems cannot support this level of redundancy and reliability. Here is an example where a conscious decision has been made by the owner to harden the computer network infrastructure, but the facilities are not in synch. With many buildings developer owned, the mission critical design aspects are often overlooked as the building is leased with "normal" building infrastructure.

As a basis for design of any office building, a "Project Business Objective" must be developed that outlines the expectations of the owner with regard to the mission that the building is to support. This will form the basis of design for the power and heating ventilating and air conditioning systems. It should also identify the more critical functions so that they can be grouped to minimize the need to harden the entire facility.

Different design philosophies can also be implemented depending on the differing business requirements for uninterrupted uptime. Fortunately, the market has recognized the need for mission critical hardening for smaller systems. An array of products are now available that can meet this requirement.

**FEA** has completed numerous mission critical designs for corporate office buildings. One of these projects was for an insurance company that was moving to a developer owned facility. For this project the "Project Business

Objective" determined that the Owner required redundant air conditioning and dual UPS power for the dual power cord equipment in the server room. The critical nature of the customer interface being conducted in the building also dictated that selected workstations be powered from both UPSs so that if one UPS should fail it would only affect a portion of the workstations. The "Project Business Objective" also identified that minimal heating was required for the building. The standby generator was sized for not only the life safety systems and mission critical facilities, but also to power heating for the building. It was also determined that at some later date all workstations may require UPS power so that the workstations were connected to dedicated panels that would allow for ease of converting to UPS power without re-wiring the branch circuits.

This design was specific to this client but other criteria can be implemented depending on the "Project Business Objective". With the design criteria developed at the very outset of the project, the Owner's requirements were met with minimal cost impact to the project budget.

Remember, not all critical business operations are located in the data center and some business operations and market interfaces may require the same level of mission critical support systems as the data repository.

# TRENDS IN STATIC TRANSFER SWITCH IMPROVEMENTS

By Rafiq G. Bulsara, P.E. - **FEA**

Most leading manufacturers of the Static Transfer Switch (STS) have or will soon announce a new generation of STS products claiming new features and enhanced reliability. There is one new manufacturer with an STS product which has interesting features not previously offered.

Designs employing STSs bring the redundant power paths much closer to the critical loads which proves to be much more reliable than design configurations using isolated redundant or parallel redundant UPSs only.

However, the STS itself becomes the single point of failure making reliability of the STS of paramount importance.

The key to designing a reliable STS is to make its logic boards and control system fault tolerant. Logic boards are required for data acquisition; data processing and decision-making; and semiconductor control. Normally, STSs include redundant power supplies and, sometimes, redundant logic boards but the control path itself remains a single point of failure. If a control board fails, the STS will lock on to the active source of power and alarm. This type of control topology is called Single Module Redundant (SMR). Reliability can be improved significantly by pro-

viding independent control paths instead of one, and there is now a manufacturer that provides "Triple Modular Redundancy" (TMR) topology. A failure of one control path still leaves two control paths and "decision making" capability intact, as the remaining two inputs will "out vote" the input from the failed path. Based on critical system design used in spacecraft and modern aircraft control systems, TMR topology keeps the STS capable of emergency switching even when a critical control component of the STS fails.

Use of optical fibers instead of copper for communications between system control boards can also greatly enhance the reliability of an STS, as optical fiber is not susceptible to electrical 'noise'.

With the utilization of high-speed optical fiber communications, diagnostic features such as automatic waveform capture and detailed data logging with sub-cycle time stamps similar to a Black Box data recorder can be implemented with the ability of getting to the root cause of an event. Such root cause analysis could be crucial in devising a means to minimize a repeat of the event.

Other new features that we have seen include a web enabled STS (TCP/IP Ethernet Connectivity) for remote monitoring and voice prompted maintenance bypass procedures.

***FEA** would like to thank Anthony Pinkey of Layer Zero Power Systems, Inc. for furnishing information for this article.*

# FOOD FOR THOUGHT

Redundant systems must be properly monitored to insure that notification is received if redundancy is lost.

In an N+1 system, the failure of a pump or other piece of equipment must be monitored to insure that notification is received when the base unit fails; otherwise, the system will continue to operate properly until the second (redundant) unit fails and the facility is adversely affected. This is not only true of equipment but also of system controls. Many sensors that are critical to the proper operation of a system may also have a second function as an alarm indicator. Dual sensors should be installed where critical control and monitoring are required. **FEA** designs often include electronic and backup mechanical sensors to insure reliability.

With more pressure on facilities departments to do more with fewer personnel, centralized monitoring is becoming a necessity and it must be redundant and reliable.

Contact Leo Soucy at **FEA** with any comments or questions.  
Facilities Engineering Associates  
128 Garden Street  
Farmington, CT 06032  
Tel. 860-677-2285  
Email lsoucy@feace.com