Fault-Tolerant Power Certification Is Essential When Buying Products for High-Availability

By Kenneth G. Brill, Ed Orchowski, and Lars Strong P.E.

IT organizations report that 25% of all information downtime results from the interaction of computer hardware with its physical environment. These failures occur within the site infrastructure (uninterrupted power, stable cooling, fire protection, physical access, cabling and connectivity systems) or are caused by human error. Often, these failures are overlooked in a classical outage analysis because they deal with the physical environment and are infrequent. Although environmental faults total only 4% of all outages, when they do occur, the impact on information availability can be disastrous. Recovery from a facility environmental event can take several hours and many or all hardware platforms may be simultaneously affected.

This white paper:

- Argues that high-availability cannot be achieved without considering the concurrent maintainability and the fault-tolerance of the underlying site infrastructure which powers and cools Information Technology (IT) hardware.
- Outlines the negative availability consequences of the widespread disconnect between IT hardware choices and the facility availability expectations of their data center.
- Traces the evolution of site infrastructure from Tier I in the sixties to the current Tier IV and the organizational and engineering discontinuity between IT and facilities.
- Presents Product Fault Tolerant Power Certification as an essential and foundational element in any high-availability strategy.
- Outlines the benefits of product certification to IT.
- Provides the 13 technical requirements of the Fault-Tolerant Power Compliance Speciation Version 2.0.
- Provides a website link to UPTIME CERTIFIED products.

Disconnects Prevent High-Availabilty

Why are the reliability objectives for site infrastructure systems and IT hardware similar, but entirely different communities of interest are engineering them independently? This can cause poor alignment between hardware and its physical environment. Although all computer vendors stress their high-availability and functionality in marketing messages, many vendors have traditionally focused their availability strategy around their silos of operating systems, applications, and hardware. As a result, fault management and the interface between IT hardware and its physical environment continues to be the "user's responsibility."

Need for Certification

IT industry leaders have long recognized that no single company could identify the root causes of the 4% of outages causing 25% of all information downtime. Up until now, an information gap has existed at the computer hardware/site infrastructure boundary that has left IT executives lacking the key decision information necessary to design and execute the best fault-tolerant infrastructure. These IT executives saw the need to certify computer products for maximum uptime fit with the physical environment. The Uptime Institute, Inc.® (*Institute*) has been a leader in developing certification metrics to address this issue.

The *Institute* is a pioneer in creating and operating knowledge communities to improve uptime management in data center facilities and information technology organizations. The

Institute's network of 68 IT industry leaders, the Site Uptime Network® (*Network*), is focused on solving the rigorous uptime management challenges necessary to ensure the success of an enterprise. The *Institute* started with a root-cause analysis of abnormal incidents experienced by the *Network* members (who collectively manage three million square feet of raised floor). This information has been further extended via the information exchange that the *Institute* has and continues to foster among its membership and industry vendors. The *Institute* statistically catalogs fault sources and incident proof points of mission-critical support systems. Their work has resulted in key benchmarks to measure IT product design for fault tolerance. These benchmarks have evolved into a product certification process. Using these criteria, a product is evaluated and hardware meeting the criteria is awarded the "UPTIME CERTIFIED" seal.

Fault-Tolerant Power Compliance

One of the early success stories is a certified dual power path strategy. Certification of computer products compliant with dual power path criteria simplifies the purchase decision for mission-critical-conscious customers. This paper explains how this certification originated, why dual power is essential for achieving high availability, and overviews the process of fault-tolerant power certification.

Introduction

As the former Chairman of AT&T, Robert Allen stated in the company's full-page apology for the communication outage that affected the entire Northeast, which appeared in the Wall Street Journal, "If you don't have POWER, it doesn't matter how many alternate (communications) routes you have."

Critical to the fault-tolerance of a data center is how a computer interacts with its physical environment—and it all starts with power. Although the percentage of site facilities-attributable outages, including power, is relatively small (about 4% of total), faults of this nature account for up to 25% of total information downtime, with electric power faults being the major offender. As illustrated by the AT&T case, the consequences of a fault are noteworthy—a very visible power failure that crashed millions of users and left more than 1,400 planes in the air with no way to communicate with control towers. Factors that affect the availability of power include:

Hardware Requirements

Mission critical data centers are continuously re-inventing and redesigning themselves. Competitive pressure, demand for new applications, new lines of business, and workload consolidation require newer, smaller, better price/performance hardware. The challenge is new generations of IT hardware boxes, and even successive models within a generation, frequently require more, less, or even different kinds of electric power and cooling than predecessor boxes.

Circuit Churn

What hardware is physically installed in a data center is constantly changing. Data from *Network* members indicates an average annual churn of 24% (see Table 1), which translates into a total asset rollover every 4 years. Significant downtime risk occurs each time a product is uninstalled and its replacement installed. Doing this work means changing electrical circuits in active electrical panels. Best practice would be to power down the entire panel, but this would require shutting down unaffected hardware, and that is often unacceptable. As a result, electrical circuit changes must be done hot, and outages occur as a result of circuit breakers accidentally being bumped or tripped, wrong breakers being opened by mistake, loose wires shorting, screws not being fully tightened, and other unintended problems. *Network* members report an overall 99.87% success rate for doing hot work, but this level of performance still translates into 1.3 failures for every 1,000 circuit changes. (Removal of the old circuit counts as one risk exposure and its replacement with a new circuit is a separate risk exposure.) To reduce this failure rate, *Network* members have developed careful procedures to mitigate hot-work risks. But different sites have widely varying success rates ranging from 100% to 99.45%. While even the worst case of a 99.45% success rate would be considered outstanding performance in many industries, the IT manager of such a site will be a lot more concerned about the failures than the statistical success rate. Even with stringent procedures in place, large sites with a high number of circuit changes still have a statistical risk of 1.7 failures per year.

Table 1.

Circuit Changes and Asset Churn at 46 sites	
Total circuit changes	18,781
Highest number of circuit changes	1,331
Average number of circuit changes	408
Average number of active circuits	1,710
Average churn	24%

The Human Factor

Customer engineers, cabling technicians, movers, plumbers, mechanics, electricians, and cleaning personnel are all part of the human flux in a data center. More critical applications have been crashed for hours by an errant broom handle, a mistaken emergency power off, or "I think this is the right circuit breaker, try it," than outright sabotage.

Despite these challenges, facilities engineers are now tasked to power (and cool) a heterogeneous environment at mainframe reliability levels. Although information technology customers have come to expect Five Nines as a benchmark for IT availability, site infrastructure availability falls short of this expectation. A site needs to be both concurrently maintainable and fault tolerant, or business leadership can be a painful memory. Given these requirements, the solution is obvious: all equipment using electric power needs dual-power sources to eliminate single points-of-failure the standard practice in military combat aircraft design and other high-performance systems in other industries. Like multilane highways compared to a country road, distribution on two power paths would minimize the roadblocks of computer outages and enable the necessary circuit changes for new asset installation (as well as periodic maintenance).

Defining the Problem: Early Facilities-Oriented Forums

Beginning in about 1990, leading edge IT user companies, who recognized the substantial but largely hidden cost to their business of environmental faults, began to discuss the problem. Their objective was to further quantify elements of fault-tolerant IT performance. Among the early groups to bring site infrastructure environmental leaders and expertise from both users and IT hardware manufacturers together into a forum were the 7 X 24 Exchange and the *Institute*.

As noted above, a major problem to solve was the ability to provide continuous electric power to critical equipment. Unlike the mainstream database and data management specialists at GUIDE and SHARE organizations, these new groups were facilities focused, and openly discussed topics such as circuit breaker faults, the human factor component in outages, electronic grounding issues, and energy density. Interestingly, despite more discoveries of the "best construction practices," the root cause for many facility outages was still not intuitive.

To further focus on the rigorous uptime management challenges to ensure the success of an enterprise, the *Institute* provided the basis for a Site Uptime Network® (*Network*). The *Network* began by bringing together companies from the Fortune 100 community. Their mission was to establish fault-tolerant IT performance requirements from the user perspective— in the user environment. Various companies have implemented their vision of a high-availability site infrastructure for a wide variety of reasons. As noted above, the first major problem to solve was the supply of continuous electrical power to critical equipment.

Starting at literally the ground floor, the differences in data center construction were analyzed. Results of this work identified a common standard for site infrastructure construction. This was simplified as a series of tiers in data center fault-tolerance levels Tier I being the 1960s-style data center (with predictable outage incidents) and Tier IV exemplified by United Parcel Service's Windward, Alpharetta, GA data center commissioned in 1994. Tier I design provides a "good enough" computing availability, where unscheduled outages can still be tolerated. In contrast, Tier IV-level data centers have a design point enabling survival in a worst-case scenario and will remain active, without the benefit of external utility power or water for extended intervals.

Just as the *Network* members discovered with their high-availability building construction best practices, a clear identification of solutions to power path anomalies required a root-cause analysis of faults along the power path. *Network* members captured their knowledge formally by tracking outage-related incidents. As each participating member submitted an Abnormal Incident Report or "AIR", the incident was analyzed for root cause.

Abnormal Incident Report (AIR) analysis of more than 3,000 Site Uptime Network member incidents had indicated the majority of power outages were due to incidents that occurred within the facility itself, but downstream of the Uninterruptible Power System (UPS). This profound observation was made possible by the large database of problems submitted by members that allowed trend analysis that no single company had enough data to observe. These findings underscored the need for a true dual-power fed product design that moved the last-point-of-power redundancy down from the UPS to within the computer hardware. This was the only solution the *Institute* members could identify that solved their uptime reliability problems. And despite having invested in expensive Tier IV site infrastructures, information blackouts still happened because the IT hardware was not fully compatible, giving dual power a bad name.

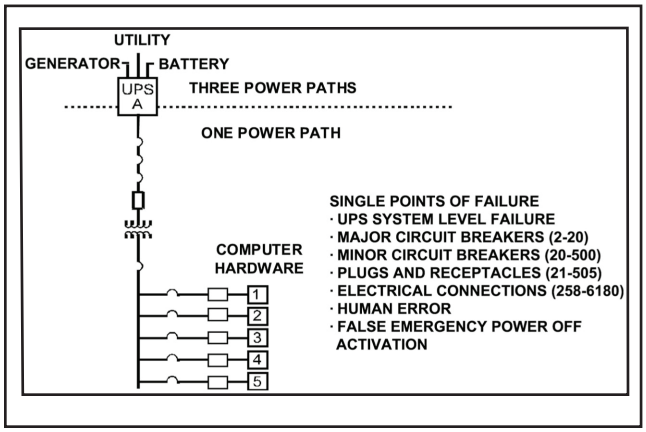

Figure 1.
Single Power Path: Typical of Tier I and Tier II Site Infrastructure Designs.

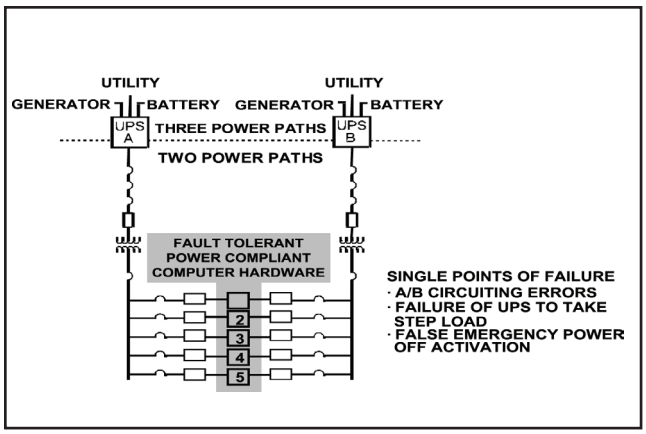

Figure 2.
Dual Power Path: Typical of Tier III and Tier IV Site Infrastructure Designs. Requires that computer hardware (indicated by numbered boxes) be Fault-tolerant Power Compliant.

Implicit in the Tier IV design is a dual-power distribution strategy employing two active, independent, diverse, full capacity power paths to the IT resource (or "critical load" in facilities terms). The dual-path strategy assures concurrent electrical system maintenance capability and fault resiliency if one power path has a disruption. Full exploitation of the dual-power data center, however, presumes that the site will have IT hardware with an internal dual power path consistent with the fault-tolerance level of the Tier IV site infrastructure. (For more information on tier classification, please refer to the white paper published on the *Institute* website: www.uptimeinstitute.org/whitepapers.html.)

Tier Classifications Define Site Infastructure Performance

As *Institute* members discovered through continuing information outages, what constituted dual-power IT hardware was open to many interpretations. While many IT products have multiple power cords, in actual practice, few are able to meet user uptime expectations.

The substantive results of this teamwork have raised the design bar for computer hardware and component suppliers, just as the more traditional IT/vendor partnerships resulted in improvements and new client applications. *Network* members' experience has also driven realistic content for Service Level Agreements, which now encompass both IT and site infrastructure components. Also, as the cost penalty for site-caused outages can be studied and quantified, high availability procurement practices are much easier to justify, as yielding cost savings in the long run. Predictably, even today, power interruptions still head the outage incident list for environmental faults.

Defining the Certification Requirement

The *Site Uptime Network* has recognized that full exploitation of the dual-power data center requires that the data center install hardware that can take advantage of the dual-power path design concept. New computer products and services touting improved uptime are being announced regularly, some advertise "dual power." Yet until now, the burden of determining whether or not a truly integrated fault-tolerant design has been achieved has fallen to the customer and users. As demand for new applications increases, systems integrators continue to discover incompatibility among products from competing manufacturers.

Network members realized an industry standard was required for what constituted dual-power compliance. The *Institute* and its members developed, in conjunction with leading hardware manufacturers, what eventually became the Fault-Tolerant Power Compliance Specification.

Dual Power Path Certification: Test for Fit to the Site

While specifications to measure site infrastructure compliance have been defined, users identified the need to bring measurements one step closer to the final information asset. This need to evaluate products has taken the form of Uptime Certification.

Starting in 2001, the *Institute* took the further step of testing products for compliance with the Fault-Tolerant Power Compliance Specification. Products are tested against the specification criteria, derived from the *Site Uptime Network* outage experience. (The specification can be found following the summary section of this white paper.) If the product passes the test, an end user is assured maximum availability and best fit within a Tier IV dual power path infrastructure environment.

This third-party testing relieves end users of the test burden and provides all vendors with the same customer requirement set. This customer-oriented certification strategy differs from the safety-oriented strategy of organizations such as Underwriters Laboratory.

Lessons Learned

Some of the lessons learned by *Institute* members seem amusing in retrospect: a few of the dual power designs offered by computer vendors became favorite *Institute* roundtable topics "more hype than engineering went into 'dual' power server design having three cords." Of special interest, few of the IT products that have multiple power cords are able to meet the *Institute's* Fault-Tolerant Power Compliance Specification. The certification specification closes the dual-power loopholes, for example: dual power with singular cooling does not meet the "Power In, Heat Out, Always"SM reality of the critical computer environment. Some other dual-power implementations were observed to take as much as 10-30 minutes to restore power in a fault situation, which fails certification criteria. The specification has many subtleties to address real world requirements.

To quote Ken Brill, Executive Director of the *Institute*, on the importance of this certification:

> "We've observed billions being invested in corporate and Internet-hosting data centers to implement the dual power distribution concept. In 1993, United Parcel Service, for example, architected both of its data centers for dual-power distribution before any computer vendor had announced a dual-power capable server a very visionary commitment. Although United Parcel Service committed to a higher initial investment in their site infrastructure, they, like the rest of our membership, have validated the logic of their investment decision by subsequently achieving significantly greater uptime.
>
> Each year, our membership reports a growing number of "saves" that can be directly attributed to fault-tolerant power. Unfortunately, several incidents each year that should have been "saves" are failures instead because IT hardware failed to work as advertised.
>
> The detailed performance specification [Editor's Note: This specification immediately follows this page.] contains 13 criteria for real problems brought to us by *Network* members. They identified real world, Power In, Heat Out, Always performance problems of supposed dual power products. Today, *Network* members are making dual power a requirement for procurement.
>
> Clients outside the *Institute* sometimes question why they should purchase a certified product. In response, if mission critical or high availability is a requirement, an Uptime Certified product based upon root cause analysis of more than 3,000 abnormal incidents from members of the *Site Uptime Network* is the proof point for uptime excellence and offers the best fit for mission-critical environments."

Product Certification Progress

Why aren't all computer hardware vendors eager to offer true dual-power implementation? One reason may be that although the last five decades of IT history records the exponentially increasing demand for fault-tolerant systems, computer product vendors have been driven to shorter development schedules. These "faster time-to-market" strategies must also satisfy the marketplace's expectation for decreasing product price with increasing product performance. With the emphasis on cost effective development, some vendors have yet to embrace system-wide fault-tolerant requirements.

The *Institute* also sees part of the challenge to computer vendors in that they must risk being measured against a consistent specification, by a neutral party. The cost of incorporating a dual power path concept into a product at the onset of a development cycle adds minimal expense compared to the customer benefit. But once internal space has been allocated and power supply concepts have been set, dual power cannot easily be "tacked on" during later product enhancements.

Indeed, several manufacturers have offered product candidates that almost passed the certification process, but failed one or more parts of the specification. The *Institute* suspects that these vendors will attempt certification again after redesign of their product, but they may have to wait until a new development cycle begins, which may be 24 months or longer. Meanwhile, the race to achieve improved fault-tolerance continues. And while some vendors might view UPTIME CERTIFICATION as a hurdle, leading edge vendors who truly embrace fault-tolerance from a customer's perspective, view UPTIME CERTIFICATION as the achievement it truly is.

The *Institute* provides all certification reports as public documents posted on its website, www.uptimeinstitute.org/tui_certification.html.

Site Uptime Network®
FAULT-TOLERANT POWER COMPLIANCE SPECIFICATION VERSION 2.0

Fault-tolerant power equipment refers to computer or communication hardware that is capable of receiving AC input from two different AC power sources. The objective is to maintain full equipment functionality when operating from A and B power sources or from A alone or from B alone. Equipment with an odd number of external power inputs (line cords) generally will not meet this requirement. It is desirable for equipment to have the least number of external power inputs while still meeting the requirement for receiving AC input from two different AC power sources. Products requiring more than two external power inputs risk being rejected by some sites. For equipment to qualify as truly fault-tolerant power compliant, it must meet all of the following criteria as initially installed, at ultimate capacity, and under any configuration or combination of options. (The designation of A and B power sources is used for clarity in the following descriptions.)

1. If either one of two AC power sources fails or is out-of-tolerance, the equipment must still be able to start up or continue uninterrupted operation with no loss of data, reduction in hardware functionality, performance, capacity, or cooling.
2. After the return of either AC power source from a failed or out-of-tolerance condition, during which acceptable power was continuously available from the other AC power source, the equipment will not require a powerdown, IPL, or human intervention to restore data, hardware functionality, performance, or capacity.
3. The first or second AC power source may then subsequently fail no later than 10 seconds after the return of the first or second AC power source from a failed or out-of-tolerance condition with no loss of data, reduction in hardware functionality, performance, capacity, or cooling.
4. The two AC power sources can be out of synchronization with each having a different voltage, frequency, phase rotation, and phase angle as long as the power characteristics for each separate AC source remain within the range of the manufacturer's published specifications and tolerances.
5. Both external AC power inputs must terminate within the manufacturer's fault-tolerant power compliant computer equipment. In the event that the external AC power input is a detachable power cord, the equipment must provide for positive retention of the female plug so the plug cannot be pulled loose accidentally. Within the equipment, the AC power train (down to and including the AC to DC power supplies) must be compartmentalized such that any power train component on either side can be safely serviced without affecting computer equipment availability or performance and without putting the AC power train of the other side at risk.
6. For single or three phase power sources, the neutral conductor in the AC power input shall not be bonded to the chassis ground inside the equipment. This will prevent circulating ground currents between the two external power sources.
7. Internal or external active AC input switching devices (e.g., mechanical or electronic transfer switches) are not acceptable.
8. A fault inside the manufacturer's equipment that results in the failure of one AC power source shall not be transferred to the second AC power source causing it to also fail.
9. An internal Uninterruptible Power System (UPS) or internal power batteries (batteries for cache memory are acceptable) or other type of energy storage equivalent is allowable only for the purpose of a prompt, orderly shutdown. The existence and volt-ampere capacity of an internal UPS or batteries and the time required for a prompt orderly shutdown must be identified.
10. For single- or three-phase power sources, with both AC power inputs available and with both inputs operating at approximately the same voltage, the normal load on each power source will be shared within 10% of the average.
11. For three-phase power source configurations, the normal load on each phase will be within 10% of the average.
12. An external alarm must alert the user within 60 seconds via the equipment's software or the host's operating system when an AC power source fails or is outside the manufacturer's published tolerances. This software alarm must also create a permanent record of the abnormal condition, the time it occurred and the time it was corrected.
13. The manufacturer will supply a written certification that the equipment meets or exceeds this specification for fault-tolerant power compliance.

Version 2.0 Effective: March 1, 2002

This Fault-Tolerant Power Compliance Specification has been established by the 68 members of The Uptime Institute's Site Uptime Network. The specification pertains to all computer and communication equipment critical to maintaining uninterrupted information availability. Be warned that many products claiming to be dual power compliant do not meet the performance requirements of this specification.

Incorporated in Version 2.0 is a new criterion 6. This criterion was added to address members' concerns about the potential for ground current to circulate between the two input power sources if the neutral conductor was grounded within a power supply. Intentionally grounding the neutral conductor in the power supply would be a violation of common sense and several codes. As a result, computer manufacturers have already complied with this criterion if they have a UL listing for their products. Criterion 6 has been added merely to codify what is already a standard industry practice.

Version 2.0 will supersede Version 1.2 on June 30, 2002. After June 30, 2002, hardware products will only be certified and listed if they meet Version 2.0 of the specification.

The *Institute* independently tests hardware products submitted by manufacturers to verify and certify conformance with the Fault-tolerant Power Compliant Specification. A listing of currently certified products is maintained at www.uptimeinstitute.org/tui_certification.html

Use of the Fault-Tolerant Power Compliance Specification Version 2.0 is made available at no charge to those companies desiring to make fault-tolerant compliance part of their procurement process. The specification may be quoted or reproduced in its entirety at no charge with the proviso that the the Institute exclusively reserves the right to test and certify hardware products as complying with the specification. The version number must be included and copyright credit given to The Uptime Institute's Site Uptime Network whenever the specification is quoted by reference or reproduced in its entirety.

Continuing updates to this specification are expected. For the most recent version, visit the *Institute's* website at www.uptimeinstitute.org/tuifault_specs.html, or contact the *Institute* by calling (505) 986-3900.

Certification Projects

Now that work has been completed on Fault-Tolerant Power Compliance specification, The Uptime Institute is working with Site Uptime Network® members to bring root cause analysis to bear on IT cooling, facilities infrastructure, and facilities operations abnormal incidents. These are the next "slices of the outage pie chart" that are candidates for the certification process.

Additional Information

More details on the dual-power path test requirements, other certification projects, and information about The Uptime Institute can be found at www.uptimeinstitute.org.

Abouth the Authors

Kenneth Brill is Executive Director of The Uptime Institute and focuses his expertise on the managerial, engineering, and strategic differences between systems that "work" and complex infrastructures that never fail or fail transparently without affecting users. His expert-systems reliability rules and analytical processes systematically identify and preempt infrastructure vulnerabilities. By focusing on the business consequences of downtime, Ken has helped clients justify investments totaling over $1.9 billion. He was the principal author of the *Institute's* White Paper on Heat Density Trends in Data Processing, Computer Systems, and Telecommunication Equipment. Mr. Brill has an MBA from the Harvard Business School and is an electrical engineer with extensive practical experience in infrastructure and human reliability.

Ed Orchowski is a senior consultant at The Uptime Institute with almost 40 years experience in the large systems IT industry working extensively with Fortune 100 customers. He worked at IBM for 37 years, and received his MBA from Marist College in New York.

Lars Strong, P.E., is the program manager for The Uptime Institute's Certification Program and the network manager of the Site Uptime Network. Mr. Strong's experience includes design and construction management services for corporate data centers as well as lead engineering and project management for a private consulting firm. Mr. Strong was responsible for the development of engineering plans for projects with up to $30 million in construction costs. He has a B.S. degree in Civil Engineering from New Mexico State University.

About The Uptime Institute

The Uptime Institute, Inc. is a pioneer in creating and operating knowledge communities for improving uptime effectiveness in data center Facilities and Information Technology organizations. The 68 members of the *Institute's* Site Uptime Network® (*Network*) are committed to achieving the highest levels of availability with many being Fortune 100 companies. They interactively learn from each other as well as from *Institute* sponsored meetings, site tours, benchmarking, best practices, uptime effectiveness metrics, and abnormal incident collection and trend analysis. From this interaction and from client consulting work, the *Institute* prepares white papers documenting Best Practices for use by *Network* members and for the broader uninterruptible uptime industry. The *Institute* also conducts sponsored research and offers insightful seminars and training in site infrastructure management.

THE UPTIME INSTITUTE®
Building 100
2904 Rodeo Park Drive East • Santa Fe, NM 87505
Fax (505) 982-8484 • Phone (505) 986-3900
tui@uptimeinstitute.org • www.uptimeinstitute.org

0406 TUI 707