Server Technology, Inc.

Cabinet Power Distribution Units (CDUs):

Features & Benefits of Implementing Server Technology's Cabinet Power Distribution Units (CDUs) in Your Data Center

White Paper STI-100-003

Server Technology, Inc.
1040 Sandhill Drive
Reno, NV 89521
+1 (775) 284-2000
www.servertech.com

Benefits and Features of CDU Implementation

INTRODUCTION

With the high cost of data center floor space and current advances in technology, new installations with denser cabinets that require more power continues to be the trend. The required power depends on the equipment, how dense the cabinet is and whether redundancy is needed. These new demands have led to new and innovative solutions for providing cabinet level power utilizing CDUs (Cabinet Distribution Units). Surveys show that when asked about their top 3 concerns; Heat/Power Density is the number one concern of Data Center Management today.

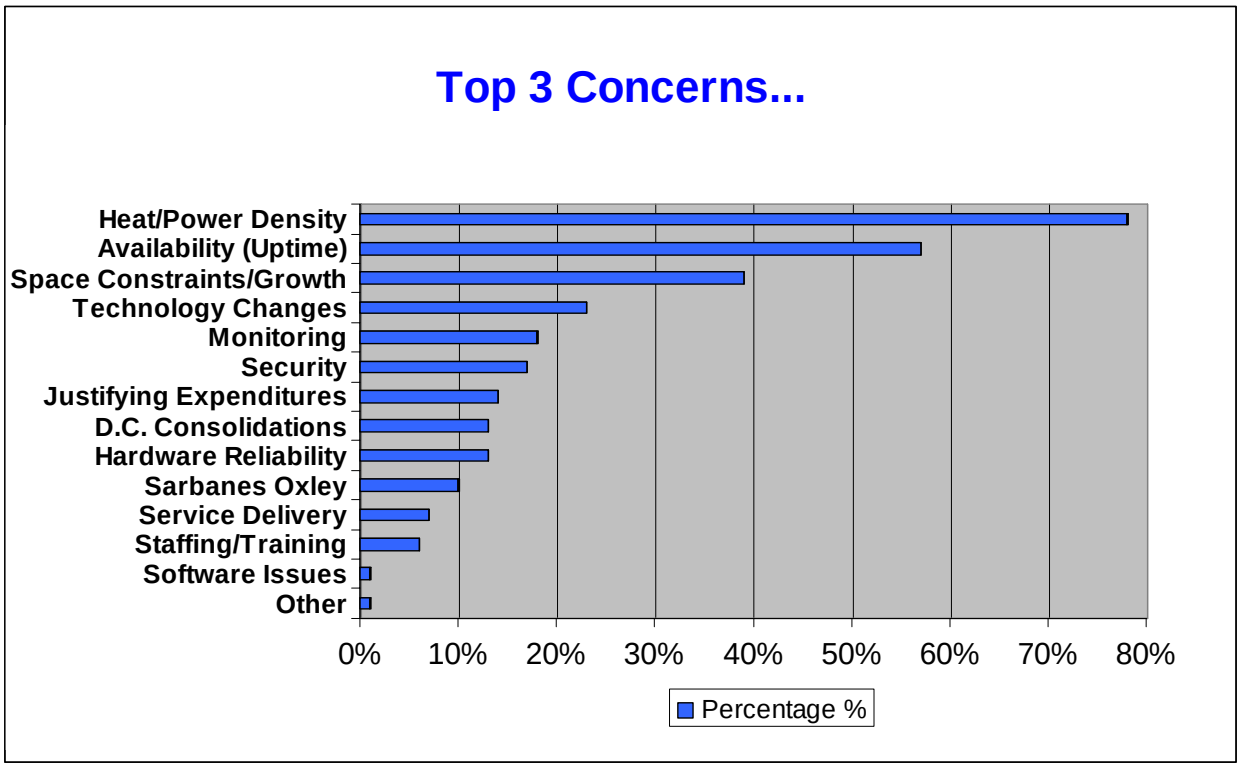

Chart 1

Reference: Data Center User's Group Conference, The adaptive Data Center: Managing Dynamic Technologies

The focus of this paper is to investigate the features and benefits of implementing Server Technology's Cabinet Power Distribution Units (CDUs) in your data center. Metered, Smart and Switched CDUs provide many solutions to common data center problems including cable management, temperature and humidity monitoring, circuit overload prevention and remote reboot capabilities, just to mention a few of the benefits. These

solutions are accomplished with advanced interface techniques, protocols and security; providing safe and simple operation.

The term Cabinet Power Distribution Units (CDUs) is used in this document so that there is no confusion between a large Power Distribution Unit (PDU) that would be installed on the data center floor and a Cabinet Power Distribution Unit (CDU) that is installed in a cabinet and distributes power to all of the devices within that cabinet.

CURRENT MONITORING USING A METERED CDU

Utilizing a CDU that provides the current load or "metered" reading for the overall CDU or in some cases the load on each branch circuit provides valuable information to the user.

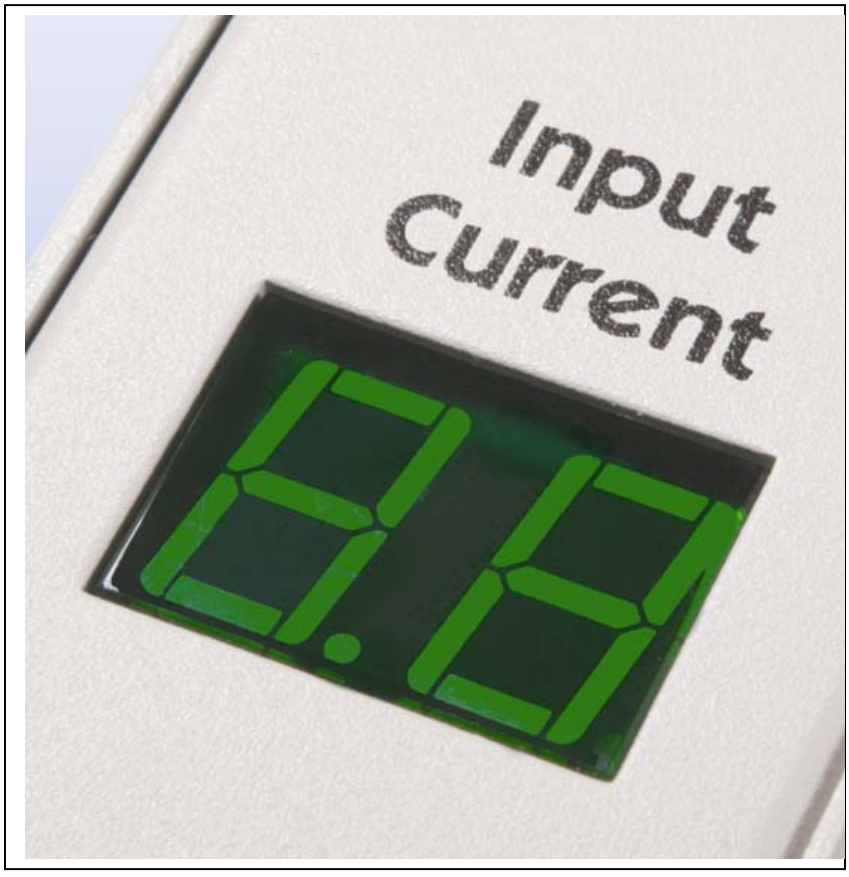

Figure 1
Current Meter indicating the current load of the CDU

Circuit/Cabinet Maximization and Safety Factors

With a CDU that has a current meter, the operator always knows how close they are to exceeding the overall current rating. This allows the cabinet to be operated with maximum efficiency and ensures that the data center is best utilizing their assets, as well as expensive cabinet space. Without current monitoring, the operator has no idea how much current is being drawn and therefore how many more devices can be added to a particular CDU or cabinet. They also have no idea how close they are to exceeding the current capacity of the circuit or providing any safety factor within their installation. The standard safety factor for de-rating power capacity is typically 80%.

Also, in many Co-Location facilities, the user is billed per each power whip or drop no matter how much of that power they are actually using. Without current monitoring, the user might be paying for power that they are not using or do not need.

True RMS Current Monitoring

Server Technology Inc, utilizes “True RMS” measuring when monitoring and reporting the current draw within our Sentry™ CDUs. True RMS current measuring is the best and most accurate way to measure dynamic waveforms. True RMS measuring must be used for non-sinusoidal (distored) current waveforms otherwise an overload condition may not be detected until a problem occurs.

Three Phase Load Balancing

Current meters also allow for a three phase power load to be balanced, which is required for proper operation of three phase circuits. Load balancing will make the most efficient use of 3-phase power and will reduce the neutral current to zero, reducing heating and other unwanted effects from unbalanced circuits. Using three separate current meters rather than just one which requires the user to press a button to cycle through the readings makes this a simple process without any confusion and provides an at-a-glance viewing if there is a problem.

BRANCH CIRCUIT PROTECTION

Over current protection is driven by the safety standard for Information Technology UL60950-1, Clause 2.7 which states that "standard supply outlets and receptacles shall be protected by an overcurrent protective device in either the equipment or the branch circuit, rated not more than the outlet or receptacle. Branch circuit protection is required on all 30A rated CDUs. The overcurrent protective device shall be of a type that is suitable for branch circuit protection in accordance with the National Electrical Code (NEC) ANSI/NFPA 70…" Branch circuit protection ensures that if there is a short circuit or other overcurrent condition that the only outlets that will be lost are the ones associated with the particular branch circuit that had problems.

There are several ways to provide branch circuit protection within a CDU, but by far the most common ways are either with fuses or circuit breakers. Server Technology has chosen to implement fuses for over current protection within our CDUs due to their simplicity, operational benefits and superior protection of which some are discussed below.

Fuses vs Circuit Breakers for Branch Circuit Protection

Selective Coordination

Selective coordination is the act of isolating a faulted circuit from the remainder of the electrical system, while maintaining uninterrupted power to the unaffected circuits. The faulted circuit is isolated by the selective operation of only that Over Current Protection Device (OCPD) closest to the over current condition. Fuses open the circuit when they 'see' a specific level of current passing through the fuse. Lower amperage fuses have a narrow range of operation and do not overlap from one amperage rating to another. Thus, fuses are easy to coordinate. Circuit breakers require a coordination study to ensure selective coordination. Inherent overlap of circuit breaker trip curves between the upstream and downstream devices often results in simultaneous operation of both breakers. This will clear the fault condition and open the circuit, but it will also remove power to all of the adjacent and/or upstream loads being served by the CDU. Proper selective coordination eliminates unnecessary power outages and reduces costly downtime. Figure 2 demonstrates selective coordination and how the upstream devices can be affected if it is not achieved.

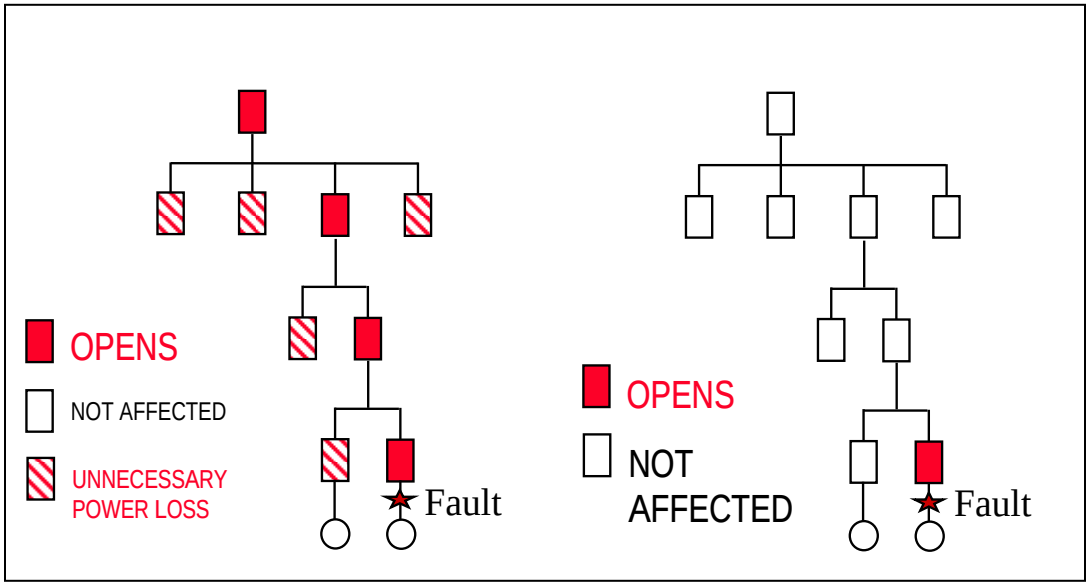

Figure 2:

Without Selective Coordination **(using circuit breakers)**

With Selective Coordination **(using fused protection)**

Component Protection

According to NEC 110.10, overcurrent protection devices shall be selected to permit the OCPD to clear a fault without damage to the electrical components of the circuit. Fuse operation is based on a simple thermal principle; the internal fuse element will rapidly melt/vaporize at a very specific level of energy. This amount of energy is well below the total amount of energy potential available during a specific fault. The resultant clearing time and the subsequent peak let-through current is significantly reduced which results in less energy than a downstream component is required to withstand. Per UL248 testing, fuses are required to meet maximum allowable energy let through values, which allows for very accurate fuse sizing.

Thermal magnetic circuit breakers are not current limiting. They do not interrupt short circuit currents in less than a ½ cycle, and typically require a full cycle to clear a fault condition. This means that the full peak current and energy of the first cycle of the fault will be let-through. Per UL489 testing, standard thermal magnetic circuit breakers are not tested to limit the maximum amount of energy let-through to downstream components.

By reducing the amount of energy which passes through to the protected device, you decrease the damage, which reduces repair and downtime. In order to successfully protect sensitive equipment, the upstream overcurrent protective device needs to be able to operate in a very short amount of time, and consistently limit the amount of peak current/energy which passes through to the downstream devices.

Maintenance

Proper maintenance of over current protection devices, as specified by the device manufacturer, is critical to effectively and consistently operate within their manufacturing specifications in the event of an overcurrent condition. Fuses do not require maintenance. Molded case circuit breakers require periodic inspection and manual operation as part of their prescribed maintenance procedures. Failure to manually exercise the mechanism can cause the internal lubricants to thicken, and cause the breaker to open slower than specified. Most manufacturers, as well as NFPA 70B, recommend that if a molded-case circuit breaker has not been operated, opened or closed, within six months time, it should be removed from service and manually exercised. Because of the highly engineered yet simple design, fuses ship from the factory calibrated to a very specific set of operating parameters. This ensures that the fuse will operate as specified without maintenance and upkeep concerns.

Interrupting Rating

According to NEC 110.9 “Equipment intended to interrupt current at fault levels shall have an interrupting rating sufficient for the nominal circuit voltage and the current that is available at the line terminals of the equipment.” Failure to comply can result in catastrophic failure of the overcurrent protective device, which will require replacement of the entire CDU, and an immediate loss of power. Worst case examples could result in a fire and/or explosion. All modern fuses employ a simple and reliable method of current limiting and are able to easily achieve interrupting ratings of 100,000 amps or higher. Standard UL489 Circuit Breakers typically tested to safely interrupt much lower levels of fault current, and are not inherently current limiting.

Physical Attributes

The fuses utilized in Server Technology’s CDUs have a very specific physical footprint and rejection style fuse holder that prevents the wrong fuse from being installed. This prevents unqualified personnel from replacing the blown device with a different device that may not provide the correct level of protection. CDU suppliers such as Server Technology utilize a Class G fuse, UL specifications file #E42730, which provides a very high degree of current limitation. After a fault occurs, fuses are replaced assuring the same level of protection that existed previous to the fault. This ensures a high level of protection and reliability, without concern for maintenance and potential mechanical damage inherent to re-settable OCPD’s.

Resettability

There are several misconceptions concerning the suitability for using re-settable devices for reliable overcurrent protection. Per OSHA 1910.334(b)(2), after a circuit has been de-energized by the operation of a circuit protective device, the circuit may not be reenergized until it has been determined that the circuit can be safely energized. A qualified person is required to determine the cause of the overcurrent condition, and in the event of a short circuit, fix the problem prior to reenergizing the circuit. Circuit breakers that have interrupted a fault approaching their listed ratings **shall** be inspected and tested to the manufacturer's instructions, according to NFPA70E 225.3. After a circuit breaker safely interrupts one short circuit fault, the breaker needs to be evaluated to determine if it can safely be put back into service, and it may need to be tested in order to determine if it will safely interrupt a short circuit in the required amount of time. This testing can involve taking the CDU out of service and taking the breaker out of the CDU. In some cases the breaker may need to be discarded and replaced.

REDUNDANCY WITH A IN-FEED AND B IN-FEED INPUT CIRCUITS

For Mission Critical Applications, or for providing redundancy to single power cord devices two CDUs should be provided or a Fail Safe Transfer Switch (FSTS) is used. Many servers and other devices today come with multiple power input feeds. These provide both redundant power to the server, and the ability to compensate should one of the power supplies within the server fail. These safety measures are designed to ensure reliability and proper up-time. Server Technology's CDUs have dual power in-feeds either for power redundancy, automatic fail over if one source fails or to meet the high power demands of today's environments.

For devices that come with a single power cord, a Sentry Fail Safe Transfer Switch provides dual power in-feeds from separate power sources (A in-feed and a B in-feed). Should one of the in-feed sources fail half of the load is transferred to the remaining power in-feed without interruption to the connected devices (see figure 4). This is a result of STI's patent pending power in-feed sharing, where each in-feed supports half of the loads, ensuring reduced wear on the FSTS as the loads being switched are much smaller, versus switching the entire load as some competitive products do. Another unique feature of the FSTS is our patented arc suppression technology which uses a combination of solid state and electromechanical relays to ensure high current transfer capability along with increased isolation between the in-feed sources. This results in less wear and longer life of the relay contacts as arcing is prevented which is due to large dv/dt voltages that can occur with in-feeds that are not phased synchronized.

Dual input CDUs or multiple CDUs within a cabinet with an A feed and B feed power source are another way to provide redundancy within a cabinet, though they don't provide the FSTS feature of switching the load upon a power loss.

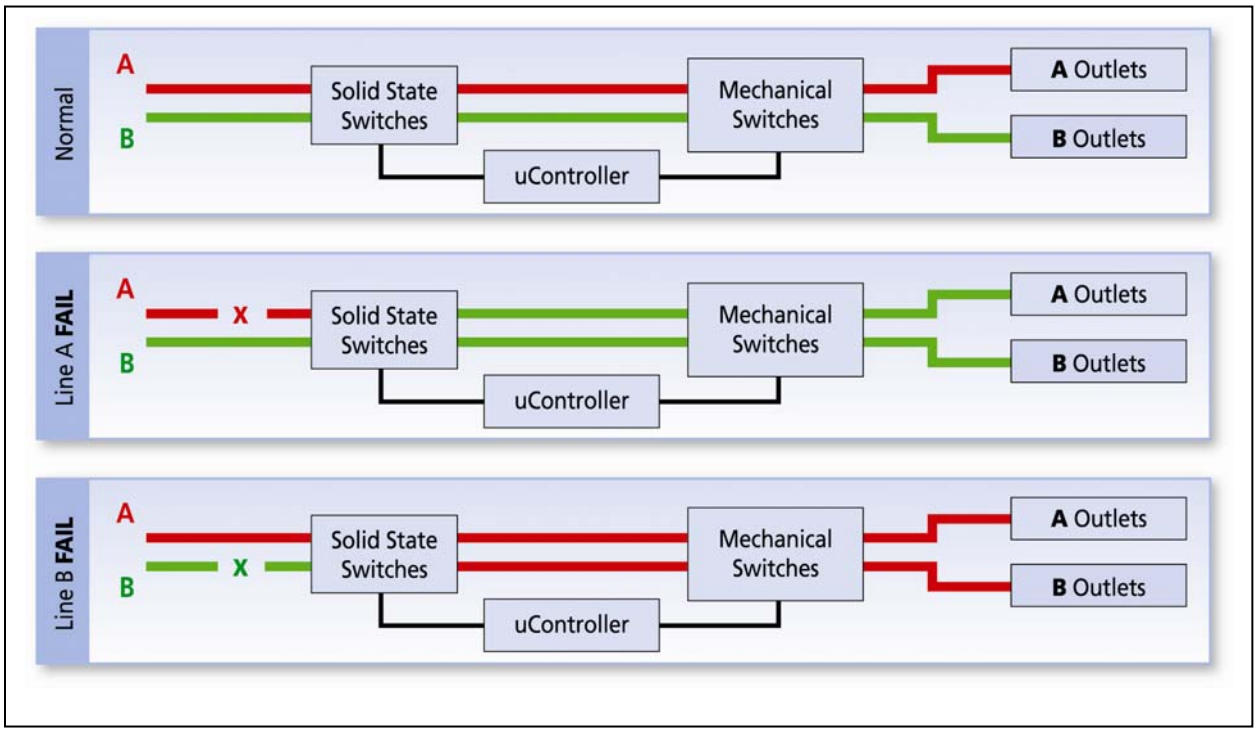

Figure 3
FSTS Arc Suppression Technology

THE TECHNOLOGY BEHIND SMART AND SWITCHED CDUS

Exclusive to Server Technology Inc. is our multi-threaded, real time operating system that handles simultaneous user access, over a variety of protocols that controls the application of power to its connected equipment as well as providing many other unique features. These unique features include dual temperature and humidity monitoring, multiple simultaneous user access, logging, linking of units (which doubles the number of outlets available on one IP address), advanced security, and many more. Firmware updates are simple to implement, with each CDU being flash-upgradeable. Also, all Smart and Switched CDUs come with a current meter to avoid overloading the CDU and for load balancing.

IP ADDRESSABLE SMART CDUS

Sentry Smart CDUs are IP addressable, which provides easy access via several protocols and also provides many valuable features for remote monitoring of devices. The IP based communication protocols include HTTP, HTTPS, Telnet and SSH.

HTTP/HTTPS

Sentry CDUs can be accessed any place in the world via most common web interfaces with either HTTP or more securely via HTTPS. This allows for easy management of remote CDUs and the devices that they are connected to.

When managing hundreds of Smart CDUs software packages are available that will allow auto discovery of all devices on the network which makes controlling and managing these devices simple and easy to do.

Telnet

The purpose of the Telnet network protocol used on the Internet or LAN is to provide fairly general, bi-directional, communications. It provides command line login sessions between hosts on the Internet. Logging in through the RS232 port requires the use of a terminal or terminal emulation software. TELNET clients have been available on most Unix systems for many years, however with recent advancements SSH has become more dominant in remote access for Unix-based machines.

SSH

Secure Shell or SSH enables secure terminal network sessions between a Sentry CDU and a remote user over an insecure network using public-key cryptography to authenticate the remote computer and secondly to allow the remote computer to authenticate the user. SSH also provides confidentiality and integrity of data exchanged between the two computers using encryption and message authentication codes. In addition to allowing secure terminal network sessions to the Sentry CDU for configuration and power management, an SSH may also be used for secure pass-through connections to attached devices.

User Access

Another key consideration when looking at remote IP access is the number of users that are allowed to access the device at one time, for some of the CDUs on the market only one user can access the unit at a time. For the

Sentry products up to 22 simultaneous logins are supported as well as a 23rd session dedicated strictly for SNMP.

SNMP Capabilities and Traps

With Server Technology's Smart CDUs remote notification is achieved via SNMP traps that can occur as well as being set for a number of different conditions. When looking at SNMP capabilities the user really needs to review the SNMP Management Information Base (MIB) and Object Identification Tree (OIDTree) to understand all of the possible SNMP interactions and objects. Server Technology makes this review easy by posting this information on our web site. Sentry has many traps that can be sent automatically such as an upon return-to-normal condition. Example: When the actual amperage exceeds the High-Load value, SNMP traps are repeatedly sent at configurable intervals. When the load returns to within the defined threshold, Sentry actually sends a return-to-normal Trap. The user can configure via the Sentry CDU which objects they wish to receive traps for and which ones they don't.

In comparing one vendor's CDU product to another's the user should get a demo device and enable SNMP. Then enable all configuration objects and traps and completely review the MIB using their SNMP Manager along with enabling polling and GETS for all of the SNMP objects. This way the user can best determine if the product truly supports all the features that they are most interested in.

Communications and Security for Smart and Switched CDUs

As mentioned above both HTTP and HTTPS CDU access is available through the internet. These communications are secured through either SSL (Secure Sockets Layer) or SSH (Secure Shell) which provide secure communications over your network. SSL provides authentication and encryption using public and private key encryption which requires the use of digital certificates. As a leader in the CDU marketplace Server Technology is the only manufacturer to have taken security concerns serious enough to have their CDUs put through the Joint Interoperability Test Command (JITC) testing with the Department of Defense (DoD). The Joint Interoperability Test Command (JITC) is an independent evaluator of information systems deployed within the Department of Defense (DoD) and is one of the responsible organizations that conducts Information Assurance (IA) and Interoperability (IOP) testing of network devices that will be connected to the Global Information Grid (GIG). JITC testing of Sentry CDUs was done for commonly known vulnerabilities and to assess its capability for resisting

attacker exploits. JITC executed testing of the Server Technology, Inc. Sentry devices in accordance with the JITC document number 3B03.001. The assessment was performed at the JITC Indian Head, Maryland test facility. Though this is not a pass or fail test both the smart and switched STI products tested were found to have **NO** vulnerabilities and therefore are suitable to be installed on the GIG. For more information request STI White Paper **(STI-100-002) "JITC Tested: Cabinet Power Distribution Units for DoD Information Technology and National Security System Applications."**

Other Communication Tools:

LDAP

Other communication tools such as LDAP (Light Weight Directory Access Protocol) are also available to be used with Sentry CDUs. When used to communicate with a Directory Service such as Active Directory, redundancy of tasks is eliminated. For example an administrator can pre-define and configure a set of LDAP groups and access rights for each. User's access rights then can be assigned or revoked simply by making the user a member of one or more pre-defined Sentry LDAP groups. User accounts can be added, deleted, or changed in the LDAP server without any changes needed on the individual Sentry products. Example: Instead of changing a pass word in hundreds of devices, or changing it on multiple software tools, the change need only occur in one place-----the directory.

TACACS+

Another supported communication tool like LDAP is TACACS+ (Terminal Access Controller Access Control System) which provides authentication and authorization via a central TACACS+ server; user accounts do not need to be individually created locally on each Sentry device. This allows administrators to pre-define an configure, in each Sentry product and in the TACACS+ server, a set of necessary TACACS+ privilege levels and user access rights for each. User access rights can then be assigned or revoked simply by making the user a member of one or more pre-defined TACACS+ privilege levels. User accounts can be added, deleted, or changed within TACACS+ without any changes needed on the individual Sentry products.

DHCP

DHCP (Dynamic Host Configuration Protocol) is a client-server networking protocol. DHCP provides a mechanism for allocation of IP addresses to client hosts. Dynamic allocation of IP addresses provides dynamic reuse of IP addresses. A network administrator assigns a range of IP addresses to

DHCP, and each client is configured to request an IP address from the DHCP server when the network interface card starts up. The request-and-grant process uses a lease concept with a controllable time period. This makes the network installation procedure for our clients (Sentry CDUs) much easier by providing centralized assignment of IP addresses.

Serial Interface

Out-of-Band, KVM or Console server access is also provided via an RS 232 console port. Command line access supports scripting.

INTEGRATED WEB-BASED GUI FOR SMART AND SWITCHED CDU'S

Once the user is securely logged into an IP addressable CDU, an easy to use and user friendly interface will guide them through configuration, monitoring and control of the CDU. With Sentry products there is no other SW to load or any other steps to be taken other than logging into the device.

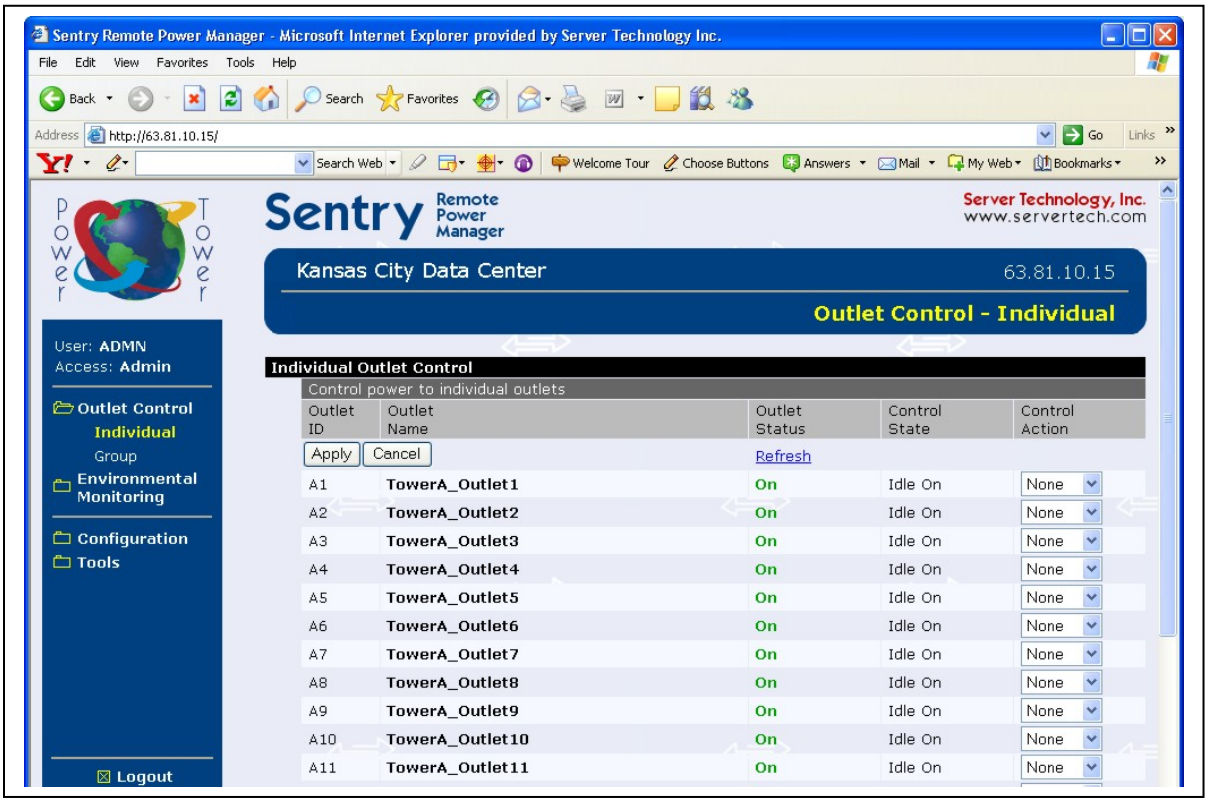

Figure 4
Integral STI Web Based GUI

The interface allows the user to simply and easily send email alerts as well as SNMP traps. It should also allow for different login and user capabilities so that the administrator can control who is allowed to access certain

devices. It allows this type of control down to the outlet level so that an engineer in the lab who needs to remote reboot his devices is not shown the other outlets on the CDU and therefore has no chance to possibly shut down or reboot somebody's else's equipment. Remote reboot of remote devices that are locked up and need to be restarted is another common application for switched CDUs and one that quickly provides huge cost savings as the IT Manger does not need to be dispatched personnel to remote locations to perform this task. One other common feature for switched CDUs is to lock out unused outlets so that additional devices cannot be plugged into the CDU without the proper permissions. This ensures that the CDU will not be overloaded and that cabinet configurations are not modified on the fly. User accounts such as Admin, User, View only, Reboot only access to outlets, groups and ports ensure proper functionality and control. Additional user accounts include a power user who has access rights to all outlets, groups, and ports, just like an administrator, but does not have any configuration rights and a reboot-only account which is restricted to only the reboot action for outlets which access rights have been assigned. This prevents a reboot-only user from leaving critical equipment in an off state. As part of the JITC testing, strong password support is implemented as an option along with the ability to configure a pre-login banner. This banner can be used for displaying text such as a security alert, legal text or disclaimers.

Some new features include the ability to upload and download a configuration. This feature allows for configuration backup and restore as well as a common template configuration to be uploaded to multiple products. This feature is supported via a built in FTP server. Simultaneous users and sessions are also an important feature. The STI interface supports 112 user accounts and 22 simultaneous sessions.

Other Web-Based GUI's

Sentry Switched CDUs are also compatible with Avocents® DSView® 3 Management Software. DSView 3 software is a secure, web browser-based, centralized enterprise management solution that allows users to remotely access, manage, monitor and control target devices through Avocent managed appliances.

Logging

Sentry CDUs can support logging of all authentications (including failed attempts), power actions, configuration changes and system events in RAM on the device. There are 4097 log entries that are written in a FIFO entry method. Should more than the standard number of entries be required or the need to permanently store them is required then the Syslog protocol is used for permanent off-product log storage.

ENVIRONMENTAL MONITORING

Smart and Switched CDUs in the market place today also offer other valuable measurements like temperature and humidity monitoring as an integral part of the device. Look for a product like Server Technology's that offers external monitoring with probes capable of being placed any where in the cabinet. Knowing the difference in temperature from the front to back of the cabinet or the top to bottom can be very informative especially when there is a problem. Environmental information is available via a web based GUI with SNMP traps and email alerts available should a problem arise. Additional SW provides thermographic mapping of your data center so a real time visual depiction of hot-spots is available and can be easily identified

FEATURES OF REMOTELY MANAGED SWITCHED CDUS

Receptacle Control

Switched CDUs offer the same features as Smart CDUs with the added ability to control specific outlets. This control can include an individual outlet or all of the outlets on one or more CDUs at the same time. The most common function of Switched CDUs is the remote reboot of equipment, on critical networks, to eliminate downtime, unsatisfied customers and unnecessary or unwanted trips to remote locations. With an easy to use web based GUI rebooting a remote device is as simple as a click of your mouse. Another way switched CDUs can save you time and money is to control unused outlets which can be turned off by the systems administrator ensuring that unwanted changes cannot be made to the cabinet's configuration unless they are authorized avoiding unwanted shut downs.

Power Sequencing

Power up sequencing is a receptacle control feature that is critical to a safe restart after power has been lost. Sequencing limits the inrush current on the power feed to a server or other device when a number of devices are started at the same time. This combined with grouping discussed below ensures that both power supplies of a dual-supply server receive power simultaneously. This avoids load imbalances and averts cumulative inrush that could otherwise trip the upstream circuit breaker.

Post-on delay and Wake Last Support

Adjustable sequencing parameters and unique programmable "Wake-Up" states such as "ON", "OFF or "Last State" guarantee proper server operation after a power loss or during start up. Programmable sequence delay allows

the administrator to manage boot dependencies during power on sequencing or group commands by delaying the sequencing of subsequent outlets after an outlet has been powered on. Wake last support ensures that upon restart that all outlets are in the same state that they were originally in.

Grouping/Linking

Grouping of outlets is a valuable feature often used dual power cord devices that in most cases require both supplies to power on at the same time to avoid current in-rush problems and tripping of the downstream breaker or general problems with the startup of the device. Linking is accomplish via our exclusive linking feature where the number of outlets can be doubled on any single IP address by connecting two of our CDU devices in a Master/Slave type configuration. Other benefits to this configuration are cost savings, not using as many IP addresses and ease of use.

Figure 5
Linking CDU's for one IP address and to group outlets

Other Advantages of Implementing CDUs
Cable Management using CDUs

A properly specified and installed CDU ensures a clean looking cabinet that is easy to maintain and upgrade. This is important when trying to trouble shoot a problem or when a device must be replaced especially if the time and trouble to label each cable has been taken. Another consideration is if your data center is going to be used by upper management as a show case giving your customers confidence in your company and the technology that you are implementing to support their needs. Working with your CDU vendor on different cable length options and connectors will make the job of cable management that much easier especially today where many devices have universal power supplies that accept a wide range of AC power and connectors.

Installation and Mounting of CDUs

With cabinet rack U space at a premium many CDUs come as vertical units that are defined by the way they mount into the cabinet as Zero U devices. Meaning that they are designed to mount in the back, front, or sides of the cabinet so that they do not take up valuable U space in the rack. Zero U units can be mounted either right side up or installed up side down depending on whether the power is being brought in from the floor or though a cable tray in the ceiling of the data center. A unit mounted upside down needs to have a current meter that can easily have its reading inverted.

One popular mounting option is to use a “buttons” that allow the Zero U CDUs to slide and lock in place. This makes the installation very quick and simple. Along with mounting, another concern is making sure that the cables plugged into the CDU stay in place and are not pulled out by a careless worker. To address this problem there are several options including cable retention clips as well as actual cable clamps that clamp around the power cable ensuring that it will not come unplugged.

Conclusion

Properly implementing Sentry CDUs provide the data center manager with a number of proven solutions to problems that they encounter every day. When dealing with a CDU vendor quality, support, features, price and delivery are all factors that must be taken into account. Customers should look for vendors willing to partner with them and work to provide solutions to their applications. By implementing Metered, Smart and Switched CDUs properly specified for the particular application cabinet installation, start-up and support are much easier to implement reducing costs and down time.