

Network-Critical Physical Infrastructure for Radio Frequency Identification (RFID) Systems

By Viswas Purani

White Paper #89

APC[®]
Legendary Reliability[®]

Executive Summary

Radio Frequency Identification (RFID) technology helps automate a variety of business processes, improving their efficiencies. It generates a huge volume of data that needs to be filtered, processed and stored, and generally requires its own virtual local area network (VLAN). To gain all the promised benefits and return on investment of RFID, the network must be highly available. The network-critical physical infrastructure (NCPI) must be assessed for vulnerabilities in power, cooling, physical security, and other NCPI elements. Failing to plan for NCPI can lead to disruption of critical business processes resulting in loss of revenue and competitive advantage. This paper provides an understanding of an RFID network and its components, identifies critical NCPI locations, and explains how to plan for high availability.

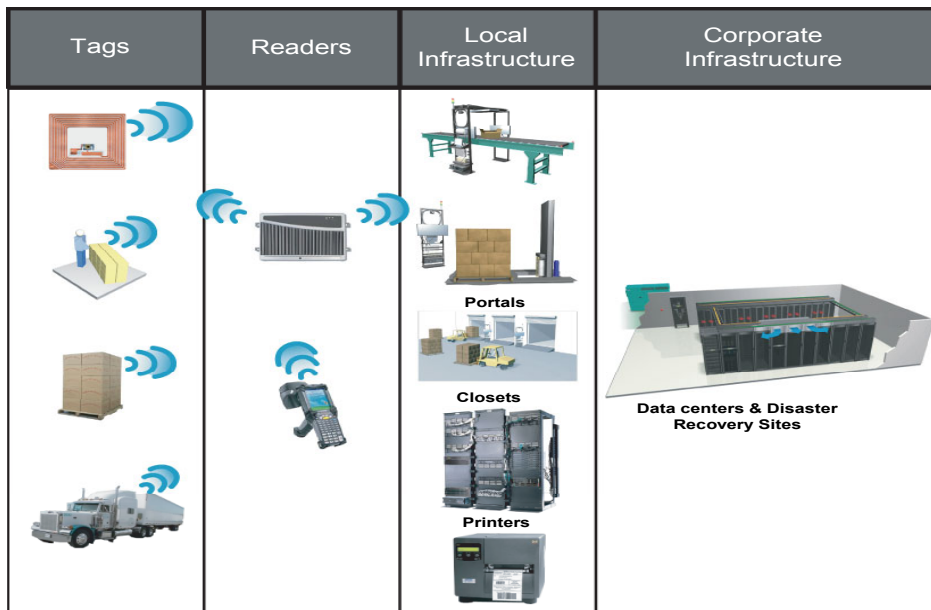
Introduction

Radio Frequency Identification (RFID) has evolved in the last few years as a promising technology. Mandates from companies like Walmart and Department of Defense have accelerated its deployment. RFID helps automate business processes throughout the supply chain, increasing their efficiencies. This results in a substantial savings to the companies that adopt it. As a technology enabler, it opens up an array of new applications like toll collection systems, asset tracking, and curbing gray market and counterfeiting. The origin of RFID goes as far back as World War II, although its current form was developed by Auto ID labs at Massachusetts Institute of Technology (MIT). The system is comprised of Electronic Product Code (EPC) and RFID technology (hardware & software) based on EPCglobal standards. The entire RFID network is referred to as EPCglobal network. EPCglobal Inc., a neutral, open, not for profit body formed by the collaboration between EAN international and UCC Inc., is responsible for promoting this EPCglobal network.

The RFID technology can be broken down into the following four basic sections / components (as illustrated in **Figure 1**):

1. Tags which store the unique EPC code
2. Readers & antennas which communicate with the tags and can read/write information
3. Local infrastructure comprising of
 - a. Portals – housing readers, antennas, PLCs, thin servers and some I/O devices
 - b. Closets – housing network switches, middleware servers, and RAID storage
 - c. Print stations – with multiple RFID printers connected to the network
4. Corporate infrastructure consisting of data centers and disaster recovery facilities

Figure 1 – Four basic sections of a typical RFID network



RFID technology automates major business processes, which increases their efficiencies, providing a significant return on investment (ROI). The components and the entire EPCglobal network deployed within the organization are business-critical and need to be highly available. This is commonly done by provisioning redundancies and fail-over mechanisms in the network switches, servers, storage devices, readers, etc. However, most often ignored is the network-critical physical infrastructure or NCPI (also referred to as physical layer or layer zero), which houses all of these critical components and systems. NCPI is the foundation upon which these critical RFID systems and networks reside. It has to be reliable, scalable, highly available, and manageable. It consists of:

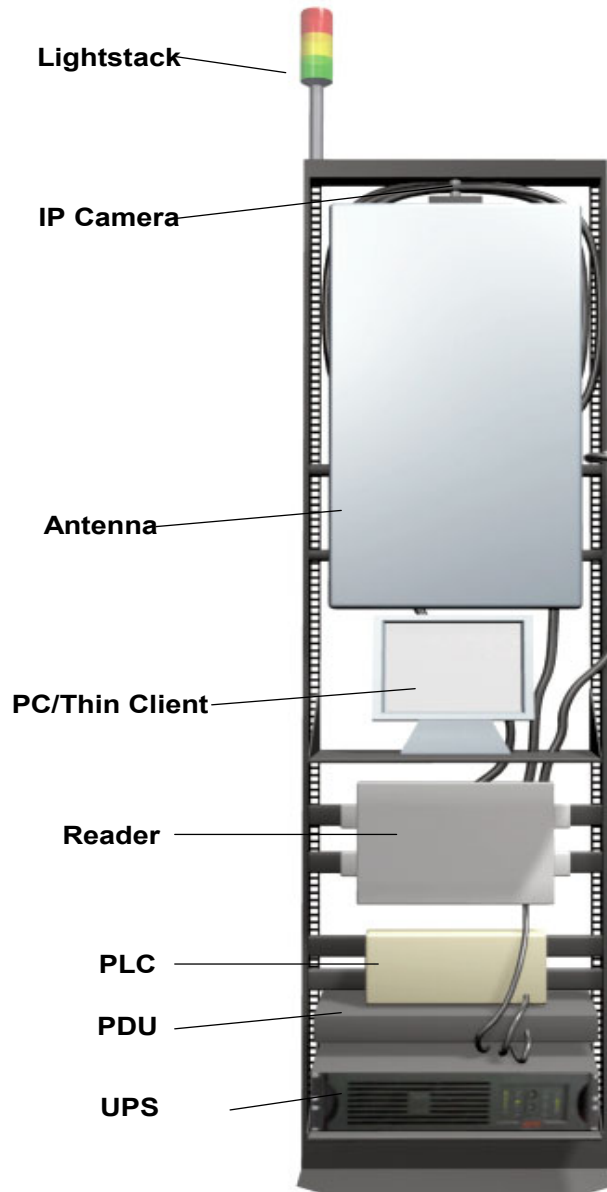
1. Racks to house the mission critical equipment like readers, antennas, middleware servers, network switches, routers, gateways, RAID Storage, and enterprise servers (running applications like warehouse management systems (WMS), supply chain management (SCM) systems, Manufacturing Execution Systems (MES), Enterprise Resources Planning (ERP) Systems.
2. Uninterruptible power supply (UPS) systems, Power Distribution Units (PDUs), isolation transformers and generators to provide uninterrupted, clean, conditioned power to the critical RFID systems.
3. Precision cooling systems to regulate temperature and humidity to provide the right operating environment to the mission critical systems.
4. Security, access control and fire protection systems.
5. Cabling to interconnect equipment.
6. Management systems to monitor and manage mission critical equipment, systems and network, locally as well as remotely to ensure their satisfactory operation 7x24x365.
7. Services to plan, design, deliver, install, commission, operate and maintain them.

NCPI must be considered locally in portals, closets and print stations, as well as corporate data centers and disaster recovery sites. RFID printers are generally networked and spread around the organization individually or in groups at print stations. Since they are expensive components, at a minimum they should have some basic form of power protection. The following sections explore these areas in detail, describing their typical environment, identifying their NCPI related challenges, and recommending best practices.

Portals

Portals are basically read stations, generally made up of RFID readers, antennas, and Programmable Logic Controllers (PLCs), with some input and output (I/O) devices to provide process automation and a PC/thin client to provide some intelligence as shown in **Figure 2**.

Figure 2 – Typical Portal



Portals are deployed all over the premises, typically at the choke points where all products have to pass (i.e. loading docks, shrink-wrap stations, and conveyor belts) as shown in **Figures 3, 4 and 5**.

Environment

Portals are generally found indoors in varied environments – from uncontrolled, hot, humid and dusty to air conditioned. They draw single phase power at 120 or 230 VAC and are generally less than 1000 VA. A typical well designed portal will house one to two readers, two to four antennas, a small PLC with optical switches or pressure transducers as input device and a light stack as an output device, a PC/thin client, UPS, PDU, and a camera, all mounted on a two post rack.

Figure 3 – Portal for loading docks

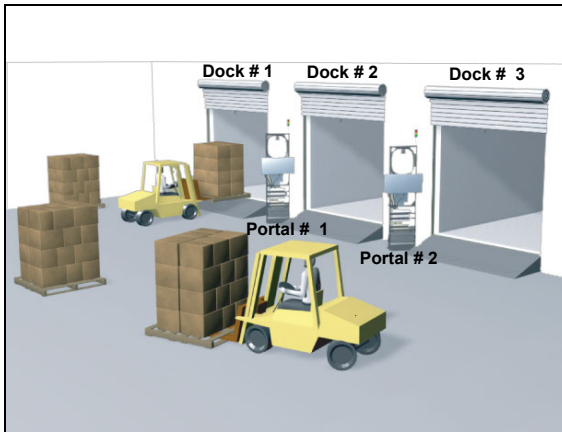


Figure 4 – Portal for shrink wraps

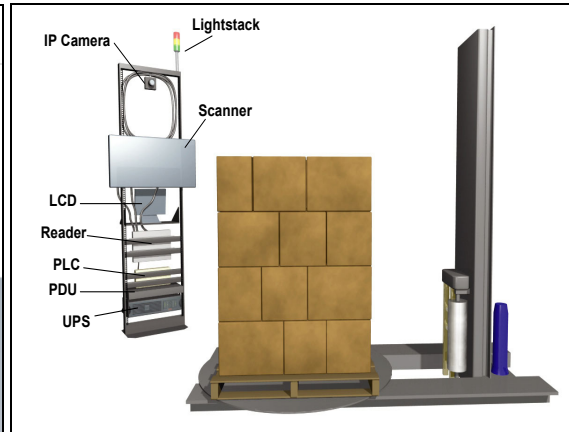
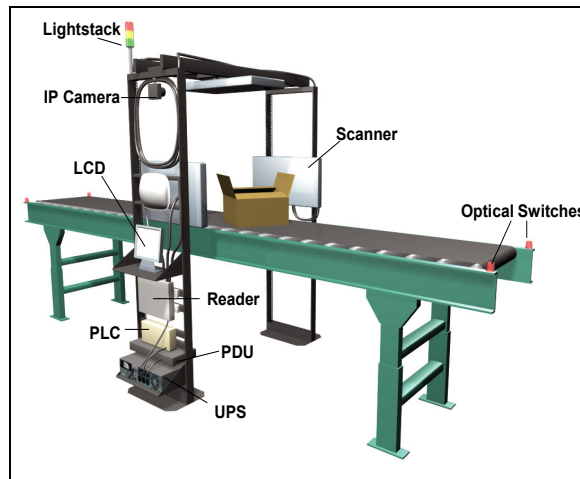


Figure 5 – Portal for conveyor belts



Challenges

Several challenges arise in the portals while deploying RFID in a warehouse, distribution, or manufacturing facility (i.e. hospitals, airports or retail supermarkets). Physical space for the portal, mounting all the equipment in one enclosure, and allowing for antenna alignments / tuning (for best RF field for maximum read) can become very difficult without proper mounting brackets and accessories. Provisioning of uninterruptible power supplies (UPS) and availability of power receptacles which are often forgotten during the planning stage can cause unexplained equipment failures, resulting in unwarranted delays to the project. Protecting all of the portal equipment from physical and environmental damage is of paramount importance in order to keep the RFID network running 7x24x365.

Best practices

- Electrically protect all the portal equipment with a UPS system since the raw utility power supply in most warehouses, distribution centers, manufacturing plants and other facility buildings is electrically polluted with sags, swells, transients, interruptions etc. Refer to APC White Paper #18, “The Seven Types of Power Problems” for more details. These power problems can cause accidental reboots of readers, PCs, and PLCs which can result in misreads, and can also cause equipment damage, like blown power supplies and printed circuit boards which can result in avoidable downtime.
- Provide enough receptacles to mount all RFID readers, antennas, PLCs, I/O devices, sensors and actuators. Often times, the UPS does not have enough receptacles, and a power distribution unit (PDU) is required. There are three common types of PDUs available in the market – (1) Basic PDUs, which simply provide extra receptacles; (2) Metered PDUs, which monitor and measure current to prevent accidental overloading and the resulting loss of power due to tripped circuit breakers; and (3) Smart PDUs, which allow the turning on and off the receptacles through a web browser so that one can remotely reboot readers, PC/thin clients, etc. Select the most appropriate PDU anticipating current and future needs.
- Two post racks are popular for mounting portal equipment due to their simplicity and price points. Ensure some form of physical security and protection to the reader, antennas and other equipment. Plexiglas or some other plastic polymer covers are popular, but many times full enclosures are used to meet the appropriate codes, regulations and requirements for the site (i.e. flame retardant, smoke retardant, and dust, moisture, temperature and other environmental conditions). Failing to anticipate and plan for facility environment and regulations can result in costly over-runs and a legal predicament later.
- Identify, group and standardize all the portals depending on their location and or function (i.e. dock door portal, shrink wrap portal, conveyor belt portal). These standardized portals should be built using standard off the shelf products to avoid any custom engineering. For example, the portals might include standard two/four post racks/enclosures, and use standard reputed brands for UPS, PDU, PLC, Light stack and other I/O devices. This will help reduce the upfront cost substantially, accelerate the speed of deployment, and make operation, maintenance and service easier, all of which will result in a lower total cost of ownership for their lifetime. Refer to APC White Paper # 116, “Standardization & Modularity in Network-Critical Physical Infrastructure” for more details.
- Proactively manage all the portals and their environment so that any abnormalities can be detected early and remedied, avoiding expensive repairs and associated downtime. Since there can be hundreds or thousands of portals within an organization deployed globally, managing them from a central management platform along with other IT and or facility equipment can be beneficial, effective and efficient.

Closets

Since RFID generates a lot of data, the RFID equipment, comprising of readers, middleware, edgware, premise servers, RAID storage, and printers, generally have their own local virtual private network (VPN). Wireless Local Area Networks (WLANs) are increasingly used for such local RFID networks within the building to connect readers, servers, and printers. The closet typically houses network switches, middleware servers, premise servers, RAID storage, wireless access points (APs), UPS systems, and other miscellaneous networking, telecom and IT equipment mounted in a two or four post rack (as shown in **Figure 6**) and are also called main or intermediate distribution frames or building distribution frames (MDFs, IDFs or BDFs). Newer generation closets also supply power over the Ethernet (PoE) to networked devices like readers, wireless APs, web/security camera, IP phones, and any other device drawing power up to 15 W. This imposes a lot of challenges on the power and cooling requirements in the closets.

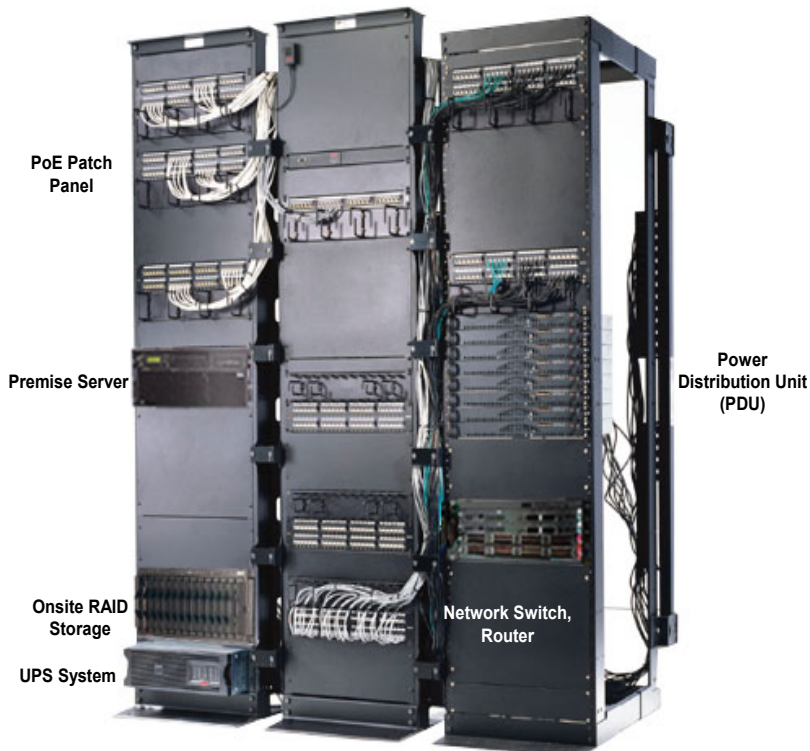
Environment

The closets are typically hidden in a remote location of a building, often times with little or no ventilation and illumination. Older closets supporting legacy telecommunication networks typically house punch-down blocks, patch panels, and a few small stackable hubs or switches. Newer closets supporting the RFID network which are capable of supplying power over the Ethernet, use and dissipate considerably more power. The RFID network switches, storage and servers generally are 19 inch (600 mm) rack mount type, and have varying air flow patterns depending on the manufacturers (i.e. side to side vs. front to back). A typical closet will house 1-3 racks of equipment and draw 500 VA to 4000 VA of single phase AC power or more. Two post racks are popular, however four post racks are increasingly used to accommodate the new heavier chassis based switches, storage devices, and servers, and to provide physical security and environmental protection to the business-critical RFID network and its equipment.

Challenges

While deploying an RFID network, these closets need the most attention in terms of power and cooling. Ensuring the right type of receptacles (i.e. L5-15, L5-20, L6-20, IEC 320 C19, and IEC 320 C13) and the right amount of power with the right circuit breaker protection to all the network switches, middleware servers and storage equipment as well as the UPS and PDU in the closet is a challenge. Managing the remote closets, its environment and all the equipments within along with cooling and airflow are often bigger but ignored problems in these closets.

Figure 6 – Closets



Best practices

- All equipment in the closet should be protected by a UPS system. The selection of the UPS should be based on:
 - The total power required in watts
 - The run time required in minutes
 - The level of redundancy or fault tolerance desired
 - The voltages and receptacles required

The UPS system is sized by taking the sum of the Watt ratings of the loads. A common rack-mount UPS such as the APC Smart-UPS will provide approximately four nines (99.99%) of power availability, while an N+1 redundant UPS with built in bypass and one hour of runtime, such as the APC Symmetra RM, will provide approximately five nines (99.999%), which is sufficient for most applications. See the Appendix of APC White Paper #69, "Power and Cooling for VoIP and IP Telephony Applications" for details on this availability analysis. When additional runtime is required, UPS products are available with extended run battery packs.

- Ideally all equipment in the closet should be plugged directly into the back of the UPS. However, if there are many devices, it may not be practical and a rack mounted PDU specifically designed for

the purpose should be used. The PDU should have enough receptacles to plug all the current equipment with some spares for future needs. PDUs with a meter displaying the current power consumption are preferred as they reduce human error from accidental overloading and resultant load drops. For the correct selection of the appropriate UPS model meeting the required power level, redundancy, voltage, and run time, the process is simplified by using a UPS selector such as the APC UPS selector at <http://www.apcc.com/template/size/apc/>. This system has power data for all popular switches, servers and storage devices, which avoids the need to collect this data. In systems like this, the choice of configuring a UPS will provide various receptacle options.

- To ensure continuous operations of the equipment in the closet, 7x24x365, cooling and airflow issues must be identified and addressed. The problem of heat dissipation and the need for supplemental air conditioning is most pronounced in closets which have no vents. Power dissipation in the wiring closet should be calculated to determine a cost effective way to solve the problem (see Table 1 & Table 2 in APC White Paper #69, "Power and Cooling for VoIP and IP Telephony Applications" for details).
- Environmental monitoring (i.e. temperature and humidity) within these wiring closets is highly recommended as it will help flag any abnormal conditions, allow for enough time to take proactive measures and avoid costly downtime.

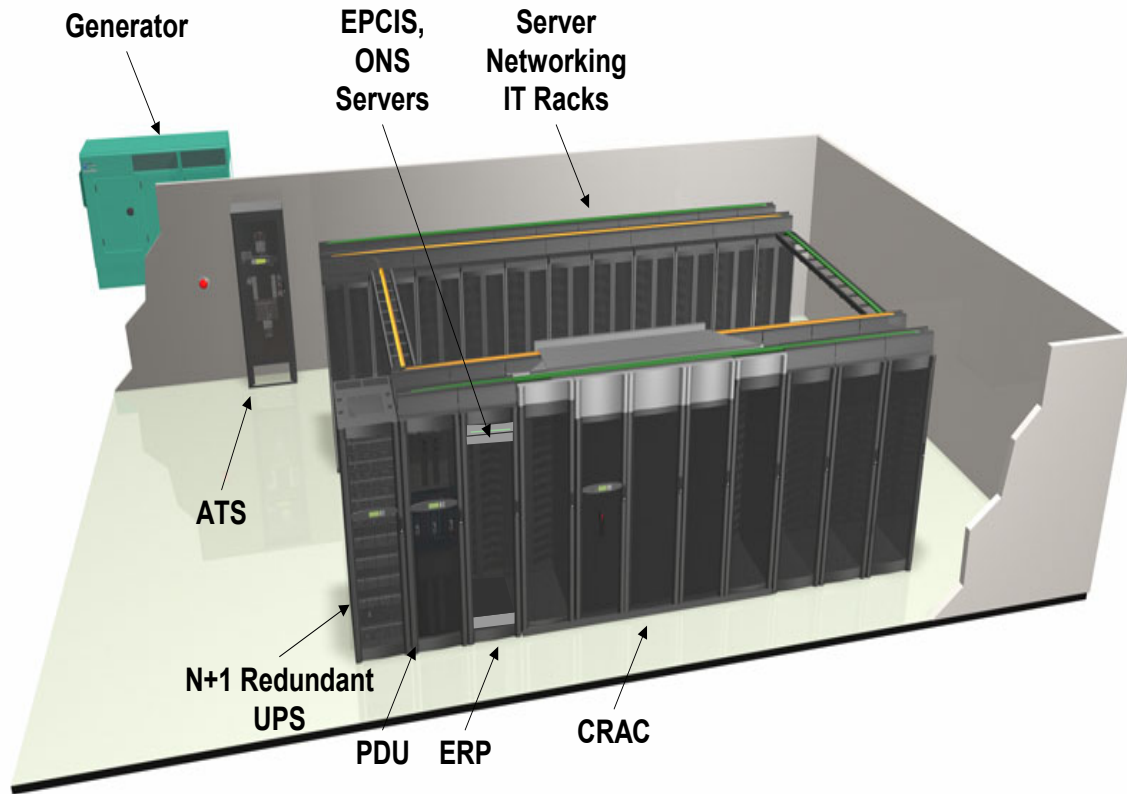
Corporate Data Centers and Disaster Recovery Sites

Corporate data centers house enterprise servers running various business-critical applications (i.e. WMS, SCM, MES, ERP systems like SAP, and Oracle) and they run enterprise storage systems, while their fail over systems reside at the disaster recovery sites. RFID deployment requires additional critical servers (i.e. EPCIS, Object Naming Server or ONS). These systems receive filtered RFID data by middleware through the Wide Area Network (WAN) connection. They allow for automation of many critical business processes such as the generation of advance ship notices (ASN), automatic billing and invoicing, and production plans.

Environment

These systems are generally housed in a secure, temperature controlled environment drawing tens of kilowatts of power on the lower side, and hundreds of kilowatts of three-phase 400 VAC or 480 VAC power on the higher side. The vast majority of these mission critical data centers and disaster recovery sites have redundant UPS, precision air conditioning units, and a back-up generator as shown in **Figure 7**.

Figure 7 – Corporate data center or disaster recovery facility



Challenges

RFID servers are some of the most critical systems within the data center. Depending on the applications they are running, they may require longer runtime and higher redundancy and availability than other equipment. Since these systems are interdependent with other enterprise systems, to form one big RFID network on which the entire organization depends for normal functioning, their availability requirements are generally 99.999% (five nines) or higher which translates to an average downtime of 5 minutes per year or less.

Best practices

- The physical infrastructure supporting the RFID network and other critical enterprise systems should provide the highest levels of redundancy while minimizing the total cost of ownership. An N+1 Redundant UPS with automatic and manual bypass is very common and is often times extended to the generator as well as the precision air conditioning systems to ensure the highest levels of availability. The entire infrastructure should be scalable to allow for future expansion, manageable like the other IT equipment, and serviceable to reduce mean time to recover. All of

these characteristics contribute to the overall availability of the system. Refer to APC White Paper # 117, "Network-Critical Physical Infrastructure: Optimizing Business Value".

- Servers and systems requiring the highest levels of availability should be identified and grouped so that they can be provided with longer runtime and higher levels of redundancy in a separate area, and in separate racks within the data center. This concept of "targeted availability" helps increase availability of business critical systems without having to incur a large capital expense for the entire data center. Higher levels of redundancy like dual feeds with dual generators and dual N+1 UPS with dual power paths all the way to the rack should be considered for highly-critical data centers and networks.
- PDUs should be able to measure and display current, which can help prevent accidental overloading and shutdown. PDUs that allow remote outlet control via the web are desirable for rapidly rebooting a hung server or a storage drive.
- Precision air conditioning equipment should have the capability to allow for expansion. Redundant air conditioning units should be considered for higher availability. For high power density racks (>2 kW/rack) additional air distribution and air removal units should be used to avoid hot spots. For more information on cooling best practices refer to APC White Paper #49, "Avoidable Mistakes that Compromise Cooling Performance in Data Centers and Network Rooms".
- To formulate best strategies to manage the NCPI in a data center, refer to APC White Paper #100, "Management strategies for Network-Critical Physical Infrastructure".

Conclusions

RFID networks need to be highly available in order to improve efficiency and deliver the promised return on investment with various business processes such as logistics, supply chain management, inventory management, and asset tracking. All RFID components, including readers, printers, servers, switches, routers and storage systems should be protected from power anomalies to avoid downtime and expensive repair services. The most vulnerable areas in terms of NCPI are the portals, closets, printing stations, corporate data centers and disaster recovery sites where the RFID systems are installed. These locations need to be audited for any NCPI related weaknesses very early in the planning stage and remedied for a successful RFID deployment within an enterprise.

References

1. APC White Paper #1: "The Different Types of UPS Systems"
2. APC White Paper #5: "Essential Cooling System requirements for next generations of Data Centers"
3. APC White Paper # 18 "The seven types of power problems"
4. APC White Paper # 24 "Effects of UPS on system availability"
5. APC White Paper #37: "Avoiding Costs From Over-sizing Data Center and Network Room Infrastructure"
6. APC White Paper #43: "Dynamic Power Variations in Data Centers and Network Rooms"
7. APC White Paper #49, "Avoidable Mistakes that Compromise Cooling Performance in Data Centers and Network Rooms".
8. APC White Paper # 69 "Power and Cooling for VoIP & IP Telephony Applications"
9. APC White Paper # 100 "Management Strategies for Network-Critical Physical Infrastructure"
10. APC White Paper # 116 "Standardization & Modularity in Network-Critical Physical Infrastructure"
11. APC White paper # 117 "Network-Critical Physical Infrastructure: Optimizing Business Value"

About the Author:

Viswas Purani is a Director of Emerging Technologies and Applications with American Power Conversion Corporation (APC) based in RI, USA. He is responsible for identifying new emerging technologies and application areas for APC products, integrating new products in the existing applications and capturing new product ideas. He joined APC in 1997 and has held various program and product management positions with global responsibilities. He has successfully started a data center solutions company in the Middle-East, Motorola semiconductor distribution in western India and was involved with technology transfers of UPS Systems and AC/DC drives from leading American and European companies. He has a Bachelors degree with a major in power electronics engineering (1988) and a Masters degree in business administration with a major in international business (1999).