Management Strategy for Network Critical Physical Infrastructure

White Paper #100

APC
Legendary Reliability®

Executive Summary

When choosing a management solution for the physical infrastructure of IT networks, management of individual devices is necessary in order to have visibility to the many data points required for the reliable operation of network-critical physical infrastructure. Element management solutions offer the optimum approach as they manage a particular type of device and have the ability to assimilate and, more importantly, make manageable the large volume of data necessary for network availability.

Introduction

The current trend towards higher availability of computing and networking resources has led to an increased focus on the underlying physical infrastructure on which those resources depend. It has become apparent that in order to optimize performance of the physical infrastructure layer, management of this layer is necessary. When choosing a management solution for the physical infrastructure layer, key factors for consideration are; the cost of deployment and maintenance, adaptability as business needs change, functionality, and ease of integration.

A manner consistent with an overall management structure is desirable and offers the benefits of; providing information on issues affecting system availability, lessening the burden of managing the system, lowering the risk of downtime and increasing IT personnel productivity.

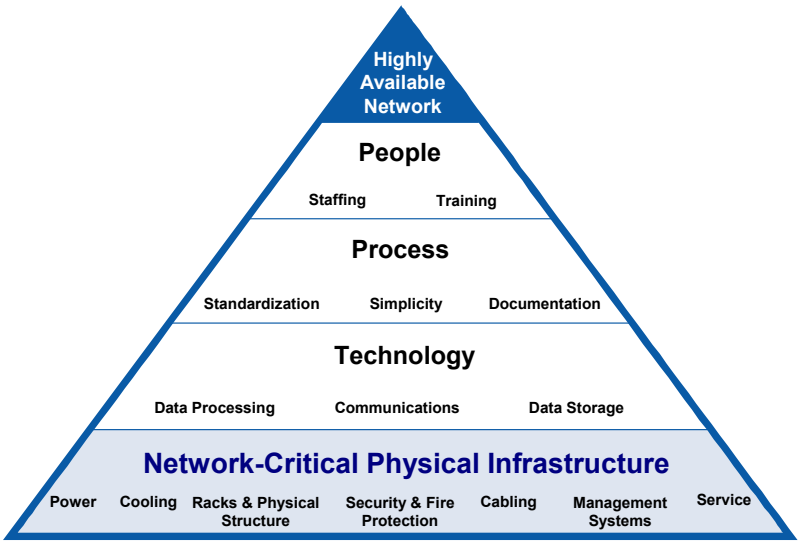
IT Network-Critical Physical Infrastructure

Network Critical Physical Infrastructure (NCPI) is the foundation upon which Information Technology (IT) and Telecommunication Networks reside as seen in Figure 1. This includes:

- Power
- Cooling
- Racks & Physical Structure
- Security & Fire Protection
- Cabling
- Management Systems
- Service

At first look, these components seem similar to those in building systems. Almost all buildings have a power, air conditioning, environmental monitoring, and security infrastructure in place. What distinguishes these systems from NCPI is the focus on availability of computing resources. The primary focus of building systems is the comfort of building inhabitants and traditional facilities functions such as building automation. The needs of these two entities differ widely. A standardized, adaptable, and integrated NCPI is essential to maintaining highly available and manageable networks.

Figure 1 *– The NCPI Layer*



NCPI marks the convergence of traditional facility responsibility and that of the IT department within an organization. NCPI responsibility may fall under the facilities or the IT department or may be shared between both. This convergence of interests creates new problems and challenges for managing physical infrastructure than has previously been the case.

The Challenges of NCPI Management Strategy

There are two major challenges that face a successful NCPI management strategy.

Architecture of NCPI Management

First, many IT and facility departments have installed specific management packages for their respective devices. Many IT departments have both device specific element managers for servers, storage and networking equipment as well as an enterprise management system such as HP OpenView or IBM Tivoli. Facility departments frequently utilize building management systems such as Johnson Controls Metasys.

It is likely, given the convergence between facility and IT departments with respect to NCPI, that both IT and facility departments will be interested in leveraging their current management package. Therefore, any NCPI management strategy must comprehend and integrate with these applications.

Architecture of Enterprise Management Systems

The designs of these management systems differ in their architecture. IT packages (Enterprise Management Systems or EMS) are 'device centric' and utilize the existing IT network. Device centric is defined as focusing primarily on individual IP addresses that represent access to information about the device as a whole. For example, one IP address may represent a single server, networking, or storage

device. Alarms and information are usually encapsulated at the device level and then propagated to the summary management package over the existing IT network. Management packages such as HP OpenView and IBM Tivoli are considered to be in this category.

Architecture of Building Management Systems

Building Management Systems (BMS) tend to be 'data point centric' and frequently utilize a network separate from the IT network. Data point centric is defined as individual data points from a given device being monitored. Therefore, the focus is not on managing the device as an entity but is on the specific information that the device can report. These networks are frequently serial-based utilizing proprietary protocols or some level of standard protocols such as MODBUS. These differences, are summarized in the table below:

Table 1 *– BMS versus EMS architectures*

Package Type	'View point'	Network Utilized
Enterprise Management System (EMS)	Device Centric	IT Network
Building Management System (BMS)	Data Point Centric	Dedicated Network

The implications of these differences highlight a significant challenge for a comprehensive NCPI strategy. Integration with two different management architectures, one device centric and one data point centric, is difficult. Any management strategy must be able to provide device-level summary information for the IT package while at the same time provide a level of data point granularity to enable integration with the facility package.

Standards of NCPI Management

The second major challenge for a comprehensive NCPI management strategy is the process of gathering a larger amount of data than has been traditionally monitored. A comprehensive strategy should incorporate information at the rack level in order to ensure reliable operation of the IT equipment. Previously this was not feasible.

Monitor Devices and Data Points Key to Availability

It is critical that all key devices and data points be monitored. These include all the devices in the NCPI layer and the surrounding environment. Best practices dictate that the following list of devices be monitored at the rack level:

- Individual branch circuits
- Two temperature data points (minimum)
- Transfer switches
- Cooling devices
- UPS systems

Monitoring of devices such as rack based transfer switches, UPSs, and cooling devices is a well-understood practice. However, monitoring of branch circuits at the rack and temperature at the rack is a relatively new concept in NCPI management.

Monitoring individual branch circuits contributes to availability by enabling an administrator to receive a notification before a circuit is overloaded. Studies have shown that a significant cause of datacenter downtime is as a result of faults at the branch circuit. Therefore, active management of these branch circuits can significantly contribute to increased availability.

Identifying racks that are running hotter than normal is necessary since elevated temperatures significantly degrade the expected life of IT equipment. The trend towards higher density of IT equipment exacerbates this problem since greater power density is directly related to greater cooling needs. Monitoring these devices enable an administrator to understand problems either with the devices themselves or the surrounding environment.

Resource Efficient Management

Centralized management has the advantage of making pertinent information available quickly. To optimize resource efficiency, information should be available in an easy-to-understand fashion, minimizing or eliminating training needs. Mass configuration and automating responses to known issues is also beneficial. In short systems should be easy to deploy and maintain.

Warnings of Critical Events

Power failures and elevated temperatures are examples of events which if not addressed impact network availability. Timely information allows corrective action to be taken before equipment is damaged or fails and is critical to the smooth operation of an NCPI management system. For example, an administrator may wish to receive a notification when the amperage consumed on a branch circuit increases by more than 1 amp, ensuring visibility to the system should unauthorized equipment is added to the circuit.

Performance Analysis and Predicting Failures

At a minimum, event and data logs should be stored so that manual performance analysis can be done. Good analysis tools help prevent problems by highlighting areas of concern and target the root cause of potential problems. Examples include; identifying older batteries and rack hot spots and highlighting chronic power line problems such as frequently occurring brown outs.

Easily Adaptable as Business Needs Change

Replacement and upgrade strategies should be devised at convenient times such that unexpected, unplanned and costly downtime can be avoided. Flexible systems support changes in configuration while minimizing downtime. Examples of changes that can be anticipated include; changing runtime, power load and redundancy requirements as well as adding support for branch offices or other network nodes.

Appropriate management of NCPI requires comprehending this large volume of data in a fashion meaningful for the administrator.

An NCPI Management Solution

Element Managers

Over the past decade IT systems were quickly put in place to solve urgent business needs leading to multiple point solutions. As a result in many installations IT departments tend to manage equipment utilizing 'element managers' for different categories of equipment. As outlined in Figure 2 below, it is common to utilize a 'storage manager' such as EMC ControlCenter, for storage, a 'network manager' such as CiscoWorks, for the networking equipment, and a server manager, such as HP Insight Manager, for servers.

The advantage of these 'element managers' is that they are generally easy to deploy and use since they are focused on managing one category of devices – in many cases devices specific to an individual vendor. The limitation of this strategy is that there is no coordination of the different element managers.

Element Managers and Enterprise Management Systems

In order to gain better visibility across the entire network, use of an Enterprise Management System such as Tivoli or HP OpenView, is necessary. These tools help coordinate the different types of devices and provide a broad view of everything occurring on the network.

However neither element managers nor an Enterprise Management System comprehend management of the network-critical physical infrastructure layer.

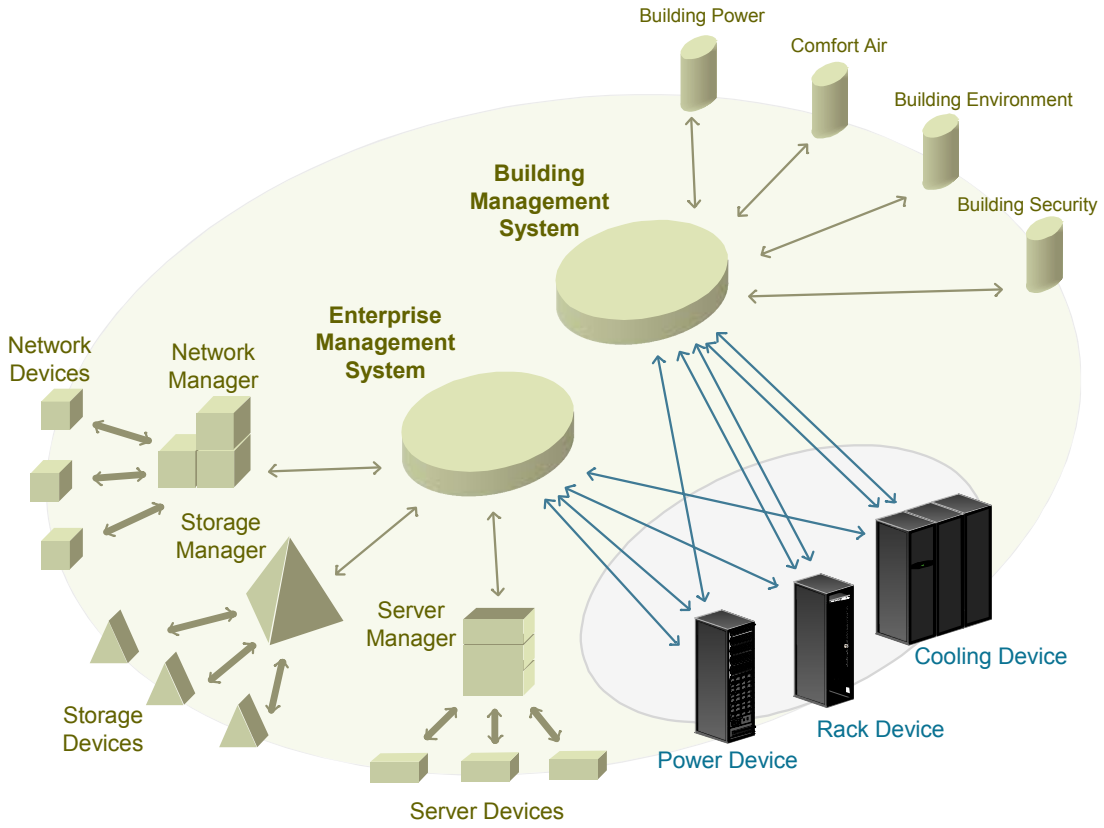
Data Points and Building Management Systems

Similarly BMSs are frequently used to manage some of the data points of NCPI. However, by nature of their architecture and the volume of information required they do not exhibit the characteristics of good NCPI management and are, therefore, inappropriate for management of the network-critical physical infrastructure.

Integrating NCPI Management

So this begs the question, how does one integrate NCPI with both existing BMS and EMS systems? A typical approach would require integration of each individual device, or data point, into the high-level management system. Figure 2 represents the integration paths of the individual devices utilizing this traditional approach.

Figure 2 *– Traditional Integration of NCPI with BMS and EMS*



The drawback of this implementation is the significant cost associated with integrating each of these devices and/or data points. This scheme can also lead to information overload for the user since there are so many devices or single data points reporting into one central location. With this model users are forced to either buy or develop unique rules for handling this information in their BMS or EMS.

NCPI Element Manager

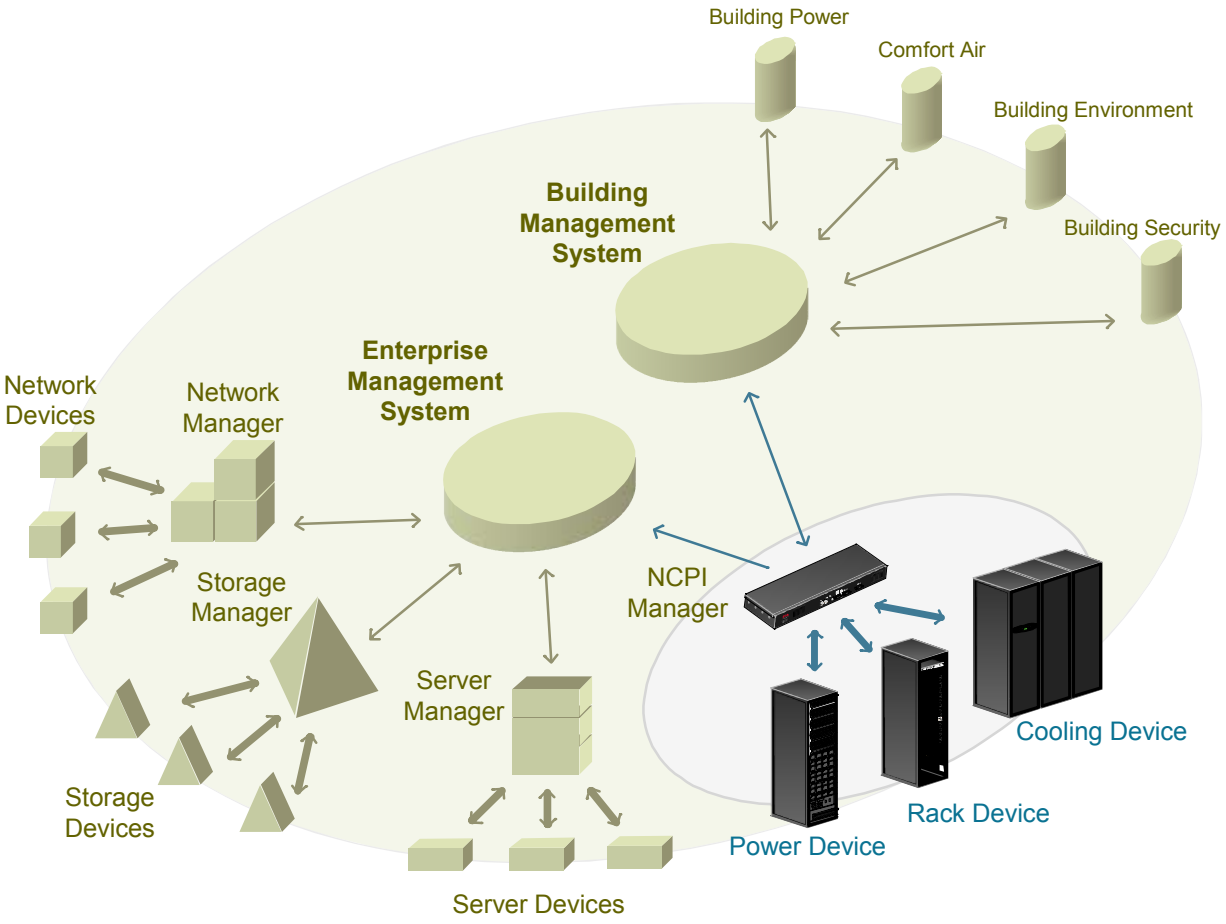
The solution is an element manager for NCPI devices as shown in Figure 3. A properly designed NCPI element manager should limit integration points necessary in the EMS and BMS by providing summary information to those platforms. Detailed information can be obtained by connecting directly to the NCPI element manager, as is the case with server, storage and network element managers.

Element managers also have the advantage of being less expensive to install. Instead of demanding individual integration with each device, the element manager aggregates this information automatically. Since the element manager has a single purpose, it is pre-programmed with select rules and policies and therefore has all the appropriate characteristics necessary for NCPI management.

By utilizing an NCPI element manager, a more flexible management scheme can be realized. Information at the aggregate level can be integrated into both EMSs and / or BMSs if so desired. Alternatively the NCPI

element manager can be utilized as stand alone management tool, as is frequently the case for server, storage and networking element managers.

Figure 3 *– Element Manager Integration of NCPI with BMS and EMS*



An NCPI Element Manager example

An example of a management tool that meets the criteria of an NCPI element manager is APC's InfraStruXure Manager. This device is a dedicated 1U rack mountable appliance for managing physical infrastructure. It provides summary alarm information for building management systems as well as enterprise management systems and also functions as an element manager.

APC's InfraStruXure Manager

Conclusions

A best in class NCPI management scheme should incorporate the use of an NCPI element manager. The advantages of utilizing an NCPI element manager are:

1. Cost effective management of the many data points required for appropriate NCPI management.
2. Optimized for functionality appropriate to NCPI.
3. Ease of integration with existing enterprise and building management systems.
4. Cost effective installation and maintenance.