CHAPTER 2

Virtualization, Thin Clients, and Industrial Data Center Description Virtualization

Virtualization is the creation of virtual resources such as a server, desktop, operating system, file, storage, or network. The main goal of virtualization is to manage workloads by transforming traditional computing to make it more scalable. Virtualization has been around for quite some time and today is being applied to a wide variety of system levels, including operating system-level virtualization, hardware-level virtualization, and server virtualization.

Some items to consider that are good and bad for virtualization include:

- Virtualization opportunities:
  - Flexibility—Old operating systems, Linux on Windows, etc.
  - Availability—VMs can migrate to another host should their host fail.
  - Speed—Server and desktop provisioning
- Virtualization challenges:
  - Anything (process, application, etc.) that requires a dongle or physical hardware.
  - Systems that require extreme performance, e.g., systems that use a lot of the resources.
  - Applications and operating systems with license or support agreements that do not permit virtualization.

Benefits of Virtualization

Benefits of virtualization include:

- **Energy Saving**—Migrating physical servers over to virtual machines and consolidating them onto far fewer physical machines means lower power and cooling costs.
- **Reduces the Data Center Footprint**—Server consolidation with virtualization reduces the overall footprint of the data center, which means fewer physical machines, less networking gear, and fewer racks and hence less required floor space.
- **QA, Test, and Lab Environments**—Virtualization allows for an easy build out of a self-contained lab or test environment operating in its own isolated network, which should be considered when rolling out patches or updates both to the OS and the IACS software.

- **Faster Provisioning**—Virtualization enables flexible capacity to provide systems (servers and desktops) very quickly as opposed to purchasing additional physical machines. This process can be done within a few minutes by simply closing an existing "master" image, template, or existing virtual machine.
- **Increased Uptime**—With the use of advanced features that are not available on physical servers, virtualization allows for better continuity and uptime. Capabilities such as VM and storage migration, fault tolerance, high availability, and resource scheduling keep virtual machines running or allow for fast recovery from failures and unplanned outages.
- **Improve Disaster Recovery**—By removing the dependency on specific hardware or server models, a disaster recovery site no longer needs to keep identical hardware that matches the production environment. Operations can save money by purchasing less expensive hardware for disaster recovery since it rarely gets used. Also, because virtualization allows for fewer physical machines, replication sites are more affordable.
- **Application Isolation**—Application isolation is usually achieved by using a "one app/one server" model. Virtualization can use components (e.g., application farms) to support specific applications and allow only specified users.
- **Extend the Life of Older Applications**—Older applications than are not able to be upgraded and will only run on older operating systems (and therefore older hardware) can be maintained on virtual machines, avoiding the need to keep and maintain outdated or non-replaceable hardware.

Thin Client Technology

A thin client is a lightweight computer which is optimized for accessing applications or desktops from a remote server-based computing platform. The server provides the majority of the computing power, including launching software programs, running calculations, and storing data. The thin client provides I/O for a keyboard, mouse, monitor, sound, and USB ports for access to USB devices.

Thin clients are used to access applications or desktops from remote locations (e.g., IDC). Some benefits of using thin clients include cost savings, reduced energy consumption (versus a PC), simplified management, enhanced security, and overall increased productivity.

Thin client technology types include:

- PC over IP (PCoIP)
- Remote Desktop Protocol (RDP)
- ThinManager® software

PC over IP (PCoIP)

PCoIP or PC-over-IP is a display protocol that permits total compression of a desktop, which is then displayed using a zero-client device over a standard IP network. With PCoIP, the entire computing experience is compressed, encrypted, and encoded in the data center before being transmitted across a standard IP network to PCoIP-enabled endpoint devices.

Remote Desktop Protocol (RDP)

RDP is used for communication between the Terminal Server Client and the Terminal Server. With RDP a remote user can add a graphical interface to another computer's desktop. This secure network communications protocol is designed for Windows-based applications that run on a server. It facilitates

encryption and application data transfer security between devices, client users, and a virtual network server. Network administrators can use RDP to remotely identify and resolve problems faced by individual subscribers.

PCoIP versus RDP

The choice of PCoIP versus RDP is based on how well either PCoIP or RDP meet your requirements.

Choose PCoIP if any of the following are applicable:

- You are using a high-speed connection and bandwidth is not a problem.
- You want to display better quality videos, graphics, and sound.

Choosing RDP would be a good decision if:

- You are unaware of your network quality; in such a case, RDP would be a better choice than PCoIP.
- The quality of sound, graphics, and video is not an issue.

ThinManager

ThinManager® software provides software solutions for IACS networks that enable secure, centralized configuration and deployment of applications and content to every PC, thin client, mobile device, and user.

ThinManager Relevance® software is a location-based mobile management platform that allows applications and content to be securely delivered to specific locations within the manufacturer's facility. ThinManager Relevance uses location resolvers and geofences like QR codes, Bluetooth beacons, Wi-Fi, and GPS to confirm that mobile users and devices only receive content in authorized areas. Content specific to a user's role can be delivered based on Relevance user credentials which can be linked to Active Directory accounts.

Within the CPwE IDC, ThinManager can be used to securely manage content delivery to thin clients from various applications and data sources in the Industrial Zone: FactoryTalk View SE and ME applications, FactoryTalk VantagePoint data, Studio 5000 Logix Designer® software, terminal shadowing, streaming video, and many others. Thin clients can receive content from Microsoft® Remote Desktop servers running these applications, as well as VNC servers (for example, FactoryTalk View ME terminals) and IP cameras.

The ThinManager solution provides additional security when introducing thin clients into the industrial environment since no production data is stored locally and content delivery can be authorized by any combination of user, location, and device.

Industrial Data Center

The IDC is a purpose-built resource that provides compute, storage, and multi-layer network switching in a pre-engineered and validated package. The IDC is located in Level 3 Site Operations where it houses the virtualized servers used in the IACS. Most IDC designs also have backup power provisions as well as smart power distribution units with dual-power source provisions. Design parameters and verification methodologies are established by CPwE architects, Rockwell Automation application specialists, and Panduit engineers to ensure that the IDC meets requirements in a robust and reliable fashion.

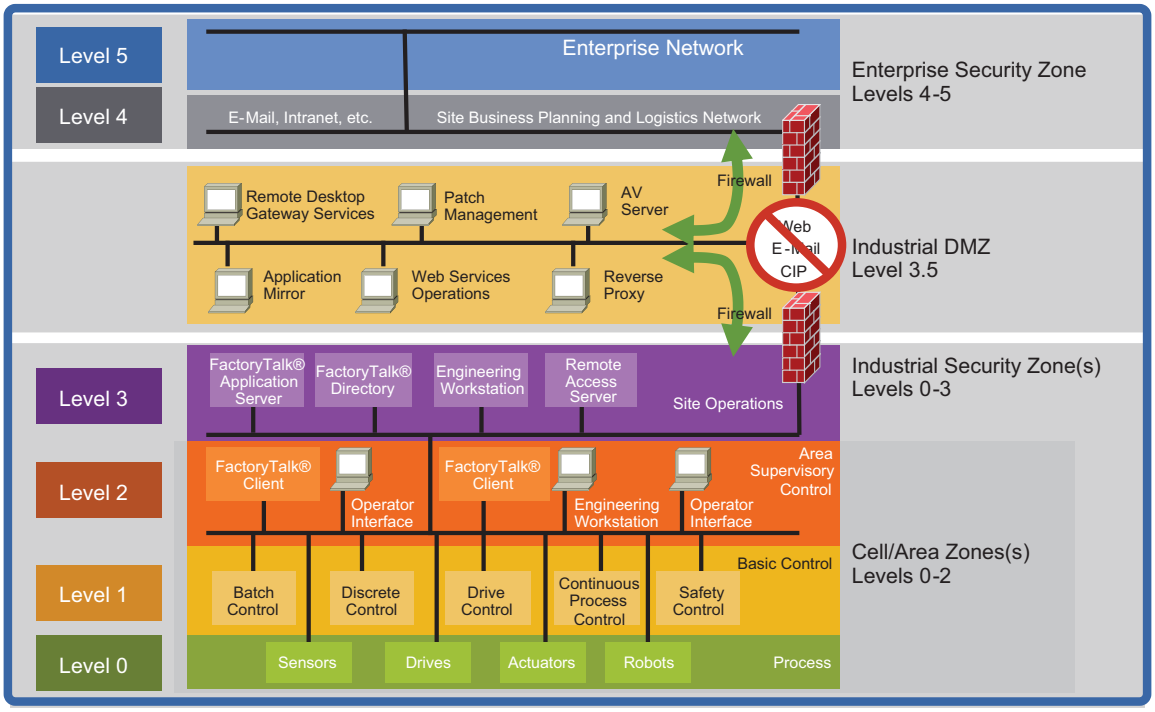
The IDC provides many key functions for a well-designed IACS network. It can provide an operating platform for enterprise grade software applications like MES software, hosts patch and version servers, etc.

There is open rack unit (RU) space within the IDC that may be used for mounting additional items such as security appliances (e.g., ISE), networking appliances, etc.

In support of the performance of the industrial network, there are many infrastructure aspects of the IDC that play an important role and must be considered in the design and implementation of it within the network.

- **Industrial Characteristics**—The IDC is typically deployed within Level 3 Site Operations of CPwE architectures (Figure 2-1). Plant networking assets and cabling used in Level 3 Site Operations are not environmentally hardened but are almost exclusively installed in IP20 or better environments. Environmental risks at Level 3 Site Operations involve thermal management of equipment heat dissipation, redundant network connections, redundant power connections, and power quality considerations.

Figure 2-1 CPwE Logical Model



- **Physical Network Infrastructure Life Span**—Industrial automation and control systems (IACS) and the plant backbone can be in service 20 years or longer. Hardware used in Level 3 Site Operations, being IT gear, has a much shorter life span, generally 3-5 years. This nominal life span is related to the technology age of the equipment rather than its ability to function past this time frame. The infrastructure used to connect and house hardware such as cabinets, cabling, connectivity, and enclosures has a much longer life span, generally 10-15 years. Consideration of higher performance cabling enables the data communications needs of tomorrow as well as today to be fully met. Choosing supporting infrastructure wisely at the time of IDC installation and commissioning avoids the future cost and disruption of installing upgraded media that matches the capabilities of the new IT equipment that is installed. Choices in media between copper and fiber optic cabling ensure higher data rate transport requirements.
- **Maintainability**—Be aware that Move, Adds, and Changes at Level 3 have dependencies that affect many Cell/Area Zones. Also, changes need to be planned and executed correctly as an error can bring down manufacturing. Proper cable management such as bundling, identification, access, etc. is vital. Use of structured cabling techniques provides maintainability benefits and provides measurable value in terms of quickly recovering from outages related to media cuts as well as delivering a high level of agility when the network must adapt to meet manufacturing process changes.

- **Scalability**—The high growth of EtherNet/IP and IP connections can strain network performance as well as cause network sprawl that threatens uptime and security. A strong physical building block design accounts for traffic growth as well as management of additional cabling to support designed network growth. Use a zone topology together with structured copper and fiber optic cabling chosen for high data throughput. The CPwE architecture lends itself readily to deployment across a zone architecture. Choose building block pre-configured solutions to enable a network infrastructure comprised of modular components that scale to meet increasing Ethernet communications needs in your IACS network.
- **Designing for High Availability**—A robust, reliable physical infrastructure achieves service levels required of present and future IACS networks. The use of standards-based cabling together with measured, validated performance ensures reliable data throughput. Use of redundant logical and physical networks assures highest availability. Properly designed and deployed pathways should be employed to ensure redundant cables paths are also resilient cables paths.
- **Network Compatibility and Performance**—Network performance is governed by the poorest performing element in any link. Network compatibility and optimal performance is essential from port to port. This compatibility requirement includes port data rate and cabling bandwidth. Cable selection is the key to optimal physical network performance.
- **Grounding and Bonding**—A well architected grounding and bonding system is crucial for industrial network performance at every level whether internal to control panels, across plants, or between buildings. A single, verifiable grounding network avoids ground loops that can degrade data and has implications for equipment uptime and even safety. In high EMI areas, where the use of shielded cabling is advisable, the performance of the shielding is inexorably tied to the quality of the grounding network that supports it.
- **Security**—Network security is a critical element of network uptime and availability. Physical layer security measures, like logical security measures, should follow a defense-in-depth hierarchy. Your Level 3 physical defense in depth strategy could take the form of locked access to data center and control room spaces and cabinet key card access to help limit access, use of Lock In Block Out (LIBO) devices to control port usage, and keyed patch cords to avoid inadvertent cross patching. Using a physical strategy in concert with your logical strategy helps prevent inadvertent or malicious damage to equipment and helps achieve connectivity service level goals.
- **Wireless**—Unified operation of wireless access points requires a Wireless LAN Controller (WLC) at Level 3 Site Operations and distribution of lightweight wireless access points across Industrial Zone and Cell/Area Zones. Autonomous wireless access points, typically Work Group Bridges, in Cell/Area Zones involves cabling for access points and Workgroup bridges. The selection of media for the industrial zone backbone as well as for cabling for access points using POE is critical for future readiness and bandwidth considerations. PoE is evolving to deliver more power over copper cabling so understanding industrial applications with scalability and environmental considerations is critical.
- **Panduit SmartZone™ Cabinet**—The IDC used in testing utilized a Panduit SmartZone Cabinet. SmartZone Cabinets enable Level 3 Site Operation data centers, co-location facilities, and remote sites with limited technical expertise and financial resources to easily order, rapidly install, and deploy fully integrated cabinets. The SmartZone Cabinet is pre-installed with SmartZone Power Solutions to provide a range of standardized, factory-integrated intelligent cabinets with pre-tested, validated access control, power, and thermal monitoring capabilities. SmartZone Rack Monitoring Software uses operational data consolidated by the SmartZone Gateway and displays it on the intuitive dashboard to provide a precise and logical reflection of the “actual” power and thermal data as well as the ability to send alerts to identify rising temperatures or other issues that may impact business resilience. This ready-to-deploy cabinet solution provides data centers with a complete Data Center Infrastructure Management (DCIM) solution that is immediately ready to begin delivering the transparency and actionable information needed to optimize energy and operational efficiencies, fully maximize existing capacity, and protect service uptime.