BR&L Consulting
208 Townsend Ct, Suite 220, Cary NC 27511 919-852-5322

The IT Implications of ISA 95 and ISA 99

Dennis Brandl
dnbrandl@brlconsulting.com

Abstract

As manufacturing operations, defined in the ISA 95 standard, moves more into the standard information technology area, there are implications for IT organizations and network infrastructure layouts. IT organizations can gain value in faster and more robust implementations if they understand the real requirements for manufacturing applications and how this affects their infrastructure systems, such as networks and servers. This is required so that production will have the robust and resilient systems they have come to expect. This presentation discusses the real-world issues of implementing an ISA 95 based system into the corporate network.

ISA 95 Levels

The ISA 95 standard defines a multi-level model for activities. Each level provides specialized functions and has characteristics response times.

- Level 0 defines the actual physical production process.
- Level 1 defines the activities involved in sensing the production process and manipulating the production process.
- Level 2 defines the activities of monitoring, supervisory control and automated control of the production process. It deals with time frames in the order of hours, minutes, seconds, and subseconds.
- Level 3 defines the activities of work flow, stepping the process through states to produce the desired end products. It deals with maintaining records and optimizing the production process. Level 3 deals with time frames of days, shifts, hours, minutes, and seconds.
- Level 4 defines the activities of establishing the basic plant schedule - production, material use, delivery, and shipping. It deals with determining inventory levels and making sure that materials are delivered on time to the right place for production. Level 4 deals with time frames of months, weeks, days, and shifts.

The four ISA 95 levels are shown in Figure 1.

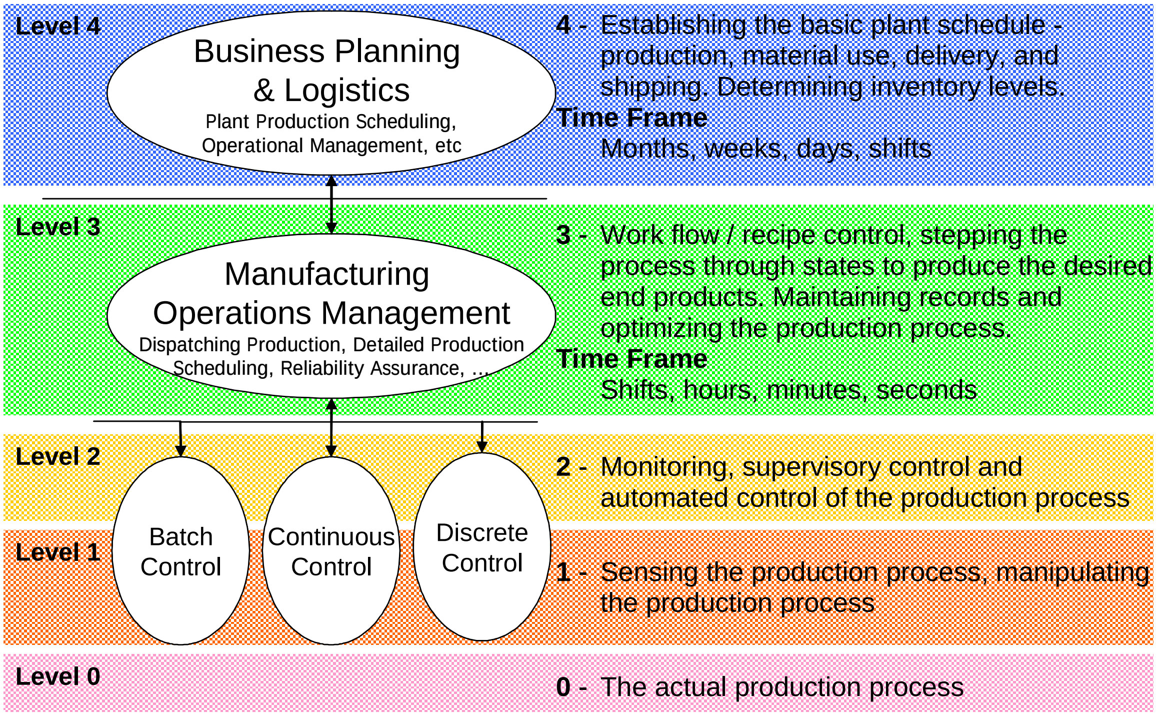

Level 4
Business Planning & Logistics
Plant Production Scheduling, Operational Management, etc
4 - Establishing the basic plant schedule - production, material use, delivery, and shipping. Determining inventory levels.
Time Frame
Months, weeks, days, shifts
Level 3
Manufacturing Operations Management
Dispatching Production, Detailed Production Scheduling, Reliability Assurance, ...
3 - Work flow / recipe control, stepping the process through states to produce the desired end products. Maintaining records and optimizing the production process.
Time Frame
Shifts, hours, minutes, seconds
Level 2
Batch Control
Continuous Control
Discrete Control
2 - Monitoring, supervisory control and automated control of the production process
Level 1
1 - Sensing the production process, manipulating the production process
Level 0
0 - The actual production process

Figure 1 - ISA 95 Levels

The standards that apply at each level are shown in Figure 2. These standards have a strong value to IT organizations, since they help in defining the choices to make at each level, and to make sure that the right networks and infrastructure can be applied at each level.

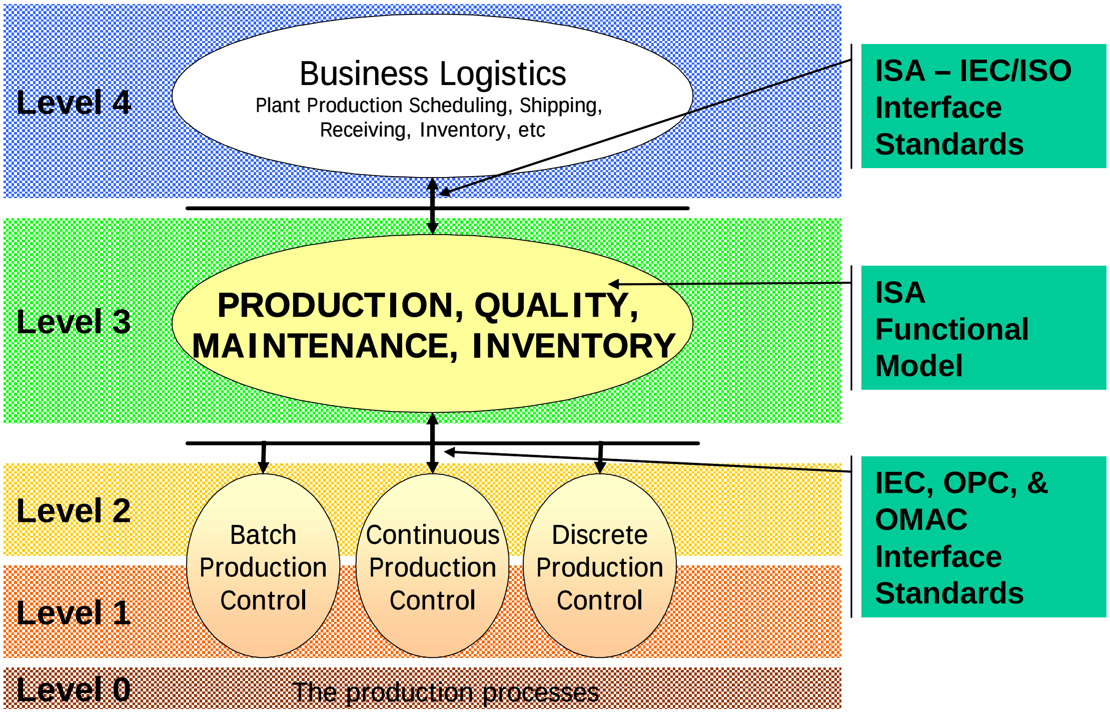

Level 4
Business Logistics
Plant Production Scheduling, Shipping, Receiving, Inventory, etc
ISA – IEC/ISO Interface Standards
Level 3
PRODUCTION, QUALITY, MAINTENANCE, INVENTORY
ISA Functional Model
Level 2
Level 1
Batch Production Control
Continuous Production Control
Discrete Production Control
IEC, OPC, & OMAC Interface Standards
Level 0
The production processes

Figure 2 - Standards at Each Level

IT View of ISA 95 Levels

While the models just define a way to describe the activities of a manufacturing company they are often also used to define levels for software applications and networks. ERP, SCM, CRM, and PLM are typical Level 4 applications. MES, LIMS, CMM, batch management and WCS (Warehouse Control Systems) are typical Level 3 applications. PLCs, DCSs, SCADA, and HMI are typical Level 2 systems and applications. There is overlap in the application area, with ERP often supporting some Level 3 functions, and DCS systems often supporting Level 3 and Level 2 functions. The typical applications used at each level are shown in Figure 3.

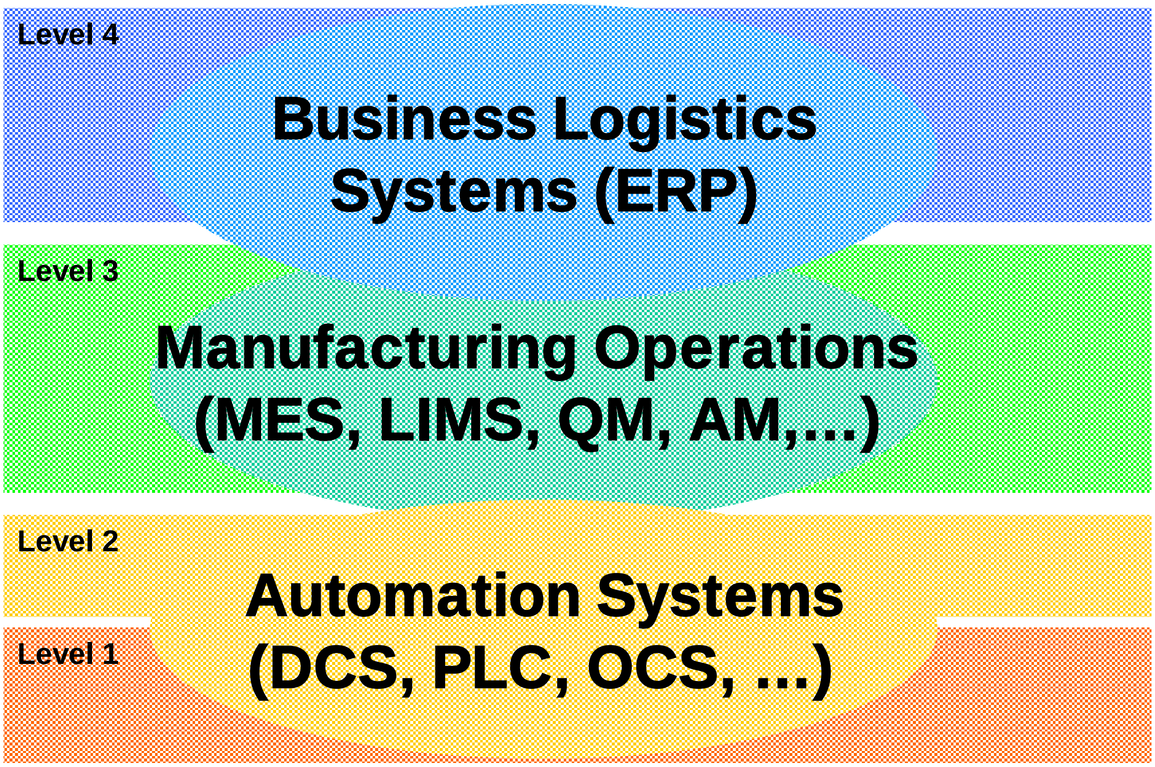

Level 4
Business Logistics Systems (ERP)
Level 3
Manufacturing Operations (MES, LIMS, QM, AM,…)
Level 2
Level 1
Automation Systems (DCS, PLC, OCS, …)

Figure 3 - Applications at Each Level

These systems where generally never designed to operate together. Each level typically runs on a separate network with separate servers and under separate account and security domains. An IT infrastructure view of the ISA 95 levels is illustrated in Figure 4.

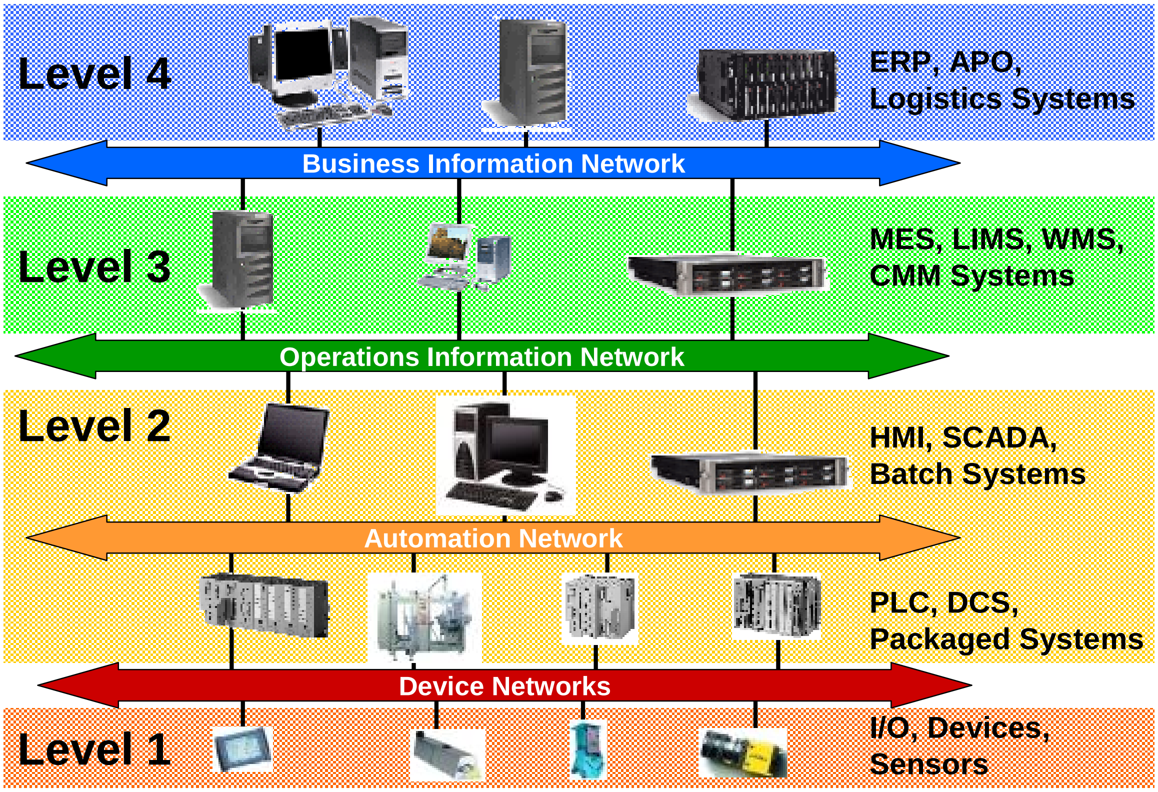

Level 4
ERP, APO, Logistics Systems
Business Information Network
Level 3
MES, LIMS, WMS, CMM Systems
Operations Information Network
Level 2
HMI, SCADA, Batch Systems
Automation Network
PLC, DCS, Packaged Systems
Device Networks
Level 1
I/O, Devices, Sensors

Figure 4 - S95 Levels as seen from an IT Infrastructure viewpoint

As companies now work to improve their efficiency and productivity these systems must be modified and/or designed to interoperate. They must coexist under the same IT infrastructure. Fortunately, there is a commonly used IT infrastructure that can be extended to connect the various application levels into a corporate infrastructure. This structure is based on the design of large scale LANS and has been effectively applied in many companies and university systems, where there are thousands of connected computers across large sites.

The ISA 95 Hierarchy model can be applied to the equipment, people, and information systems in a facility. The model defines levels that can be mapped to systems and to networks. However these systems and networks need to work together in a SAFE and SECURE manner. We do not want virus and worm attacks to corporate systems to stop production systems, yet these systems can often not be as well protected and updated as business systems. We do not want hackers to be able to access and control production systems. In order to meet these goals the network infrastructure becomes a critical part of the production "system" architecture.

A typical physical view of S95 systems is shown Figure 5. The physical structure shown in Figure 5 isolates the automation network (Level 2-3) and the operations network (level 3) from the corporate network and other corporate subnets.

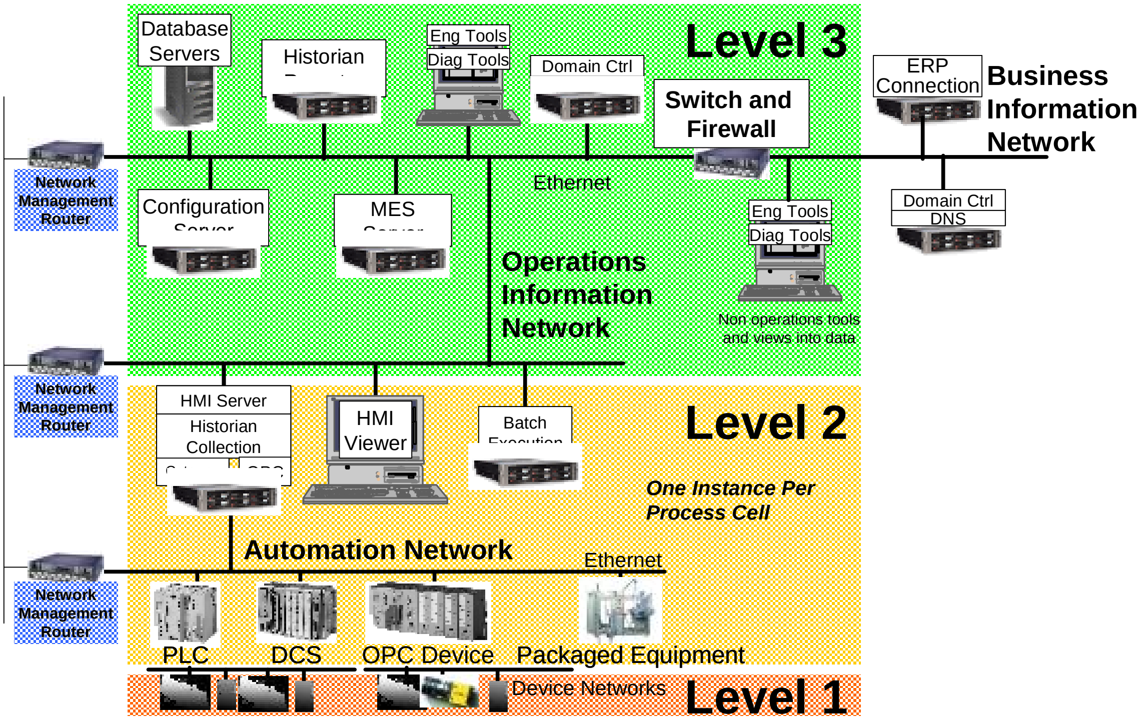


Figure 5 - A Network Physical Architecture

A Structure for ISA 95 Applications

There is a standard network structure used in the design of large scale LANS. This structure is defined in the book *Designing Large-Scale LANS* by Kevin Dooley and is also described in the Cisco Net 7 architecture definitions. Many large scale campus wide LANs follow this structure, as illustrated in Figure 6.

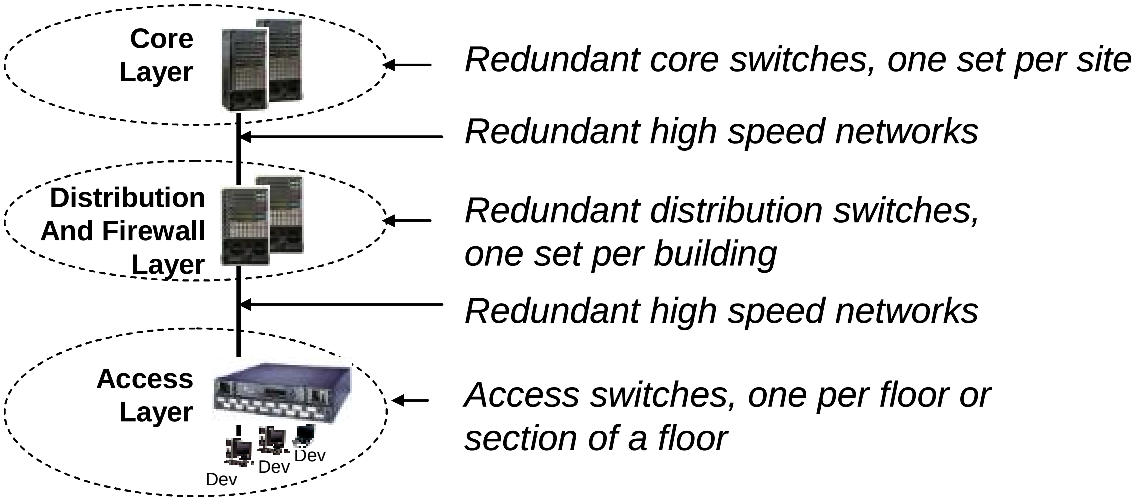

Core Layer
Redundant core switches, one set per site
Redundant high speed networks
Distribution And Firewall Layer
Redundant distribution switches, one set per building
Redundant high speed networks
Access Layer
Dev
Dev
Dev
Access switches, one per floor or section of a floor

Figure 6 - Large Scale LAN Layers

An IT network infrastructure that follows the ISA 95 level approach is a four-layer physical network. See Figure 7 for picture of the levels in the four-layer physical network. The layers should not be confused with the ISA 95 levels, but are instead layers of communication access, designed to maximize network uptime and minimize unnecessary network traffic. This structure is an extension to the standard three-layer structure shown in Figure 6. A bottom layer is added for automation equipment and for connection of the automation equipment to SCADA and HMI devices.

The bottom layer, the automation layer corresponds to connections between S95 Level 2 and Level 1 systems. This is added as a specific layer to the industry standard large system LAN design. This layer is added to specifically control automation network traffic and switch configuration in order to meet the real-time response requirements needed by automation.

Level 2-3 network communication is localized within the access layer. This localizes real-time data collection and HMI communication and also provides a measure of robustness and standalone capability. Level 3-4 network communication is localized in the distribution and firewall layer. This provides communication between all S95 Level 3 systems and also provides a single point for firewall protection of the operations network.

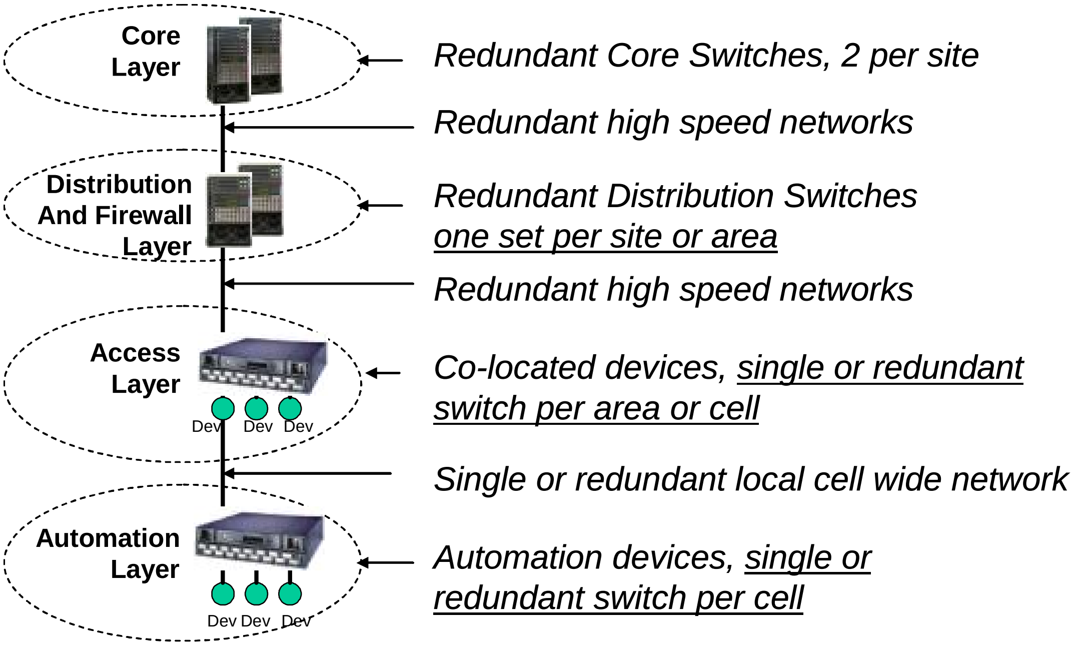

Core Layer
Redundant Core Switches, 2 per site
Redundant high speed networks
Distribution And Firewall Layer
Redundant Distribution Switches one set per site or area
Redundant high speed networks
Access Layer
Dev Dev Dev
Co-located devices, single or redundant switch per area or cell
Single or redundant local cell wide network
Automation Layer
Dev Dev Dev
Automation devices, single or redundant switch per cell

Figure 7 - Multi-layer Network Infrastructure

The manufacturing LAN Architecture is composed of four layers: Automation, Access, Distribution, and Core.

- **Automation Layer**

  Automation devices which use Ethernet as Level 1-2 communication networks should connect to an automation switch. Only one device on the automation layer should connect to the access layer, and any communication should be through an application (such as a SCADA or HMI application). (See Figure 10) Other automation devices should only connect to the automation layer. The automation layer is a physically distinct network, completely separate from the operations LAN with no hub or switch connectivity.

  The automation layer should use switches rather than hubs to optimize network performance, especially if the PLCs and other control devices use the Ethernet network to intercommunicate. A hub logically connects all of the devices on to the same network, and all nodes see all communications, a switch will limit the traffic seen to each node, providing more consistent and reliable network response times.

- **Access Layer**

  Other end devices (such as PCs, Printers, and servers) should only have access to the Access Layer. In order to have redundancy, each Access Switches should be connected to 2 Distribution Switches. Consider using redundant access switches and two connections from each end device where complete failsafe operation is required. You should also consider the scope of control of each access switch in terms of the expected growth of the system, and the risk of failure of the access point.

  A standard corporate infrastructure for the business LAN will also use an access layer and have access switches. You should make sure that the business LAN access switches are kept physically distinct from the operations LAN access switches. Generally the operations LAN access points cannot be modified at all without appropriate manufacturing and quality approval.

  The automation layer and access layer can be physically located on the same access switch, however you should consider making each layer distinct by implementing a VLAN through the access switch. The devices on an automation LAN should all be on the same access switch in order to make sure that local automation network traffic does not need to be routed between through the distribution layer.

- **Distribution and Firewall Layer**

  Distribution Switches should be implemented in pairs. Each Distribution Switch in the pair has the exact same Access Switch connections. In this way the Distribution Switches are redundant to each other. If one fails the other assumes the operation. The number of distribution switches will be based on the number of access point switches. Routing is performed in the Distribution Switch and firewall functions should be performed in the Distribution Switch.

Since all routing is performed at the distribution switch, then you should consider the scope of control of each distribution switch in terms of the expected growth of the system.

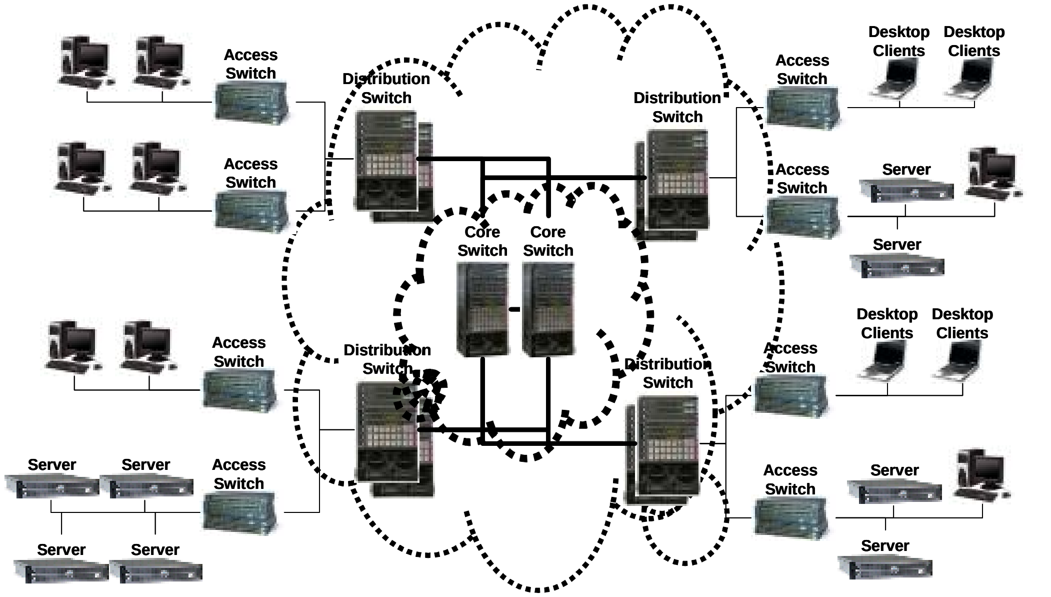
Place each manufacturing sub network that operates independently on a separate distribution switch or placed all of the manufacturing sub networks on a single distribution switch, so that manufacturing network traffic does not have to cross into the core layer. If manufacturing network traffic crosses into the core network, then failures in other systems that affect the core network may impact manufacturing operations. If possible have the Distribution Switch organization match the automation organization (process cell and area), since expected growth in most systems will impact a single process cell or area, or involve the addition of process cells or areas/buildings. Make sure that the business LAN distribution switches are kept physically distinct from the operations LAN distribution switches.

The firewall should be combined with the distribution switches, and generally high-end switches will include this functionality.

- **Core Layer**

  The Distribution Switches connect to Core Switches. There are usually only 2 Core Switches on a campus network, provided for redundancy. The Core Switches consolidate the Distribution Switches. The sole function of the Core Switch is to transfer packets between Distribution Switches as quickly as possible with little or no overhead.

Figure 8 illustrates a typical campus or site wide LAN. There are redundant core switches that only switch traffic between the distribution switches. The distribution switches are high-performance switches that route traffic between access switches and in the case of a manufacturing sub-net provide a firewall between the manufacturing and business LANs.



* Designing Large-Scale LANS – Kevin Dooley – O'Reilly Books
* Also CISCO Net 7 Architecture

Figure 8 - A Layered Network Infrastructure

When the virtual separation is applied to the corporate network, then there are multiple virtual LANs (VLANs) created, each under a separate distribution switch, or a subnet under each switch. This is illustrated in Figure 9. In this case the separate LAN's should correspond to a scope of control of a manufacturing system, either a site or an area within a site.

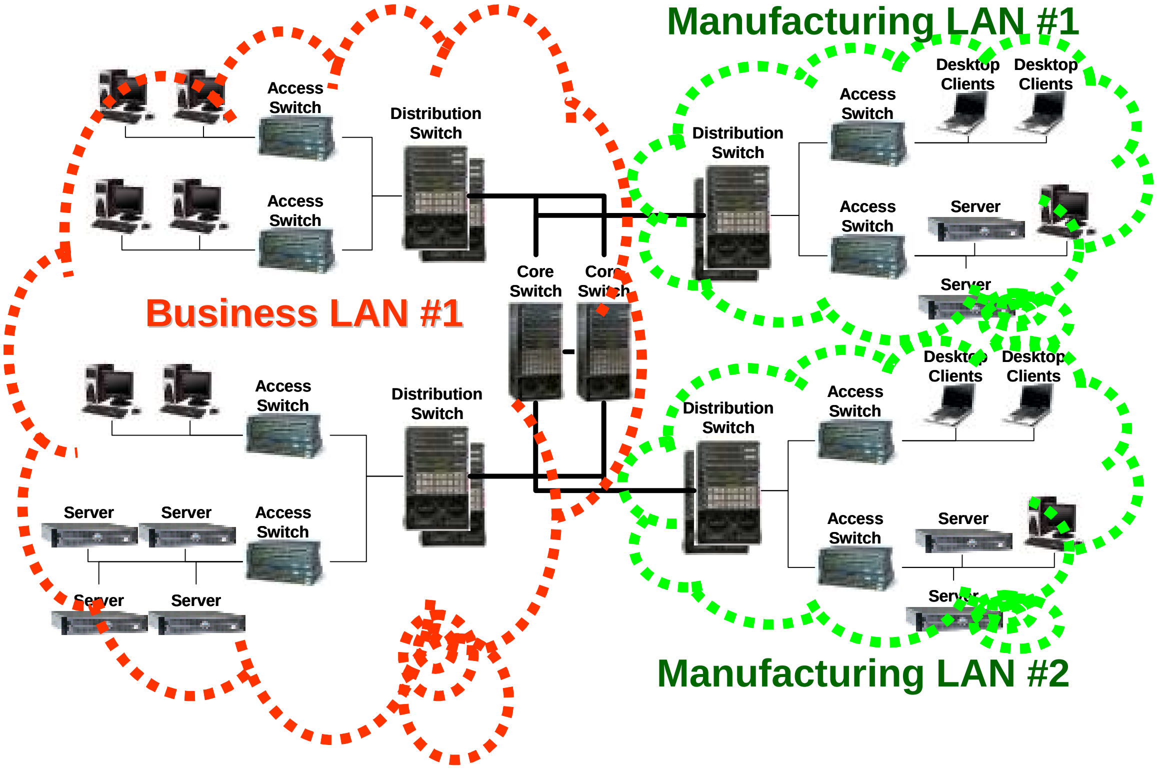
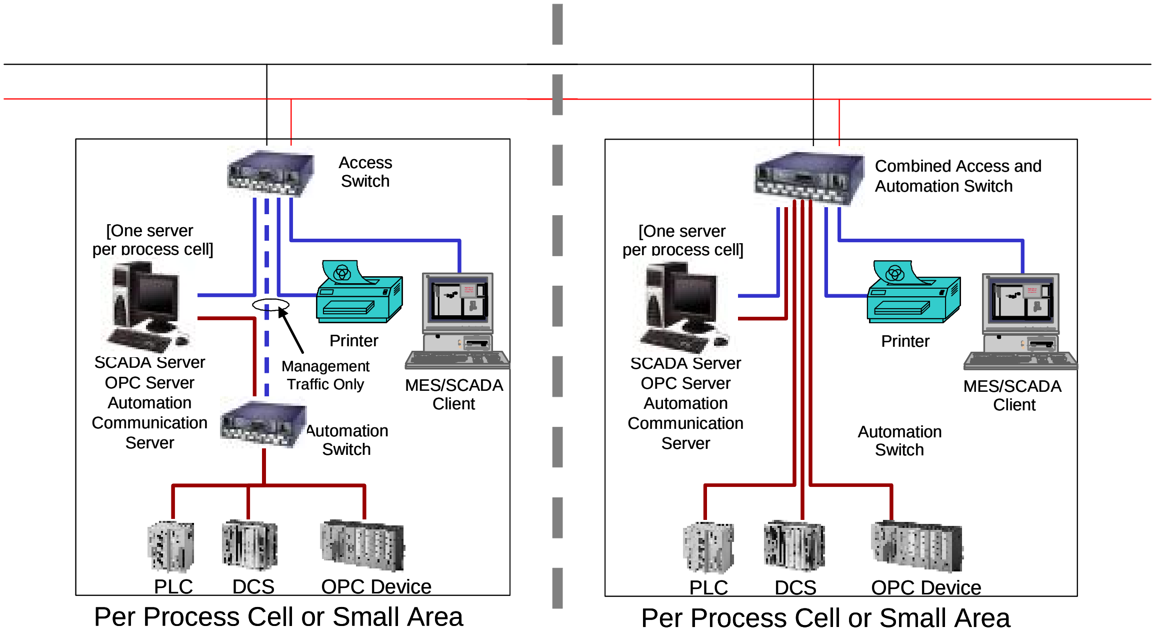


Figure 9 - Virtual Separation of Networks

Automation Layer Considerations

The left side of Figure 10 illustrates the two lowest levels of the network layout, with automation and access switches for a process cell or small area. The right side of Figure 10 illustrates an alternate physical layout that uses a single switch used for the automation layer and access layer with the automation layer as a VLAN. While this provides a measure of protection, all automation and information traffic shares a switch, and failure of the switch may stop critical control traffic.

The SCADA servers should control all communications to the automation layer through a gateway application. This controls the external network traffic allowed in the automation network, ensuring network responsiveness.



Per Process Cell or Small Area

Per Process Cell or Small Area

Figure 10 - Per Process Cell Network Layout

Firewalls

A manufacturing sub-network will often have to sit behind a firewall located in or at the distribution switch. Manufacturing applications are usually validated and can not be easily changed. In some industries this involves significant testing and revalidation if any change is required. Due to this restriction the manufacturing application servers and clients may not be running the latest anti-virus software. Some applications even preclude running anti-virus software, since it interferes with the real-time processing required for the applications. Since we cannot normally execute virus protection on each system, access control to the systems should be strengthened to take up the load. Unprotected control systems are prime targets for infection, and they need multiple layers of protection. We can strengthen the first rule by adding firewalls between the control system networks and the rest of the corporate networks. This can be handled by a firewall at the distribution switch.

Firewalls with limited port access provide an important level of protection. The firewalls should be two-way, in addition to protecting control systems from infection by corporate systems, it must protect corporate systems from the control systems. The purpose of the firewall is to protect both the corporate business systems and the Level 2-3 manufacturing operations systems.

Control at the access control routers can also be added to augment the firewall protection in the distribution switches. Access control routers allow only specified systems on one side to access systems on the other side.

Summary

Applying the ISA 95 models to real manufacturing systems requires a detailed review and design of the supporting IT infrastructure. Fortunately, by extending the standard IT network infrastructure it can meet the requirements for manufacturing applications. The extended infrastructure provides a separation of manufacturing LAN traffic from business LAN traffic, provides a location for a centralized firewall between business servers and clients and manufacturing servers and clients, and provides a special automation level for real-time systems with completely separated traffic. This structure can usually integrate with the corporate IT infrastructure with minimal impact and disruptions. It allows for manufacturing applications and the network to continue operation in the event of loss to the corporate networks, either planned (because or business system shutdowns) or unplanned (because of network failures, virus attacks, or hacker attacks). IT organizations, which must integrate manufacturing applications and networks with business networks can gain value by following the ISA 95 models in their infrastructure design. By applying the concepts of the models to a physical campus wide or corporate wide network they can design network systems that will be safe, secure, and reliable. In addition, the manufacturing systems can easily fit into the corporate infrastructure design and support organizations.