

# THE IMPORTANCE OF REFERENCE ARCHITECTURES IN MANUFACTURING NETWORKS

Brian Batke - Rockwell Automation &  
Paul Didier – Cisco Systems

Presented at the ODVA  
2007 CIP Networks Conference & 12<sup>th</sup> Annual Meeting  
September 18-20, 2007  
Englewood, Colorado USA

## Abstract

EtherNet/IP uses standard IEEE 802.3 and TCP/IP, giving automation and control users flexibility for designing and deploying a network infrastructure. Yet most users are not yet ready to become network design and implementation experts. User application scenarios vary based on physical layout, traffic type, scalability, performance and availability requirements. Other important considerations include reliability, security and management. Reference Architectures provide such design and implementation guidance from both IT and Manufacturing perspectives. Applying Reference Architectures, users can confidently deploy EtherNet/IP networks that successfully address their application challenges and integrate the factory floor with the overall Enterprise infrastructure.

## 1.0 Introduction

EtherNet/IP uses standard networking technologies: Ethernet and the Internet Protocol Suite, including IP, the Transmission Control Protocol (TCP) and others. Although these are well known technologies in an IT department, these are relatively new technologies in the automation and control arena. Combined with the need to integrate data and services from the automation and control space with applications and users in the broader Enterprise network, we see a convergence occurring of the IT and Control networks.

Control networks have been isolated for a very good reason – automation and control applications have very specific requirements that are not typically found in general Enterprise networks. Key concerns include the following:

- Performance—Ability of the network infrastructure to meet the deterministic communications requirements (predictable, real-time performance) of the automation and control systems
- Availability—Both the ability to limit the impact on operations of upgrading or maintaining the network infrastructure, and the reliability of the network infrastructure including features to handle outages with minimal impact
- Manageability—Ease of configuring, maintaining, debugging and fixing the network

IT departments have lots of experience and knowledge of deploying standard networks, but typically not for the Control Network. We suggest that Reference Architecture is an important concept to allow the application of IT experience and knowledge within a Production Control frame of mind to successfully achieve the benefits of applying standard networking technologies to Automation and Control systems.

## 2.0 What is Reference Architecture?

A Reference Architecture is the fundamental organization of a system, the relationships between its components and the environment, and the principles governing its design and evolution. Architectures provide customers with a framework for optimizing their technical resources in support of their business and technical requirements. For example, how do I integrate the Automation and Control data into the Enterprise yet maintain the deterministic qualities of the network? The Ethernet and Internet Protocol suite offer a wide

variety of tools and options to implement a network, not all of which are applicable or needed in an Automation and Control network. A Network Reference Architecture for Automation and Control will provide:

- A framework describing the relationship between components of an Automation and Control network.
- A set of principles to guide the design and implementation of the network infrastructure
- Design and implementation material to guide users in the deployment of standard networking technologies that support EtherNet/IP based systems.

A Reference Architecture should incorporate the knowledge and experience from both the IT and Production Control to outline a solution that optimally applies standard networking technologies that meet the stringent requirements of Automation and Control systems. The Reference Architecture should bring Production and IT together and focus them on one solution that will meet both their different requirements.

### 3.0 Why Reference Architectures

Reference Architectures are going to provide a way to deliver knowledge and expertise in standard networking in an Automation and Control context to increase confidence, spur take-up and drive consistency in the Industrial Ethernet market. In particular, the Reference Architecture is needed because:

- Factory networks have unique considerations from traditional Enterprise IT environments
  - Unique protocols & distinctive use of multicast traffic
  - Determinism and real-time requirements
  - Different Availability, security, and safety considerations
  - Physical requirements – driving unique products & topologies
  - Need to provide & control vendor access
  - Often decision making outside of IT control – different decision makers, different implementers (usually Automation and Control experts) and unique management considerations
- Existing architectural models don't address the unique concerns of the control network
- Significant growth in Ethernet based automation protocols driving the need for specific switching & routing, security, and wireless design guidance for successful and consistent deployments
- A focal point on which vendors and partners can:
  - educate their field, partners and market,
  - provide best practices and guidance that will enable consistent design and implementation standards and
  - direct their solutions and support to provide better service to customers.

### 4.0 Benefits of Reference Architecture

A Reference Architecture helps to ensure that end users and other solution implementers have the tools to confidently deploy the technology. Relevant partners and vendors also have an interest in seeing the end user successfully deploy network technology. A Reference Architecture can provide the following benefits:

- Focus the technology on solving the business issues at hand, in particular addressing the problems and challenges of the factory floor
- All involved parties can increasingly focus on a common solution which
  - Reduces risk of deployment by relying on known and tested solutions
  - Simplifies decision making
  - Enables more re-use
  - Provides consistent models, capabilities, and equipment
  - Helps customers buy solutions to meet their business issues, rather than components and left to put the pieces together themselves
  - Improves service and support by relying on proven solutions and a reference within which to work
- Customers Realize significant cost savings. Often, the underlying technologies have significant cost drivers. In Industrial Ethernet, that includes aspects of standard networking technologies like:
  - reliance on cheaper COTS equipment,
  - reliance on easier to find, re-usable expertise,
  - a platform on which innovation will occur and

- enable safe and secure integration with the broader Enterprise and external network
- Reference Architectures improve on this business case of Industrial Ethernet as customers spend less time, effort and money on implementing the technology.
- Bridge cultural gaps between organizations (e.g. IT and Production) bringing the expertise and knowledge of each together in a way both can agree upon and provides a common model and set of requirements for everyone by working off a single set of design recommendations..
  - Standard network technologies offer investment security through continuous innovation. A Reference Architecture leverages that by designing with future capabilities in mind, so that the system can support new capabilities rather than having to replace and upgrade.

## 5.0 Key Attributes of Reference Architecture

A Reference Architecture for Industrial Ethernet needs to address the unique considerations and challenges of modern production facilities, yet incorporate key common networking characteristics found in Enterprise IT environments. These considerations form the basic set of requirements for the network architecture. Existing architectural models don't address these concerns. Therefore, we have defined a set of key attributes of Industrial Ethernet solution architecture. They include:

- **Compatibility** with the unique industrial protocols (e.g. the Common Industrial Protocol, CIP) and the communication models they incorporate
- Determinism and real-time networking **Performance requirements** of automation and control applications usually defined as latency, jitter and minimal packet loss.
- **Logical Segmentation** that integrates logically (or physically) isolated networks of the production facility with the Enterprise and external networks to safely and securely share data, services and access from the production floor.
- **Physical requirements** of the production floor – driving unique products & topologies
- **Availability** of the automation and control systems and the supporting network has a direct correlation to the operational efficiency of a production facility.
- **Security** is always critical for production facilities and even more so when the integrated network introduces the security risks of the Internet and enterprise network to the control system
- Automation and Control network solutions must be **manageable** by a group of people that are not trained or experts in network technologies or administration.
- **Scalable** to meet the widely varying sizes of production facilities and the growth they may go through.

Each of these features will be discussed in more detail below.

### 5.1 Compatibility

By definition, Industrial Ethernet protocols should operate on standard network technologies and infrastructure if they so specify. But standard networking technologies have a wide range of service and configuration options that need to be considered to effectively support the Automation and Control application. As well, various IE protocols specify various networking features that then must be available to operate at required performance levels.

The network solution architecture needs show compatibility with the IE protocols and communication models of the applications which run upon it. That typically means supporting the types of traffic they generate (e.g. TCP, UDP – multicast and unicast) as well as any features and functions they expect of the network (e.g. Quality of Service).

There are a large number of types of traffic that may exist in an Industrial Ethernet network. They include automation and control protocols (e.g. CIP, Modbus/TCP or OPC) as well as common protocols such as web browsing (HTTP), file transfer (FTP) and many others.

A Reference Architecture will outline how to design and implement network architectures and will be tested to show that relevant Automation and Control applications do work properly.

## 5.2 Determinism/Performance

The automation network must display certain real-time communication qualities in order to meet the needs of the application. Industrial automation applications have historically used fieldbus networks that limit access and provide a defined level of deterministic communications. The familiar real-time characteristics for latency, jitter, and packet loss need to be applied to Ethernet if it is to be successfully deployed in the automation network. Today's modern, full-duplex, switched Ethernet network offers latency, jitter, and (non) packet loss capabilities that equal or surpass the older fieldbus networks it complements.

Latency is defined as the time delay between when the packet is sent and received. For example, typical latency for port to port communications within a single Ethernet switch is less than 50 microseconds depending on packet size. Latency is highly dependent on the amount of traffic, the size of the packets being passed, the configuration of the network infrastructure, the number of switches and the number of devices, as well as a number of other characteristics.

Jitter is defined as the variation in Latency. Lower jitter rates allow real-time systems to deal with latency by taking advantage of time offsets. Even if the user takes into account the network delay, if the network suffers from a high amount of Jitter (variation in delay) then packets will still arrive too late or in some cases too early. When expressed in the network terms, jitter is the spread between the smallest amount of latency and the largest. Jitter value for port to port communications is independent of packet size and runs around 100 nanoseconds.

Packet loss occurs when either the network infrastructure or even the end-device fail to process a sent packet. Packet loss can occur in any network when the devices (e.g. switches and routers) either are too constrained and simply throw-away/drop the packet or errors occur in transmission of the packet that leaves the network infrastructure unable to transmit it further. Packet loss is dealt with to an extent in the TCP protocol, but still can occur. But due to the additional overhead of TCP, many Industrial Ethernet protocols utilize UDP which has no built-in mechanism to deal with packet loss.

A Reference Architecture needs to give guidance on how to achieve the real-time requirements of the network based upon characteristics of the Automation and Control application (e.g. cycle time, request packet interval) and network parameters (e.g. # of Ethernet nodes, # of switches, bandwidth utilization, switch resource utilization).

Key Determinism/Performance considerations include:

- Consider the number of switches and routers and amount of traffic in the Layer 2 network, which affects latency and jitter.
- Ratio of LAN ports to uplink ports based on traffic loads and patterns. Typically this means using 10/100 Mbps to devices and 10/100/1000 Mbps for uplinks
- Application of Quality of Service (QoS) to focus network resources on priority traffic and limit the impact of other network traffic has on the Automation and Control systems
- Network traffic congestion when a link is oversubscribed which may occur more readily in various topologies (e.g. trunk-drop or ring)
- Use of Internet Group Management Protocol to manage the efficient delivery of multicast traffic
- Reduce excessive Rapid Spanning Tree Protocol and other network control traffic to avoid bandwidth flooding of the layer 2 domains.
- Use of the Precision Time Protocol (PTP) as defined in IEEE 1588. This protocol will be utilized in CIP Motion and CIP Sync applications.

## 5.3 Logical Segmentation

Logical Segmentation from the Enterprise network is critical for Industrial Ethernet networks. The devices, systems and applications are sensitive to disturbances and attacks. They have been designed to operate in factory-floor optimized networks where little or no other traffic existed and access was extremely limited. They have limited resources and capacity to deal with the amount and type of traffic found in modern Enterprise or external networks. Yet integrating the data and services they contain is a key priority.

Logical segmentation helps ensure availability, determinism, performance, manageability and security requirements are maintained. Logical segmentation is about preventing extraneous traffic from interfering with

critical communications between devices on the control network. In fact, logical segmentation is a requirement as Industrial Ethernet network architectures may generate traffic that is not readily compatible with general Enterprise traffic and vice versa. A good example of which is multicast traffic in a manufacturing zone may use overlapping multicast addresses as those in the Enterprise zone or traffic in either zone may set Quality of Service markings that create issues in the other zone.

Logical segmentation considerations include:

- Use additional physical or logical De-Militarized Zones (DMZ) to segregate the manufacturing controls network from the corporate IT network, especially to
  - halt the mixing of incompatible traffic
  - create clear administrative boundaries to manage organizational control and configuration differences between the zones
  - safely and securely share data and services between the zones.
- Use tiered layers of switches & routers inside the control network to further segment manufacturing functional areas.
- Limit the number of devices per Layer 2 domain to devices that must talk to each other to maintain more control over performance characteristics and easily develop a more granular security model
- Use Virtual LANs (VLANs) to create logical structure around Layer 2 domains
- Use routers/Layer 3 switches to interconnect VLANs
- Control broadcast, multicast, or unicast storms with port level rate controls where appropriate

## 5.4 Physicality

Physical constraints in the manufacturing industry are significant. The networking systems need to recognize challenges in spatial and environmental conditions. Devices located in the harsh environments, such as the shop floor, often need to meet specifications such as IEC529 (Ingress Protection) or NEMA. The device and control network layers may be located in physically disparate locations (up to miles away) and in non-controlled or even harsh conditions in regards to temperature, humidity, vibration, noise, explosive, electronic interference, etc. This drives the use of ruggedized and hardened network devices.

The physical layout of the manufacturing facility or automation equipment also impacts the network topology in manufacturing automation networks. Unlike traditional IT networks, which are largely redundant star topology networks, manufacturing networks have significant physical limitations, based on factory layout and equipment design, which sometimes drives the use of topologies such as bus and ring. In manufacturing plants with long production lines, or equipment with long runs and interconnected operations (such as a printing press, or similar types of equipment), it is often not feasible or cost effective to use a redundant star topology. Also, many manufacturing applications don't need significant bandwidth at this time, and are therefore not significantly impacted by potential bandwidth limitations of a ring or trunk-drop topology. Ring and especially trunk-drop topologies are at a disadvantage from a convergence, scalability, ease of configuration perspective and eventually may limit the application of new functions. In many cases, the manufacturing network will be a combination of topologies, with large rings connecting multiple star based production cells.

A Reference Architecture must take into consideration the physical challenges of the production facility.

Physical considerations include:

- Choose a topology that meets the performance, cost and spatial requirements of the automation and control application
- When applicable, use non-industrial routers, switches, firewalls where possible to reduce cost.
- Choice of connectivity between nodes in control networks determined by distance, noise, and bandwidth requirements (fiber vs. Cat5/6; wired vs. wireless, etc)
- Layered switches may be required to address density, distance, or communication path challenges.

## 5.5 Availability

Availability of the automation system has a direct correlation to operational efficiency of a production facility. As the network is a key aspect of the overall system, availability requirements translate directly to the network.

It should be noted that limitations in the network technology may also limit the application of high availability features. For example, inability of the network to converge quickly enough and the cost associated with redundant wiring have often led to the non-redundant topologies being implemented in industrial networking environments. A Reference Architecture should outline the capabilities of availability features so as to let customers and integrators make decisions on the level of network availability to build into the overall system.

Availability considerations include:

- Creating alternative data communication paths, regardless of the physical layout. Risk profile/opportunity cost/culture/other variables determine how much and to what level redundant paths are required.
- With critical operations consider eliminating single points of failure, including things such as dual power supplies, second conduit, redundant core manufacturing control network infrastructure - routers/switches, firewalls, etc.
- Use advanced network resiliency and convergence techniques to improve availability of the network: Etherchannel for uplinks, Trunks between redundant systems, 802.1w Rapid Spanning Tree Protocol (RSTP), Hot-Standy routing protocols (e.g. Virtual Router Redundancy Protocol - VRRP), etc.
- A redundant star topology offers the best convergence capabilities. But consider alternative/proprietary ring recovery techniques when configured in a ring topology to meet high-end convergence requirements
- Use of routing configurations and protocols (e.g. OSPF) to maintain routing capability in the case of link or device failure

## 5.6 Security

IP-based networking facilitates interconnection of the control system with the enterprise and thereby the external network. Many industries have implemented enterprise applications for more efficient production, and Internet business applications in order to communicate more efficiently with their suppliers, customers, and business partners. Internet-based enterprise resource planning (ERP) and supply chain management (SCM) systems simplify connections both to other organizations and to internal business processes. These connections can enable greater efficiencies in processes and manufacturing. In large manufacturing or utility operations, small percentage increases in efficiency can translate into significant cost savings.

However, connecting the control network to the enterprise LAN brings all of the security risks of the Internet to the control system. Mitigating these risks is more difficult and more imperative than in the Enterprise network because of the higher requirement for availability in a control system. Of the three security properties of confidentiality, integrity, and availability, control systems are first and foremost concerned with availability. Many of the physical processes that they control cannot be stopped or interrupted without serious physical or financial damage. On the other hand, in enterprise networks that are the primary design consideration for IP, confidentiality and integrity are the primary design considerations. It is preferable for an e-commerce server to be temporarily unavailable than for it to lose transactions or divulge credit card numbers. Consequently, network architectures, firewall configurations, IDS configurations, etc. for enterprise networks are not quite appropriate for control systems. The control systems industry has been struggling for several years to determine how to build secure, reliable control systems based on IP.

Any Industrial Ethernet Reference Architecture must have a broad and complete perspective on how to apply network security. Standards bodies such as ISA SP99 are still debating security design axioms but there is at least some rough consensus on what a secure industrial architecture should provide. This includes a control network that is highly available and redundant, has fast convergence (meaning reconfiguration and restoration of network services after a disruption), is deterministic and thus suitable for real-time control, and is secure against both outside and inside threats.

Key Security considerations include:

- Control data flows between control and enterprise/external networks via a De-Militarized Zone that applies Access Control Lists, Firewalls, Intrusion Protection Systems, VLANs, etc.
- Not allowing any direct communication between control or manufacturing systems and enterprise systems
- Restrict real time production traffic to the manufacturing control network
- Restrict enterprise access to mirror/replicated versions of production data to DMZ
- Authenticate and authorize user access based on level within manufacturing network and role (read/read-write/local/remote/vendor/partner)
- Control rogue access inside manufacturing (port level MAC address controls, administratively shutdown unused ports, etc)
- Control what devices can be plugged to the IE switch (e.g. port security, DHCP snooping)
- Detect and mitigate malicious traffic originated from infected devices that are plugged into the control network
- Detect and mitigate malicious traffic originated from the corporate IT network
- Secure connectivity for remote access to automation devices
- DMZ design options based on costs and levels of security and redundancy required
- Limit rogue network communication activity from impacting networking devices (set root bridge, SNMP capabilities, etc)
- Document and define policy and risk appropriate for the environment

## 5.7 Scalability

Factory systems come in a wide range of sizes, from the small OEM solutions to the extremely large factory complexes (e.g. an automotive plant), the factory automation and control system may include only a small number of devices to multiple 10,000s of devices. Additionally, scalability should also consider adding additional features and capabilities to the automation and control systems. The Reference Architecture concepts and recommendations must recognize the assortment in sizes and identify how.

Key scalability considerations include:

- Network Infrastructure sizing and performance constraints
- Network infrastructure tiering to meet spatial, size and performance criteria
- Link aggregation to achieve higher bandwidth requirement
- IP Addressing schema and allocation mechanism
- Maintenance and management considerations as manual tasks have greater impact in large environments

## 5.8 Manageability

Manageability is a key consideration for automation and control systems. First, those typically responsible for managing and operating a production floor may not have training and knowledge in standard networking, as would typically be found in an IT support organization. As well, they usually deploy a different set of tools and applications to manage the operations.

Key manageability concerns include:

- Make installation and configuration of switches as simple as possible. Apply menu driven (e.g. wizard), pre-configured switches and where possible enable basic configuration via existing Automation and Control applications (requires network infrastructure compatible with the relevant protocols). When specific configuration is required easy to understand and navigate GUI-based applications should be used. Use of command-line interfaces which require detailed knowledge of the switch should be avoided and reserved to network experts.
- Leverage existing SNMP based management systems when and where they make sense. Often these do need tailoring for the production users.
- The network devices such as routers and security appliances should utilize similar functionality and applications for configuration

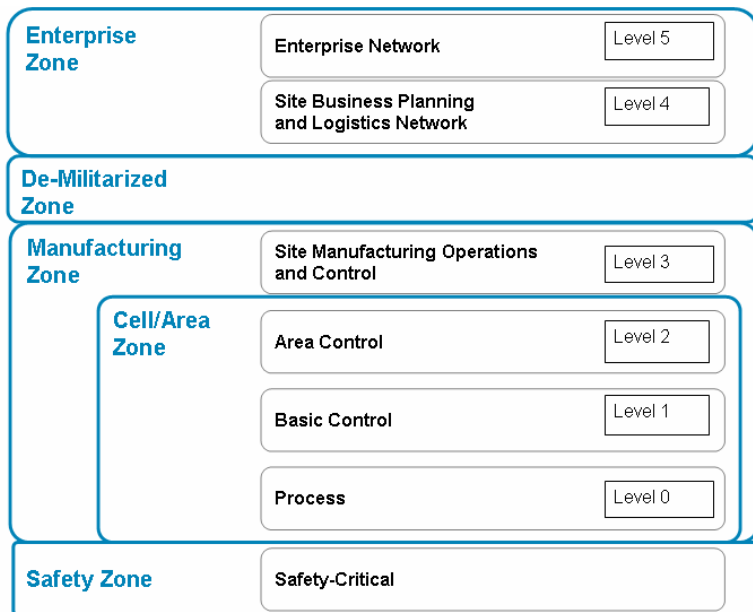
- Use pre-assigned port configurations (e.g. SmartPort templates) for easy port configuration based on application or device types
- Assign consistent IP addresses to devices as these are often coded into the logic and configurations various automation and control devices
- Consider different zero touch replacement options for network elements
- Utilize systems that offer notification of control network event (e.g. an Ethernet link goes up or down) via control protocols (e.g. CIP)
- Stage and test software upgrades for network devices
- Allow for patch management of Windows-based automation devices
- Standardize hardware and software elements where ever possible

## 6.0 Reference Model for the Network

What is needed now is a framework in which to refer the requirements, components, attributes and consideration of the Industrial Ethernet network. A framework should be meaningful to the production environment. A framework should adequately and simply describes the key aspects of the Automation and Control systems. The framework will be used to structure how to provide network services to the devices and equipment found on a factory floor and integrate those into the wider enterprise network.

As noted above, the production facility often has different networking requirements than a typical IT network. The key components they require are deterministic and highly available network services. Those requirements are typically achieved through segregation and domains of control. Segregating the control network from other control networks and the enterprise eases achieving these goals.

We therefore put forward the following framework for structuring an Automation and Control Industrial Ethernet network. The framework reflects an existing framework that identifies the levels of a control network, the Purdue Model for Control Hierarchy (reference ISBN 1-55617-265-6). This model is commonly referred to in the industry. The framework incorporates these levels.



Additionally, we define five zones as relevant to Automation and Control networks. The zones include:

- The enterprise zone is typically defined as the site (plant) and enterprise IT environments, and includes corporate data centers, general access local area networks (LAN) and wide area networks (WAN), email systems, business applications, etc.
- The De-militarized Zone provides a buffer zone where data and services can be safely and securely shared between the enterprise and manufacturing zones,

- The manufacturing zone consists of the different “cells/areas” within a specific production facility and the application, systems, and services required for ongoing manufacturing operations. There may be multiple manufacturing zones in any enterprise.
- The cell/area zone, a subzone within the manufacturing zone, typically consists of systems that need to interoperate and communicate on a frequent or real-time basis. A cell/area zone may consist of multiple PLCs, robotic devices, and the human-machine interfaces (HMIs; either stand-alone or distributed) associated with related or interdependent steps in the manufacturing process. There are typically multiple cell/area zones within a manufacturing zone.
- The safety zone is where safety devices and applications exist. These are the systems that shut-down areas of the production facility when safety is breached to protect the personnel and machines from harm and damage.

This Framework can be used to:

- Describe key Industrial Ethernet network design considerations
- Focus components and technologies to particular areas or functions of the production floor
- Deliver Design and Implementation guidance for those deploying Industrial Ethernet networks
- Describe organizational and administrative control and management between IT and Production
- Provide training and knowledge in a production control context for both IT and production personnel

## 7.0 Establishing the Reference Architecture

Establishing a Reference Architecture is similar to a project to deploy an Industrial Ethernet solution. The process includes a set of activities; requirements definition, design, implementation and test. The deliverables of each of these activities can be used by customers and implementers in their own projects to deploy Industrial Ethernet. Vendors can enhance the base solution with additional features and technology.

### 7.1 Requirements Definition

Requirements definition establishes the key features and attributes to be provided by the reference architecture. Requirements information gives customers a set of primary considerations they can use before embarking on an Industrial Ethernet solution. The reference architecture requirements also provide a benchmark for what can be supported.

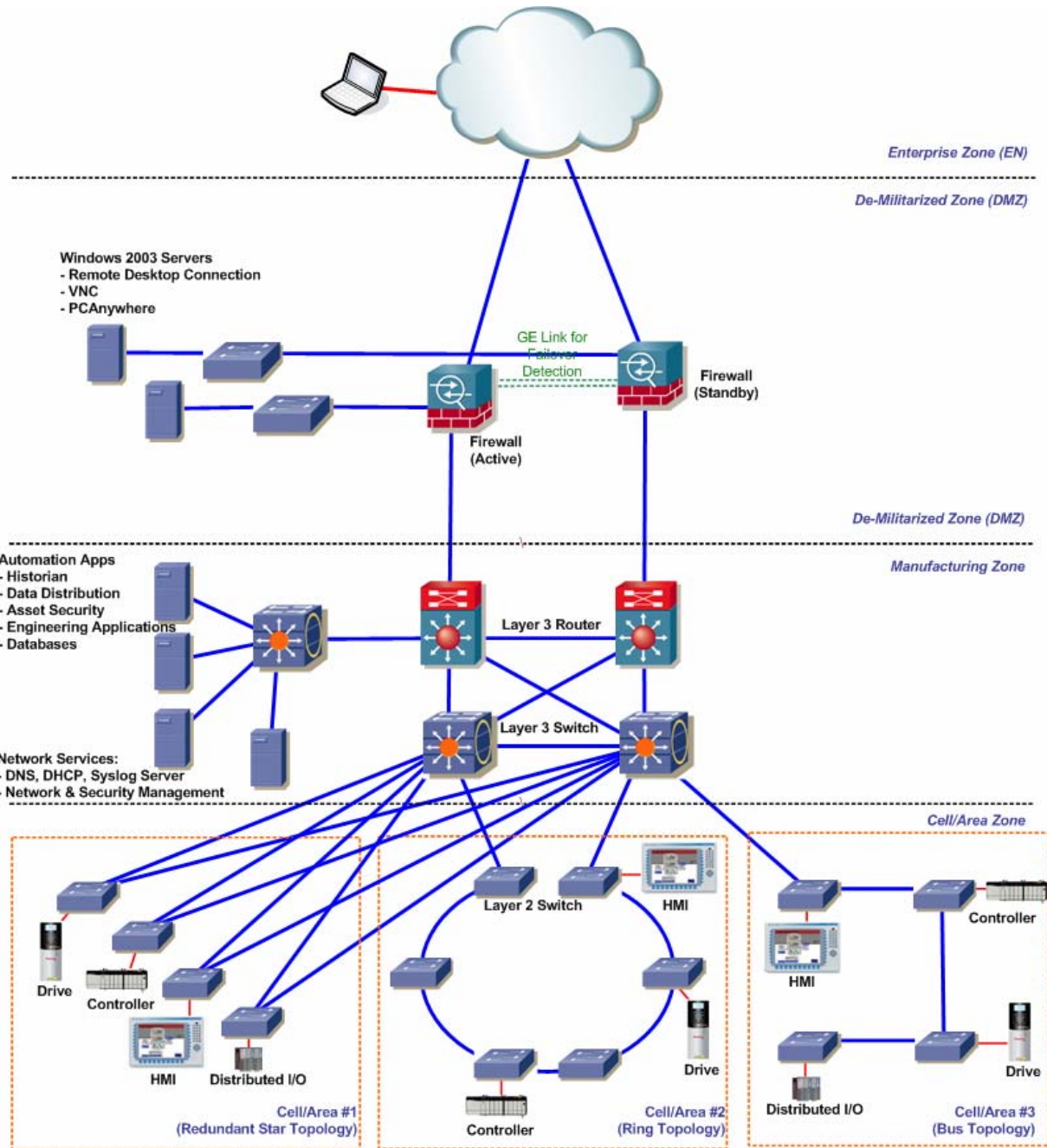
See section 4.0 for a list of key reference architecture attributes.

### 7.2 Design

In the design phase, detailed designs are created for the Solution Architecture. This includes such topics as:

- Specify detailed requirements of the network – what needs to be interconnected and what are the key service criteria (latency, jitter, packet loss sensitivity)
- Identify Components (Hardware and Software) used in the solution
- Identify Topologies required to support the solution
- Develop use cases and Traffic flow diagrams to describe network traffic patterns
- Identify segmentation requirements (e.g. subnets, VLANs and zones)
- Outline required network services (e.g. QoS, Multicast management, Spanning Tree etc.)
- Develop Security designs
- Develop High Availability designs

Design documents for the reference architecture will provide key considerations and recommendations for customer implementations. Below is an example network design on which testing can be conducted



### 7.3 Implementation

The implementation aspect will deliver specific guidance on how to deploy and configure the solution architecture to meet the specific application needs. The key implementation steps are installing and configuring the equipment.

- Configuration recommendations and guidance
- Example configuration scripts
- Screen shots and training material for key configuration applications

## 7.4 Test

To verify the design and implementation, a variety of tests are performed on the network architecture to verify the attributes are maintained and to provide valuable feedback and insight to those looking to implement the Reference Architecture.

Test cases and relevant results include:

- Performance results (latency, jitter and dropped packets) under a variety of conditions
- Fault testing including network convergence under a variety of conditions to display network availability characteristics
- Function and Usability testing to validate support for automation and control systems
- Security testing to verify that specific risks/threats are repelled

## 8.0 Conclusions

Reference architectures for Industrial Ethernet enables both vendors and end users to more easily and more successfully deploy network installations in the industrial automation environment.

Proven reference architectures can:

- Provide common models for talking about the problem and solution, facilitating communication between users and vendors, IT and Control Engineering.
- Increase confidence relying on proven and tested concepts and designs
- Identify the key features and attributes that are most critical to a successful network installation.
- Help bound the solution space, allowing users to better navigate the many possibilities and options in deploying a network infrastructure.
- Give important design tradeoffs and recommendations, in particular as they apply to the unique needs of industrial automation applications.

The ultimate value in reference architecture is the savings in time and resources – for both end users and vendors – by applying proven guidelines and solutions. Ease of network deployment then leads to increase adoption overall for Industrial Ethernet.

---

DeviceNet, DeviceNet Safety, CIP, CIP Motion, CompoNet, CIP Safety and CIP Sync are trademarks of ODVA. EtherNet/IP is a trademark of ControlNet International under license by ODVA. Other trademarks are property of their respective owners.

The ideas, opinions and recommendations expressed herein are intended to describe concepts of the author(s) for the possible use of CIP Networks and do not reflect the ideas, opinions, and recommendation of ODVA per se. Because CIP Networks may be applied in many diverse situations and in conjunction with products and systems from multiple vendors, the reader and those responsible for specifying CIP Networks must determine for themselves its suitability and the suitability of ideas, opinions, and recommendations expressed herein for intended use.

Copyright ©2007 Open DeviceNet Vendor Association, Inc. (ODVA). All rights reserved.  
For permission to reproduce excerpts of this material, with appropriate attribution to the author(s), please contact ODVA on:

TEL +1 734-975-8840  
FAX +1 734-922-0027  
EMAIL [odva@odva.org](mailto:odva@odva.org)  
WEB [www.odva.org](http://www.odva.org)