APPENDIX A

Key Terms and Definitions

This appendix lists and defines the key terms used in this document.

AAA
Authentication, authorization, and accounting. Pronounced "triple a." For more on Authentication Protocols, see: http://www.cisco.com/en/US/tech/tk59/tsd_technology_support_protocol_home.html
ACL
Access Control Lists are used for purposes filtering IP traffic generally for security reasons. For more on ACLs, see IP Addressing Services – Access Lists: http://www.cisco.com/en/US/tech/tk648/tk361/tk821/tsd_technology_support_sub-protocol_home.html
Active Directory
Microsoft's application that delivers LDAP and other AAA services.
Cell/Area Zone
A logical section or subset (physical, geographical or function) of the production facility. It typically contains Level 0-2 devices (see Automation and Control Reference Model).
CIP Common Industrial Protocol
The Common Industrial Protocol (CIP™) encompasses a comprehensive suite of messages and services for the collection of manufacturing automation applications—control, safety, synchronization, motion, configuration and information. CIP is owned and maintained by the Open Device Vendor Association. The ODVA is an international association comprising members from the world's leading automation companies.
Control Plane
Control plane refers to network protocol traffic (e.g. routing, resiliency) that usually passes between network infrastructure devices to maintain the network's functions. Examples of control plane traffic include Spanning Tree and EIGRP.
CSMA/CD
Carrier sense multiple access collision detect. Media-access mechanism wherein devices ready to transmit data first check the channel for a carrier. If no carrier is sensed for a specific period of time, a device can transmit. If two devices transmit at once, a collision occurs and is detected by all colliding devices. This collision subsequently delays retransmissions from those devices for some random length of time. Ethernet and IEEE 802.3 use CSMA/CD access.

Data Plane

Data plane refers to the application data the network switches and routes being sent to and from end-devices. CIP is considered data plane traffic.

DHCP

Dynamic Host Configuration Protocol. Provides a mechanism for allocating IP addresses dynamically so that addresses can be reused when hosts no longer need them.

Determinism

A property of an overall automation and control system that behaves determined only by initial state and input. Many factors impact the deterministic nature of a system, including network performance. For the purposes of this document, we will consider the network low latency, minimal jitter and minimal packet loss as the key network criteria that impact the deterministic nature of the overall automation and control system.

DMZ, Demilitarized Zone

Refers to a buffer or network segment between two network zones. A DMZ is commonly found between a corporate network and the internet where data and services can be shared/accessed from users in either the internet or corporate networks. A DMZ is typically established with network firewalls to manage and secure the traffic from either zone.

For an example of a network DMZ, see Scenario: DMZ Configuration: http://www.cisco.com/en/US/docs/security/pix/pix72/quick/guide/dmz_p.html

DNS

Domain Name System. System used on the Internet for translating names of network nodes into IP addresses.

Ethernet

Baseband LAN specification invented by Xerox Corporation and developed jointly by Xerox, Intel, and Digital Equipment Corporation. Ethernet networks use CSMA/CD and run over a variety of cable types and speeds. Ethernet is a family of frame-based networking technologies or standards (IEEE 802.3) for local area networks. It defines standards for common addressing format and the physical and data link (or Media Access Control) layers of the OSI Model.

See the IEEE 802.3 working group's site (http://www.ieee802.org/3/) for more details on the set of standards.

For more on Ethernet, see Ethernet – Introduction: http://www.cisco.com/en/US/tech/tk389/tk214/tsd_technology_support_protocol_home.html & Internetworking Technology Handbook-Ethernet: http://www.cisco.com/en/US/docs/internetworking/technology/handbook/Ethernet.html

IKE

Internet Key Exchange. IKE establishes a shared security policy and authenticates keys for services (such as IPSec) that require keys. Before any IPSec traffic can be passed, each router/firewall/host must verify the identity of its peer. This can be done by manually entering pre-shared keys into both hosts or by a CA service.

Industrial Automation and Control Systems (IACS)

Refers to the set of devices and applications used to automate and control the relevant manufacturing process. Rather than use various terms with a similar meaning (e.g., production systems, factory floor systems, we standardized on this term for use in this paper). That is not to suggest any specific focus or limitations. We intend that the ideas and concepts outline herein are applicable in various types of manufacturing including but not limited to batch, continuous, discrete, hybrid and process. Other documents and industry references may refer to Industrial Control Systems (ICS). For the purpose of this document, those terms are interchangeable. This document simply choose to use IACS, as reflected in the ISA 99 standards.

IP

Internet Protocol. Network layer protocol in the TCP/IP stack offering a connectionless internetwork service. IP provides features for addressing, type-of-service specification, fragmentation and reassembly, and security. Defined in RFC 791.

For more on IP, TCP and UDP, see Internetworking Technology Handbook-Internet Protocols: http://www.cisco.com/en/US/docs/internetworking/technology/handbook/Internet-Protocols.html

IP Protocol Suite

Is a set of networking standards on which the internet and most enterprise networking is based. It includes the Layer 3 Internet Protocol (IP), the Layer-4 Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).

IPS

Intrusion Prevention Systems is a network security device that monitors network activity for malicious or unwanted behavior.

See more on Intrusion Prevention Systems at widpedia: http://en.wikipedia.org/wiki/Intrusion-prevention_system or Cisco IPS: http://www.cisco.com/en/US/products/sw/secursw/ps2113/index.html

IPSec

IP Security. A framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPSec provides these security services at the IP layer. IPSec uses IKE (See above) to handle the negotiation of protocols and algorithms based on local policy and to generate the encryption and authentication keys to be used by IPSec. IPSec can protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.

For a more in-depth understanding of IPsec, see the following URL: http://www.cisco.com/en/US/tech/tk583/tk372/technologies_tech_note09186a0080094203.shtml.

ISA-99

ISA-99 focuses on security for industrial automation and control systems, For more, see http://www.isa.org/MSTemplate.cfm?MicrositeID=988&CommitteeID=6821

ISA-95

The standard for the integration of enterprise and control systems, see http://www.isa.org/Template.cfm?Section=Find_Standards&Template=/Customsource/ISA/Standards/TaggedStandardsCommittee.cfm&id=2360

Jitter

Refers to the variation in Latency (see definition below). Jitter is important as often larger variations in the delay due to communications can negatively impact the 'deterministic' nature of the relevant system.

Latency

Refers to the delay in communications due to processing and transmission media (Switches, Routers and cables) between any two end-devices. Latency could also refer to the processing time in an application to process a message.

Layer

Generally refers to layers of the OSI Model which logically describe the functions that make up networked communications (see Chapter 1, Figure 8).

Level

Refers to levels of the Automation and Control Reference Model (see Chapter2) that describe functions and domains of control within manufacturing organizations. This Model is based upon the Purdue Control Hierarchy model and is used in a variety of Industrial standards (e.g. ISA 95 and 99).

LDAP

Lightweight Directory Access Protocol. Protocol that provides access for management and browser applications that provide read/write interactive access to an X.500 compliant directory service. X.500 specifies a standard for distributed maintenance of files and directories.

Manufacturing Zone

The Manufacturing zone is a network zone in the Automation and Control Reference Model (see Chapter 2) The zone contains the complete set of applications, systems, infrastructure and devices that are critical to the continued operations of the plant.

In other documentation (for example ISA 99), this zone may also be referred to as the Control zone. The terms are interchangeable in this regard.

NAC

Lightweight Directory Access Protocol. Protocol that provides access for management and browser applications that provide read/write interactive access to an X.500 compliant directory service. X.500 specifies a standard for distributed maintenance of files and directories.

NAC

Network Access Control is a security approach that allows only compliant and trusted endpoint devices, such as PCs, servers, and PDAs, onto the network, restricting the access of noncompliant devices, and thereby limiting the potential damage from emerging security threats and risks.

For more on Network Admission Control, see:
http://www.cisco.com/en/US/netsol/ns466/networking_solutions_package.html

NAT Network Address Translation

Network Address Translation is a mechanism for reducing the need for globally unique IP addresses. NAT allows an organization with addresses that are not globally unique to connect to the Internet by translating those addresses into globally routable address space.

Network Convergence

The period of time the network requires to restore normal network traffic handling after an outage or event. For our testing and test results, convergence time is measured using the following formula:

Convergence in milliseconds = [(Tx - Rx) / packet rate] * 1000 ms/s

Where:

Tx = Packets transmitted

Rx = Packets received

Packet rate tested = 10,000 packets per second

ODVA Open Device Vendors Association

ODVA is an international association comprising members from the world's leading automation companies. Collectively, ODVA and its members support network technologies based on the Common Industrial Protocol (CIP™). These currently include DeviceNet™, EtherNet/IP™, CompoNet™, and ControlNet™, along with the major extensions to CIP — CIP Safety™ and CIP Motion™. ODVA manages the development of these open technologies, and assists manufacturers and users of CIP Networks through its activities in standards development, certification, vendor education and industry awareness. Both Rockwell Automation and Cisco are members of the ODVA.

OSI Model

The Open Systems Interconnection model is a Network architectural model consisting of seven layers, each of which specifies particular network functions, such as addressing, flow control, error control, encapsulation, and reliable message transfer. The lowest layer (the physical layer) is closest to the media technology. The lower two layers are implemented in hardware and software whereas the upper five layers are implemented only in software. The highest layer (the application layer) is closest to the user. The OSI reference model is used universally as a method for teaching and understanding network functionality

The term layer in this document generally refers to a layer or layers of the OSI Model.

See Chapter 1, Figure 8 for a diagram of the OSI Model.

Plant

Plant, Production Facility, Factory or Factory Floor—This document chose to use the term *plant* as a keyword to describe the area in which the manufacturing process and control takes place. This is not to exclude similar words such as factory, production facility, or any other term used to refer to the area in which the manufacturing process exists. In fact, they can be used interchangeably, but for the purpose of consistency, we chose to use Plant.

Port

A port can refer to two things in networking.

1. Physical Interface on an internetworking device (such as a router).

2. In IP terminology, an upper-layer process that receives information from lower layers. Port is an application-specific or process-specific software construct serving as a communications endpoint used by Transport Layer protocols of the Internet Protocol Suite such as Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). Ports are numbered (a port number), and each numbered port is associated with a specific process. For example, SMTP is associated with port 25. A port number is also called a well-known address. For a list of official port numbers see *The Internet Assigned Numbers Authority (IANA)* at the following URL: http://www.iana.org/assignments/port-numbers.

For the purpose of this document, port refers to the second meaning.

RADIUS

Remote Authentication Dial In User Service (RADIUS) is a networking protocol that provides centralized access, authorization and accounting management for pe.ople or computers to connect and use a network service. When a person or device connects to a network often “RADIUS” authentication is required.

Remote Terminal Session

Remote Terminal Session of Remote Desktop refers to a set of protocols and software that enable one computer or user to remotely access and control another computer through graphical Terminal Emulation. Software that makes it appear to a remote host as a directly attached terminal, including Microsoft’s RDP, Remote Desktop Protocol and VNC Virtual Network Computing.

SSL

Secure Socket Layer. Encryption technology for the Web used to provide secure transactions, such as the transmission of credit card numbers for e-commerce.

Subnet or Subnetwork

In IP networks, a subnet is a network sharing a particular subnet address. Subnetworks are networks arbitrarily segmented by a network administrator in order to provide a multilevel, hierarchical routing structure while shielding the subnetwork from the addressing complexity of attached networks.

TCP

Transmission Control Protocol. Connection-oriented transport layer protocol that provides reliable full-duplex data transmission. TCP is part of the TCP/IP protocol stack.

For more on IP, TCP and UDP, see *Internetworking Technology Handbook-Internet Protocols*:
http://www.cisco.com/en/US/docs/internetworking/technology/handbook/Internet-Protocols.html

UDP

User Datagram Protocol. Connectionless transport layer protocol in the TCP/IP protocol stack. UDP is a simple protocol that exchanges datagrams without acknowledgments or guaranteed delivery, requiring that error processing and retransmission be handled by the application or other protocols. UDP is defined in RFC 768.

For more on IP, TCP and UDP, see
http://www.cisco.com/en/US/docs/internetworking/technology/handbook/Internet-Protocols.htm

VLAN

virtual LAN. Group of devices on one or more LANs that are configured (using management software) so that they can communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible.

For more on VLANs, see *Internetworking Technology Handbook-Lan Switching*
http://www.cisco.com/en/US/docs/internetworking/technology/handbook/LAN-Switching.html

VPN

Virtual Private Network. Enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses "tunneling" to encrypt all information at the IP level.

For more on VPNs, see "*How VPNs work*":
http://www.cisco.com/en/US/tech/tk583/tk372/technologies_tech_note09186a0080094865.shtml or *"IPSec VPN WAN Design Overview"*
http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/IPSec_Over.html#wp1006588

WINS

Windows Internet Naming Service. Microsoft's NetBIOS name translation service, analogous to DNS.