PANDUIT®

Rockwell Automation

CONFIDENTIAL DOCUMENT

ETHERNET LOGICAL & PHYSICAL NETWORK DESIGN

Prepared for

Customer Inc

RA Document 800445064-IND
Project Number 800445064
March 19, 2020
Version 1 Revision 0

infrastructure for a connected world

LISTEN. THINK. SOLVE.℠

CONTENTS

FIGURES

TABLES

1 DOCUMENT CONTROL

1.1 Document Approval

Table 1.1 – Document Approval

Date	Company	Name - Title	Initials
03/19/2020	Rockwell Automation	Isaac Nuse Donkor – Network & Security Consultant	IND

Document Approval – Rockwell Automation	
Printed Name	**Isaac Nuse Donkor**
Signature	
Date	
Document Approval – Customer inc	
Printed Name	
Signature	
Date	

1.2 Revision History

Table 1.2 – Revision History

Date	Version	Description	Author
03/19/2020	v1r0	Initial Draft	IND

1.3 Design Documentation

Table 1.3 - Design Documentation

Date	Version	Description	Author
03/19/2020	v1r0	Customer's Network Design Report (this document)	Rockwell Automation

Date	Version	Description	Author
03/17/2020	v1r0	Customer's Network Design	Rockwell Automation
03/03/2020	v1r0	Customer's Network Port-Maps-1	Rockwell Automation
03/03/2020	v1r0	Customer's Network Port-Maps-2	Rockwell Automation
03/03/2020	v1r1	Customer's Vlans and Subnets	Rockwell Automation
03/10/2020	v1r0	Customer's Network BOM	Rockwell Automation

1.4 Reference Documentation

Table 1.4 – Reference Documentation

Resource	Description	Author
Cisco / Rockwell Automation Converged Plant-wide Ethernet (CPwE) Design and Implementation Guide Publication **ENET-TD001**	This publication describes the design and implementation guidelines of a Converged Plant-wide Ethernet Network for Industrial Ethernet Applications.	Cisco Systems & Rockwell Automation
Deploying a Resilient Converged Plant-wide Ethernet Architecture Publication **ENET-TD010**	This publication details design considerations, best practices and implementation considerations to help with successfully designing and deploying a holistic resilient plant-wide network architecture; made up of multiple technologies (logical and physical) deployed at different levels within the plant.	Cisco Systems & Rockwell Automation
EtherNet/IP Media Planning and Installation Manual Publication **PUB00148RO**	This publication by the ODVA describes the required media components and how to plan for, verify, troubleshoot and certify EtherNet/IP networks.	ODVA
Guidance for Selecting Cables for EtherNet/IP Networks Publication **ENET-WP007**	This publication provides guidance to the user on selecting cabling based on the application, environmental conditions, and mechanical requirements.	Rockwell Automation
Fiber Optic Infrastructure Application Guide Publication **ENET-TD003**	This publication details methods for deploying a fiber optic physical infrastructure to support the Converged Plant-wide Ethernet Network.	Panduit, Cisco Systems & Rockwell Automation
Industrial Ethernet Physical Infrastructure Reference Architecture Design Guide Publication **PANDUIT / Physical Infrastructure Reference Architecture Guide**	This publication provides guidance for designing, deploying and managing the physical infrastructure for an Industrial Ethernet network following the Converged Plant-wide Ethernet Network.	Panduit, Cisco Systems & Rockwell Automation
Ethernet Design Considerations Reference Manual Publication ENET-RM002	This publication provides an overview of Ethernet concepts including; network layout and components, network infrastructure devices, network infrastructure features, and protocols.	Rockwell Automation

Resource	Description	Author
Deploying Industrial Data Center within a Converged Plantwide Ethernet Architecture Design Guide Publication ENET-TD014	This publication outlines key requirements and application considerations to help with the integration of the Industrial Data Center (IDC) product within a CPwE architecture. It describes the IDC and validates some potential use cases.	Panduit, Cisco Systems & Rockwell Automation
OEM Networking within a Converged Plantwide Ethernet Architecture Design Guide Publication ENET-TD018	This publication outlines key requirements and design considerations to help with the successful design and deployment of managed industrial Ethernet switches (IES) in the Cell/Area Zone and sub-zones for connecting Industrial Automation and Control Systems (IACS) devices.	Cisco Systems & Rockwell Automation

1.5 Disclaimer

All information contained herein is provided without any warranty, expressed or implied, as to the accuracy or relevance of such information to the Customer Inc-Customer inc environment. This information is to be considered as preliminary and informative, and is subject to review and revision at any time by Customer inc or Rockwell Automation. This document further includes information that may be proprietary, confidential, or otherwise sensitive from both Customer inc and Rockwell Automation. Prior to any dissemination outside of Customer inc or Rockwell Automation of any part or whole of this document, the associated companies must agree in writing. The information contained herein may be considered volatile and preliminary, subject to revision, addition, or removal.

Unlike standard Rockwell Automation CPwE network design deliverables, some information contained within this document intentionally deviates from current Cisco Validated Design (CVD) hardware. This does not infer that the recommended hardware within this design lacks the ability to meet the specification requirements or is not suited for the designed purpose. The specified hardware is currently undergoing testing for addition to the Cisco CVD program for OT (Operational Technology) environments. Creation of the hardware specification in this document included consultation with Rockwell and Cisco, and at the request of, the end-user for the Customer inc IACS network design project. Rockwell Automation assumes no liability for the hardware not meeting design requirements, including items unforeseen such as network convergence times, interoperability with current network infrastructure, lack of product offering, product changes, etc. due to the selection of the non-CVD OT network hardware.

2 BACKGROUND AND OVERVIEW

2.1 Executive Summary

Customer Inc has approved Rockwell Automation to design an Industrial Automation and Control System Ethernet Network for the Buildings B2/W2 & B3/W3, production sites in Austin, TX. The goal of this network design will be to provide a future ready, stable and robust process control network to allow for reliable operation over the lifespan of the network.

This report provides comprehensive documentation of the proposed Ethernet Network Architecture. Figure 2.1 illustrates the phases that will be required to implement the new Control System Network.

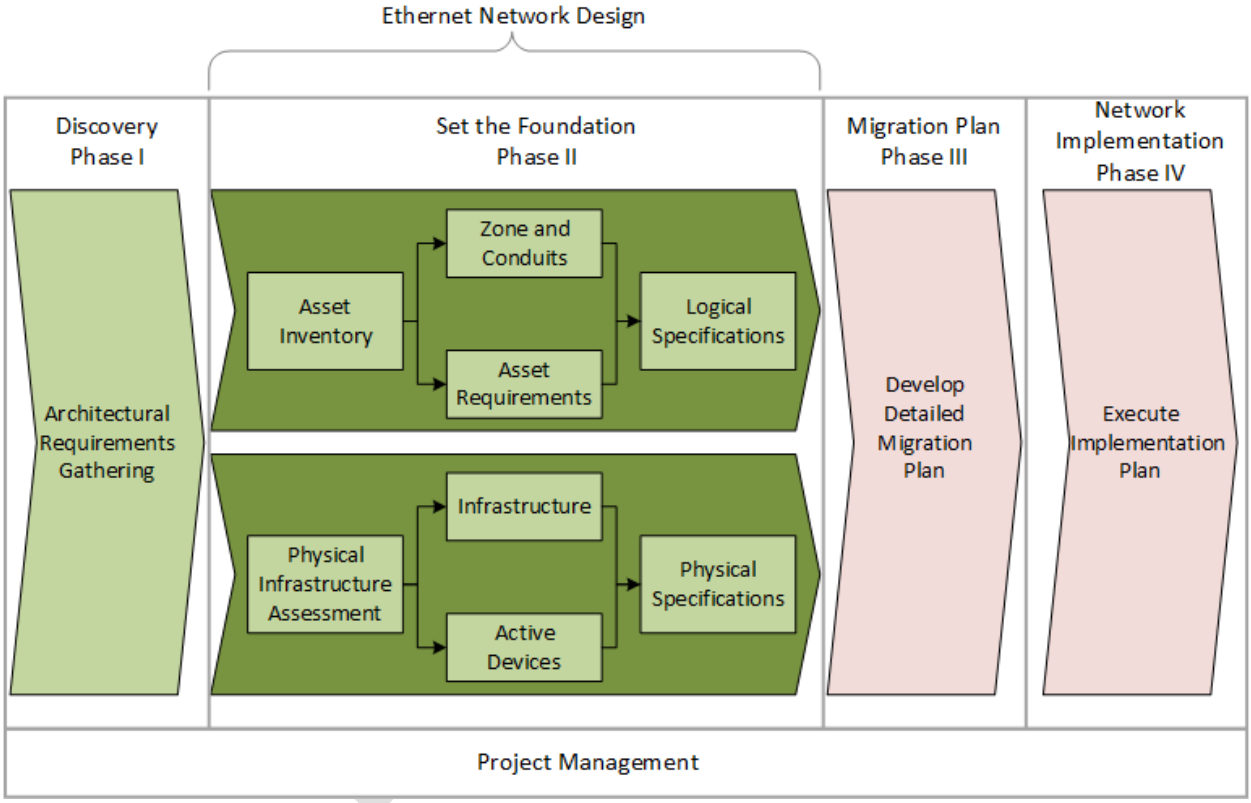

Figure 2.1 - Design Phases

Figure 2.1 includes two main areas: the Logical Design and Physical Design recommendations. Rockwell Automation will complete the Logical Design, which encompasses the method under which the data will flow logically throughout the network. Rockwell Automation has provided reference to elements of the Physical Design throughout this report; however, a complete Physical Design is not an aspect of the current deliverable. The Physical Design includes detailed construction documentation required to build the physical infrastructure and is not included in this report.

It is important to note that the current deliverable from Rockwell Automation completes the logical design and provides some building blocks for the physical design. However, the completion of the physical design, including detailed physical layer drawings and construction specifications, is considered part of a separate deliverable.

Customer inc has contracted Panduit for the detailed physical layer drawings and construction specifications. The Panduit Physical Design Package should be referenced for details.

This report includes data for the Logical Design and a few aspects of the Physical Design to illustrate the design intent. Logical aspects of the design are accompanied by associated drawings to detail the methodology. References to the drawings and documents included in the set of deliverables will be highlighted in the relevant sections and should be used in parallel to this document.

2.2 Objective

The primary objective is to design a robust, future ready Ethernet Network for the Customer inc plant that will be the backbone for plant level communications. This document includes references to standards, guidelines and best practices, and the specific logical details for this Ethernet Network Design to accomplish this goal.

The stated project goals are as follows:

- Design an OT infrastructure using industry best practices referencing the CPwE design and implementation guides.
- Design an OT network that provides new, dedicated OT infrastructure (logical and physical). This includes switches, cabling (fiber and copper), new enclosures, etc.
- Create an architecture that provides a foundation for adding future security features, while maintaining availability and operability of the Process Control Systems
    - Rockwell Automation recommends that an Industrial De-Militarized Zone (IDMZ) be reviewed and considered at a later stage after the network design and deployment.
- The architecture must adhere to the following requirements:
    - Architecture must be standard and scalable in nature
    - Architecture must follow industry standard guidelines
- Create an architecture that is future-ready so additional equipment can be integrated in the future.
- Create an infrastructure that includes all managed switches and allow these to be managed by OT personnel.
- Rockwell Automation recommends a Virtualized Infrastructure for all Manufacturing Information System applications. The new network design will need to support the compute infrastructure for a complete virtualized environment.
    - A Rockwell Automation Industrial Data Center (IDC) should be reviewed and considered as it helps to provide a robust, scalable, highly resilient and efficient virtual infrastructure for all manufacturing information systems.

2.3 Scope

2.3.1 Austin, TX Buildings B2/W2 &B3/ W3 Project

2.3.1.1 Project Description (Customer inc Engineering Specification)

Austin Texas is home to the Customer inc production facility in the United States. Customer inc intends to build a new state-of-the-art data center and information technology infrastructure to support the production operations in Buildings B2/W2 and B3/W3 while facilitating the overall business process.
The new Industrial Automation and Controls Systems (IACS) network will be developed with the intent of creating a robust, highly resilient and secure network infrastructure backbone with minimal response times and maximum throughput of data exchange in real time. The IACS network will be designed to be easily scalable and to accommodate newer equipment and future expansion to other buildings at the Austin TX facility, while maintaining a negligible impact to production.

The design intent is that the IACS infrastructure utilize the converged architecture model where the Manufacturing and Enterprise networks will be separated by an Industrial Demilitarized Zone (IDMZ). Discussions on the deployment and integration of an IDMZ are currently in progress. While the discussion of an IDMZ is outside the scope of this document, it is recommended that an IDMZ be reviewed for potential deployment and integration between the Enterprise network and the new IACS network.

2.3.1.2 Network Design Deliverable

As explained in the network design proposal, the scope of this Network Design Package is the Industrial Automation and Controls System (IACS) infrastructure network encompassing Buildings B2/W2 & B3/W3 at the Austin TX facility. The new IACS infrastructure will be stood up in parallel to the existing infrastructure and Customer inc will migrate the existing nodes to the new infrastructure as time and schedules permits.

The network design will include the Plantwide Core, Distribution, and Access switches.

Security boundaries and Enterprise connections are also outside the scope of this design package. These should be defined within an IDMZ Design Package and delivered separately. Some IDMZ design elements will be discussed at a high level to convey the design intent.

Similarly, some IDC design elements will be discussed at a high level to convey the design intent. Detailed elements of an IDC would be included in an IDC documentation package and delivered separately, should Customer inc choose to purchase and commission an IDC.

2.3.1.3 Building Description

The B2/W2 and B3/W3 Buildings are currently used for production and warehouse storage. Networking equipment to support production is currently located across all areas in both buildings. The B2 building is a 1 level production floor with a mezzanine level that links to W2. There is a total of 6 production lines in the B2/W2 area.
The B3/W3 building likewise, has a single level production layout that houses 2 production lines.

Table 2.1 provides an estimate of the assets that will be connected to the plantwide infrastructure. The network design package will detail the switching infrastructure required to support the Buildings B2/W2 & B3/W3 production networks.

Table 2.1 – Buildings B2/W2 & B3W3 Asset Estimates by Building.

Building	Level	# of Assets
B2/W2	**1**	72
W3	**1**	113
	Total	185

2.3.2 Ethernet Network Design Data Collection

Isaac Nuse Donkor, a consultant from Rockwell Automation's Network and Security Services Team, and Steven Brewster, a solution architect from Panduit's Infrastructure Services Team, visited the Customer inc site in December 2019 to gather information in support of the Ethernet Network Design project. The following items were reviewed, collected or discussed:

- Drawing review - obtain a better understanding of the physical layout of the plant and the future network requirements
- Review of planned switch cabinet locations
- Identification of potential switch cabinet locations
- Met with the engineering team to discuss key objectives to be included in the design
    - Reviewed the asset list of expected devices communicating on the network
    - Discussed future assets planned
    - Reviewed the type of communications and data flows expected
    - Reviewed the type of communications and data flows currently in use
- Discussed interconnectivity with OEM equipment (e.g., Filling Lines, Case Packers, etc.), and planned virtualization applications
- Discussed the possibility of hosting Virtual Host servers in MDC Enclosures.
- Discussed enclosure specifications required for Network equipment hosted on the production floor.
- Discussed VLAN and IP Subnet schema for future IACS network.
- Discussed future manufacturing application server requirements and cyber security initiatives around CLAROTY.
- Discussed concerns and known issues that have occurred over the years at the site
    - Remediations that arose as a result of the comprehensive network assessment (utilizing patch panels, cable bend radius, proper termination of shielded cables, etc)
    - Brief discussions on the role of an IDMZ in data exchange between IT and OT
        - This should be further addressed in a future IDMZ Design effort.
- Availability & Resiliency
    - Stacked OT Core to be located in MDC enclosure in B3/W3 with fiber downlinks to a collapsed Core/Distribution stack located in the MDC enclosure in B2.
    - Local static routes for all B2/W2 subnets to be configured in collapsed Core/Distribution stack located in B2 MDC enclosure.
    - Utilize Fiber EtherChannel links between switches. 10GB links between Core and Distribution layers. 1GB links between Distribution and Zone Enclosures/Access layers.

2.3.3 Ethernet Network Requirements Analysis and Specification

The requirements analysis and specifications provided in this document will be based upon the above-mentioned Ethernet network meeting findings and will further define the following:

- Network Availability and Future Ready Requirements

- Physical constraints and media limitations
  - Plant layout with respect to cabling and access to locations
  - Network media and infrastructure hardware evaluations
  - Identify redundancy requirements (i.e. fault tolerance, failover, and fault recovery requirements) at the media and infrastructure component levels
- Hardware Specifications
  - Switches
  - Enclosures
  - Cables (includes routing, type, termination, and connectors)
- Broadcast Domains
- Multicast Requirements
- Spanning-Tree Version
- VLAN Schema
- IP Address Schema
- Scalability and Expandability Requirements
- Switch Port Maps

2.4 Solution Summary

This document provides the detailed design solution required for implementation of the logical aspects and key physical aspects of the proposed Ethernet Network Architecture at the Customer inc plant. The Ethernet network design proposed was developed in accordance with industry standard practices to provide flexibility in addressing the key elements outlined below.

- Redundancy and fault tolerance on the development and modification of a new dedicated OT Control System Network.
- Physical isolation from the Enterprise Network in accordance with Industry Standards and best practices.
- Incorporation of virtualized platforms (e.g., HMI Servers, Data Servers, Historians, etc.) into the proposed Ethernet network.
- Accommodates growth of additional devices on the network.
- Traffic segmentation using a combination of physical and logical methods
- Support of Ethernet and Ethernet/IP communications.
- Ability to control, manage, monitor and diagnose aspects of the Control System Network, using the functional capabilities of a managed switch.

DWG REF

Customer's Network Design v1r0 – Network Overview

The Network Overview drawing illustrates a high-level solution summary of the Ethernet network architecture.

2.4.1 Additional Logical Design Specifications / Details

Based on discussions between Customer inc and Rockwell Automation, the following are additional general specifications and assumptions regarding the logical aspect of the design:

- Existing controls assets are mostly on a flat network with unmanaged switching infrastructure. All controls system assets will need to be readdressed when the assets are migrated from the existing infrastructure to the new infrastructure.
- All private IO Networks will be brought up to the managed plant communications/IACS network. Logical segmentation via VLAN and IP Subnets will be used to segment Controls traffic based on physical/process zones identified on each line.
- All NAT translations on the IACS network will be discontinued. Static routes in the core router will be used as appropriate to enable communication between various subnets.
- The network design should allow for Messages and/or produced/consumed tags (unicast) to be used to communicate between the controllers.
- Routing will be distributed between the Customer inc Production Buildings. The Central Core will be located in the B3/W3 building MDC/Datacenter Enclosure. This will have static routes for all subnets in B3/W3 and will also have static routes to the collapsed Core/Distribution stack in B2 and other future MDCs that will be located in future buildings. The Collapsed Core/Distribution stack in B2 will handle routing for all subnets in B2/W2 and also have static routes to forward traffic to the Central Core in B3/W3 based on application requirements.
- If the fiber connection to B3/W3 is severed or lost, all manufacturing processes and applications in B2/W2 should continue to operate.
- B3/W3 will utilize ZDF/IDFs as enclosures for Distribution level switches however, due to physical spacing and other constraints in B2/W2, Network Zone Enclosures (NZEs) will be utilized in key areas of B2/W2. The Switches in the NZEs will have single 1GB downlinks to managed Stratix 5700/5400 access switches in the various control panels and dual 1GB fiber uplinks to the MDC enclosure in B2.
- All switch hardware will be mounted in suitable enclosures for the environment (i.e., Control Panels for DIN rail mounted switches, Network Zone Enclosures for DIN rail mounted Intermediate Distribution Switches, Industrial Distribution Frames (IDFs) for rack mounted switches and Main Distribution Frames (MDF/MDC) for rack mounted switches within the Data Center).
- The design should utilize switches running on the Cisco IOS platform, which would include Cisco and the Stratix family of switches.
    - Existing unmanaged OEM Equipment Level switches will be upgraded to managed Stratix 5700/5400 series switches.
- The Industrial Automation and Control Systems (IACS) network will be managed by Customer's Control System Engineering team.
- Use redundant fiber cabling between the Core, Distribution and Access/Zone Enclosure switches.
- All network enclosures (MDC/MDF, ZDF/IDF, NZE) will be located on the production floor. The enclosures will be equipped with the appropriate cooling systems, redundant power supplies and have appropriate NEMA & IP ratings to prevent ingress of water/moisture and dust.

2.4.2 Primary Network Infrastructure Locations

The network infrastructure locations are defined as follows:
B3/W3 Building:

OT Core/Datacenter Main Distribution Frame (MDF/MDC)

- 5G-B3-MDC-E07: Adjacent to existing enclosure DP-2 #26.28.30 within grid E07
    - Network Equipment
        - Core Switches
        - Fiber Distribution

        - Servers for Virtual Infrastructure (future device)
        - iDMZ equipment (future device)

Industrial Distribution Frame (IDF)

- 5G-B3-ZDF-E07: Adjacent to 18091 LCP1 Control Panel
    - Network Equipment
        - Fiber Distribution
        - Distribution Switches

- 5G-B3-ZDF-F10. Adjacent to 17181 LCP1 Control Panel
    - Network Equipment
        - Fiber Distribution
        - Distribution Switches

B2/W2 Building:

B2 Main Distribution Frame (MDF)

- 5G-B2-MDC-A00: Back end of B2 Southside wall. Adjacent to existing 50ml Control Panel
    - Network Equipment
        - Fiber Distribution
        - Collapsed Core/Distribution Switches
        - Redundant Virtual Infrastructure server (future device)

B2 Network Zone Enclosures (NZE)

- 5G-B2-NZE-A00: South Point NZE
    - Network Equipment
        - Fiber Distribution
        - Stratix 5400 Full Gigabit Switches

- 5G-B2-NZE-A06: Midpoint NZE
    - Network Equipment
        - Fiber Distribution
        - Stratix 5400 Full Gigabit Switches
- 5G-B2-NZE-A09: Northpoint NZE
    - Network Equipment
        - Fiber Distribution
        - Stratix 5400 Full Gigabit Switches

W2 Network Zone Enclosures (NZE)

- 5G-W2-NZE-MCC4: W2 NZE
    - Network Equipment
        - Fiber Distribution
        - Stratix 5400 Full Gigabit Switches

All unmanaged access level switches existing in the various control panels along all 8 production lines will be upgraded to managed Stratix 5700/5400 switches as part of this design and subsequent implementation efforts. The locations of these Access switches were not indicated above however, they are indicated in the Network Design Drawings and will be included in the BOM for this design effort.

3 MANUFACTURING NETWORK INFRASTRUCTURE

A dedicated, well-designed network infrastructure will be built at the Customer inc facility to support the IACS networks in Buildings B2/W2 & B3/W3 and their requirements.

To allow for separation of operationally different types of traffic, the segmentation techniques outlined in this design follow industry best practices from various standards. Although it is outside the scope of this design, these standards also outline recommendations for safe and secure connection of production environments to Enterprise environments via the use of an Industrial De-Militarized Zone (IDMZ). The specific standards are as follows:

- NIST SP-800
- ISA SP-99 standards for the Industrial Control System and SCADA environments
- DHS INL/EXT-06-11478

These standards convey a strategy of defining logical demarcation between different traffic types along with physical demarcation between enterprise and manufacturing zones. Figure 3.1 illustrates the CPwE Industrial Network Security Framework that leverages a defense-in-depth approach.

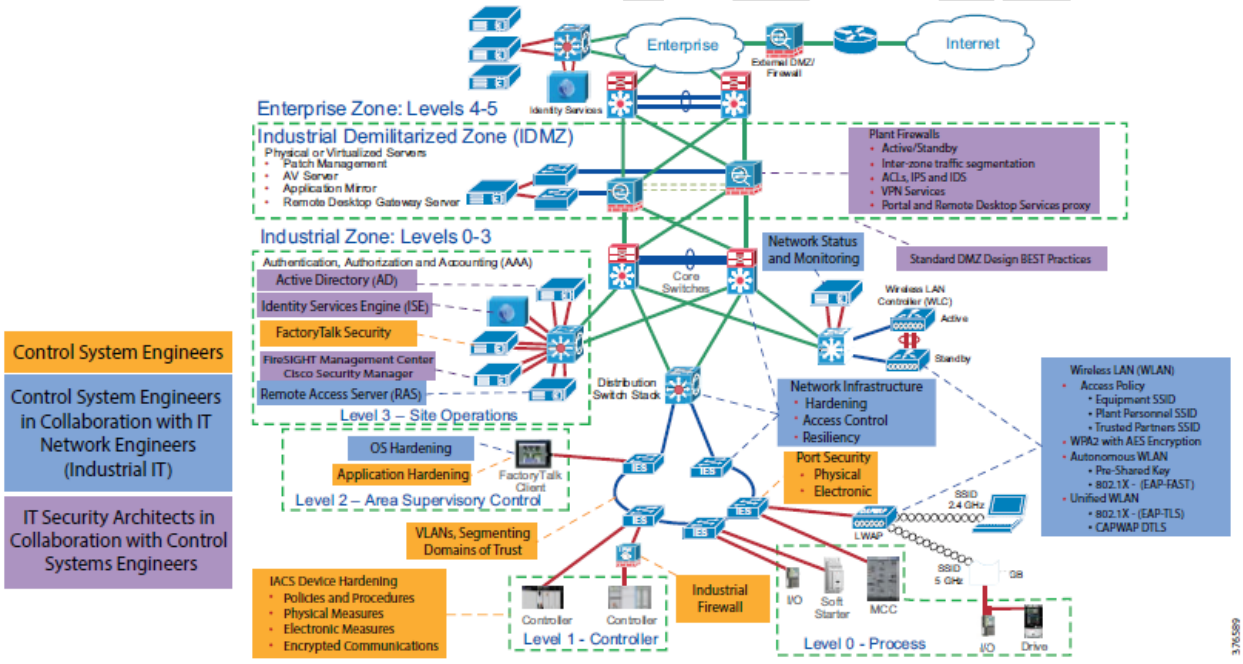

Figure 3.1 - CPwE Industrial Network Security Framework

Although integration of the enterprise network with the overall plant level communications via an Industrial De-Militarized Zone is outside the scope of this design, it is important to consider the key aspects of these standards when this phase is being completed.

Benefits of using these standards for this design include the following:

- Dedicated Core and or Distribution routing services configured within the industrial production zone using only connected and static routes.
- Place manufacturing elements into logically segmented zones based on operational dependencies.

- Allows for the creation of policies and procedures that meet the requirements of manufacturing assets, for e.g. aligning maintenance schedules with production schedules.

3.1 Methodology Used

The methodology used as the basis for the plant network design is the logical Manufacturing Framework, which provides a template for segmenting traffic logically based on function. Although the scope of this design does not include the development of an IDMZ, it is important to understand the method under which this is accomplished. Both ISA-95 and the Purdue Model for Control Hierarchy segment industrial control devices into hierarchical "Levels" of operations within a manufacturing facility. This is depicted in Figure 3.2.

This design incorporates the devices and infrastructure used in Levels 0-3 of the standards. The key however is that the additional Levels 4 and 5 can be integrated into the architecture during future upgrades to the networks via an IDMZ. By using this standard throughout the design, the inclusion of additional levels can be viewed as "building blocks" that allow future connectivity of the plant environment to the Enterprise.

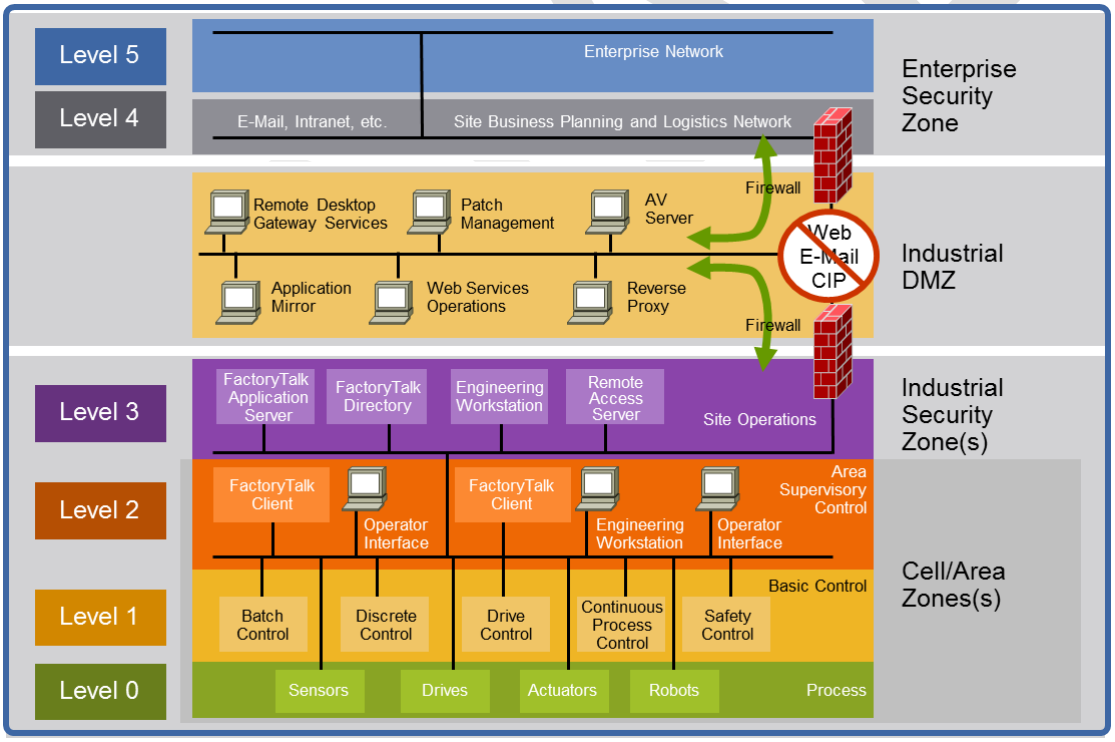

Figure 3.2 - Logical Framework

3.2 Enterprise Campus Network Model

Cisco's Enterprise Campus Network model describes various systems, components and their relation to each other in context with networking function, integrating the knowledge and expertise from the perspectives of both Operations Technology (OT) and the Information Technology (IT) folks.

Table 3.1 provides perspectives of the key network attributes between the Enterprise network and a Control System Network.

Table 3.1 - Differences between Enterprise and Control System Networks

	Enterprise Network	Control System Network
Reliability	Occasional Failures tolerated	Outage intolerable
Security	Focus on central server security	Has proprietary information so security is required Focus on edge control device stability
Performance	High delay and jitter accepted	Delay and jitter not accepted
Risk Impact	Loss of Data ok	Loss of Data not accepted
Risk Management	Recover by reboot	Fault tolerant system needed
Environment	Climate Controlled	Harsh

In large scale applications a three layer model, depicted in Figure 3.3 is used which integrates a core switch pair, various distribution switches based on size and scale of the application, and access level switches that each connect into a distribution switch.

In smaller applications, it is possible to consolidate some layers of the model. This could result in consolidating the core and distribution layers into a single collapsed Core/Distribution layer or consolidating the distribution and access layers into a single Distribution / Access layer. Consolidation of the layers can provide similar functionality with less complexity and associated hardware.

Although the collapsed model does not necessarily provide the full scalability of the three-layer model, it is often more suited for use in Industrial Automation Control System (IACS) applications based on their size.

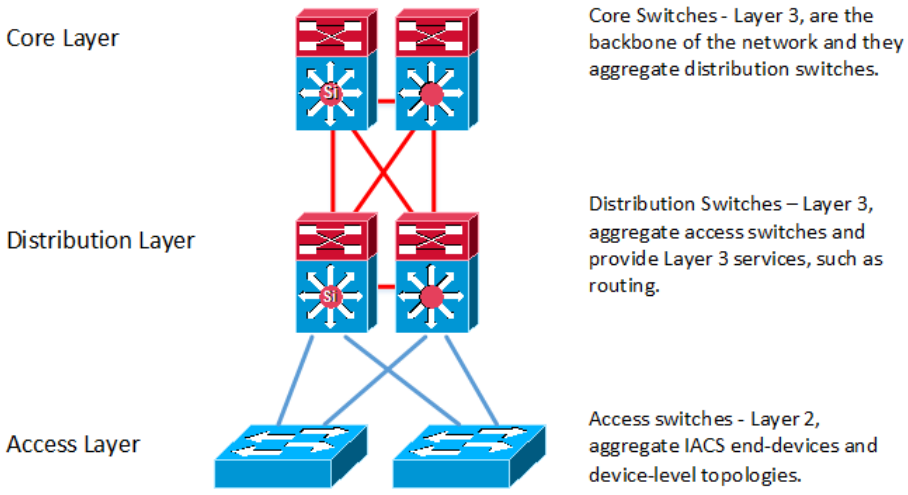

Figure 3.3 - Hierarchical Campus Model

For the Customer inc deployment, Rockwell Automation's recommendation is to use the three-layer model with Core, Distribution, and Access layers. Additionally, the Distribution/Access layer for B2/W2 will be divided into Zone Level and Device Level or OEM equipment level.

4 LOGICAL TOPOLOGY DESIGN

The Customer inc Control System Network architecture design outlined in this document has the following key elements incorporated.

Star Topology – Core, Distribution, and Access Layers

- **Design:** Minimizing the number of switch hops helps minimize latency and jitter.
- **Performance:** Data does not have to pass through excessive numbers of nodes.
- **Isolation:** Each device is inherently isolated by the link that connects it to the switch. This isolation also prevents any non-centralized failure from affecting the network.
- **Centralization:** High-performance with minimal bottlenecks. Centralization also allows the inspection of traffic through the network. This facilitates analysis of the traffic and detection of suspicious behavior.
- **Fault detection:** Simplified topology allows faults to be isolated and located.
- **Installation:** Installation and configuration is simplified since every device only requires a single interface or redundant pair of interfaces.
- **Expansion:** A Star topology can be expanded to increase the network size with minimal impact to operational network.
- **Redundancy:** A Star topology provides a high level of redundancy and flexibility for the network layout.

This document will expand upon these key elements and will highlight the specific features that are used to achieve them.

4.1 Network Switch Topology

The interconnection of network infrastructure equipment has two aspects for consideration: physical and logical. The physical interconnection outlines the path in which the cabling is physically laid throughout the plant. In contrast, the logical interconnection outlines the path over which data flows between various devices. In many instances, the physical path over which cabling is laid is different from its logical functionality.

4.1.1 Redundant Star Topology

The redundant star topology along with the concepts of the three-layer network model will be used in this architectural design. It divides the Control System Network into three layers. Each layer provides functions and services to the entire network. The model provides flexibility to expand as the plant adds more Ethernet nodes to the network.

To form the redundant star logical topology, there is a minimum of two network uplinks between switches. These two links are ideally routed via unique paths. This provides fault tolerance using divergent physical paths in the event that one of the switch uplinks fail.

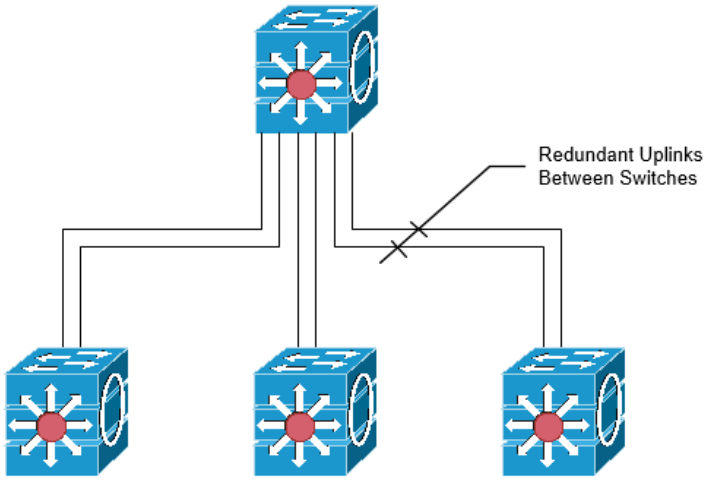

Figure 4.1 - Redundant Star Logical Connection

To be able to handle the redundant links, various protocols exist to ensure that loops within the architecture are not formed. These protocols actively manage the redundant links to monitor status and initiate a convergence event if a topology change is detected.

4.1.1.1 EtherChannel

EtherChannel is recommended as the resiliency protocol running over the redundant inter-switch links for the following connections:

- Core switches to Distribution switches
- Core switches to Server switches (for future IDC phase)
- Distribution switches to Network Zone Enclosure Switches (NZE) in B2/W2
- Distribution switches to Access level switches in Control panels (W3)

Note

The connections from Zone Level switches (NZE) to Equipment Level Access switches are single copper connections so EtherChannels cannot be used and no resiliency between the switches exist.

Customer inc understands and accepts the risk of a link failure in this scenario specific to the B2/W2 building.

EtherChannel has the following advantages:

- Allows for increased bandwidth between switches by aggregating links (i.e., 2 x 1Gbps links = 2Gbps bandwidth)
- Load balancing across the channels for optimal performance
- Fast network convergence upon a link failure (over fiber links)
- Deployed across many platforms and switch vendors allowing for ease of interoperability

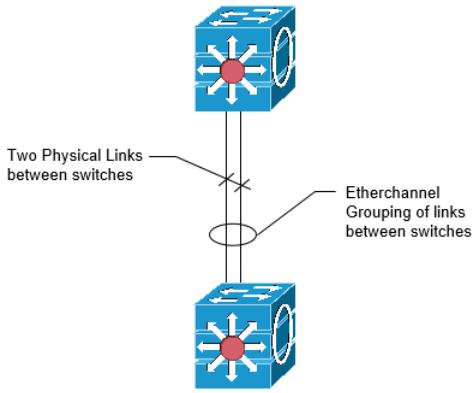

Figure 4.2 - EtherChannel Link Depiction

4.1.2 Solution Summary

Requirements including availability, security, resiliency, scalability, Customer inc preferences, and design considerations of the technologies and capabilities to be used have driven the proposed design. Some of the key points are summarized below.

Core

- In B3/W3, a redundant pair of Core switches (Cisco Catalyst 9500 Series).
- The Core switches will be interconnected using Stackwise Virtual technology to form a single logical switch entity.
- Collapsed Core/Distribution switches in B2 will be a redundant pair of Catalyst 9500 switches in a Stackwise Virtual configuration.

Distribution

- Distribution switches will be redundant pairs (Cisco Catalyst 9300 Series).
- The Distribution switches will be interconnected using Stackwise-480 technology to form a single logical switch entity.
- The Distribution switches will have fiber uplinks to each of the Core switches in the SV pair. The uplinks will be managed using EtherChannel link aggregation protocol.
- In B2/W2, the collapsed Core/Distribution switches will have dual fiber downlinks to each of the Network Zone Enclosure (NZE) switches. The downlinks will be managed using EtherChannel link aggregation protocol.
- In B3/W3, the Distribution switches will have dual fiber downlinks to each access switch located in the line control panels. The downlinks will be managed using EtherChannel link aggregation protocol.

Network Zone Enclosure

- Network Zone Enclosures will be utilized in B2/W2 and will serve as a sub distribution layer in this building.
- NZEs will utilize x2 Stratix 5400 Gigabit Ethernet Managed switches.
- Each Stratix 5400 switch in an NZE will have a single 1GB copper downlink to managed Stratix 5700/5400 access switches located in control panels across the production lines.
- Each Stratix 5400 switch in an NZE will have dual fiber uplinks to the B2 MDF enclosure. This link will be managed using EtherChannel link aggregation protocol.

Access Level

- Access level switches will be comprised of managed Stratix 5700/5400 switches located in control panels along each production line (these include OEM panels).
    - Switch selection will be determined by port density and uplink speed requirements within control panels.
    - Access Level switches will have copper downlinks to connect end devices within a given area.
- In B2/W2, the Access Level switches will use a single 1GB copper uplink to the designated NZE for an area. While in W3, the Access Level switches will use a dual fiber uplink to the Distribution switches in the corresponding line IDF. This dual fiber uplink will be managed by EtherChannel link aggregation protocols.

Cabling

- Infrastructure communication between Core and Distribution layers will be done via Single-mode fiber optic cabling. The redundant 10Gbps connections will create a shared 20Gbps link under optimum conditions (i.e., no connection failures).
- The Stackwise Virtual Link (SVL) to create the virtual stack for the Core switch pairs will require four (x6) 10Gbps connections.
- The Dual Active Detection link between the Core switch pair will require two (x2) 10Gbps connections.
- Infrastructure communications between the Core and Distribution layers will be done via Single-mode fiber optic cables. A redundant 10Gbps connection will create a shared 20 Gbps link under optimum conditions.
- Infrastructure communications between the Distribution and Access layers in B3/W3 and also, communications between the collapsed Core/Distribution Switches and the NZEs in B2/W2 will be done via Single-mode fiber optic cables. The redundant 1Gbps connections will create a shared 2Gbps link under optimum conditions.
- Infrastructure communications between the Access Switches and End Devices will be connected together with a minimum of Cat6 Copper cabling to provide a 10/100/1000 Mbps connection, depending on the end device.
- Redundant fiber links between the Core, Distribution, and Access layers will utilize divergent paths whenever possible. The redundant links are to support the following failures:
    - Single Core Switch
    - Single Core Interface
    - Single Distribution Switch
    - Single Distribution Interface
    - Single Access Interface
    - Transceiver connected at the Core, Distribution, and Access switches
    - Single fiber termination connected at Core, Distribution, and Access switches
    - Single patch cable on Core, Distribution, and Access Switches

Redundant switch to switch connections using 1Gbps copper is not recommended for Class 1 traffic (i.e., I/O or Produced/Consumed). The detection of a link loss on 1Gbps copper physical interfaces can be up to 750ms. This can result in dropped connections between the controller and end devices.

DWG REF

Customer's Network Design v1r0 – B3/W3 L7 Logical Topology
Customer's Network Design v1r0 – B3/W3 L8 Logical Topology
Customer's Network Design v1r0 – B2 NZE Logical Topology
Customer's Network Design v1r0 – B2/W2 NZE Logical Topology
Customer's Network Design v1r0 – B3 Physical Topology
Customer's Network Design v1r0 – B2 Physical Topology

The Logical Topology drawings illustrate the hierarchal view of the Core, Distribution, Zone Level and Access level switches, and the links that connect them. The Physical Topology illustrates the physical connections between the switching infrastructure required to support the designed network.

DOC REF

Customer's Network Port-Maps-1 v1r0 Workbook
Customer's Network Port-Maps-2 v1r0 Workbook

The Customer's Network Port-Maps document provides a detailed overview of the connections required for each process area. The various device types and counts were used to determine the best options for the network architecture and switch models to utilize.

4.2 Network Switch Specifications

There are three types of switches selected within this design: the Core Layer, Distribution Layer, and Access Layer. The Access Layer (Zone Level, Device Level, OEM) includes DIN mount switches that connect to end devices. To reduce the number of models and maintain compatibility between switch platforms the following switch families are used within the design

- Cisco Catalyst 9500 Series (Rack mount)
- Cisco Catalyst 9300 Series (Rack mount)
- Stratix 5400 and 5700 Series (DIN rail mount)

Each switch type provides the speed, and functional capabilities required for its use within the Customer inc IACS network architecture.

4.2.1 Core Switch

The Core layer provides routing services within the Customer inc IACS network. Additionally, connectivity to the Enterprise network through an IDMZ (out of scope for this design) can be accomplished via the Core switch.

The selection for Core switch is the Cisco Catalyst C9500-40X-A, with Network Advantage Licenses. The switch can provide 10Gbps connectivity for its downstream connections. It also features the Stackwise Virtual failover technology between a pair of switches.
To cater to redundancy requirements outlined by Tito's, B2/W2 will also feature a collapsed Core/Distribution switch housed in an MDF Cabinet. The selection for this switch is the Cisco Catalyst C9500-16X-A, with Network Advantage Licenses and an 8 port 10Gbps uplink module (C9500-NM-8X) for uplinks to the Site Wide Core switch in B3/W3.

The Core switch requirements for acceptability within this design are as follows:

- Serve as an aggregation point for all distribution switches and potential connectivity to a future IDMZ
- Access Control Lists (ACL)
- Core Redundancy (SV failover technology)

- Provide full layer 3 services and connectivity for all devices within the B2/W2 and B3/W3 network
- Create broadcast domains via the use of traffic segmentation
- High data transfer rate
- High Availability
    - Core failover
    - Link redundancy
    - Redundant Power Supplies
    - Redundant Power
- Routing
    - Inter-VLAN Routing via the use of connected and static routing
- Virtual Local Area Networks (VLANs)
- IGMP Querier and Snooping – Multicast traffic management
- Quality of Service (QoS)
- Loop Resolution Protocols
- Diagnostic Capabilities
- Simple Network Management Protocol (SNMP)
- IEEE 802.1Q Trunking Protocol
- Direct fiber connectivity
- Network Time Protocol (NTP)
- Must be installed in a permanent and secured location / cabinet

4.2.1.1 Stackwise Virtual Technology

The Cisco Stackwise Virtual technology is a clustering technology that pools two Cisco Catalyst 9500 Series Switches into a single virtual switch.

An example of Stackwise Virtual is shown in Figure 4.3. The figure depicts the physical and logical connections of a Stackwise Virtual Distribution Switch to Access Switches.

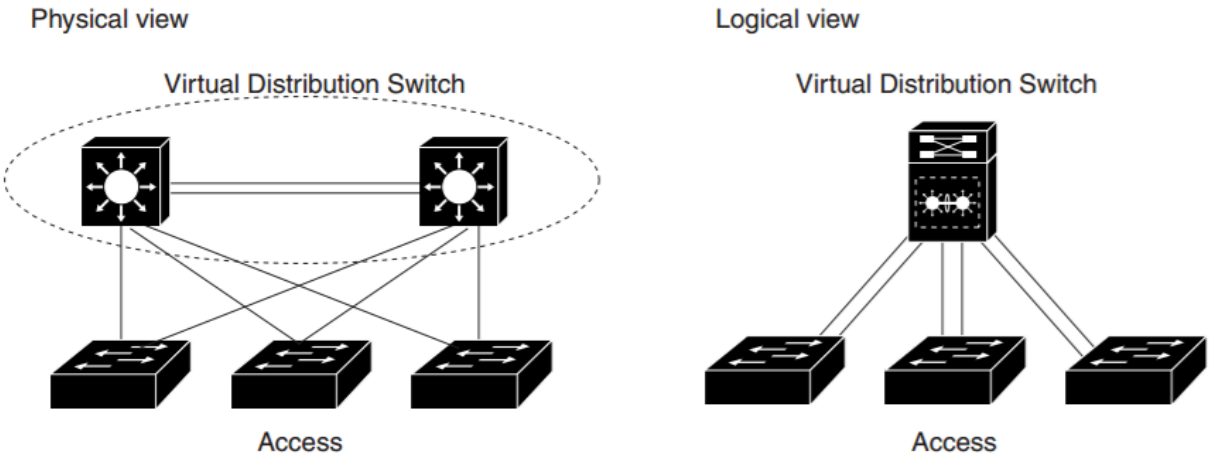

Figure 4.3 – Stackwise Virtual Physical and Logical Views

Stackwise Virtual combines a pair of switches into a single network element. Stackwise Virtual manages the redundant links, which act as a single port-channel for neighboring switches. It also simplifies network configuration and operation by reducing the number of Layer 3 routing neighbors and by providing a loop-free Layer 2 topology.

In a Stackwise Virtual pair, one chassis becomes the active chassis, and the other chassis becomes the hot standby. The active chassis controls the virtual stack. It runs the Layer 2 and Layer 3 control protocols for the switching modules on both chassis. The active chassis also provides management functions such as module online insertion and removal (OIR) and the console interface.

The active and hot standby chassis perform packet forwarding for ingress data traffic on their locally hosted interfaces. However, the hot standby chassis sends all control traffic to the active chassis for processing via the Stackwise Virtual Link (SVL).

For the two chassis to act as one network element, they need to share control information and data traffic. The Stackwise Virtual Link (SVL) is a special link that carries control and data traffic between the two chassis. The SVL is implemented with a minimum of two and a maximum of up to eight links. The SVL gives control traffic higher priority than data traffic so that control messages are never discarded. Data traffic is load balanced among the SVL links.

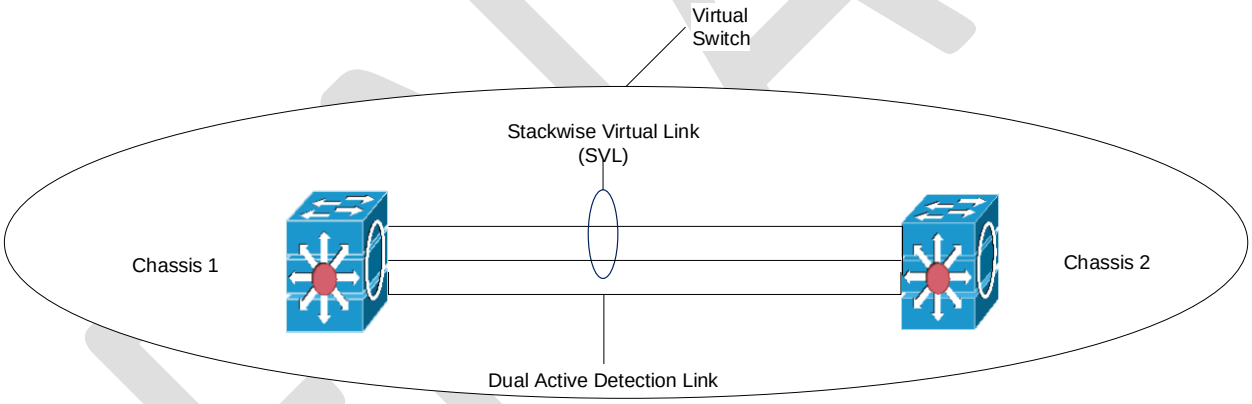

Figure 4.4 – Stackwise Virtual Link (SVL)

In a Stackwise Virtual configuration, the supervisor engine redundancy operates between the active and hot standby, using stateful switchover (SSO) and nonstop forwarding (NSF) technologies. The peer chassis exchange configuration and state information across the SVL and the standby supervisor engine runs in hot standby mode. The hot standby chassis monitors the active chassis using the SVL. If it detects failure, the hot standby chassis initiates a switchover and takes on the active role. When the failed chassis recovers, it takes on the hot standby role.

If the SVL fails completely, the hot standby chassis assumes that the active chassis has failed and initiates a switchover. After the switchover, if both chassis are active, the dual-active detection feature detects this condition and initiates recovery action.

4.2.2 Distribution Switch

The Distribution layer provides connectivity between the Core and Access layers. All Distribution layer switches are connected directly to the Core switch using two, 10Gbps uplinks that forms a 20Gbps redundant connection.

The selection for the Distribution switch is the Cisco Catalyst C9300 series, with 24/48 1G SFP ports and a Network Essential License (C9300-24S-E/C9300-48S-E). An 8-port 10G SFP Network Module (C9300-NM-8X) will be added to the switch to support the 10G uplinks to the Core switch. The Distribution switch will feature the redundant failover technology of Stackwise-480 technology between the Distribution switch pair.
For the B2/W2 building, Stratix 5400 switches mounted in Network Zone Enclosures (NZE), will serve as a sub-distribution layer. A total of 4 NZEs with two (x2) Stratix 5400 switches each, will be deployed in key areas within B2/W2. The NZE switches will have single 1Gbps copper downlinks to Access switches in control panels around the vicinity of each NZE. This solution was chosen due to physical constraints within B2/W2 which prevent deploying of IDF cabinets around this building. It was also not feasible to run fiber cables to each control panel within B2/W2 and hence, the choice of copper downlinks between the NZE switches and controls panels in their vicinity.

The Distribution switch requirements for acceptability within this design are as follows:

- Serve as an aggregation point for all access switches
- Provide connectivity between access and core layers
- Distribution Redundancy (Stackwise-480 and Stackpower technologies where applicable)
- Provide full layer 2 services and connectivity for all devices
- Create broadcast domains via the use of traffic segmentation
- High data transfer rate
- High Availability
    - Distribution Switch failover
    - Link redundancy
    - Redundant Power Supplies (where applicable)
    - Redundant Power
- Virtual Local Area Networks (VLANs)
- IGMP Querier and Snooping – Multicast traffic management
- Quality of Service (QoS)
- Loop Resolution Protocols
- Diagnostic Capabilities
- Simple Network Management Protocol (SNMP)
- IEEE 802.1Q Trunking Protocol
- Direct fiber connectivity
- Network Time Protocol (NTP)
- Must be installed in a permanent and secured location / cabinet

4.2.2.1 StackWise-480 Technology

StackWise-480 is available on the latest generation of Cisco switches (e.g., Cisco 9300 and also available on some earlier models like the 3850 series switches). StackWise-480 has a stack bandwidth of 480Gbps and uses Stateful switchover (SSO) to provide resiliency within the stack. Stacking technology allows multiple switches to be stacked together creating a single logical switch grouping. The stack behaves as a single switching unit that is managed by an active switch elected by the member switches. The active switch automatically elects a standby switch within the stack. The active switch creates and updates all the switching, routing and wireless information and constantly synchronizes that information with the standby switch. If the active switch fails, the standby switch assumes the role of the active switch and continues to keep the stack operational. Access points continue to remain connected during an active-to-standby switchover unless the access point is directly connected to the active switch. In this case, the access point will lose power and reboot.

A working stack can accept new members or delete old ones without service interruption. The stack member number (1 to 9) identifies each member in the Switch stack. The member number also determines the interface-level configuration that a stack member uses. A higher priority value for a stack member increases the probability of it being elected the active switch and retaining its stack member number. The priority value can be 1 to 15 with the default being 1.

The Cisco Catalyst 9300 Switch deployed in stack mode is designed to deliver deterministic non-blocking switching performance. Cisco StackWise-480 provides a robust distribution forwarding architecture through each stack member switch and a unified, fully centralized control and management plane to simplify operation in a large-scale network design.

To enable Stateful switchover (SSO) resiliency in Cisco StackWise-480 mode, you must configure each switch with the same Cisco IOS XE Software version and license. In stacking mode, the Cisco Catalyst 9300 active switch automatically performs Stateful switchover (SSO) protocol synchronization with the standby switch. By default, Nonstop Forwarding (NSF) subsystems in all the switches in a Cisco Catalyst 9300 Switch stack operates in NSF helper mode and supports nonstop data forwarding and graceful recovery during active to standby (Layer 3) switchover. Implementing NSF capability allows the remaining Cisco Catalyst 9300 switches in the stack to continue forwarding data while the new active switch gracefully recovers the protocol state machines.

Figure 4-5 describes the complete process of an election using different numbers of switches in a stack.

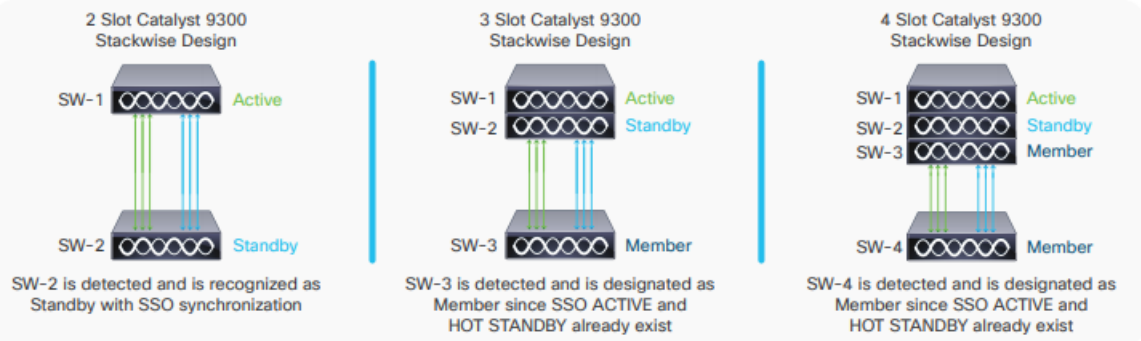

Figure 4-5 - Stackwise-480 Election Process

During a failover from the Active switch to the Standby switch, timeouts between routed applications could occur.

The Control System Network Distribution switches will be connected using the 50 cm Type 1 Stacking cables (STACK-T1-50CM) to achieve the Distribution switch hardware redundancy.

DWG REF

Customer's Network Design v1r0 – Stackwise 480 Configuration

The Stackwise 480 Configuration drawing illustrates the switch stack configuration and cable connections.

4.2.3 Access Switch

This layer represents the network edge, where manufacturing zone traffic enters/exits the network. In other words, the access layer will provide end device connectivity to all nodes on all of the production lines. There are a few different types of Access switches used in the network architecture based on location and functional requirements.

The Access layer switches used in this design will consist of Equipment/OEM Level switches:

- Equipment Level – All unmanaged switches at the equipment level (Control Panels including OEM Panels), will be upgraded to managed Stratix 5700/5400 series switches and will have direct connections to either the NZE level or Distribution level switches in B2/W2 and B3/ W3 respectively. In B2/W2, all access switches will employ single 1Gbps copper uplinks to the nearest NZE while in B3/W3, access switches will utilize dual 1Gbps fiber uplinks to the respective IDF along each production line within B3/W3.
    a. The Allen-Bradley Stratix 5700 and 5400 Series switches, with Full firmware are to be used in all equipment level areas. The specific models of the Stratix 5700/5400 managed switches will be selected based on port density, speed and uplink requirements at the various equipment level panels.

The Access Switch Requirements are as follows:

- Allow Devices to communicate using services provided by the Core, Distribution and other Access switches
- Gigabit link speeds for uplink connections to Distribution switches or NZE switches
- 10/100/1000 Mbps speeds for control end device connections
- Port Level Security
- High Availability
    - Link redundancy where possible
    - Redundant Power
- Virtual Local Area Networks (VLANs)
- IGMP Querier and Snooping – Multicast traffic management
- Quality of Service (QoS)
- Traffic thresholds
- Loop Resolution Protocols
- Diagnostic Capabilities
- Simple Network Management Protocol (SNMP)
- IEEE 802.1Q Trunking Protocol
- Direct fiber or copper connectivity
- Network Time Protocol (NTP)

Access Switch (Stratix 5700/5400) Additional Recommended Requirements

- Connectivity to Logix based controllers for remote configuration and troubleshooting
- High Availability
    - SD Card w/configuration for quick replacement

4.3 Small-Form Factor Pluggable (SFP) Specifications

The SFP Transceiver modules are hot-swappable devices that plug into transceiver ports. The wavelengths for transceivers on each end must match. Table 4.1 shows the transceiver modules selected based on their compatibility with the selected switches and their use in a Single Mode fiber environment.

Table 4.1 – SFP Connections

Vendor	SFP Part Number	Description	Switch Connectivity
Cisco	SFP-10G-LR-S=	Cisco 10GBASE-LR SFP+ Module for Single-mode Fiber. Enterprise Class	Cisco Core and Distribution Switches
Cisco	GLC-LH-SMD	1000BASE-LX/LH SFP transceiver module, MMF/SMF, 1310nm, DOM	Cisco Distribution Switches
Cisco	GLC-TE=	1000Base-T SFP Copper Transceiver Module	Cisco Core and Distribution Switches, Copper Connectivity
Allen-Bradley	1783-SFP1GLX	Stratix Fiber SFP, 1000Base-LX/LH Single-mode Fiber, 1300nm wavelength	Stratix 5700/5400 Access Switches

4.3.1 Guidelines for Handling SFPs

SFP modules are static sensitive. Rockwell Automation recommends wearing an ESD-preventative wrist strap and connecting its other end to the chassis in order to prevent electro-static discharge (ESD) damage. Always store spare or unconnected SFP modules with the optical bores, as they are sensitive to dust accumulation. Do not remove and insert SFP modules more often than necessary. Repeated removals and insertions can speed up the SFPs estimated mean-time-before-failure (MTBF).

5 PHYSICAL DESIGN

The Physical Design Elements section will provide an overview of the physical infrastructure and building blocks to utilize for the completion of the physical design. Although not included as a deliverable for this aspect of the project, Construction Specifications and Drawings for the physical installation of the network are critical. The construction documents provide detailed drawings showing the physical infrastructure systems, written specifications for the installation and testing of all aspects of the physical infrastructure, and a list of materials needed. These should be completed prior to finalizing the design phase of the project.

Areas to be covered include:

- Physical topology to achieve logical design
- Overview of the physical infrastructure
  - Network Switch Enclosures
  - Fiber backbone cable and connectivity
  - Copper cable and connectivity
  - Pathway Routes
  - Power Specifications
  - Grounding and Bonding
  - Labeling and Identification
- Construction Documents / Drawings
  - Detailed drawing plans showing space planning
  - Proposed Fiber Optic cable pathway routes
  - Cable one-line diagrams
  - Cable schedules
  - Cabinet placement and mounting details
  - A list of materials and written specifications for the installation and testing of all aspects of the physical infrastructure systems

It is important to note that the current deliverable from Rockwell Automation completes the logical design and provides some building blocks for the physical design. However, the completion of the physical design, including detailed physical layer drawings and construction specifications, is considered part of a separate deliverable.

Panduit will take ownership for the detailed physical layer drawings and construction specifications. The Panduit Physical Design Package should be referenced for details.

5.1 Physical Topology

The physical network infrastructure is comprised of a structured cable wiring plant and zone network topology that adheres to the Converged Plant-wide Ethernet (CPwE) reference architecture and aligns with the logical design described in the previous sections to form the redundant and resilient star topology specified. The zoned network topology is a highly effective way to deploy EtherNet/IP solutions in an industrial plant floor environment.

Utilizing a zoned network topology and following CPwE guidelines is a best practice, providing a highly scalable and flexible deployment that leverages a building block approach.

By using a zone cabling architecture approach, network cabling becomes easier to locate, manage, and maintain because each additional device is routed within the same pathways and enclosures. Managed cabling helps reduce the number of home runs throughout a facility and helps reduce abandoned cable in plenum spaces, helping make the workplace run more efficiently and safely.

The cabling for the plant is comprised of high-performance fiber optic cables creating dual network uplinks between the switches (Core, Distribution, Access). Copper downlinks are utilized from the access switches to their designated end devices. Specially designed and engineered system enclosures, optimized for the industrial environment, will house the Customer's IACS network switches. The enclosures will be installed in designated locations along production lines in B2/W2 and B3/W3.

Customer's Network Design v1r0 – B3/B2 Physical Topology

The Physical Topology illustrates the proposed physical connections for the network infrastructure.

5.2 Network Switch Enclosures

Industrial environments can be dusty requiring network enclosures to provide protection against dust, so the switches maintain their life expectancy or mean-time-before-failure (MTBF). However, creating a properly sealed enclosure can cause non-industrial switches to not have proper ventilation and overheat, which is even more detrimental to the life of the switch. These facts have been taken into consideration when selecting the enclosure and the switches.

There are multiple types of network enclosures expected to be used for the Control System Network.

MDF – Pre-Configured Micro Data Center (Panduit PN: MDC82NL) with cutout for 20k BTU AC unit.

- 5G-B3-MDC-E07 - Located within grid E07 of B3/W3, adjacent to the existing DP-2 #26.28.30 enclosure.
- 5G-B2-MDC-A00 - Located within grid A00 of B2, adjacent to existing inter-building conduit entrance.

IDF – 26RU NEMA 4/4x/12 Enclosure with slot for AC unit. (Panduit PN:ZDF48-6RA)

- 5G-B3-ZDF-E07 - Located within grid E07 of B3/W3, adjacent to LCP1 18091 Panel
- 5G-B3-ZDF-F10 - Located within grid F10 of B3/W3, adjacent to LCP1 17181 Panel

NZE – Network Zone Enclosure. (Panduit PN: Z23N-1548)

- 5G-B2-NZE-A00 - On existing auxiliary channel at 6' AFF to BOE between 350 & 750ml Control Panels
- 5G-B2-NZE-A06 - On existing auxiliary channel above existing Filler/Capper PLC enclosure
- 5G-B2-NZE-A09 - On existing auxiliary channel above existing 750ml Full Line PLC
- 5G-W2-NZE-MCC4 – On new auxiliary channel at 12" above existing MCC4 enclosure.

Control Panel Enclosures

- OEM Control Panels
    - Lines 1 through to 8

5.2.1 MDF Core Enclosures

A Pre-Configured Datacenter Cabinet (Panduit PN: MDC82NL) will be used to install dedicated OT networking equipment (e.g., fiber distribution enclosure, cable management components, core switches, etc.). The cabinet will include the connectivity and cable management necessary to enable rapid installation of the switches.

The cabinet will be a NEMA Type 12 enclosure with 42U, one solid side panel, one side panel with cutout for 20k BTU AC, network cabling, patch panels, cable management, grounding, and casters

The MDF cabinet in B3/W3 will also house future IDC and IDMZ hardware.

5.2.2 IDF Enclosures

A customized Panduit Industrial Distribution Frame enclosure (Panduit PN: ZDF48-6RA) will be used to install dedicated networking equipment (e.g., fiber distribution enclosure, cable management components, distribution switches, etc.).

This design will specify that the IDFs in B3/W3 be housed in 26RU Dual Hinge NEMA 4/4x/12 Enclosure; Quarter-Turn Slotted Latches are Included Providing Access Control to the Enclosure; Accommodations for an Optional Air Conditioner; 316L Stainless Steel W/ #4 Stainless Finish; Installed Front and Rear Cage Nut Rails in Optimized Positions for Equipment Mounting; Installed Power Receptacle on ZDF48-6RA Only; Installed Fiber Enclosure (72 Fiber Capacity); Installed (2) 48-Port Patch Panels; Installed Cable Management; Installed Door Ground Whips; Equipment Ground Whips (One End); Installed Ground Bar; Infrastructure Ground Cable; Power Cords, Labeled and Length Optimized on ZDF48-6RA Only; 10" Long DIN Rail Mounting Provision; Cable/Fiber/Power Penetration Recommendation Template; Instructions for Cable Routing and Management.

5.2.3 NZE

A customized Panduit Industrial Network Zone Enclosure (Panduit PN: Z23N-1548) will be used to install dedicated zone networking equipment (e.g., fiber distribution enclosure, cable management components, sub-distribution switches, etc.).

The NZEs will be integrated Network Zone Systems, 24" x 36", 316 stainless steel enclosure, Stratix 5400 1783-HMS8TG8EG4CGR, 4 fiber 1783-SFP1GLX SFP Modules (SM fiber cords) for uplink(s), 16 copper STP Cat 6A patch cords and jacks for downlink(s), (2) HD Flex cassettes Redundant power supplies, Battery UPS (100-250V input).

DWG REF

Customer's Network Design v1r0 – B2/W2 Switch Locations
Customer's Network Design v1r0 – B3/W3 Switch Locations
Customer's Network Design v1r0 – B3 Core Cabinet Rack Elevation
Customer's Network Design v1r0 – B3 IDF Cabinet Rack Elevation
Customer's Network Design v1r0 – B2 MDF Cabinet Rack Elevation
Customer's Network Design v1r0 – B2 NZE Panels

The Switch Location drawings show expected room locations for each of the networking enclosures (MDF, IDF and NZE). The Rack Elevation drawings illustrate the new enclosures expected to be used in Customer's IACS network Project. Each Rack Elevation drawing includes an example population of the networking components to be utilized within the enclosure.

5.3 Cable Specifications

The following section further outlines the fiber and copper cable specifications. The Control System Network is designed in accordance with Open Device Net Vendors Association (ODVA) Ethernet/IP network specifications and/or the appropriate EIA/TIA specifications.

5.3.1 Fiber Optic Cable and Connectivity

Optical fiber will be utilized for the network infrastructure backbone. All switch-to-switch connectivity (Core, Distribution and Access) will utilize Single-mode fiber where possible.

5.3.1.1 Single-mode Fiber

Single-mode fiber has a smaller core size and uses a single wavelength to transmit light. The single wavelength prevents wavelength from overlapping and distorting light allowing further distance transmissions without the use of repeater. In some applications Single-mode fiber can reach distances up to 50 times multimode fiber distances.

Single-mode fiber also supports higher bandwidth capabilities at greater distances. Since fiber optic cabling is expected to last 15-20 years and new products are coming on the market with greater bandwidth, Single-mode fiber is recommended for new or upgraded network deployments.

Table 5.1 provides a comparison the various fiber types and the bandwidths each can support. Actual achievable bandwidth and distances are dependent on the fiber optic cable and fiber transceiver specifications provided by the manufacturers.

Table 5.1 - Fiber Media Comparison

			Model Bandwidth MHz-km								
			Overfilled w/LED		Effective w/VCSEL	100 Megabit	1 Gigabit		10 Gigabit		
Fiber Type	Fiber Designation	Core Size / Cladding (µm)	Wavelength @ 850 nm (MHz-km)	Wavelength @ 1300 nm (MHz-km)	Wavelength @ 850 nm (MHz-km)	SFP: 100BASE-FX 100Mbps (1310 nm)	SFP: 1000BASE-LX/LH 1Gbps (850 nm)	SFP: 1000BASE-SX 1Gbps (850 nm)	SFP: 10GBASE-SR 10Gbps (850 nm)	SFP: 10GBASE-LR 10Gbps (1310 nm)	SFP: 10GBASE-ER 10Gbps (1550 nm)
Multimode	OM1	62.5/125	200	500	n/a	2000 m 6562 ft	550 m * 1804 ft	275 m 902 ft	33 m 108 ft	n/a	n/a
Multimode	OM2	50/125	500	500	n/a	2000 m 6562 ft	550 m * 1804 ft	550 m 1804 ft	82 m 269 ft	n/a	n/a
Multimode	OM3	50/125	1500	500	2000	2000 m 6562 ft	550 m * 1804 ft	1000 m 3281 ft	300 m 984 ft	n/a	n/a
Multimode	OM4	50/125	3500	500	4700	2000 m 6562 ft	550 m * 1804 ft	1000 m 3281 ft	400 m 1312 ft	n/a	n/a
Singlemode	OS2	9/125				n/a	10,000 m 32,821 ft	n/a	n/a	10,000 m 32,821 ft	40,000 m (engineered links) 131,234 ft

* A mode-conditioning patch cord, as specified by the IEEE standard, is required regardless of the span length. Note how the mode conditioning patch cord for 62.5-µm fibers has a different specification from the mode-conditioning patch cord for 50-µm fibers.

5.3.1.2 New Fiber Optic Cabling

The new network infrastructure will require new fiber optic cabling. When selecting any optical fiber, the device port must first be considered and must be the same on both ends, (that is, port types cannot be mixed). In general, the port determines the type of fiber and glass grade. If the device port is SFP, it is possible to select compatible transceivers and the optimal transceiver for the application. Other considerations include the number of strands, mechanical protection, outer jacket protection, and expected cable routing.

The SVL (Stackwise Virtual Link) links used in the SV(Stackwise Virtual) platform for the Core switches must support 10Gbps. The links used to connect the Core switches to the Distribution switches will support 10Gbps. The links used to connect the Distribution switches to the Access switches will support 1Gbps.

The optical fiber to be used for backbone distribution between B2 and B3, routing the primary and secondary connections between the two MDF cabinets in B3 and B2, shall be listed as a 9um OS2 Indoor/Outdoor DDJ cable Panduit PN: FSJD924. The optical cable shall be:

- OS2 Single-mode, 24-strand, indoor/outdoor
- Dielectric Double Jacketed cable
- ROHS compliant
- Riser rated Fiber optic cable (OFNR-LS)

The optical fiber to be used for backbone distribution, routing the primary and secondary connections from MDF to IDF or NZE locations and also routing between IDF or NZE to Control Cabinets within the same building will be the Panduit PN: FSJD912). The optical fiber cable shall be:

- OS2 Single-mode, 12-strand, indoor/outdoor
- Dielectric Double Jacketed cable
- ROHS compliant
- Riser rated Fiber optic cable (OFNR-LS)

All new strands of Single-mode fiber optic cable should be terminated to OS2, splice-on connector, pre-polished duplex Latching Clasp (LC) connectors (Panduit PN: FLCS2/9SOCU9BU). The new cabling should connect to Fiber Adapter Panels (e.g., FAP; Panduit PN: FAP6WBUDLCZ) installed in Fiber Distribution Enclosures (e.g., FDE; Panduit PN: FCE1U, Panduit PN: FCE4U).

The following optical fiber patch cables should be used between the Fiber Adapter Panels and the network switches. The optical fiber patch cable shall be:

- Single-mode OS2, 9/125µm, OFNR, 2-fiber, duplex LC, push-pull, standard insertion loss, RoHS compliant, yellow (Panduit PN: F92ERQ1Q1SNM***

where *** denotes length in meters (001 – 050 in one-meter increments).

5.3.2 Copper Cable and Connectivity

Generally, copper cabling falls into two categories; horizontal (bulk) cable and patch or equipment cords. Horizontal cable will be used within the plant floor infrastructure and patch cords (patch panel to patch panel) or equipment cords (patch panel to active equipment or active equipment to active equipment) will be used within enclosures. Equipment cords will also be used for connections between switches and end devices.

For all connections within the control panels where the access switch is located, these cables will be factory-terminated patch cords. In cases where the end-point devices are located separately from the zone enclosure or the control panel, a "permanent link" copper cable will be installed for these connections.

If a permanent link copper cable is necessary, the cable will be terminated to 8P8C (i.e., RJ45) jacks on each end. In the Control Panels, the jacks will be placed in an appropriate patch panel or module adapter.

The maximum end-to-end channel length for an individual copper segment is 100m (328 ft.). This generally consists of a 90m (295 ft.) permanent link between the patch panel and the telecommunications outlet/connector, plus 5m (16 ft.) for patch cords or equipment cords at each end. However, the actual cable segment could be de-rated based on the environment or media selection.

All cable segment and cable connectors must follow the same Category specification; otherwise the installation is only as good as the weakest link. Higher category numbers indicate higher performance. Other considerations include EMI shielding, mechanical jacket, outer jacket protection and desired lifespan.

An example of the minimum copper cabling to be considered for new installations is a high-quality Category 6a cable. The specific copper horizontal cabling to be used will be as follows:

- Recommended Field terminated copper cabling should be:
  - Cat6A, UTP Vari-MaTriX, CMP, 4-pair, 23 AWG, 0.25"/6.5mm nominal outside diameter, solid conductor (Panduit PN: PUP6AV04GR-G).

All copper horizontal cabling throughout the project will be terminated with 8P8C (RJ45) connectors.

The following copper patch cables should be used to connect the copper patch panels to network switches.

- For patching in telecommunication rooms and enclosures:
  - Cat6A, UTP, CM/LSZH, 4-pair, 28 AWG, 0.19"/4.8mm nominal outside diameter, solid conductor, 8"/203mm length, green (Panduit PN: UTP28X8INGR)
  - Cat6A, UTP, CM/LSZH, 4-pair, 28 AWG, 0.19"/4.8mm nominal outside diameter, solid conductor, green (Panduit PN: UTP28X*GR)

  where * denotes length in feet (1 – 50 feet in one-foot increments, 55 – 130 feet in five-foot increments)

- For patching in control panels:

- Cat6A, SF/UTP, CMR, 4-pair, 26 AWG, 0.29”/7.4mm nominal outside diameter, stranded conductor, teal (Panduit PN: ISTPH6X**MTL)

where ** denotes length in meters (0.3 meter, 0.6 meter, 1 – 5 meter in 0.5 meter increments, 7 meter, 10 – 20 meter in five meter increments)

It will be the responsibility of the Contractor, in conjunction with Customer inc, to determine the quantity and length of each equipment cord needed.

5.4 Pathways and Routing

The pathways and routing section provide information and the materials needed to install the cabling. This section provides an overview of the Contractor requirements and best practices to be followed.

Actual routing shall be determined by the Contractor at the time of installation. Prior to installation of any materials associated with this project, the Contractor must:

- Coordinate with Customer inc for confirmation of preferred routing
- Provide “As-Built” drawings depicting the actual routes to be used

Cabling pathways include:

- The Primary and Redundant Optical Fiber Backbone Pathways, which separately route between the B3/W3 and B2/W2 MDF Cabinets.
- The Optical Fiber Backbone Pathways, which route the optical fiber connections from the MDF to IDF or NZE and from the IDF to Control Panels.
- Copper twisted pair downlink connections from the NZE switch locations to end points or Equipment Level Access switch locations.

Pathways and routing details including specific products required will need to be identified after the final network and control panel locations are determined and a contractor is able to review and evaluate potential paths to these locations. It is the responsibility of the installation contractor to confirm maximum cable distances are not exceeded.

5.4.1 Pathway Types

It is anticipated that a mix of pathway types (e.g., wire mesh cable tray, dedicated optical fiber pathways, conduit, etc.) will be required.

Within enclosed spaces, all cables shall be supported using means and methods suitable for the application and approved by the Authority Having Jurisdiction (AHJ). Suitable means and methods include properly installed wire mesh cable tray, dedicated optical fiber pathway or rigid metallic conduits.

When using conduit, the requirements of TIA-569-D standard shall be complied with. Standard conduit bodies are not permitted as they do not provide the required bend radius control.

The CSI MasterFormat Division 27 20 00 – Telecommunications Pathways Specifications, will need to be completed. The Telecommunications Pathways Specifications explain the requirements for installing the pathways using the products specified.

5.4.2 Conduit Installation Guidelines

Conduit will be required in certain areas to route the copper cabling between network enclosures, from network enclosures to control cabinets, or from enclosures and control cabinets to end devices. The details of this routing are to be defined by Customer inc. These guidelines are included here for reference.

Conduit and media installation shall meet or exceed the following installation requirements:

- TIA-569-D Commercial Building Standard for Telecommunications Pathways and Spaces
- Minimum Conduit Bend Radius 6X internal diameter of conduit
- Maximum conduit length between pull boxes shall be 100 ft.
- A pull point shall be provided if there are more than two (2), 90°-degree bends or equivalent in a conduit segment
- Maximum conduit segment length 280 ft.
- A conduit run shall serve not more than three (3) network outlet boxes
- Cable runs in conduit shall not exceed 40% fill rate or conduit fill capacities specified by cable manufacturer
- A pull string shall remain in the conduit to support future cable installation.
- If media must cross power lines, it should do so at perpendicular angles.
- Conduit should be run in the most direct route possible.

5.5 Cable Management

The Cable management from a network perspective is often an afterthought, or is entirely overlooked, during Industrial Network designs. Cable management should be designed to support the goals of manageability, reliability, security, and scalability. For the Control System Network, patch panels and cables will be used in all locations.

Table 5.2 lists the generally accepted practices for network cable management.

Table 5.2 - Generally Accepted Practices for Cable Management

Practice	Description
Include Sufficient horizontal and vertical cable management	Vertical cable managers between racks must be at least 83 mm (3.25 in) wide; 250 mm (10 in) is recommended for rows having two or more racks Vertical cable managers at the ends of a row of racks should be at least 150 mm (6 in) wide
Provide bend radius control wherever cables turn corners	• Slack managers and transitions into pathways should be designed with the proper bend radius • Cables should be guided into the horizontal and vertical cable managers by fingers that are engineered with radiused edges
Make the most of the space available	High-density solutions, like angled patch panels and vertical cable management with matched fingers, can fit more connections into a smaller footprint
Protect critical infrastructure	Create different levels of security with cabinet locks and cages

Practice	Description
Route cables to allow hot-swap ability	When routing cables away from the equipment, consider how the fan assemblies, modules, and power supplies are removed and inserted when it comes time for upgrades or replacements
Respect airflow patterns	Place patch fields in an alternating pattern with the switching infrastructure to maximize airflow
Document and manage changes to the physical layout	The patch field contains hundreds of ports, so it is essential that the patch field be labeled to allow technicians to quickly identify what each port and fiber strand represents
Benefits of using interconnection	• Less space • Fewer connections, thus lower insertion loss • Lower up front cost • Easier to trace
Weigh the trade-offs for interconnection versus cross-connection	Reasons to use interconnection: • Less space • Fewer connections, thus lower insertion loss • Lower up front cost • Easier to trace Reasons to use cross-connection: • Less possibility of damaging the switch • Only choice for switch cabinets • More flexibility • Compatible with Physical-layer management

For detailed information, refer to ANSI/TIA-1005 and ANSI/TIA-1005-1, Telecommunications Infrastructure Standard for Industrial Premises and its first addendum covering Industrial Pathways and Spaces. These documents are based on the ANSI/TIA/EIA-568-B and TIA-569-B series of standards, and they include appropriate allowances and exceptions to those standards for industrial premises. They also contain techniques to mitigate mechanical, ingress, climate/chemical, and electromechanical (M.I.C.E.) effects across multiple areas.

5.5.1 Cable Routing External to Enclosures

Table 5.3 defines cable routing external to enclosures. This is to minimize cross talk from nearby cables.

Table 5.3 - External Enclosure–to–Enclosure Routing Requirements

Cable in contiguous metal wireway or conduit?	Route Cable at this Minimum Distance	From Noise Source of this Strength
Yes	0.08 m (3 inches)	Category 1 conductors less than 20 Amps
	0.15 m (6 inches)	AC power lines of 20 Amps or more, up to 100 KVA
	0.3 m (12 inches)	AC power lines greater than 100 KVA
No	0.15 m (6 inches)	Category 1 conductors less than 20 Amps
	0.3 m (12 inches)	AC power lines of 20 Amps or more, up to 100 KVA
	0.6 m (24 inches)	AC power lines greater than 100 KVA

5.5.2 Cable Routing Internal to Enclosures

Table 5.4 defines the cable routing internal to enclosures.

Table 5.4 - Internal Enclosure–to–Enclosure Routing Requirements

Route Cable at this Minimum Distance	From Noise Source of this Strength
0.08 m (3 inches)	Category 1 conductors less than 20 Amps
0.15 m (6 inches)	AC power lines of 20 Amps or more, up to 100 KVA
0.6 m (24 inches)	AC power lines greater than 100 KVA

5.6 Cable Testing

As part of the physical infrastructure installation, all new cabling that is to be installed as part of the project should undergo certification testing and the test results documented. The cable test reports should typically be available for review prior to onsite network commissioning. The cable test reports should be provided in raw form (i.e., Fluke Networks LinkWare Database, .flw format) and in PDF format.

- Cable testing should include all new Fiber and Copper cabling
  - Channel tests (i.e., end device connections - end to end cabling including patch cords and equipment cords) should be conducted whenever possible
  - Permanent link tests (i.e., backbone infrastructure – MDF to IDF or NZE, IDF to Access, etc.) should only be used if a channel test is not possible
  - All cables including any unused should be tested
  - Cable test results provided should clearly identify the cable tested
  - Rockwell Automation recommends that an approved tester manufactured by Fluke Networks be used.
    - The field-test instrument should be within the 1-year calibration period and a copy of the calibration certificate made available.

- Fiber Optic Cable Testing
  - Tests typically include: Optical Loss Test Set (OLTS), Optical Time Domain Reflectometer (OTDR), and Fiber Microscope
- Copper Cable Testing
  - Tests typically include: Wire Map, Length, Propagation Delay, Delay Skew, DC Loop Resistance, DC Resistance Unbalance within a pair, DC Resistance Unbalance between pairs, Insertion Loss, NEXT (Near-End Crosstalk), PS NEXT (Power Sum Near-End Crosstalk), ACR-N (Attenuation to Crosstalk Ratio Near-End), PS ACR-N (Power Sum Attenuation to Crosstalk Ratio Near-End), ACR-F (Attenuation to Crosstalk Ratio Far-End), PS ACR-F (Power Sum Attenuation to Crosstalk Ratio Far-End), Return Loss, TCL (Transverse Conversion Loss), ELTCTL (Equal Level Transverse Conversion Transfer Loss), PS ANEXT (Power Sum Alien Near-End Crosstalk, Average PS ANEXT (Average Power Sum Alien Near-End Crosstalk), PS AACR-F (Power Sum Alien Attenuation to Crosstalk Ratio Far-End), Average PS AACR-F (Average Power Sum Alien Attenuation to Crosstalk Ratio Far-End)

Cable Test Guidance

The Cable Test Guidance document provides users with a guide to executing cable tests for new Industrial Ethernet network deployments. It describes the minimum test requirements for the most

commonly specified cabling used in Industrial Ethernet network designs today. It includes an overview for testing both copper and fiber optic networks.

Some cable manufacturers offer a system warranty for the cabling infrastructure. Each cable manufacturer will specify the certification testing requirements and documentation required for the registered links to be eligible for warranty coverage.

If the cable manufacturer offers a system warranty, then please refer and adhere to the requirements as specified by the manufacturer. The cable manufacturer's system warranty requirements may be more or less stringent than the Cable Test Guidance document referenced.

5.7 Cable Labeling and Identification

Cable labeling and identification requirements will need to be developed and agreed upon between the Contractor and Customer inc. It will be the responsibility of the Contractor to furnish and install labeling products according to these specifications.

The requirements for labeling and identification are identified in TIA-606-C. It will be the responsibility of the Contractor to furnish and install labeling products in compliance with this standard.

All components of the installed system shall be uniquely identified by location, function, unit, and sub-unit. All cables must be fitted with a self-laminating label surrounding the outermost jacket, placed within three 3" (75mm) of the end of the sheath at each end bearing the appropriate cable identifier indicating origin & destination.

Block terminated cables shall be identified with a wiring block identifier in place of the panel ID. Patch panels and enclosures shall be identified by the RU position of the upper leftmost corner of the panel. Ports within the patch panel shall be identified using a sequential numeric. Adapter panels within and enclosure shall be identified using an alphanumeric designator, assigned left to right, top to bottom. Ports within an adapter panel shall be identified using a numeric designator.

All equipment enclosures will be fitted with a self-adhesive label affixed to the top, center of the front and rear doors, bearing its respective identifier as directed by the Owner. Each Fiber Distribution Enclosure shall be fitted with a self-adhesive label, affixed, at the top center of the front and rear face. The label shall bear its respective identifier, in block characters.

Conduits and pathways must be labeled, at a minimum, within 18" (0.5m) of each end, where exposed and accessible. It is recommended to provide additional labeling every 10' (3m) of exposed length.

Customer's Network Design v1r0 – Cable Labeling Schema

The Cable Labeling Schema drawing provides a proposed method of labeling cables: Switch to Patch Panel, Switch to Switch, and Switch to End Device.

The CSI MasterFormat Division 27 10 00 - Structured Cabling System Specifications, will need to be completed. The Structured Cabling System Specifications explain the requirements for labeling and identification.

5.8 Power Specifications

The power specifications includes details on the UPS specifications and StackPower for stacked switches.

The Owner is responsible to provide the required Facility Power to the network infrastructure. This includes provisioning 120V/20A circuits to each IDF enclosure and provisioning two (2) 208V/30A Single-Phase power circuits terminated to NEMA L6-30R receptacles for each MDF cabinet.

5.8.1 Uninterruptible Power Supply (UPS)

Uninterruptible Power Supplies (UPS) provide uninterrupted power to a switch in the event the power source to the switch is disrupted. When a switch is powered off traffic flows on the network can be impacted and result in data and connection losses to equipment. The primary purposes for protecting switches with a UPS is to ensure the switch is not rebooted during power loss events and to condition power into the switch.

UPS hardware should be sized based on the number and types of network hardware connected to the UPS. Depending on the installation environment, industrialized UPS hardware may be required.

There are a few possible reasons for selecting a UPS for a given location, 1) condition power, 2) allow a device to remain powered on during a brief temporary outage/fault, or 3) keep a device powered on for a long power outage or until the backup generators come online.

Localized UPS hardware or centralized UPS hardware may be used. Localized UPS hardware is generally mounted in the enclosure and can be either DIN rail mountable or rack mountable. Centralized UPS hardware is often located in power distribution rooms or data communication rooms. For Customer inc, local UPS systems will be utilized for all servers and network switches.

It is recommended that Customer's and Panduit have discussions around providing appropriately sized UPS units for all switch enclosures/cabinets used for this design.

5.8.1.1 UPS Requirements (from User Requirement Specifications)

- The Data Center (DC) shall have adequately sized UPS installed in every server rack to provide up to 20 minutes of emergency power for all Servers in the DC.
- The UPS shall be monitored for diagnostics and an alarm shall be generated to notify system administrator via email if a problem occurs on the UPS system.
- All network switches are to be maintained by an in-panel UPS in case of a power failure. The UPS is to maintain the network for at least 20 minutes.

5.8.1.2 Local UPS – Rack Mounted Switches

For the MDF network cabinets, a rack mount UPS is needed. The recommended UPS is the Eaton 9PX UPS (Eaton PN: 9PX6K) with AC 200/208/220/230/240V - 5.4 kW - 6000 VA - Ethernet 10/100, RS-232, USB - PFC - 3U -19". This unit is also the standard offering in the IDC Server cabinet. It is recommended that all network cabinets (MDF & IDF) use the rack mount UPS models. Recommended rack mount UPS models are as follows:

- Qty x2 Eaton 9PX6K units for B3/W3 MDF
- Qty x1 Eaton 9PK6K unit for B2/W2 MDF
- Qty x1 Eaton 9PX-3000 unit for each IDF in B3/W3

Note

If equipped with a backup generator, Customer inc will need to verify the time required for the backup generator to come online and compare that with the time the UPS can maintain temporary power to the equipment. The total load should be calculated once final hardware is chosen for each networking cabinet to ensure the UPS meets the loading requirements.

Figure 5.1 shows the battery runtimes for the UPS. Runtimes can be extended if extended battery modules are used.

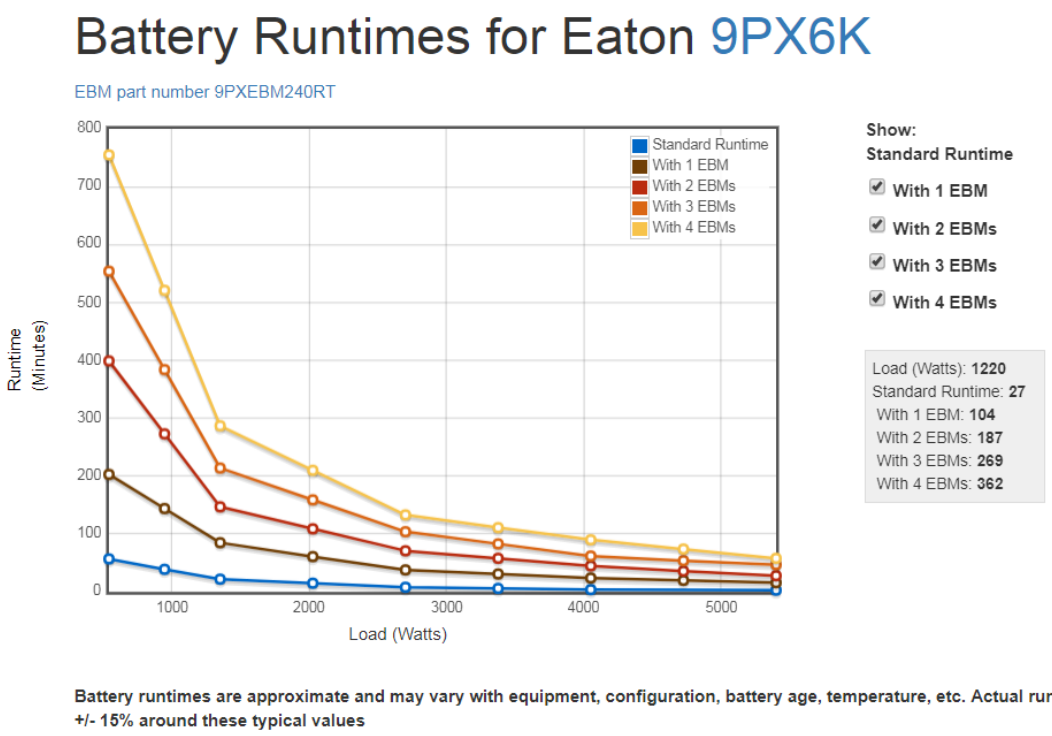

Figure 5.1 - Eaton UPS Battery Runtimes

For additional product information and technical specifications, refer to the Eaton Specification Sheet TD153001EN.

5.8.1.3 Local UPS – DIN Rail Mounted Switches

For locations that utilize DIN rail mounted switches (e.g., NZEs, Control Panels, etc.), battery-free UPS technologies are often used. These UPS use ultra-capacitors with a wide temperature range and a long lifetime. These UPS

systems can include EtherNet/IP ports embedded with CIP objects that allow faceplates and alarm integration with the IACS to improve system maintainability and uptime.

For the IDFs and NZE enclosures, DIN rail mounted capacitive UPSs are available.

- Panduit Uninterruptible Power Supply, 100 Watts, 24VDC in/out, DIN rail mount (UPS00100DC)

NZEs should include 24VDC power supplies, Panduit load sensing modules, and Panduit Uninterruptible Power Supply.

5.8.1.4 Network Infrastructure Power Consumption

Customer inc will need to verify the expected load for all the controls equipment to be protected by the UPS to ensure its capacity is not exceeded. If equipped with a backup generator, Customer inc should also verify the time required for the backup generator to come online and compare that with the time the UPS can maintain temporary power to the equipment.

Table 5.5 shows the power requirements for the expected network devices that will need to be connected to the UPS. The load is assuming steady state conditions.

Table 5.5 - Network Device Power Consumption

Switch Layer	Switch Model	Power Consumption Load
B3/W3 Core	Cisco C9500-40X-A	950 W Max per switch
B2/W2 Collapsed Core/Distribution Switch	Cisco C9500-16X-A	950 W Max per switch
Distribution (IDF)	Cisco C9300-24S-E/C9300-48S-E with C9300-NM-8X	715 W Max per switch
NZE/Access – Equipment Level Allen-Bradley	Stratix 5700 – All Models Stratix 5400 – All Models	30W Max per switch 120W Max per switch

5.8.2 Stack Power

The Cisco StackPower technology is an innovative feature that aggregates all of the available power in a stack of switches and manages it as one common power pool for the entire stack. The key aspect to the Cisco StackPower technology is the way power is supplied and distribution to a switch in the stack. A switch requires power to be provided at different voltage levels, such as 5V DC and 48V DC, and a traditional power supply provides those voltages. These requirements make the power supply more complex, and this complexity affects efficiency.

Cisco StackPower technology implies a new approach to power supply design and power distribution in a switch, but its effects are most significant in a stack of switches. The Cisco Catalyst 9300 Series Switches are designed for power supplies that provide a single power voltage. This approach simplifies the power supply design and allows aggregation of power, from power supplies in a single switch and across switches in a power stack. Cisco StackPower technology creates a pool of power that share a common load consisting of all the switches in the power stack. This capability to manage power as a shared resource is unique to a stack of switches that can operate as a single unit.

All power available in the power stack is combined into one single large pool of power, and the stack becomes a large single load to the power pool.

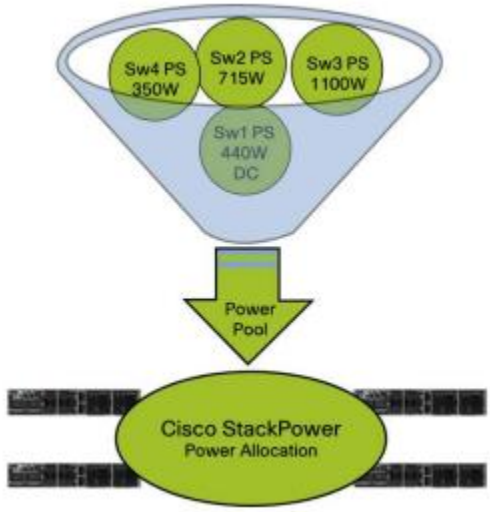

Figure 5-2 - Cisco StackPower; One Power Pool, One Load

A surplus of power in a power stack enables features such as Zero-Footprint RPS and 1+N redundancy instead of the classic 1:N redundancy with dedicated external RPS. Redundancy with Cisco StackPower is already inline (1+N), as opposed to being switched from one source to another, as in a classic RPS (1:N). The 1+N) redundancies are less susceptible to problems because the power is already available inline.

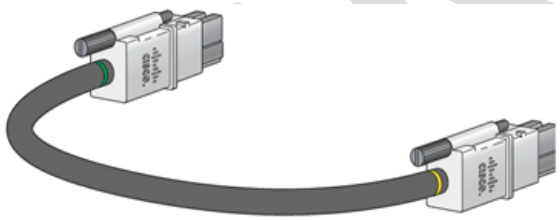

Figure 5-3 - StackPower Cable

5.9 Bonding and Grounding (Earthing)

A properly implemented bonding and grounding (earthing) system should be intentional, visually verifiable, and properly sized. It should be sized properly per TIA-607-C standards. Non-reversible two-hole compression style lugs shall be used (Optionally: use lugs qualified to NEBS Level 3 testing). #6 AWG TEBC (Telecommunications Equipment Bonding Conductor) should be utilized from the Secondary Bonding Busbar (SBB) to each floor-standing cabinet or equipment enclosure.

Equipment should be bonded via manufacturer's bonding screws w/ #6 AWG jumpers or, if not present, via mounting holes utilizing grounding hardware. For consistency and to meet the visually verifiability standards of TIA-607-C, it is also recommended to include proper grounding of control panels and end devices within them.

Note: *All specific grounding requirements for each device type and enclosure should be followed based on the installation instructions for each device or enclosure.*

All references to Grounding, Bonding, and Earthing in this document only discuss the Telecommunications Grounding & Bonding System as defined by TIA-607-C and TIA-942-B standards. Power and Utility Grounding & Bonding is governed by law as determined by NEC. Local and National codes and regulations should always be followed and supersede any recommendations within this document.

The requirements for a bonding and grounding (earthing) system that complies with TIA-607-C will be included in the CSI MasterFormat Division 27 10 00 - Structured Cabling System Specifications document. It will be the responsibility of the Contractor to furnish and install the grounding and bonding products according to these specifications.

The CSI MasterFormat Division 27 10 00 - Structured Cabling System Specifications, will need to be completed. The Structured Cabling System Specifications explain the requirements for a grounding and bonding system.

6 NETWORK SEGMENTATON

Network Segmentation is the creation of operational boundaries within the network. This helps in connecting specific plant operations with each other regardless of network affiliation and helps with isolation.

Network segmentation provides the following benefits:

- Maximize bandwidth use
- Reduces Latency and Jitter (variance of Latency) due to decreased broadcast messages on the network
- Increases data Availability, Integrity and Confidentiality
- Creates Layer 2 network boundaries based on operational dependencies
- Constrain broadcast and multicast traffic within a segmented domain
- Limits the fault domain ensuring network problems in one area do not affect another area
- Reduces the time it takes to isolate and troubleshoot the network & mean time to repair
- Provide the ability to create security boundaries

Two different forms of segmentation are possible in the Control System Network environment. These are physical segmentation and logical segmentation. These methods will provide the functional isolation required for a robust network as well as lay the foundation for creating secure boundaries within the network scheme.

Using both methods will facilitate the transition from the current network to the new network implementation while also segmenting different traffic types (e.g., SCADA, IO, etc.).

The following sections will detail the segmentation plan, including the physical segmentation requirements, the logical segmentation requirements, the functional zones that facilitate the segmentation plan, the VLAN schema, the IP address schema, and guidelines for capacity and expansion.

6.1 Physical Segmentation

Physical segmentation in the overall network will be achieved by utilizing separate switching hardware for the Customer inc Enterprise Network and the Industrial Automation and Controls System (IACS) Network. The use of separate hardware ensures that:

- Network anomalies and events that may occur on other network segments, do not affect the Control System Network (e.g., spanning-tree convergence).
- Traffic within other network segments does not use unnecessary bandwidth (i.e., Streaming Applications, Video Camera's, and IP Phones) needed for the higher availability requirements of the Control System Network.
- Potentially limit the Control System Network susceptibility to network security events that could potentially occur on the other network segments. Though no direct security features are included within this design, the foundation for a secure network is laid within the architecture.

6.1.1 Functional Traffic Type Segmentation

In the IACS network, Physical segmentation based on expected traffic capacity will be implemented wherever possible. To accomplish this, multiple communications cards in each Allen Bradley ControlLogix racks would be required.

6.1.2 Dual-Homed Network Interface Cards

Server or Host dual-homed network interface cards (NICs) should not be used for any reason, to create a connected bridge between the Customer inc Enterprise Network and the IACS Network. All communication should traverse the layer 3 boundaries that will exist between the two networks. This is to once again, provide a foundation, for enhanced security practices in the future.

Note: *This includes the combined use of wireless and wired technologies.*

6.2 Logical Segmentation

Logical segmentation will be used as the primary form of segmentation and will be deployed using distinct Virtual Local Area Networks (VLANs). VLANs provide the broadcast isolation, policy implementation, and fault-isolation benefits that are required in a highly available architecture.

Each VLAN will use a unique and distinct subnet. The benefit that a VLAN provides over a sub-netted network is that devices in different physical locations, not going back to the same router, can be on the same network. The Control System Network VLAN structure will allow grouped stations to segment logically by functionality, line, building, and other plant characteristics. VLAN segmentation also provides a level of isolation between zones in the event of a network anomaly. The Core Layer 3 (routing) switches will handle all routing between the VLANs in the Control System Network.

Note: *Some Multicast traffic cannot be routed between VLAN segments. If the Time to Live (TTL) of a Multicast protocol is 1, all Group Members will be required to remain on the same VLAN (as with ControlLogix redundancy). If the Multicast protocol TTL is greater than 1, this is not a requirement.*

6.2.1 Functional Zones

The functional zones identified will be logically segmented for the Control System Network. These zones were determined by the Customer inc Controls Engineering team based on the physical and functional areas.

The following Zones are present in the B3/W3 building:

- Logical Zones are broken down by sub-processing function. The Control Panels required to achieve this functionality are grouped into a single vlan.
- Switch Management Zone

The following Zones are present in the B2/W2 building:

- Logical Zones are broken down by sub-processing function. The Control Panels required to achieve this functionality are grouped into a single vlan.
- Switch Management Zone

6.2.2 VLAN Schema

The network will be configured with multiple Virtual Local Area Networks (VLANs) to support the operation of the Control System Network. Though the VLAN end device counts may seem small for some systems, they have been segmented by functional purpose to minimize topology interdependencies between systems and to assist in enforcing logical and physical isolation.

VLANs can be edited or added to as needed to meet future expansion.

Customer's VLAN and Subnets v1r1 – VLAN & IP Schema

The VLAN and Subnets workbook provides the VLAN IDs, names, IP Address ranges and description of their function.

6.3 IP Address Schema

The IP Address assignments and VLANs are used to create logical segmentation within the IACS network. IP address ranges are assigned to areas based on operational dependencies and maximum multicast IP segment sizes.

The subnet mask determines the number of node address that can be assigned within an IP address range. Within an IACS network the maximum number of nodes available should not exceed 1022, subnet mask of 255.255.252.0. This maximum is based on limitations within the Multicast protocol.

IP Address schema requirements are assumed as follows:

- Unique between functional zones.
- Allows for ease of maintenance and troubleshooting within the Control System Network.
- Ability to route between functional zones.
- Outside support can securely access the network from a remote location.
- A specific information flow strategy will be specified for communication above the Control System Network.
- Not an IPv6 schema.

The IP address assignments are designed to allow Classless Inter-Domain Routing (CIDR) to limit the routing table entries required to reach the Control System Network nodes. A complete IP Address list should be developed at the time of implementation.

Customer's VLAN and Subnets v1r1 – VLAN & IP Schema

The VLAN & IP Schema sheet provides the addressing ranges available within each network. Each subnet is assigned to a process area or function.

6.4 Capacity and Expansion

The physical and logical guidelines presented also must incorporate the realistic nature of future growth. This architecture is highly scalable both physically and logically.

- Expansion will be based on:
  - Functional Requirement

- Bandwidth
- Port Density
- Utilization

Additional requirements when expansion is needed include:

- Connection details of each end node will be assigned based on the manufacturer recommendations of either auto/auto or 100/Full, Flow Control Disabled, PortFast enabled.
- Future Network expansion beyond the original scope of this design will require switches that are compatible in all ways with the switches specified in this design.
- Unmanaged switches and hubs are prohibited for any reason, at any time, unless isolated from the rest of the network.

The following items are best practice guidelines used by Rockwell Automation during the design phase.

- There should be at least one (1) port available in every switch for maintenance.
- Switches should not exceed 80% port usage.
- Daisy chaining additional switches off the Access Switches is prohibited.
- Redundant media links where possible should be utilized between switches at all levels.

7 NETWORK CONFIGURATION DETAILS

This section will provide information surrounding the configuration guidelines for all switches within the architecture including:

- Switch Firmware
- Switch Capabilities / Switch Configuration Information
- Switch Port Maps

The information will provide a guide to the capabilities to be leveraged in the switch and the key commands used for implementing the capability. Final switch configurations are subject to change during the implementation phase based on the latest information available.

7.1 Switch Firmware

The firmware used in the Customer inc IACS Network is a critical aspect to ensure that the system functions as desired. The following sections will further detail the recommended firmware for the critical infrastructure hardware along with the associated known caveats for implementation.

Note: *The actual firmware to be deployed during the implementation phase may not align with the recommended firmware documented here.*

If a newer version has been released, the firmware/IOS should be evaluated to determine its use in the application. Pay close attention to the anomalies addressed in the release and any open anomalies. Before selecting to use a newer version, it is important to assess when it was released to understand its stability.

7.1.1 Cisco Catalyst 9500 Firmware

Recommended Firmware = Cisco IOS XE Release: Gibraltar-16.12.2 ED, Release Date: 23-Nov-2019
Link to release notes = Release Notes

7.1.2 Cisco Catalyst 9300 Firmware

Recommended Firmware = Cisco IOS XE Release: Gibraltar-16.12.2 ED, Release Date: 23-Nov-2019
Link to release notes = Release Notes

7.1.3 Allen-Bradley Stratix 5700/5400 Firmware

Recommend Firmware = IOS Release 15.2(7)E1a, Release Date: 1/2020
Link to release notes = Release Notes

7.2 Switch Capabilities / Switch Configuration Information

Switches must be managed and have the required capabilities to build and meet the availability and fault tolerance goals of the Control System Network. No unmanaged switches or hubs are to be authorized on the network or in the network infrastructure.

- All switches should at minimum support the following:
    - IEEE 802.1w Rapid Spanning- Tree Protocol (RSTP)
    - IEEE 802.1Q VLAN
    - VLAN Trunking Protocol (VTP)
    - IGMPv3, v2, v1 snooping and querying
    - SSHv2 (for remote configuration)
    - SNMP (for remote statistical analysis)
    - NTP (optional – to synchronize time across the network infrastructure)
    - IEEE 802.1x Port Based Access Control (optional)
    - Port Mirroring
    - SPAN/RSPAN
    - Quality of Service (QoS)
    - EtherChannel
    - Flex Links
- Core and Distribution switches should also support the following:
    - Redundancy (e.g., Stackwise Virtual or Stackwise 480 Technology)
    - Routing
        - Inter-VLAN Routing via the use of connected and static routing
        - Policy-Based Routing (PBR)

7.2.1 Spanning-Tree

The Spanning-Tree Protocol (STP) is designed to ensure a loop free Ethernet Network. Network loops are avoided by switches deterministically blocking network interfaces that create network loops and putting them into the "err-disable" state. If a link failure occurs on a network, Spanning-Tree is responsible for establishing new paths for network data.

The logical center of the network is the Spanning-Tree root bridge. An election process on the network will determine which switch is elected as the root bridge. Since Spanning-Tree establishes the logical center of the network, the default behavior of the root-bridge election process must be modified to allow for the optimal logical network topology in each architecture. This is required to ensure efficient data flow and limit the number of switches a data packet has to cross between nodes (due to specific ports that are placed into the blocking state thus avoiding network loops).

The architecture designed for the Control System Network is intended to be loop free within the switch-to-switch links. In this application, redundancy has been recommended for Core to Distribution, Core to NZE, and Distribution to Access by using a link aggregation protocol.

Cisco switches by default are configured for per-VLAN spanning tree plus (PVST+). The Stratix Series Switches by default are configured for Multiple Spanning-Tree Protocol (MSTP). All switches in the IACS network should be running the same spanning-tree protocol version. Therefore, the switches will need to be configured for a consistent version of spanning-tree protocol.

The recommended version of Spanning-Tree to be used in the Control System Network architecture is Rapid Per VLAN Spanning-Tree Protocol (Rapid PVST). Rapid PVST is the Cisco proprietary version of IEEE 802.1w.

The switches will need to be reconfigured for Rapid PVST to achieve spanning-tree consistency. To configure the spanning-tree mode, use the following command.

(config)# spanning-tree mode rapid-pvst

Although there are no planned loops within the architecture outside of the resilient links from the Access switches to the Distribution, NZE to Core switch and the Distribution switch to the Core switch, the Spanning-Tree configuration will still be vital to provide a stable network. The Core switch should be configured as the Spanning-Tree root bridge for all Control System Network VLANs.

By default, all switches within the architecture will have the same root bridge default priority. The switch with the lower MAC Address will by default, win the election process. This is not desirable. Therefore, it is recommended to change the Priority Value for the desired root bridge. Setting the priority value to the lowest value compared to the other switch priority value settings will give it precedence, resulting in the switch being selected as the root bridge. The applicable values for the Bridge ID are listed in Table 7.1.

Table 7.1– Spanning-Tree Priority Values Within the Bridge ID

Priority Value				Extended System ID (Set Equal to the VLAN ID)											
Bit 16	Bit 15	Bit 14	Bit 13	Bit 12	Bit 11	Bit 10	Bit 9	Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1
32768	16384	8192	4096	2048	1024	512	256	128	64	32	16	8	4	2	1

In this architecture, the Control System Ethernet Network Core located in the B3/W3 MDF cabinet should be configured as the spanning-tree root bridge. The following command is used to hard configure the spanning-tree root bridge.

(config)# spanning-tree vlan *vlan-id* root primary

The spanning-tree priority can also be configured. A lower priority value is given root precedence. Table 7.2 will define the switch priorities for spanning-tree priority configuration.

Table 7.2 – Spanning-Tree Priorities for each Control System Network Switch

Switch	Switch Purpose	Priority
5G-B3-MDC-E07-SW01	Core Switch	4096
5G-B2-MDC-A00-SW01	Collapsed Core/Distribution Switch	8192
5G-B3-ZDF-E07-SW01	Distribution Switch	16384
5G-B3-ZDF-F10-SW01	Distribution Switch	20480

The following command is used to hard configure the spanning-tree priority for each VLAN on each switch.

(config)# spanning-tree vlan *vlan-id* priority

Note: *Changing the Spanning-Tree configuration will cause a network convergence and will cause a temporary disruption to network traffic. Depending on the topology changes, normal network data flows will be disrupted for a minimum of 15 seconds up to several minutes and may cause the manufacturing network to shut down. Spanning-Tree configuration changes must be carefully planned and executed.*

7.2.2 VLAN

Support of IEEE 802.1Q VLAN protocols is a requirement within this architecture. Multiple VLANs will be used and have been previously defined in proposed VLAN Schema. The purpose of the deployment of VLANs is to limit the size of the broadcast domain and provide a more deterministic structured network.

Guidelines

- Define IACS control VLANs
    - Assign devices with similar traffic patterns or conversations
    - Group assets by function, role, logical area, physical area, or a hybrid of these
    - Limit the flow of traffic to only the required devices
- Do not use the default VLAN 1; VLAN 1 is seen a potential security vulnerability and is therefore recommended to always be shut down.
- Define and use a Native VLAN; do not use the default which is VLAN 1
- Define and use a Management VLAN for switch management functions; this VLAN should be a dedicated purpose VLAN
- Manually configure the VLANs in each switch (i.e., configure the switch for VTP transparent mode); Manual VLAN configuration lowers the risk of operational issues due to inadvertent VTP updates.

Additional VLAN configuration requirements are provided as follows:

- The use of VLAN 1 will be prohibited for use with control traffic, meaning VLAN 1 will be shut down on all switches. VLAN 1 is seen a potential security vulnerability and is therefore recommended to always be shut down.
- All switch interfaces will be configured either in a VLAN access mode state or as a Trunk port.
- Trunk ports will be configured between all switch-to-switch connections.
- A Native VLAN will be defined and configured for all inter-switch links. (e.g., VLAN 99)
- VLANs will be manually configured on all switches.
- VLAN pruning will be used to limit unnecessary VLAN traffic from trunk ports.
- All switches will be configured in VTP transparent mode.

7.2.2.1 Native VLAN

The Native VLAN represents traffic sent on a trunk interface using the IEEE 802.1Q encapsulation protocol that does not have a tag. Please note that it is only relevant for trunk ports as they are ports that can pass multiple VLANs over a single logical link.

The Cisco technology switches within this architecture use the default Native VLAN 1. As previously mentioned, the default VLAN 1 will be shut down on all switches and therefore a different Native VLAN needs to be configured on each trunk link. If the Native VLAN is not reconfigured on all switches and the default Native VLAN 1 is still active on one side of the trunk link, a trunk with mismatched Native VLANs error will occur. The following command is used to configure the Native VLAN.

(config)# interface *interface-id*
(config-if)# switchport trunk native vlan 99

7.2.2.2 VTP Mode and VLAN Pruning

VLAN Trunking Protocol (VTP) allows a user to make configuration changes centrally on one or more switches and have those changes automatically communicated to all the other switches in the network. Without VTP, you cannot send information about VLANs to other switches, requiring the VLANs to be manually created on each switch.

VTP can carry inherent risk as inadvertent changes could have significant impact to the IACS network. Therefore, it is recommended that VTP not be used in the IACS environment. This is done by configuring the switch in VTP transparent mode using the following command.

(config)# vtp mode transparent

With the switches configured in VTP transparent mode, a few more configuration steps are required. The first is defining all the VLANs on each switch. The second is pruning VLANs from trunk ports on switches that do not contain end devices (access mode ports) within a given VLAN.

Switches will be configured with the defined VLANs appropriate for the logical zone in which the switch resides, creating a simple and consistent switch configuration deployment across the architecture. Pruning of the VLAN traffic prevents a switch from flooding traffic across all trunk links even if a switch does not have access mode ports configured in a particular VLAN.

VLAN pruning will be manually configured on a per port basis for all ports in trunk mode. By default, a trunk interface carries traffic for all VLANs. To specify that only certain VLANs be allowed on the specified trunk, list only those VLANs. The following command is used to configure/prune the VLANs on a particular interface port.

(config)# interface *interface-id*
(config-if)# switchport trunk allowed vlan *vlan-id*

7.2.2.3 Management VLAN

A separate management VLAN should be utilized for the configuration and monitoring of the networking hardware. This keeps switch management traffic off of the process network while enforcing a different set of policies between the differing VLAN functions.

7.2.3 Internet Group Management Protocol (IGMP)

The use of Internet Group Management Protocol (IGMP) is essential to manage efficient delivery of multicast traffic prevalent on control system networks.

The ability to control multicast traffic in the control system network is a critical aspect of the network devices. The figure below shows how, without multicast control features, the bandwidth requirements in an industrial automation and control network application increase exponentially (versus a linear increase) with the increase in the number of devices. This is just an example of the type of network design, configuration, and implementation considerations specific to industrial automation and control protocols.

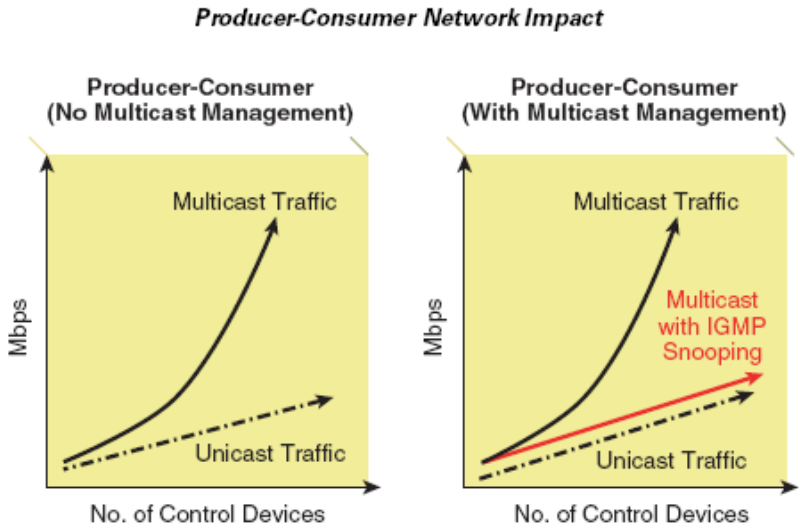

Figure 7.1 – Producer – Consumer Network Impact

Ethernet switches should be configured to perform IGMP snooping. When IGMP snooping is enabled, the switch listens to IGMP traffic and develops a table that lists the multicast groups and the end devices. When a multicast packet is received, the switch forwards it only to end devices that have signed up for that group. In addition, a Layer 3 switch that provides an IGMP querier function is required and must be properly configured.

IGMP Snooping and Querier function is required on all Control System Network Switches. The Primary IGMP Querier for the Customer inc Control System Ethernet Network is recommended to be the most stable switch on the network namely being the B3/W3 Core Switch. The IGMP Querier election process selects the switch with the lowest assigned IP address in the network that is configured to support IGMP Querier functionality. IGMP Querier function is configured on all switches to ensure the Querier functions are available on all switches in the event that any of the switches are disconnected.

The IP addressing design is limited to 8-bit node addressing by utilizing a subnet mask of 255.255.255.0. Host addressing utilizing 11 bits has the potential to create overlapping Multicast Addressing. In the event that the IP Addressing on the Control System Network is modified in the future, the subnet mask should be limited to no more than 22 bits. The maximum recommended subnet mask is 255.255.252.0. This restricts the host part of the IP address to be 10 bits or less, thus removing any chance of overlapping IGMP group addresses. This design has limited the subnet mask to 255.255.255.0 therefore mitigating this risk. The following commands are used to configure IGMP Querier and Snooping functionality.

```
(config)# ip igmp snooping
(config)# ip igmp snooping querier
```

IGMP has developed over time and three major versions of the protocol exist. They mostly build upon each other and are generally backward compatible. The majority of IACS EtherNet/IP devices support IGMP Version 2 and in this design, all the devices specified support IGMP Version 2. The switches used in this design use IGMP Version 2, as it is the default setting. All systems on the subnet must support the same version. A switch does not automatically detect Version 1 systems and switch to Version 1.

The version of IGMP will be verified and if the IGMP version is not version 2, then the following commands can be used to configure the device to use IGMP version 2 to avoid any compatibility issues.

(config)# interface *interface_number*
(config-if)# ip igmp version 2

7.2.4 QoS

The configuration of Quality of Server (QoS) provides preferential treatment to specific types of traffic at the expense of non-preferential traffic types. Two different forms of QoS exist and the type of QoS is dependent on the switch model. The two types are MLS QoS and MQC QoS.

The Stratix switches implement MLS QoS. The QoS policies are configured when the global macro is applied during Express Setup. The macro will configure QoS settings and will classify traffic types (e.g., CIP, PTP, etc.). Smartport macros then leverage the QoS policies, applying the policy based upon the end device specified during the switch port configuration.

The Cisco switches use either MLS QoS or MQC QoS depending on the switch model (e.g., the Cisco 3850 uses MQC and the Cisco 2960XR uses MLS). The QoS policies prioritizing EtherNet/IP control traffic types (CIP, PTP, etc), will be implemented on all Cisco Core and Distribution switches.

Guidelines

- Plantwide networks should prioritize IACS traffic (CIP) over other traffic types (HTTP, SMTP, etc.) to ensure deterministic data flows with low latency and low jitter.
- QoS should be deployed consistently throughout the EtherNet/IP IACS network.

7.2.5 Network Infrastructure Access

7.2.5.1 Passwords

Global password encryption, local user-password encryption, and enable secret are features available in the industrial Ethernet switches to help secure locally stored sensitive information.

Guidelines

- Enable automatic password encryption. Once configured, all passwords are encrypted automatically, including passwords of locally defined users.
- Define a local enable password using the enable secret global command.
- Define a line password with the password line command for each line you plan to use to administer the system.
- Use the Authentication, Authorization and Accounting (AAA) method for access control to the network infrastructure.

7.2.5.2 Secure Shell (SSH)

Secure Shell (SSH) is a protocol that provides a secure, remote connection to a device. SSH provides more security for remote connections than Telnet does by providing strong encryption when a device is authenticated. SSH also supports these user authentication methods:

TACACS+

RADIUS
Local authentication and authorization

RSA keys are required as part of the initial setup for configuring SSH. The following commands are used to configure the RSA keys.

```
(config)# hostname
(config)# ip domain-name domain_name
(config)# crypto key generate rsa modulus 4096
```

The following commands are used to configure SSH.

```
(config)# ip ssh version [1|2]
(config)# ip ssh {timeout seconds | authentication-retries number}

(config)# line vty line_number [ending_line_number]
(config-line)# transport input ssh
```

Guidelines

- Enable SSH access when available rather than the unsecured Telnet.
- Use at a minimum 2048-bit modulus size.
- SSH requires AAA or local accounts.

7.2.5.3 RADIUS Server

A RADIUS server should be implemented within an IDC Server environment and used to authenticate users for access to the IACS network infrastructure. A local user account is still required to allow access to the network infrastructure if the RADIUS server is down.

The following commands are used to first look to the RADIUS server and if it is down then look to the local users defined within the switch.

```
(config)# aaa authentication login default group radius local
(config)# aaa authorization exec default group radius local
```

The following commands are used to define the RADIUS server within the switch. The RADIUS server's name, ip address, and shared key are required. The shared secret text string used between the device and the RADIUS server must match.

```
(config)# radius server server-name
(config-radius-server)# address ipv4 ip-address
(config-radius-server)# key string
```

To restrict access to the Management VLAN, the following command is used.

```
(config)# ip radius source-interface vlan nnn
```

7.2.5.4 Port Security

Port security is a critical function of resiliency and reliability. Switch port security limits the access to the network by unknown devices and limits the number of devices or MAC addresses on any network port. Port security builds a list of secure MAC addresses in one of two following ways, configurable on a per-interface basis:

- Dynamic learning of MAC addresses—defines a maximum number of MAC addresses that will be learned and permitted on a port. Useful for dynamic environments, such as at the access edge.
- Static configuration of MAC addresses—defines the static MAC addresses permitted on a port. Useful for static environments, such as a server farm, a lobby, or a Demilitarized Network (DMZ).

Guidelines

- Apply dynamic learning on switch ports to limit the number devices that can access a port.
- Utilize the Error Disable feature to help protect the switch; configure the errdisable recovery interval to restore the port after a certain time period if the number of MAC addresses is exceeded.
- Disable unused ports or assign the ports to an unused VLAN or maintenance VLAN if appropriate.

7.2.6 NTP

Network Time Protocol (NTP) is designed to time-synchronize a network of devices. NTP runs over User Datagram Protocol (UDP), which runs over IP. NTP distributes time across the network. NTP is extremely efficient; no more than one packet per minute is necessary to synchronize two devices to within a millisecond of one another. NTP uses the concept of a stratum to describe how many NTP hops away a device is from an authoritative time source.

In a LAN environment, NTP can be configured to use IP broadcast messages instead. This alternative reduces configuration complexity because each device can simply be configured to send or receive broadcast messages. However, information flow is one-way only. The time kept on a device is a critical resource; you should use the security features of NTP to avoid the accidental or malicious setting of an incorrect time. Two mechanisms are available: an access list-based restriction scheme and an encrypted authentication mechanism.

Note: *An NTP source will need to be defined and access to the NTP source will need to be validated during the implementation process.*

To configure the Core switch to receive NTP updates from the NTP Source, the following commands are used. The source VLAN is usually the Management VLAN and the ip address of the NTP Source is assigned within this VLAN. Note: For systems monitored by Rockwell Automation's Remote Support group, the NTP Source is usually the Virtual Support Engineer (VSE) however, for this design, we recommend using a rack mount NTP hardware unit with external GPS antenna (Sonoma D12 Network Time Server).

(config)# ntp source vlan *nnn*
(config)# ntp server *ip-address* prefer

For added security, an authentication key can be created and used between switches. The key is shared between switches. The non-Core switches would receive their NTP updates from the Core switch and the following commands would be applied.

On the Core switch, these commands would be added.

(config)# ntp authentication-key *number-key* md5 *string*

(config)# ntp authenticate
(config)# ntp trusted-key *number-key*

On all other switches, these commands would be applied.

(config)# ntp authentication-key *number-key* md5 *string*
(config)# ntp authenticate
(config)# ntp trusted-key *number-key*
(config)# ntp source source vlan *nnn*
(config)# ntp server *CoreSW-ip-address* key *number-key* prefer

These commands will allow all other switches to receive NTP broadcast packets from the core switch, which will receive NTP packets directly from the rack mount NTP Server unit.

7.2.7 Dynamic Host Configuration Protocol (DHCP)

Due to the configured data connections and static nature of a manufacturing environment, Dynamic Host Configuration Protocol (DHCP) is sparingly used to assign IP addresses to end devices. DHCP is often used on the maintenance VLAN where connected laptops may receive an address locally, when necessary. This reduces the necessity for research of an approved static address prior to connecting to the network and could potentially provide easier connection when compared to static addressing.

7.2.7.1 DHCP Persistence (per port)

To configure a consistent control device IP address, DHCP Persistence can be configured on a per-port basis. This configuration requires additional setup during the initial installation but reduces the configuration time required to change out a failed device. The following guidelines are recommended when deploying DHCP persistence:

- Use all addresses configured in the DHCP Pool to avoid incorrect assignment of IP addresses
- Use the DHCP Snooping option to keep all requests restricted to the connected switch
- Not compatible with DHCP for Ring Devices

7.2.8 Speed and Duplex

Switch port interfaces and end device configurations must align speed and duplex settings. If one device (e.g., switch) is configured to auto negotiate the speed and duplex then the other device (e.g., end device) must be configured to auto negotiate. The same is true if one device is manually configuring with the speed and duplex; both ends must match.

Full duplex link connections are to be used to allow for bidirectional communication at all times on each link. This will prohibit collisions and therefore retries causing latency on the link.

Most new IACS devices are capable of 100Mbps (minimum) with some next generation IACS devices now being released with Gigabit interfaces on board.

For new networks, designs should be developed for architectures that can support 10Gbps.

7.2.9 EtherChannel

EtherChannel port groups treat multiple physical switch ports as one logical switch port. These port groups act as a single logical port for high-bandwidth connections between switches or between switches and servers. An

EtherChannel balances the traffic load across the links in the channel. If a link within the EtherChannel fails, traffic previously carried over the failed link changes to the remaining links. You can group multiple trunk ports into one logical trunk port, group multiple access ports into one logical access port, group multiple tunnel ports into one logical tunnel port, or group multiple routed ports into one logical routed port.

When you configure an EtherChannel, you create a port-channel logical interface and assign an interface to the EtherChannel.

- For Layer 3 interfaces, you manually create the logical interface by using the *interface port-channel* global configuration command. Then you manually assign an interface to the EtherChannel by using the *channel-group* interface configuration command.
- For Layer 2 interfaces, use the *channel-group* interface configuration command to dynamically create the port-channel logical interface. This command binds the physical and logical ports together. All ports in an EtherChannel must be assigned to the same VLAN or they must be configured as trunk ports.

Link Aggregation Control Protocol (LACP) will be used as the EtherChannel protocol within the Control System Network. To configure EtherChannels between the Core and Distribution switches, Core and NZE switches, and the Distribution and Access level switches, use the following commands.

(config)# interface *interface-id*
(config-if)# switchport mode trunk
(config-if)# channel-group *channel-group-number* mode *{active | passive}*

7.2.10 Routing

Plant production environments are traditionally static in nature. For this reason, static routing is usually deployed within the environment. Within the Control System Network, or traffic being routed internally to the network, connected routes will be automatically configured into the routing tables via connection of the network directly to the switch.

All routing for the Control System Ethernet Network will be performed at the B3/W3 Core switch. In addition, distributed routes will be configured between the B3/W3 site wide Core switch and the B2/W2 Collapsed Core/Distribution switch.

The following commands show an example for configuring a static route.

(config)# ip route *a.b.c.d* 255.255.255.0 *e.f.g.h*

Where a.b.c.d is the destination subnet and e.f.g.h is the ip address of the next hop router.

7.2.11 Interface Port configuration

The following example shows the typical and recommended access level switchport configuration that would be used to connect to a control system end device within the architecture (i.e., PLC, drive, etc.). Note: the commands may vary slightly based on the switch model and firmware being used.

(config)# interface FastEthernet x/y
(config-if)# description *Add port specific description*

(config-if)# switchport access vlan *xxx*
(config-if)# switchport mode access
(config-if)# switchport port-security
(config-if)# speed 100
(config-if)# duplex full
(config-if)# spanning-tree portfast
(config-if)# spanning-tree bpduguard enable
(config-if)# end
Switch # copy running-config startup-config

7.2.12 Stratix Switch Global Macro

The Stratix Series managed switches can be setup for IACS applications quickly by utilizing pre-engineered macros that set (configure) common switch parameters used in industrial network applications. Running Express Setup on the Stratix switch applies the Rockwell Automation Global Macro. Global macros configure switch wide parameters and Smartport macros configure switch port parameters based on the end device to be connected. It is recommended that Express Setup be utilized during commissioning of Stratix 5700/5400 Access layer switches.

7.2.13 Errdisable Recovery

Cisco and Stratix network hardware will place an interface into errdisable state (turns the port off) when the interface experiences certain errors. When in the error disable state, the interface will not forward traffic. When error disable recovery is enabled the interface will attempt to turn back on when the network hardware detects the error state has been corrected. To allow the auto recovery option to take effect, error disable recovery needs to be enabled. A time is used to determine how long the device should wait until attempting to recover from the error disable state. The default timer value in the network hardware configurations will be modified to attempt recovery in 60 seconds.

Error recovery configuration example:

errdisable recovery cause udld
errdisable recovery cause bpduguard
errdisable recovery cause security-violation
errdisable recovery cause channel-misconfig (STP)
errdisable recovery cause pagp-flap
errdisable recovery cause dtp-flap
errdisable recovery cause link-flap
errdisable recovery cause sfp-config-mismatch
errdisable recovery cause gbic-invalid
errdisable recovery cause l2ptguard
errdisable recovery cause psecure-violation
errdisable recovery cause port-mode-failure
errdisable recovery cause dhcp-rate-limit
errdisable recovery cause pppoe-ia-rate-limit
errdisable recovery cause mac-limit
errdisable recovery cause vmps
errdisable recovery cause storm-control
errdisable recovery cause inline-power
errdisable recovery cause arp-inspection
errdisable recovery cause loopback

errdisable recovery cause small-frame
errdisable recovery cause psp
errdisable recovery interval 60

7.2.14 Telnet Support

The following commands for Cisco and Stratix hardware are to be used to support telnet to the switches. If no SSH services or a centralized authentication server is available and telnet is used to manage the network hardware, then the following commands are recommended.

service nagle
service tcp-keepalives-in
service tcp-keepalives-out

7.2.15 Switch Logging Configuration

The following commands are recommended to modify the default logging behavior for switches and routers.

service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service sequence-numbers
logging buffered 16384
no logging console

7.3 Networking Infrastructure Hardware Port Maps

Understanding and defining a consistent port mapping schema is vital for decreasing mean-time-to-repair, change control management, and during the migration and implementation phase. This section provides examples of port mappings for the Control System Network switches.

Customer's Network Port-Maps-1 v1r0
Customer's Network Port-Maps-2 v1r0

The Port Maps document provides an example of the port map schema for the network switches. It includes the configuration, intended use and description for each interface port.

8 DISASTER RECOVERY AND CONFIGURATIONS BACKUP

Carefully thought and implemented, a Disaster Recovery plan, regardless of the industry type, allows an organization to recover from unforeseen events, such as security breaches, hardware failures or natural disasters.

It is recommended that the running configuration for all switches should be backed up periodically. Care must be taken to ensure sending the configuration files does not affect normal data flows. The backups should be staggered and setup on a periodic basis (possibly weekly or monthly based on the normal frequency of changes).

The location where the configuration files are backed up should be available to designated engineers or network administrators. They should be able to access the files and use them with a live spare switch to quickly recover a failed switch.

The “live spare switch” is an additional switch deployed on the network and powered (hot). Ideally, a site will have at least one spare of each switch model used in the architecture. In larger applications, more than one hot spare geographically dispersed may be desired.

The “live spare” will have a basic configuration that allows the switch to be accessed via a secure connection. When a production switch fails, authorized personnel can obtain the failed production switch’s backup configuration from the server and load it into the live spare switch.

Then any available field engineer or electrician can pick up the live spare and replace it with the failed switch. No networking skills are required for the physical swap. Since the configuration uploaded and the hardware are the same as the failed switch, network connectivity can resume as soon as the live spare switch boots up successfully.

This solution brings an enormous advantage in minimizing the network downtime caused by a hardware failure, therefore reducing the impact on production. Once replaced, a new “live spare” switch can be put in place at a later time.

9 BILL OF MATERIAL

9.1 Detailed Bill of Materials

The Bill of Materials (BOM) accounts for all equipment required to achieve the Logical design as presented in this report.

Customer's BOM v1r0

The workbook provides the detailed Bill of Materials (BoM) for the Customer inc Control System Network Design.

The Bill of Materials (BOM) to implement the physical installation will need to be developed within the Construction Specification development phase and amended by the installation Contractor as necessary. Once the Contractor has completed a walk-through of the site and identified the actual material required to implement the design, a more detailed/refined BOM can be completed.

END OF DELIVERABLE

10 APPENDIX

10.1 Commonly Accepted Industrial Automation Abbreviations

Abbreviation	Definition
AC	Automation Control
AFT	Adapter Fault Tolerance
ANSI	American National Standards Institute
AP	Application Software
BOM	Bill of Materials
CIP	Common Industrial Protocol
CLX	ControlLogix
CNC	Computer Numeric Controllers
CPR	Coordinated Product Release
CRC	Cyclic Redundancy Check
CSA	Canadian Standards Association
CSN	Control System Network
DCS	Distributed Control System
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
FQDN	Fully Qualified Domain Name
FTA	FactoryTalk Activation
FT	FactoryTalk
FTP	Foil Twisted Pair
HMI	Human Machine Interface
HTML	Hyper Text Markup Language
IACS	Industrial Automation Control System
IC	Industrial Controls
ICM	Integrated Condition Monitoring
IEC	International Electotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPSec	Internet Protocol Security
IPT	Internet Protocol Telephony
ISO	International Organization for Standardization
LAN	Local Area Network
MCC	Motor Control Center
MITM	Man-In-The-Middle
MTBF	Mean Time Between Failure
NEC	National Electric Code
NEMA	National Electrical Manufacturers Association
NFPA	National Fire Protection Agency
NIC	Network Interface Card
ODVA	Open DeviceNet Vendors Association
OEM	Original Equipment Manufacturer
OI	Operator Interface
OSHA	Occupational Safety and Health Administration
OSI	Open Systems Interconnection
PAC	Programmable Automation Controller
PLC	Programmable Logic Controller

Abbreviation	Definition
PLX	ProcessLogix
RSI	Rockwell Software, Inc.
SCADA	Supervisory Control And Data Acquisition
SCM	Supply Chain Management
SDLC	Software Development Life Cycle
SFT	Switch Fault Tolerance
SI	System Integrator
SLC	Small Logic Controller
SSTP	Screen Shielded Twisted Pair
STP	Shielded Twisted Pair
TIA	Telecommunications Industry Association
UDP	User Datagram Protocol
UTP	Unshielded Twisted Pair
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAN	Wide Area Network

10.2 Additional References

10.2.1 Managed Security Services

Managed Security Services encompass a wide range of offerings to help you manage and maintain your plant floor security.

- **Remote Monitoring** can be offered in conjunction with our InSite Services or can be implemented in an ad-hoc, non-real-time fashion to diagnose your long-term potential security and network issues.
- **Incident Response** includes management, coordination and resolution services that entail assessing / verifying security incidents and providing you with guidance on further action as necessary.
- **Disaster Recovery**, in support of your Disaster Recovery Plan, includes assisting you when a business continuity-impacting event has occurred. Rockwell Automation can offer you a range of support from technical support to managing the disaster recovery actions.

10.2.2 Recommended References For Policy Generation

- ISA SP-99 TR99.00.01 (Technical Report 1)
- ISA SP-99 TR99.00.02 (Technical Report 2)
- ISA SP-99 d99.00.01 (Models, Definitions, and Terminologies)
- ISA SP-99 d99.00.02 (Security Program Considerations)
- ISO 17799 (properly interpreted and revised for a control environment)
- NIST SP-800 Documents (freely available)
- NIST PCSRF activities (contact NIST PCSRF for more information)
- Internal IT policies and standards
- Internal corporate information management policies

10.2.3 ISA

- ANCI/ISA S95, multiple sections
- ISA-TR99.00.01-2004, Security Technologies for Industrial Automation and Control Systems
- ISA-TR99.00.02-2004, Integrating Electronic Security into Manufacturing and Control ISA SP-99 Security, in draft form

10.2.4 Governmental

- US FDA Modernization Act
- 21CFR Part 11
- US HIPAA
- US Sarbanes – Oxley Act
- EU E-Signatures
- Annex 11 of the EU GMPS
- FDA Supply Chain Traceability Initiative
- EU Date Product Safety
- Directive
- FDA Bar Code Initiative
- FDA GMP Initiative
- FDA PAT Initiative
- FDA Counterfeit Drug Initiative
- Drug Pedigree Laws
- IEEE Standards
- HACCP
- Bioterrorism Act

10.2.5 NIST

- NIST SP 800-12 The NIST Handbook
- NIST SP 800-14 Generally Accepted Principles and Practices for Securing Information Technology Systems
- NIST SP 800-18 Guide for Developing Security Plans for Information Technology Systems
- NIST SP 800-26 Security Self-Assessment Guide for Information Technology Systems
- NIST SP 800-27 Rev A Engineering Principles for Information Technology Security (Baseline for Achieving Security)
- NIST SP 800-30 Rev A Risk Management Guide for Information Technology Systems
- NIST SP 800-37 Guide for the Security Certification and Accreditation of Federal Information Systems
- NIST SP 800-53 Recommended Security Controls for Federal Information Systems
- NIST SP 800-55 Security Metrics Guide for Information Technology Systems
- NIST SP 800-60 Guide for Mapping Types of Information and Information Systems to Security Categories
- NIST SP 800-65 Integrating IT Security into Capital Planning and Investment Control Process
- NIST SP 800-70 Security Configuration Checklists Program for IT Products
- NIST SP 800-72 Guidelines on PDA Forensics

- FIPS 199 Standards for Security Categorization of Federal Information and Information Systems

10.2.6 The Institute Of Electrical And Electronics Engineers

- ”Software Engineering Standards”, Third Edition, August 1990: (Get the latest versions).
- ANSI/IEEE Std 729-1983 “Glossary of Software engineering Terminology”
- ANSI/IEEE Std 730.1-1989 “Software Quality Assurance Plans”
- ANSI/IEEE Std 828-1983 “Software Configuration Management Plans”
- ANSI/IEEE Std 829-1983 “Software Test Documentation”
- ANSI/IEEE Std 830-1984 “Software Requirements Specifications”
- ANSI/IEEE Std 1008-1987 “Software Unit Testing”
- ANSI/IEEE Std 1012-1986 “Software Verification and Validation Plans”
- ANSI/IEEE Std 1016-1987 “Software Design Descriptions”
- ANSI/IEEE Std 1028-1988 “Standard for Software Reviews and Audits”
- ANSI/IEEE Std 1042-1987 “Guide to Software Configuration Management”
- ANSI/IEEE Std 1058.1-1987 “Standard for Software Project Management Plans”
- ANSI/IEEE Std 1063-1987 “Standard for Software User Documentation”