**Network & Security Services**

Because Infrastructure Matters

*CONFIDENTIAL DOCUMENT*

# NETWORK & SECURITY STANDARD ASSESSMENT

**Prepared for**

***Customer A***

***Location A***

**3/8/2016**

**DRAFT**

**Scope of Work Ref #: OCNOKR0482**
**Project #: 7000295741**
**RA Document Version: 1.0**

LISTEN. THINK. SOLVE.℠

Allen-Bradley • Rockwell Software

Rockwell Automation

# CONTENTS

# FIGURES & TABLES

# 1 DOCUMENT CONTROL

## 1.1 Interview Participants

**Table 1:1 – Interview Participants**

| Date | Name | Title | Company |
|---|---|---|---|
| 2/8/2016 | Brent Groh, P.Eng. | Network and Security Consultant | Rockwell Automation |
| 2/8/2016 | Interviewee A | Maintenance Electrician | Customer A |
| 2/8/2016 | Interviewee B | Information Technology – MRP Integration | Customer A |
| 2/8/2016 | Interviewee C | Information Technology | Customer A |
| 2/8/2016 | Interviewee D | Manager of Strategic Maintenance | Customer A |

## 1.2 Reference Documentation

**Table 1:2 – Reference Documentation**

| Date | Version | Description | Author |
|---|---|---|---|
| 1991 | v2 | Purdue Reference Model for Control Hierarchy | Purdue Research Foundation |
| Nov-11 | 1.0 | ISA-99/IEC62443 Industrial Automation and Control Systems Security | International Society of Automation |
| Jun-11 | - | NIST 800-82 Guide to Industrial Control Systems Security | National Institute of Standards |
| Jan-07 | - | Network Infrastructure for EtherNet/IP: Introduction & Considerations | ODVA |
| Oct-09 | - | DHL INL/EXT-06-11478 Strategy for Securing Control Systems | Department of Homeland Security |
| Sep-11 | 3.0 | Converged Plantwide Ethernet Design and Implementation Guide | Cisco and Rockwell Automation |
| Oct-11 | - | Top 10 Recommendations for Plantwide EtherNet/IP Deployments | Cisco and Rockwell Automation |
| Jun-13 | - | Segmentation Methods Within the Cell / Area Zone | Cisco and Rockwell Automation |
| Jul-15 | - | Securely Traversing Data across the Industrial De-Militarized Zone | Cisco and Rockwell Automation |

## 1.3 Revision History

| Date | Version | Description | Author |
|---|---|---|---|
| 3/8/2016 | 1.0 | Original draft document release for review with Customer A | Brent Groh – Rockwell Automation |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

## *1.4 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 A environment. This information is to be considered as preliminary and informative, and is subject to review and revision at any time by Customer A or Rockwell Automation. This document further includes information that may be proprietary, confidential, or otherwise sensitive from both Customer A and Rockwell Automation. Prior to any dissemination outside of Customer A or Rockwell Automation of any part or whole of this document, both companies must agree in writing. The information contained herein may be considered volatile and preliminary, subject to revision, addition, or removal.

The information in this document is intended to provide a grade with respect to industry regulations, standards, and best practices. All recommendations involving changes to the Industrial Automation Control System (IACS) network should be discussed thoughtfully and no changes should be implemented without careful consideration and testing of the impact they may have on operations within the IACS.

# 2 BACKGROUND & OVERVIEW

In February 2016, Rockwell Automation provided Customer Support and Maintenance consulting services to Customer A in Location A. The consultation services were for a Standard Network & Security Assessment as detailed in Scope of Work reference number OCNOKR0482.

This report provides a summary of the observations that were made and the issues that were found during Rockwell Automation's consultation at the Location A site of Customer A, as well as during other related discussions with Customer A. The details of the network assessment provided throughout this report will lay the framework for moving forward and potentially rectifying the issues found during the assessment. The subsections below provide the background and overview of the consultation services performed, with a high-level summary of the assessment results that are provided in detail within the remaining sections of this report.

Rockwell Automation would like to thank Customer A for utilizing the Connected Services Customer Support and Maintenance consulting services. As a world-class supplier of high-speed factory-floor equipment, Rockwell Automation also offers one of the most comprehensive suites of assessment and design consultation services in the industry, which Rockwell is pleased to implement at Customer A Location A facility.

If Customer A has any questions or requires any clarification of the data in this report, please do not hesitate to contact Rockwell Automation. Please be assured that Rockwell Automation's professional consulting team is always at Customer A's service should there be any further customer support or maintenance needs in the future.

**NOTE** The definitions of abbreviations for common terminology that are used throughout this report, as well as external reference documentation pertaining to this report, are provided in **Section 9**.

## 2.1 Executive Summary

The goal of completing our standard network assessment offering at the Customer A, Location A facility is to provide an in-depth overview of the Industrial Automation and Control System (IACS) network. The key aspects of the production network that are evaluated are as follows:

- Physical Network Infrastructure (Detailed in Section 5 of this Document)
- Logical Network Infrastructure (Detailed in Section 6 of this Document)
- Industrial Security and Safety (Detailed in Section 7 of this Document)

In addition to these items, a comprehensive listing of the network infrastructure hardware used in the production environment is also included in Section 4 of this document. This details the part numbers, current state of each device, the associated environmental aspects of the infrastructure equipment, and the life cycle information for planning purposes.

Finally, an evaluation of the production network with special consideration as to any issues that were outlined during discussions while on-site is completed. This helps in qualifying potential items of concern and provides the opportunity to offer potential avenues for remediation should it be desired.

Based on these key focus areas of the standard network architecture review, the details listed in the following subsections are the main summary points regarding the current issues being faced and the findings of the network architecture review. Please note that the goal is to provide further insight into the current operation of the network while offering opportunities for improvement in production

environment efficiencies via the IACS network. Please do not hesitate to contact any of the available resources within Rockwell Automation's Connected Services group to discuss these points further.

## *2.1.1 Specific Network Related Issues as Outlined by Customer A*

The main network related items outlined by Customer A, Location A as current issues within their production environment were as follows:

- Slow uploading time from some PLCs on-site
- Slow times in transferring data between specific PLCs via message (MSG) instructions
- Production downtime has been experienced without specific related causes being determined and may point to a network related issue

## *2.1.2 Identified Potential Causes of Network Related Issues*

To understand the potential causes and impact of the issues listed in Section 2.1.1, a thorough evaluation of all aspects of the network equipment was completed. During this time a few key items were found:

- **Single Control Subnet / VLAN Architecture –** A single subnet with 254 available IP addresses (ie: 192.168.10.0 with 255.255.255.0 or /24 subnet mask) is used to communicate between all Programmable Automation Controllers (PAC) / Programmable Logic Controllers (PLC) in the plant. Additionally, multiple Ethernet end devices are also placed on this single VLAN that communicate directly with their local associated PAC / PLC. Although this approach provides ease of deployment in the current network architecture, various issues can occur with this style of "flat" network as follows:
  - Introduces a single fault domain whereby potential network related issues that start in one area of the plant can easily propagate and affect other areas. This stems from the fact that traffic is not segmented between various mills / processes.
  - A single VLAN architecture severely limits the growth of the network and can quickly exhaust the available number of IP addresses as more Ethernet enabled devices are placed on the network. It is important to note that most new IACS devices (ie: drives, I/O, starters, etc.) have Ethernet ports on-board resulting in significantly increased requirements for IP addressing availability during equipment upgrades or retrofits.
  - Introduces a large broadcast domain decreasing the determinism of the network. Determinism is a measure of the variability of the latency in the network (time that it takes for a packet to traverse the network from sender to receiver) and should be kept to a minimum on IACS systems.
- **Physical Cabling, Routing, and Installation –** In many situations the state of the Ethernet cabling within cabinets may be creating issues within the network. The physical cabling and routing aspect of industrial Ethernet is a critical consideration as Electro-Magnetic Interference (EMI) is prevalent in the industrial environment. This can create significant communication issues on the Ethernet network within the IACS and pose challenges during troubleshooting. For further information on the specific findings within our network assessment please reference Section 5 of this document. For general guidelines and recommendations on deploying Ethernet in an industrial environment please consult the "Network Infrastructure for EtherNet/IP: Introduction and Considerations" document referenced in Section 1.2.

- **Non-Optimized Managed Switch Configurations –** The configuration of the managed switches in the plant network have often been left at the default state aside from solely assigning an IP address to the switch. Default configurations do not provide prioritization of EtherNet/IP traffic as should be completed on an IACS network. Additionally, the default configuration on the Cisco switches that are used to aggregate the connections for the mills will actually prioritize video, voice and standard Ethernet traffic over all others. This places EtherNet/IP packets far lower in the switching queue decreasing the determinism and increasing the latency of the IACS network.

- **CIP Bridge Backplane Segmentation –** In a few situations (ie: Mill 1 Quick Settings panel), multiple Ethernet cards are used in the ControlLogix rack to segment traffic between the plant subnet and local machine control subnets. Although this is a suitable method to segment traffic and limit broadcast domains as per our "Segmentation Methods Within the Cell / Area Zone" document detailed in Section 1.2, it does not provide a scalable architecture that allows for future expansion. This is primarily due to the fact that there are limits on the number of communication cards possible in a ControlLogix rack. Additionally, it is important to note that it does not provide the ability to obtain a unified architecture that allows for direct communication from the plant network to an end device. This can greatly limit the troubleshooting capabilities (ie: drive embedded webpages cannot be accessed from the plant network to help in diagnosing issues) as well as impact the future readiness and scalability of the network.

### *2.1.3 Potential Follow-Up Items for Network Improvements*

After an in-depth review of the existing network related infrastructure and with special focus being given to resolving the issues presented by Customer A, Rockwell Automation sees some key areas within the production environment where improvements to the current network can be made. These improvements look to target specific aspects of the network by increasing performance and resiliency, expanding ease of use when maintaining / upgrading equipment, providing security enhancements, and bringing together an all-encompassing design approach so that operating efficiencies can be realized.

With Rockwell Automation's history in successful deployments of networking upgrades and optimizations, we believe that we are well positioned within the industry to provide Customer A with the services necessary to successfully implement these recommendations and maintain them throughout their production lifecycle. Please do not hesitate to contact any of the resources available within Rockwell Automation's Connected Services division to discuss these items further.

Please be aware that the deployment of the items listed in this section is not recommended for completion in a single network overhaul. The upgrades are a process that occur throughout multiple planned phases within a larger overall project. This process is one that is to be well defined and scoped at the onset of the project to ensure that all parties involved understand their responsibilities and the related impacts to their area of focus.

The following are the key items that Rockwell Automation believes should be evaluated in relation to improving the network at Customer A, Location A:

- **Develop an Industrial Networking Plan –** One of the key initial aspects within any network upgrade is to come up with a set of standard design principles that will be deployed throughout the process. This set of design principles is critical to enabling a future ready architecture that can scale to the requirements of your production environment as more machines are upgraded and Ethernet enabled end devices are added. Please note that this networking plan is something to be developed prior to any components being selected or design decisions being made. The key takeaway is that a suitable design for your application environment with proper infrastructure should be the prime focus when looking for a future ready, high performance production network.
  For further information on the key aspects of designing for Ethernet deployment into your production network, please refer to the Top 10 Recommendations for EtherNet/IP Plantwide Deployments document referenced in Section 1.2.

- **Providing a Highly Deterministic and Highly Available Network via the Use of Segmentation and Resiliency –** One of the key considerations for industrial plant networks is to limit the latency of packets (time it takes for the traffic to traverse the network from sender to receiver) while also minimizing the variance of the latency so that a highly deterministic network can be obtained. This is a critical function for IACS networks as controls devices require low latency and high determinism to ensure proper operation and minimize the potential of device timeouts.

  As of this point within the Customer A, Location A production environment all plant level communications with PLCs / PACs are done via a single subnet (192.168.10.0 / 24). It is important to note as well that various end devices are also placed in this same subnet creating additional traffic due to the Class I implicit EtherNet/IP messages from the controller to the end device for control.

  To provide a highly deterministic network, the technique of segmentation using multiple subnets (and associated VLANs) is used to limit the size of the broadcast domains and thus provide a higher performance network. This becomes a critical factor as more devices are placed on the Ethernet network since each device still requires the high level of determinism to function properly. It is important to note that all of Rockwell Automation's new devices (ie: drives, I/O, starters, etc.) are being provided with on-board Ethernet ports therefore making it even more important to properly plan for upgrades in the future.

  To tie all of the various subnets / VLANs together, a Layer 3 device will be required. The Layer 3 device allows for routing of traffic between the various subnets in the system (ie: for controller to controller communications) to tie all devices together in a unified architecture. Please note that it is recommended as per our standard practices that routing be completed locally within the production environment and not be done within the Enterprise.

  An additional aspect in providing a high performance network is to incorporate the use of resilient links from each of the machine zones back to the Layer 3 device. Resilient links are often desired as they allow for a single point of failure resiliency and higher system availability. This approach is deployed with the goal of increasing Overall Equipment Effectiveness (OEE) and machine availability as required. For further information on cabling resiliency options, please refer to Section 8.2 of this document.

  To obtain a better understanding of the various segmentation methods available, please reference the recommended "Segmentation Methods within the Cell/Area Zone" document outlined in Section 1.2. Please note that although each segmentation method listed in that document are acceptable, each have their inherent advantages and disadvantages. This should be reviewed thoroughly to understand the design considerations that need to be addressed for each type of implementation.

  To provide an idea of a standard reference architecture used in IACS networks, please reference Figure 2:1 listed below. This architecture outlines the use of both VLANs for segmentation between the various areas of the overall plant while also incorporating resilient links for a highly available system. Again, please refer to the "Segmentation Methods within the Cell/Area Zone" document outlined in Section 1.2 for further information.

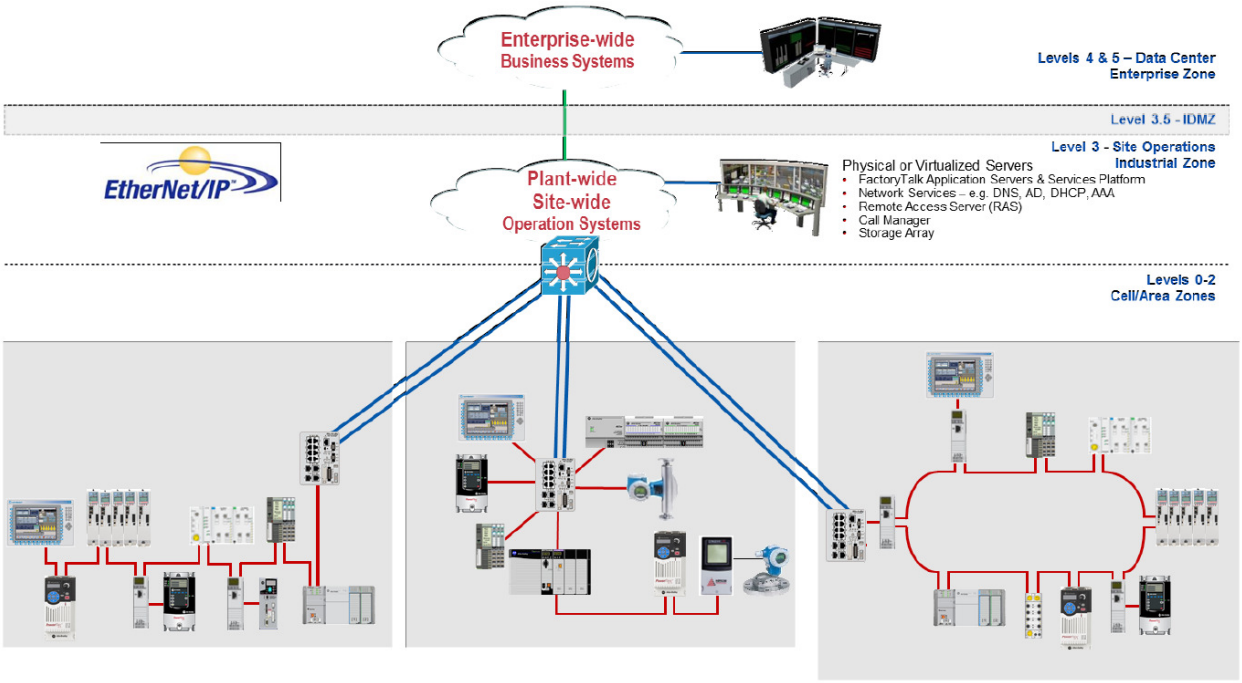


**Figure 2:1 – Example Scalable, Resilient IACS Network Architecture**

- **Address Physical Aspects of the Network –** To obtain a highly reliable and scalable network, various physical aspects within the current architecture require attention. The current state of the physical infrastructure does not follow industry recommended practices for cable management, cable routing, cable connectors, and cable labelling. This can lead to extensive issues caused by Electro-Magnetic Interference (EMI) as well as extended troubleshooting times from poor cable routing and labelling practices. For further information on the findings of our network assessment please review Section 5 of this document.

- **Configuring Managed Switches –** At this point, many of the switches used within the production environment are not configured with special consideration for the application and have solely been given an IP address for management. Managed switches provide the ability to prioritize specific types of traffic (ie: EtherNet/IP within the production environment) as well as provide enhanced security features. The deployment of these advanced features will allow for a more robust, secure, and higher performance network and should be evaluated as to their applicability within the production environment.

- **Evaluate Critical Infrastructure Life Cycles –** During the assessment it was found that many of the network infrastructure components used were either in Active Mature (ie: newer products exist for replacement) or Discontinued (no longer available for purchase) state. This is a critical item for consideration as spares for equipment may not be as readily available with potential extended lead times. Key infrastructure items should be upgraded to current product offerings proactively to avoid potential long term outages that may be required to replace failed, discontinued hardware. For further information on the particular network infrastructure items affected, please review Section 4 of this document.

- **Terminal Services using Virtualization –** To eliminate the need to continuously maintain multiple maintenance technician laptops with various versions of the required software used in the production environment (ie:

RSLogix™, FactoryTalk® View, FactoryTalk® Activation Manager, etc.), virtual machine instances can be stored on a remote access server (RAS) that are continuously available and ready for connection. This allows for Enterprise connected laptops, production environment connected laptops, and even remote access laptops (as deemed appropriate by Customer A via VPN), to connect to the RAS and easily go online with any of the available PLCs without the need to obtain versioning / licensing on the local laptop. Please note that a proper network infrastructure to handle this type of connection is required and is outlined below for further reference:

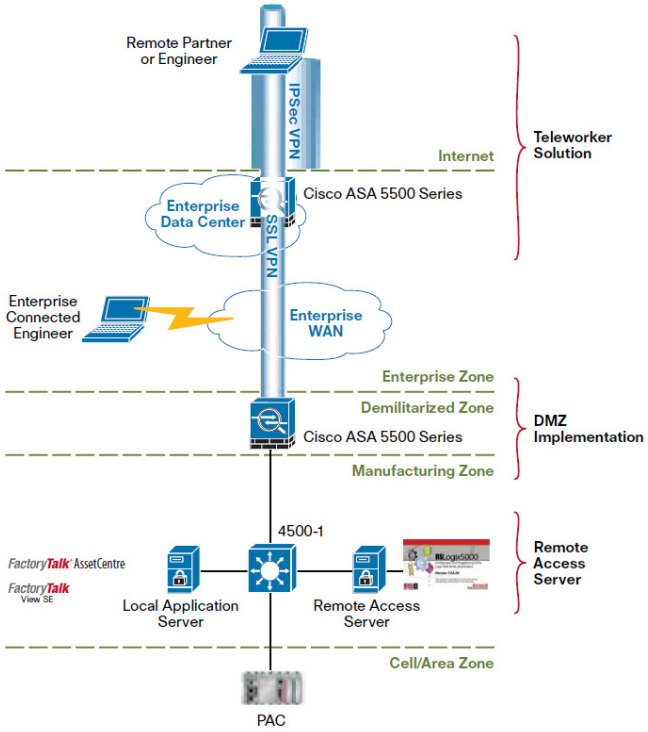


**Figure 2:2 - Example Remote Access Server Network Architecture**

The remote access server will host the approved automation and control applications, such as FactoryTalk® View ME and RSLogix™ 5000. By executing applications on a secure, dedicated server, the versioning of the applications along with associated licensing can be performed locally allowing for ease of connection to the PLCs / end devices. The focus is that this architecture allows for scalability as the network architecture grows and provides an easy to use, seamless method for the user to connect to each of the PLCs and HMIs in the production environment.

- **Provide Clear Demarcation Lines via an Industrial De-Militarized Zone (IDMZ) between Enterprise and Production –** Based on our Cisco and Rockwell Automation partnership, various guidelines and architectures have been established in our Converged Plantwide Ethernet Design and Implementation Guide (CPwE DIG). These guidelines outline that no data should pass directly between the production and enterprise environments and should always be replicated via the use of a replication server. Rather than solely using a firewall as currently implemented in the architecture, multiple technologies and methodologies should be applied to obtain a Defense-In-Depth implementation for the production environment that follows accepted industry standards.

  This goal of a properly designed IDMZ implementation is to provide enhanced security for the production environment while maximizing productivity and Overall Equipment Effectiveness (OEE). This implementation allows for secure connections while the IDMZ is in place or complete disconnection between the enterprise and

production environment if any issues or security breaches are seen. This ensure that the production environment continues to run even if a security breach is detected. For further information on this approach, please visit Section 8.1 of this document.

Listed below is a further depiction of our Converged Plantwide Ethernet (CPwE) approach for enabling secure, scalable, future ready connection of the production environment to the enterprise. For further details please also reference the "Converged Plantwide Ethernet Design and Implementation Guide" (CPwE DIG) reference in Section 1.2.

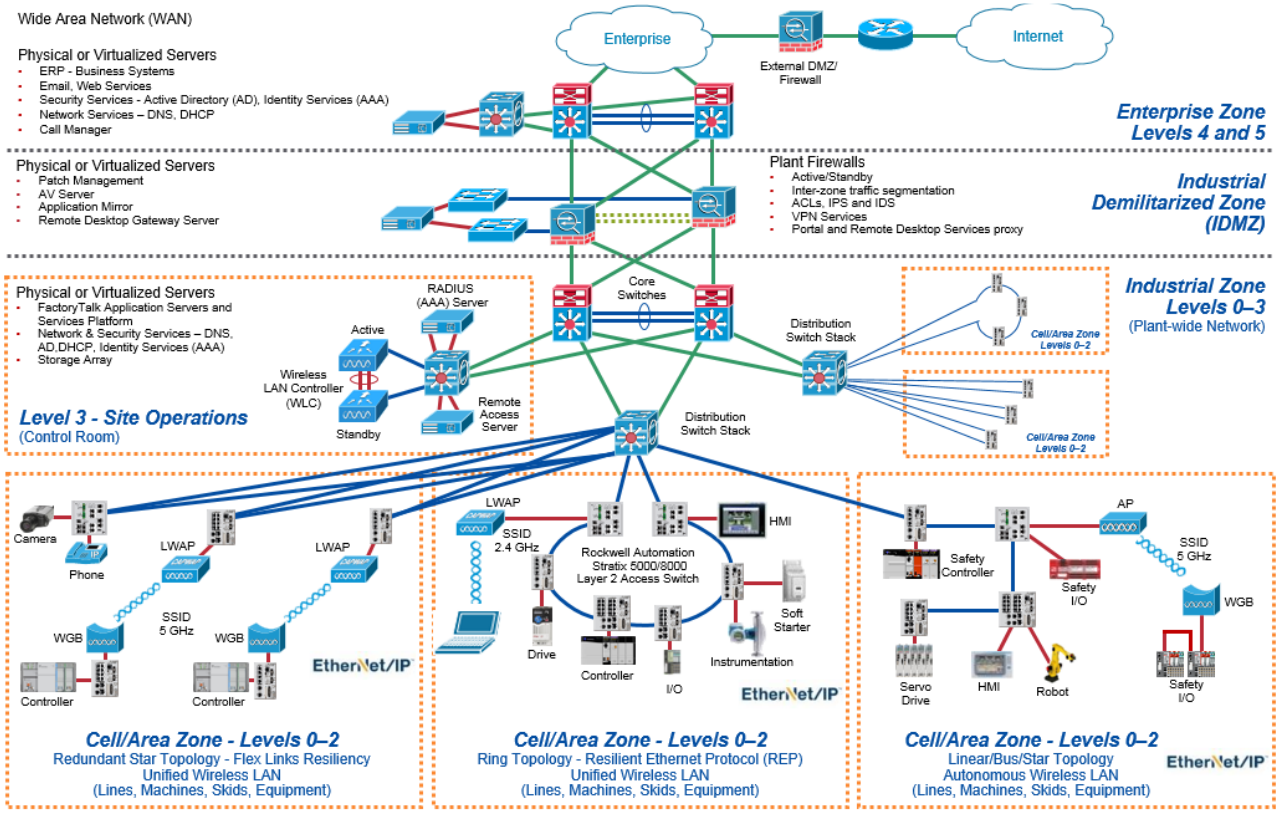


**Figure 2:3 - Cisco / Rockwell Converged Plantwide Ethernet (CPwE) Recommended Architecture**

It is important to note that for all of the remediation items listed in this document, Rockwell Automation recommends that any network upgrades completed be designed to meet the needs of the production environment for a minimum of 15 years. Contrary to traditional approaches within the IT space of completing upgrades every 5 years, production environments are traditionally designed to longer life cycles and therefore approaches outlined today must be able to be future ready.

In noting this approach, it may appear that some of the items listed within this document are extensive for the current number of Ethernet enabled devices within the production environment. It is however important to take the expected life cycle of network infrastructure equipment into consideration as the Ethernet network will undoubtedly grow and evolve significantly in the next 15 years. This is a critical item and one that should be closely evaluated when reviewing the items listed within this section.

To obtain further information on these remediation approaches or ideas as to a phased approach for your plant, please contact Rockwell Automation's Connected Services team. We look forward to discussing the various aspects of the design in further detail with you and your team members at Customer A.

## *2.1.4 Summary of Physical / Logical / Security Network Aspects*

This report will provide an in-depth overview of the network architecture along with the potential recommended actions. A high-level summary of the items observed can be seen in Table 2:1 below and will be expanded upon further within their respective sections.

**Table 2:1 – Summary of Observations**

| Network Physical Infrastructure | | Total Rating: | HIGH |
|---|---|---|---|
| **Section** | **Section Name** | **Impact Rating** | **Recommended Action** |
| 5.1 | Physical Topology | HIGH | Develop network design plan to incorporate a fault tolerant network topology that meets network downtime requirements and provides redundancy to critical assets. |
| 5.2 | Switch Selection | LOW | Monitor switch performance and periodically evaluate if switches on the IACS network are meeting requirements. |
| 5.3 | Router Selection | MODERATE | The use of a single subnet within the production environment eliminates the need of a router. Please note however that segmentation is recommended to minimize the size of broadcast domains and fault domains. |
| 5.4 | Ethernet Communication Modules | MODERATE | Evaluate module configurations and firmware continuity and ensure they are meeting system requirements. |
| 5.5 | Environmental Conditions | ACCEPTABLE | Monitor the environmental conditions of the network devices to ensure they are continuing to meet degradation requirements. |
| 5.6 | Enclosures | ACCEPTABLE | Monitor enclosures periodically to ensure they are continuing to meet environmental requirements. |
| 5.7 | Cable Selection | HIGH | A copper and fiber infrastructure plan needs to be developed to replace cables and connectors that do not meet specifications. A cable validation is recommended. |
| 5.8 | Cable Management | HIGH | Develop cable management standards for enclosures and where excess cable exists. Any cables that have not been managed to meet specifications require cable testing so any damaged cables can be identified and replaced. |
| 5.9 | Conduit & Routing | LOW | Monitor cable routing and periodically evaluate to ensure cables have not been compromised and are continuing to meet requirements. |
| 5.10 | Cable Labeling | LOW | Monitor cable labeling to ensure that cable labeling standards are being applied and upheld. |
| 5.11 | Power Redundancy System | MODERATE | Monitor power redundancy requirements for infrastructure to ensure the strategy in place is continuing to meet requirements. |
| 5.12 | Grounding | ACCEPTABLE | Monitor grounding of devices to ensure they are continuing to meet the manufacturers installation requirements. |

| Network Logical Infrastructure | | Total Rating: | HIGH |
|---|---|---|---|
| **Section** | **Section Name** | **Impact Rating** | **Recommended Action** |
| 6.1 | Logical Topology | HIGH | A logical flow map needs to be developed for the IACS network. Network segmentation needs to be implemented so data can be monitored and controlled. Network design assistance is recommended. |

| | | | |
|---|---|---|---|
| 6.2 | Security Zone | MODERATE | A standard for firewall use and configuration needs to be developed that meets the requirements of the enterprise network and the IACS network. |
| 6.3 | Manufacturing Zone | HIGH | A network design needs to be performed immediately so the network can meet industrial requirements for a future ready, scalable, hierarchal network. |
| 6.4 | Cell/Area Zone | HIGH | Access level device configurations need to be assessed immediately to ensure they are meeting IACS devices and topology requirements. |

| Industrial Security & Safety | | Total Rating: | HIGH |
|---|---|---|---|
| **Section** | **Section Name** | **Impact Rating** | **Recommended Action** |
| 7.1 | Asset Management | MODERATE | Establish a technology refresh plan via an Industrial Networking Plan. Conduct inventory inspection to confirm accuracy of master inventory list assets, categorization and prioritization. |
| 7.2 | Governance | LOW | Maintain operations alignment with security policies, standard operating procedures and practices and initiate periodic reviews to ensure necessary enhancements are incorporated into the documents. |
| 7.3 | Risk Assessment & Management | HIGH | Initiate activities to develop a Risk Assessment and Management Plan to include methodologies to identify resident threats and vulnerabilities specific to industrial automation and industrial control systems. Develop a communication plan inclusive of incident response procedures and resources with requisite responsibilities and authority to take action during a security incident. |
| 7.4 | Access Controls | HIGH | Identify hardware devices and software applications required in performing access control roles and initiate a review of their respective features and capabilities. Develop traceability mappings between users of systems and their respective asset access requirements. Specify strength and attribute requirements for access credentials and ensure such are consistent with industry best practices and regulatory requirements (if applicable). Document device configurations and user access permission requirements to ensure single point of accountability, principles of least privilege and network segregation are achieved. |
| 7.5 | Awareness & Training | LOW | Continue to uphold the tenets defined in the existing training and awareness plan. Review periodically and make changes as necessary. |
| 7.6 | Data Security | HIGH | Develop a security architecture specification that identifies cryptographic requirements for data-at-rest, data-in-transit and message verifications considered to be critical or sensitive. The cryptographic security architecture should identify the system and application interfaces and file locations where critical or sensitive data traverses or is stored. Cryptographic technologies should be selected based upon existing best practices and government tested algorithms. |
| 7.7 | Maintenance | LOW | Maintain existing operations associated with maintenance and repair activities. Review checklists and logs with maintenance operators to ensure accuracy. Perform changes as necessary. |
| 7.8 | Incident Detection | MODERATE | Review and revise the existing Incident Detection and Response Plan for effectiveness and ensure the Plan's procedures are tested at least annually for consistency with operations. Revise as required. Provide maintenance operators and system administrators with training and |

| | | | |
|---|---|---|---|
| | | | awareness to ensure familiarity with IACS system behaviors associated with specific incident types. |
| **7.9** | **Physical Security & Safety** | **ACCEPTABLE** | Monitor safety and security standards to ensure they are continuing to meet company and regulatory requirements. |

## 2.2 Objective

The Rockwell Automation Network & Security Standard Assessment obtains network information about the production environment by using a cooperative approach. An assumption about the network health of the production environment is determined through a physical inspection process and an interview process with the professionals that work in the Customer A, Location A environment every day. By utilizing the knowledge of these professionals, the status of critical network infrastructure is determined to identify the risk to the production environment, as well as organizational risks to Customer A, Location A. This Network & Security Standard Assessment deliverable outlines the network health for network physical infrastructure, network logical infrastructure, and industrial security and safety. These three main sections encompassing the production network are assessed and measured against industry leading standards for industrial control networks.

The objective of this deliverable is to present the findings of the physical inspection and interview process. The analysis uses a streamlined information method to provide technical descriptions and classifications of vulnerabilities. A diagnosis of findings will rate the prioritization and criticality of vulnerabilities as expressed by impact and exploitation potential, and recommends mitigation actions.

The Network & Security Standard Assessment is completed without the use of Ethernet analyzer tools and does not include any modification or remediation. Additional services including comprehensive network assessment, network design, security design, and remediation can be provided in a separate engagement.

## 2.3 Scope

Detailed information regarding contractual specifics for deliverable can found in the agreed upon proposal, OCNOKR0482.

# 3 METHODOLOGY

The methodology used as the basis for this Network & Security Standard Assessment combines the logical manufacturing framework and common industry physical infrastructure practices as defined by the Reference Documentation in Table 1:2, and a proprietary algorithm which defines the impact of observations based on these guidelines. The Rockwell Automation Standard Network Assessment proprietary algorithm calculates the impact of observations gathered during the physical inspection walk through and the questionnaire sections. For each observation, recommendations for remediation and remediation criticality are described. A remediation rating of "High" implies that the finding potentially creates a serious risk to production system availability and security or human safety. A remediation rating of "Moderate" suggests security risks or networking issues exist in the architecture, network or system that may impact production system operation, but that risk is neither imminent nor human safety related. Finally, a remediation rating of "Low" is indicative of findings that either require additional analysis to remediate or their expected impact to the production system's environment is minimal but could impact repair or maintenance.

**Criticality Ratings**:

- **HIGH** = Indicates a potentially serious risk to production system availability or human safety. Remediation should be accomplished at the earliest opportunity.
- **MODERATE** = Indicates an issue that may impact production. The risk is neither imminent nor human safety related. Remediation can be scheduled for a planned maintenance activity.
- **LOW** = Indicates an issue that may have minimal impact to production but could improve network maintenance and/or management. Remediation can be scheduled when convenient.

# 4 NETWORK ASSET EVALUATION

The IACS inventory information provided is not inclusive of all devices in existence on the IACS network. It is a sample of the primary IACS communication devices which includes network switches, controller communication modules, and other devices where observations made their documentation relevant to the scope of this section.

**Table 4:1 – Network Asset Evaluation**

| Vendor | Name Plate Model | Location | Current Condition | Environment | End of Life Info |
|---|---|---|---|---|---|
| Allen-Bradley | 1785-ENET | Mill #1 - TWS | Good | Fair | Discontinued |
| Allen-Bradley | 1756-ENBT | Mill #1 - QS Main | Good | Good | Active Mature |
| Allen-Bradley | 1756-ENBT | Mill #1 - QS Main | Good | Good | Active Mature |
| Allen-Bradley | 1756-ENBT | Mill #1 - QS Main | Good | Good | Active Mature |
| Allen-Bradley | 1783-EMS08T | Mill #1 - QS Main | Good | Good | Active |
| Allen-Bradley | 1783-EMS08T | Mill #1 - QS Main | Good | Good | Active |
| Allen-Bradley | 1783-EMS08T | Mill #1 - QS Main | Good | Good | Active |
| Allen-Bradley | 1756-ENBT | Mill #1 - DRC Drives | Good | Good | Active Mature |
| Allen-Bradley | 1785-ENET | Mill #1 - TCOS | Good | Fair | Discontinued |
| Allen-Bradley | 1756-ENBT | Mill #1 - TCOS | Good | Fair | Active Mature |
| Cisco | 2960-S | Mill #1 - IT Cabinet | Good | Fair | Active Mature |
| Cisco | 2960-S1 | Mill #1 - IT Cabinet | Good | Fair | Active Mature |
| Allen-Bradley | 1756-ENBT | Mill #1 - Canada Stamp | Good | Good | Active Mature |
| Allen-Bradley | 1756-ENBT | Mill #1 - Bundler | Good | Fair | Active Mature |
| 3-COM | Baseline 2016 - 3C16470 | Mill #1 - Bundler | Good | Fair | Active |
| Allen-Bradley | MicroLogix 1400 | Mill #1 - Bundler | N/A | N/A | Active |
| Allen-Bradley | MicroLogix 1400 | Mill #1 - Bundler | N/A | N/A | Active |
| Allen-Bradley | 1756-ENBT | Slitter #2 | Good | Fair | Active Mature |
| Allen-Bradley | 1756-ENBT | Slitter #4 - Main | Good | Good | Active Mature |
| Allen-Bradley | 1756-ENBT | Slitter #4 - Main | Good | Good | Active Mature |
| Allen-Bradley | 9300-RADES | Slitter #4 - Main | Good | Good | Active Mature |
| Hirschmann | Spider 8TX | Slitter #4 - Main | Good | Good | Active |
| Allen-Bradley | 1785-ENET | Mill #2 - TWM | Good | Good | Discontinued |
| Allen-Bradley | 1785-ENET | Mill #2 - Strip Prep | Good | Good | Discontinued |
| Allen-Bradley | 1756-ENBT | Mill #2 - Drives PLC | Good | Good | Active Mature |
| Allen-Bradley | 1756-ENBT | Mill #2 - QS | Good | Good | Active Mature |
| Allen-Bradley | MicroLogix 1400 | Mill #2 - QS | N/A | N/A | Active |
| Allen-Bradley | MicroLogix 1400 | Mill #2 - QS | N/A | N/A | Active |
| Cisco | 2960-S | Mill #2 - IT Cabinet | Good | Good | Active Mature |

| | | | | | |
|---|---|---|---|---|---|
| | | (Drives Room #1) | | | |
| Cisco | 3550 | Mill #2 - IT Cabinet (Drives Room #1) | Good | Good | Active |
| Cisco | 2960-S | Mill #2 - IT Cabinet (Drives Room #2) | Good | Good | Active Mature |
| Cisco | 2960-S | Mill #2 - IT Cabinet (Drives Room #2) | Good | Good | Active Mature |
| Cisco | 3550 | Mill #2 - IT Cabinet (Drives Room #2) | Good | Good | Active |
| Allen-Bradley | SLC-5/05 | Mill #2 - PTA | Good | Good | Active Mature |
| Allen-Bradley | SLC-5/05 | Mill #2 - Bundler | Good | Good | Active Mature |
| Allen-Bradley | 1756-ENBT | Mill #2 - Bundler Remote | Good | Fair | Active Mature |
| Allen-Bradley | 1783-EMS08T | Mill #2 - Bundler Remote | Good | Fair | Active |
| Allen-Bradley | MicroLogix 1400 | Mill #2 - Bundler Remote | Good | Fair | Active |
| Allen-Bradley | MicroLogix 1400 | Mill #2 - Bundler Remote | Good | Fair | Active |
| Allen-Bradley | 1756-ENBT | Mill #2 - E-Line | Good | Good | Active Mature |
| Allen-Bradley | 1756-ENBT | Mill #2 - Saw / Cutoff / Blade | N/A | N/A | Active Mature |
| Allen-Bradley | 1756-ENBT | Mill #2 - Saw Carriage | Good | Good | Active Mature |
| Allen-Bradley | 1783-EMS08T | Mill #2 - Saw Carriage | Good | Good | Active |
| Allen-Bradley | 1783-EMS08T | Mill #2 - Saw Operator Panel | Good | Fair | Active |
| Allen-Bradley | 1783-BMS20CGL | Mill #1 - QS Encoder Panel #1 | Good | Good | Active |
| Allen-Bradley | 1783-BMS20CGL | Mill #1 - QS Encoder Panel #2 | Good | Good | Active |
| Allen-Bradley | 1783-EMS08T | Mill #1 - QS Encoder Panel #3 | Good | Good | Active |
| Allen-Bradley | 1768-ENBT / L43S | Mill #2 - Safety Prep | Good | Good | Active |
| Allen-Bradley | 1783-ETAP | Mill #2 - Safety Prep | Good | Good | Active |
| Allen-Bradley | 1783-BMS10CGA | Mill #2 - Safety Prep | Good | Good | Active |

**NOTE: "**Active Mature" status outlines that the product is still supported and available for purchase however a newer replacement product is available. Products with "Active Mature" status should be evaluated and a method to upgrade to current product releases for critical infrastructure items should be examined. Products with "Discontinued" status are no longer available for purchase from the manufacturer and should be replaced with an "Active" status item to ensure support may issues arise.

# 5 NETWORK PHYSICAL INFRASTRUCTURE

The current architecture at Customer A, Location A employs a mixed star and linear topology for switch connections. Resilient connections are not used within the production network environment.

In regards to plant level connections, all connections from PLCs to the main Cisco 2960-S for that particular area within the plant are done in a star configuration. In saying this, some panels use a managed switch to aggregate local machine connections (often a Stratix 6000 or Stratix 5700) whereas others use direct connection from the PLC.

From the 2960-S local within each area of the plant (ie: Mill 1 Drives Room, Mill 2 Drives Room #1, Mill 2 Drives Room #2) connections back to Primary Server room Cisco 2960-S1 are aggregated via fiber connection using both star and linear topology. The Cisco switch located in the Primary Server Room is then aggregated to a Mill Firewall for connection to the Office LAN / Enterprise.

To provide a better depiction, please reference the physical topology drawing below as provided by Customer A.

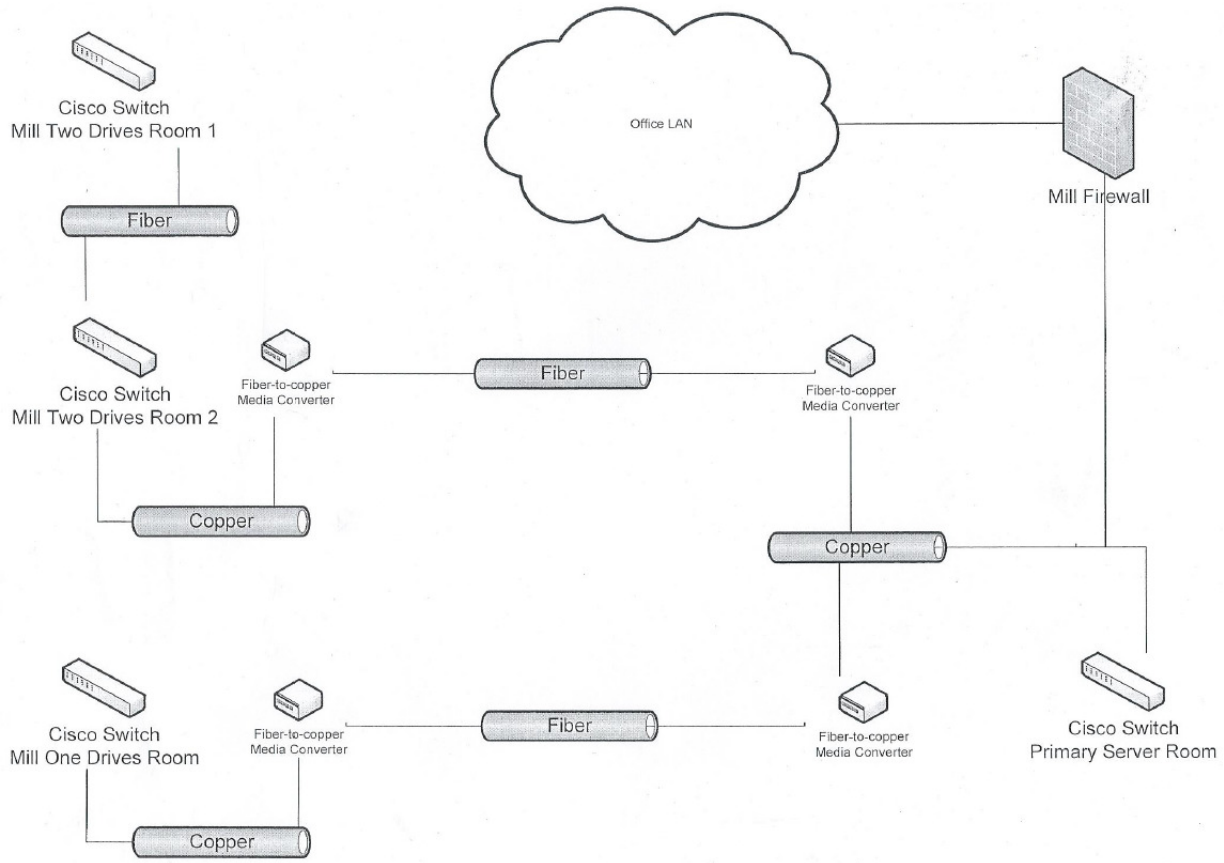


**Figure 5:1 - Production Network High-Level Topology**

It is important to note that all plant level connections via processors are currently communicating on a single subnet (192.168.10.0 /24). Additionally, various end devices are communicating via Class I implicit EtherNet/IP communication back to their associated controller. Due to the fact that all devices are on a single subnet, a dedicated router within the production environment is not used or required at this point.

## 5.1 Physical Topology

The network infrastructure is arranged in a mixed star and linear topology at Customer A, Location A. The main star topology back from each mill (ie: Mill 1 Drives Room and Mill 2 Drives Room 2) provides the best bandwidth capabilities for each line however cabling resiliency in the event of a link loss is not incorporated into the system. Additionally, the linear chain formed between Mill 2 Drives Room 2 and Mill 2 Drives Room 1 could pose potential issues as issues with the Mill 2 Drives Room 2 switch would then affect all of Mill 2 communications back to the Primary Server Room. All communications to line panels managed switches is done from each of the respective Drives Room switches via a star arrangement.

To provide a high availability network, the use of a star only configuration between Drives Room switches and the Primary Server Room is recommended (rather than the mixed linear / star architecture). Additionally, the use of dual redundant links from each managed switch (ie: both line switch panels as well as Drives Room switch cabinet) to its overlying switch is recommended to provide resiliency to mitigate a single point of failure. This is an extremely important point when designing a future ready network that is designed to meet the needs of production systems as the number of Ethernet devices grows.

It is important to note that systems have not been prioritized for availability / fault tolerance requirements of highly critical items. This should be evaluated as downtime could occur from the loss of network infrastructure / hardware.

**Table 5:1 – Physical Topology Observation Results**

| ***Physical Topology*** | | ***Section Rating:*** | ***HIGH*** |
|---|---|---|---|
| ***Observation*** | ***Comments*** | ***Recommendation*** | ***Criticality*** |
| The physical topology of the IACS network is mixed. | A mixed topology of star and linear is used for inter-switch communications | Information Purposes Only | LOW |
| The IACS network was not designed to meet a specific availability rating. | | Availability ratings provide an indication of downtime that can be anticipated based on the network design and the hardware used in the network. A requirements analysis will identify critical network elements that may need increased availability. (CPwE DIG) | LOW |
| Fault tolerance has not been incorporated into the IACS network design. | Resilient links between switches are not currently implemented. | Determine how much network downtime can be tolerated if a network fault occurs. Availability calculations can determine if the existing network architecture provides availability within that tolerance window. A requirements analysis will identify critical elements of the network so fault tolerance can be designed to maximize network availability based on | HIGH |

| | | | |
|---|---|---|---|
| | | those requirements. (CPwE DIG) | |
| Fault tolerance does not incorporate redundancy of end devices. | Solely simplex controller chassis are employed at this point (ie: ControlLogix redundancy is not utilized) | Determine if the redundancy of end devices is required to meet uptime requirements and implement accordingly. (CPwE DIG) | LOW |
| Fault tolerance does not incorporate redundancy of switches. | Cisco aggregation switches used in the Drives rooms could be implemented in a stacked configuration to provide switch level resiliency. | Determine if the redundancy of switches is required to meet uptime requirements and implement accordingly. (CPwE DIG) | LOW |
| Fault tolerance does not incorporate redundancy of routers. | **NOTE:** No routing is currently used in the plant environment however this point is included for reference information | Determine if the redundancy of routers is required to meet uptime requirements and implement accordingly. (CPwE DIG) | LOW |
| Fault tolerance does not incorporate redundancy of firewalls. | A singular firewall is used between the production environment and the Enterprise | Determine if the redundancy of firewalls is required to meet uptime requirements and implement accordingly. (CPwE DIG) | MODERATE |
| Fault tolerance does not incorporate redundancy of links/media paths. | Solely singular links are provided between all switches in the production environment | Determine if the redundancy of links/media paths are required to meet uptime requirements and implement accordingly. (CPwE DIG) | LOW |
| Dual NICs are employed in devices on the IACS network. | A few of the ControlLogix chassis in Mill 1 use multiple NICs to provide segmentation | It is recommended that NICs segmentation be minimized as it does not provide a scalable architecture and one that is easy to troubleshoot. This limits the overall future-ready aspect of the network | MODERATE |

## 5.2 Switch Selection

The predominant use of managed switches allows for advanced network functionality in the production environment at Customer A, Location A. In saying this, it is important to note that many of the features of the managed switches in place are not deployed / configured and therefore potential to increase performance is underutilized. Key features such as Smartports (custom configurations to prioritize the functionality of each port), prioritization of EtherNet/IP traffic, and port-based security (ie: MAC address detection, number of devices connected, etc.) are not implemented greatly limiting the performance and security of the production network.

Managed switches should continue to be used wherever possible in the production environment. The key however is that these managed switches need to be configured for each application to increase network performance, determinism and security while decreasing the likelihood of downtime.

**Table 5:2 – Switch Selection Observation Results**

| ***Switch Selection*** | | ***Section Rating:*** | ***LOW*** |
|---|---|---|---|
| ***Observation*** | ***Comments*** | ***Recommendation*** | ***Criticality*** |
| A single switch vendor is not used consistently throughout the network. | Although Cisco and Rockwell Automation switches are predominant, various other vendors are deployed (3-COM, Hirschmann, etc.) | Switch vendor consistency improves equipment interoperability and simplifies troubleshooting, maintenance and spare parts inventory. (CPwE DIG) | LOW |
| Managed switches are used throughout the IACS network. | There is only a few instances where unmanaged switches are currently used in the production environment (Slitter #4 Main Panel, Mill #1 Bundler, etc.) | Information Purposes Only | ACCEPTABLE |
| Switches are mounted in environmentally suitable cabinets. | The environmental condition of most panels was very good | Information Purposes Only | ACCEPTABLE |
| Switches are designed for the environment in which they are used. | | Information Purposes Only | ACCEPTABLE |
| Switches are not under a maintenance/support agreement. | | Determine if placing switches under a maintenance/support agreement is necessary to maintain plant uptime requirements. (CPwE DIG) | LOW |
| Spare switches are stocked on site. | The approach of stocking spare switches on-site is used to replace the need for maintenance / support agreements with the vendors. | Information Purposes Only | ACCEPTABLE |

## 5.3 Router Selection

Due to the fact that all traffic within the production network is currently on a single subnet, routing is not currently required. The approach of using a single subnet limits scalability as well as produces a large broadcast domain and can create significant challenges should an issue be encountered. Segmentation of traffic within the production environment is highly recommended as outlined within the Executive Summary in Section 2 as well as the Logical Summary in Section 6 of this document.

Please note that traditional recommendations from our CPwE documentation (referenced in Section 1.2 along with Section 8 of this document) outline that dedicated routing infrastructure for the production environment should be used. Please refer to our joint Cisco and Rockwell Automation CPwE document for further information.

**Table 5:3 – Router Selection Observation Results**

| ***Router Selection*** | | ***Section Rating:*** | ***MODERATE*** |
|---|---|---|---|
| ***Observation*** | ***Comments*** | ***Recommendation*** | ***Criticality*** |
| A router is not currently installed in the network. | As all traffic on the plant production network is currently on a single VLAN, a router is not necessary and therefore not installed | Placing all traffic on a single subnet within the production environment limits scalability and produces a single fault domain when issues arise. Therefore, segmentation of traffic as listed in Section 6 of this document is highly recommended | MODERATE |

## 5.4 Ethernet Communication Modules

Various different controller platforms are currently in use within the production environment at Customer A, Location A based on functionality required and the age of the equipment. This results in the use of communication cards particular to each platform being employed (ie: ControlLogix, Compact GuardLogix, , MicroLogix, PLC-5, etc.).

Upgrading of firmware to the highest level available for both controllers and communication module hardware is recommended to take advantage of new features and better security / resiliency on each platform.

**Table 5:4 – Ethernet Communication Modules Observation Results**

| *Ethernet Communication Modules* | | *Section Rating:* | *MODERATE* |
|---|---|---|---|
| ***Observation*** | ***Comments*** | ***Recommendation*** | ***Criticality*** |
| Switch port speed/duplex settings are configured correctly for the controller interface. | | Information Purposes Only | ACCEPTABLE |
| Firmware revisions of similar controller interfaces are not consistent with each other. | Multiple versions of firmware are currently in use on the various controller platforms | Consistent firmware revisions improve interoperability, troubleshooting and maintenance. (CPwE DIG) | MODERATE |
| Spare controller interface modules are stocked on site. | | Information Purposes Only | ACCEPTABLE |

## 5.5 Environmental Conditions

Essentially all panels are in good shape and provide suitable protection for the network equipment. Only very minor situations of concern of environmental condition were present (outlined below). Please continue to uphold the standards for the panel deployment / maintenance currently in place.

**Table 5:5 – Environmental Conditions Observation Results**

| *Environmental Conditions* | | *Section Rating:* | *ACCEPTABLE* |
|---|---|---|---|
| ***Observation*** | ***Comments*** | ***Recommendation*** | ***Criticality*** |
| The environmental conditions have been assessed at locations containing network equipment. | | Information Purposes Only | ACCEPTABLE |
| The network equipment is properly rated for the environment. | | Information Purposes Only | ACCEPTABLE |
| Corrosion/material degradation is not evident on network hardware. | | Information Purposes Only | ACCEPTABLE |


**Figure 5:2 - Mill #2 Rea-JET Cabinet Filter**

## 5.6 Enclosures

All enclosures are properly rated for the environment and provide adequate protection for the infrastructure related equipment.

**Table 5:6 – Enclosures Observation Results**

| *Enclosures* | | *Section Rating:* | *ACCEPTABLE* |
|---|---|---|---|
| ***Observation*** | ***Comments*** | ***Recommendation*** | ***Criticality*** |
| The network equipment is mounted in enclosures. | | Information Purposes Only | ACCEPTABLE |
| The enclosures are properly rated for the environment. | | Information Purposes Only | ACCEPTABLE |
| Open post networking cabinets do not exist outside of protective environments on the IACS network. | | Information Purposes Only | ACCEPTABLE |

## 5.7 Cable Selection

Currently, standards are not consistently followed for cable usage within the production environment at Customer A, Location A. Various types of copper cable were seen with different termination types (over molded, crimped, etc.). In contrast, fiber optic connections appear to be standardized within the production environment for long distance communications.

Establishing standards for copper cable selection will provide consistency within the production environment. This can lead to reduced downtime and decreased troubleshooting efforts when potential issues are encountered.

**Table 5:7 – Cable Selection Observation Results**

| *Cable Selection* | | *Section Rating:* | *HIGH* |
|---|---|---|---|
| ***Observation*** | ***Comments*** | ***Recommendation*** | ***Criticality*** |
| There is no specification for cable/connectors to be used. | Copper links use many different types of cabling and some that are not suitable for the production environment | Specifying cable and connectors ensures they are suited to the installation and perform to expectations. (ODVA Ethernet/IP Media Planning & Install Guide ) | LOW |
| Cables are not certified to perform to TIA/EIA-568 specifications. | Cables are not validated to meet specifications upon installation and are solely verified based on functionality of the link. | Implement a cable testing program to test all cables in order to verify they can perform to TIA/EIA-568 specifications. (ODVA Ethernet/IP Media Planning & Install Guide ) | LOW |
| Certification testing is not performed as part of a regular maintenance program. | | A cable certification and testing program should be implemented and made a part of a regular maintenance program. (ODVA Ethernet/IP Media Planning & Install Guide ) | LOW |
| CAT5e Cable is installed. | | Information Purposes Only | ACCEPTABLE |
| Copper cables have been in use for 10 years or more. | Various implementations within the mill have been in service for more than 10 years. | Certification testing should be done to verify performance meets TIA/EIA-568 specifications. Failing cables should be replaced immediately. Cables meeting specifications can continue in service until a planned replacement time. | HIGH |
| Shielded cables are installed. | Some instances of shielded cable being used was seen however this is not consistently deployed within the plant | Any shielded cable being used should have the shield terminated at the switch end only. (ODVA Ethernet/IP Media Planning & Install Guide ) | LOW |
| High-flex cables are not installed. | Not required in the environment for | Information Purposes Only | ACCEPTABLE |

| | | | |
|---|---|---|---|
| | Ethernet communications | | |
| There are no cable runs longer than 100m. | None were seen however this was not explicitly validated. Please ensure that no runs exceed 100m. This should include total distance for permanent link and patch cables. | Information Purposes Only | ACCEPTABLE |
| The maximum length of the permanent link cables allow for the use of patch cables so that total length does not exceed 100m (328ft). | | Information Purposes Only | ACCEPTABLE |
| Manufacturer certified patch cables are not used. | In some instances certified patch cables were deployed however these were not used consistently. This is something to be evaluated for any network upgrades to be completed. | Manufacturer certified patch cables are recommended to meet performance expectations. (ODVA Ethernet/IP Media Planning & Install Guide ) | LOW |
| Fiber optic cables are used in the network. | Fiber cabling is used when longer distance communication outside the standard specification for copper (100m) is required | Information Purposes Only | ACCEPTABLE |
| There is a specification for cable/connectors to be used. | Please ensure that the corporate standard is applied to all cables within the production environment as required | Information Purposes Only | ACCEPTABLE |
| The installed cable/connectors comply with specification. | Please ensure that the corporate standard is applied to the production environment as required | Information Purposes Only | ACCEPTABLE |
| Certification testing is not performed as part of a regular maintenance program. | | A cable certification and testing program should be implemented and made a part of a regular maintenance program. (ODVA Ethernet/IP Media Planning & Install Guide) | LOW |
| Media converters are used. | Media converters are deployed in various situations when converting from legacy protocols to EtherNet/IP | Media converters should be avoided. They complicate network management, maintenance and troubleshooting. (ODVA Ethernet/IP Media Planning & Install Guide) | MODERATE |

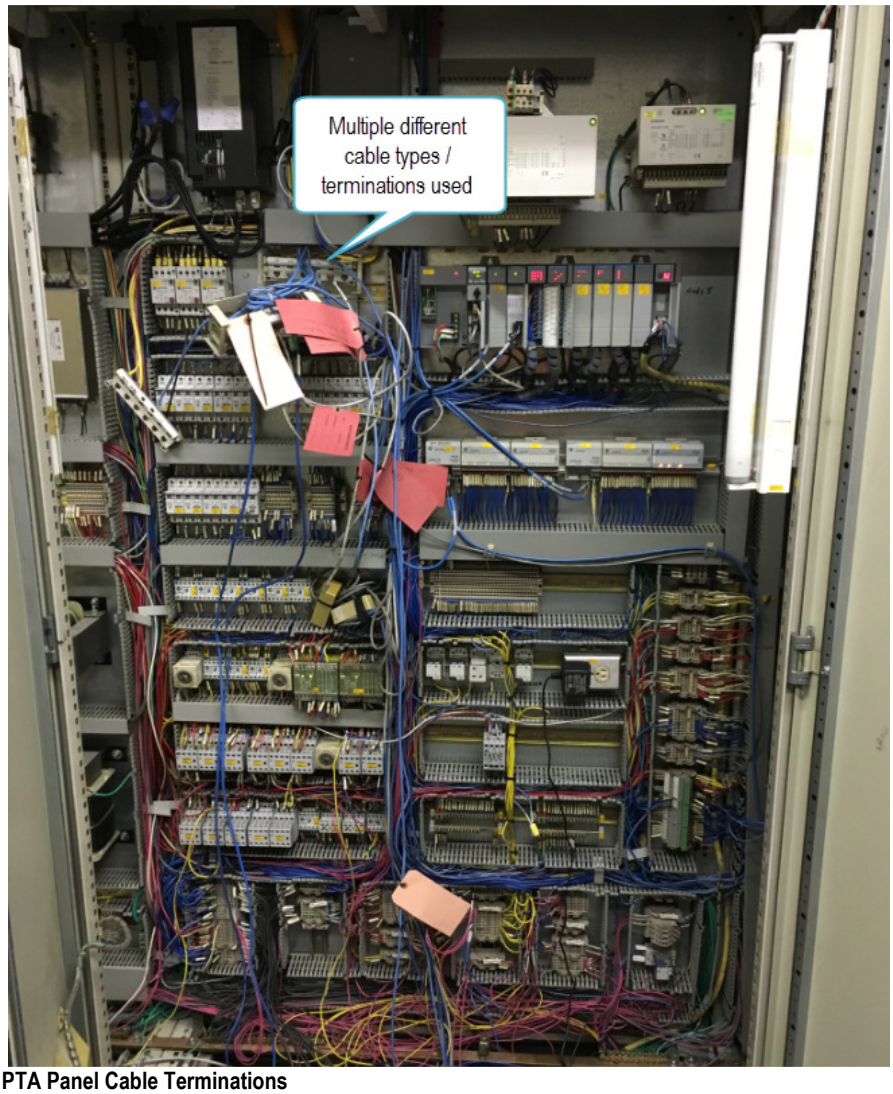


**Figure 5:3 - Mill #2 PTA Panel Cable Terminations**


**Figure 5:4 - Mill #2 TWM Cabling**

## 5.8 Cable Management

Many situations were seen with improper cable management in the production environment at Customer A, Location A. These situations included the following:

- Improper crimping of connections
- Excessive strain on crimped connectors
- Excessive cable lengths coiled in the bottom of the panel
- Squeezed cables resulting in potential loss of connection
- Cables not being routed in appropriate wire way
- Cables not being routed away from power connections
- Cables being routed near fluorescent lighting

These items are seen as a significant potential risk for the production environment as they can be a significant contributor to lost production and downtime. All points of concern in each of the panels should be resolved so that a robust physical infrastructure can be obtained as these connections are the cornerstone of reliable communications in the production environment.

**Table 5:8 – Cable Management Observation Results**

| *Cable Management* | | *Section Rating:* | *HIGH* |
|---|---|---|---|
| ***Observation*** | ***Comments*** | ***Recommendation*** | ***Criticality*** |
| Cable management practices are not used in areas containing network equipment. | Standards should be established to ensure that cables are properly managed both within panels as well as throughout the production environment | Cable management refers to dressing and routing cables, in the vicinity of network equipment, in a manner that | LOW |

| | | | |
|---|---|---|---|
| | | protects the cable and alleviates strain on connections. | |
| Cables are not contained in wire ways inside enclosures. | Many panels did not have proper routing of Ethernet cables | Cables should be secured physically to prevent damage to the cables, prevent movement of the cable, and to prevent damage to the connectors/ cable. If not within a wire way, then secure the cable using recommended best practices for the securing of communication cables in an IACS network. | LOW |
| Cables are secured with plastic cable ties. | Many situations of cable ties being overtightened are evident and create the potential of significant downtime should a connectivity issue arise | Verify that cable ties have not been tightened excessively. Overly tightened cable ties can damage the cable causing poor signal propagation and/or premature cable failure. | LOW |
| Cables are not susceptible to damage from doors opening/closing. | | Re-route cables within cabinets/enclosures away from doors to prevent pinching. | ACCEPTABLE |
| Cables are stretched or dangling in a manner than places strain on cable connectors. | | Re-route cables to prevent strain on cable connectors due to stretching or dangling. | HIGH |
| Cables are stretched or dangling in a manner than places strain on device connectors. | | Re-route cables to prevent strain on device connectors due to stretching or dangling. | HIGH |
| There is less than 12 inches of slack in the cable. | | Re-run cable and terminate so that there is at least 12 inches of slack. | LOW |
| Cable bend radius is tighter than 4x cable diameter. | | Minimum bend radius is 4 x cable diameter. | HIGH |
| Large coils of excess cable are present. | Multiple situations of excess cable coiled in panels was observed. This should be addressed as it can result in lost communications due to Electro-Magnetic Interference (EMI) present in the production environment | Large coils of excess cable distort the capacitive and inductive properties of the cable and affect the signal propagation of the cable. Large coils of excess cable should be removed. | LOW |
| Permanent link cables terminate in patch panels. | Termination methods into the patch panels should be validated to ensure suitable connectivity | Information Purposes Only | ACCEPTABLE |

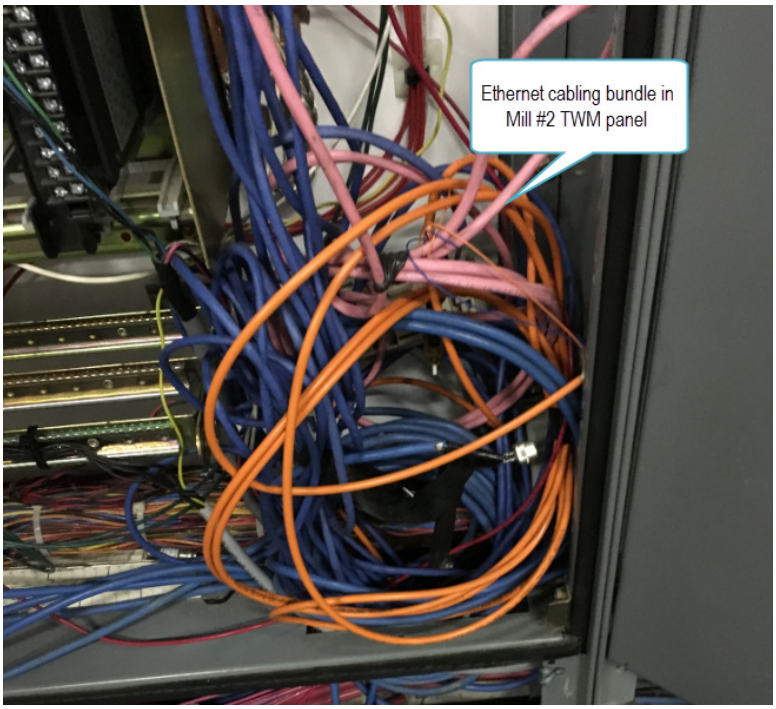


**Figure 5:5 - Mill #2 TWM Panel Cable Routing**

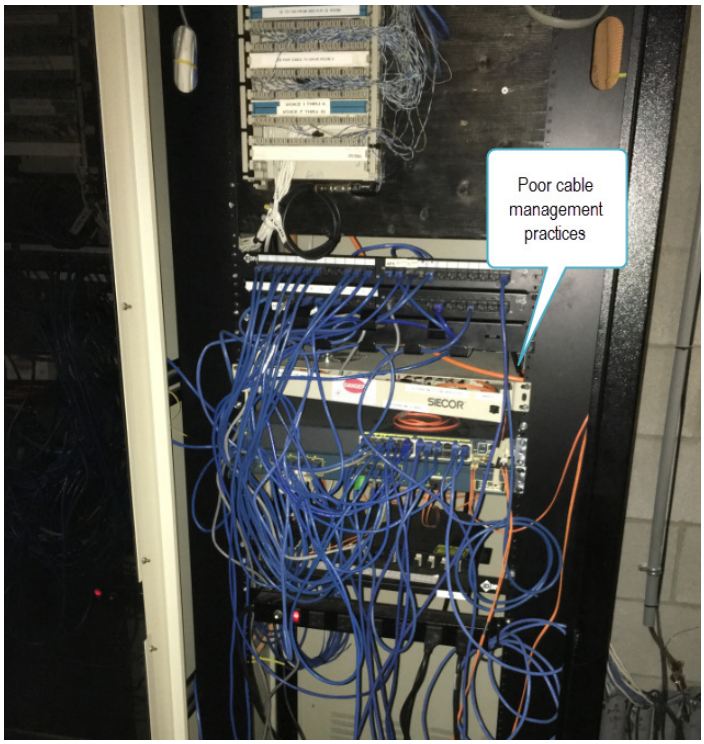


**Figure 5:6 - Mill #2 Drives Room #1 IT Cabinet**

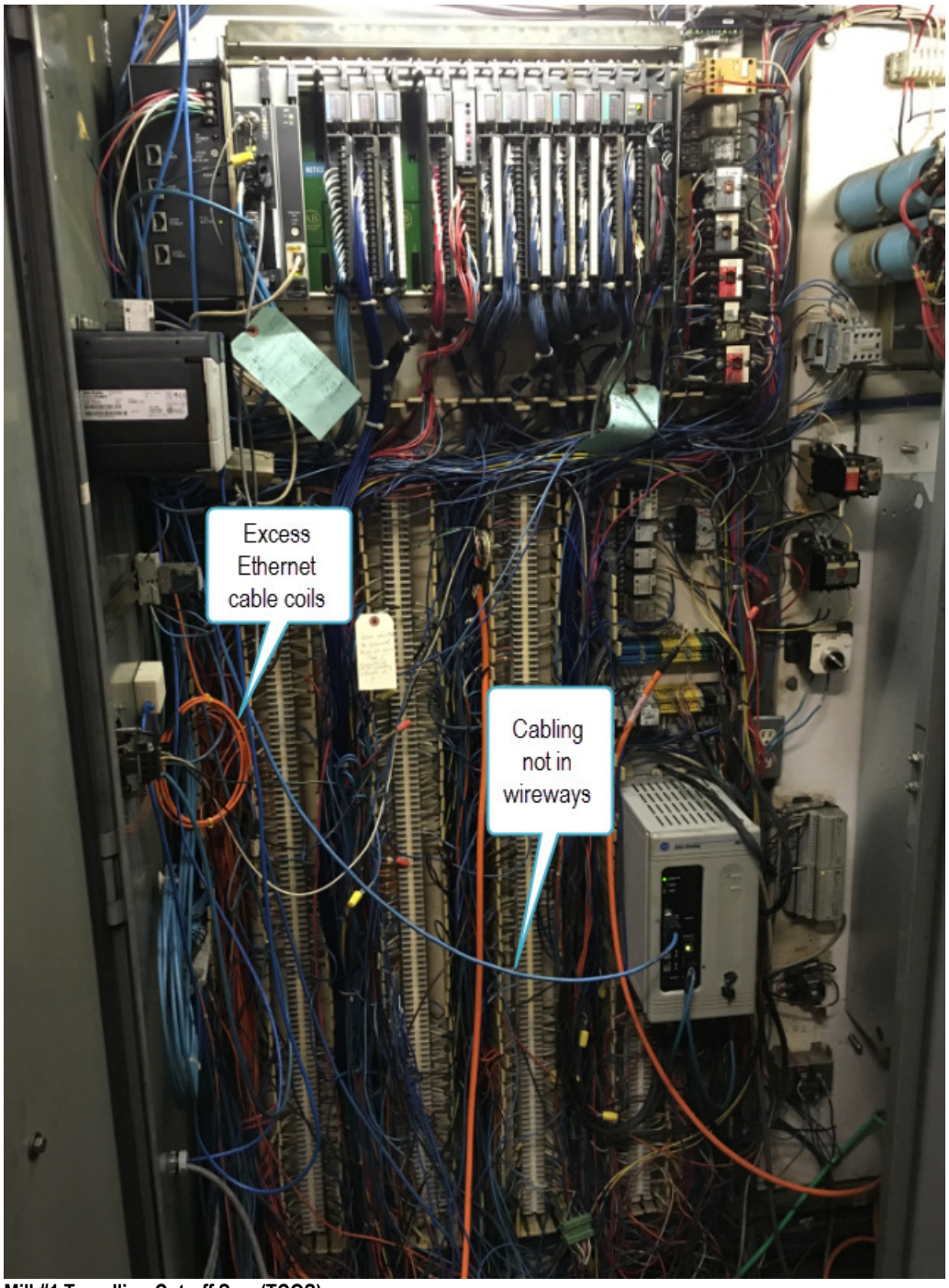


**Figure 5:7 - Mill #1 Travelling Cut-off Saw (TCOS)**

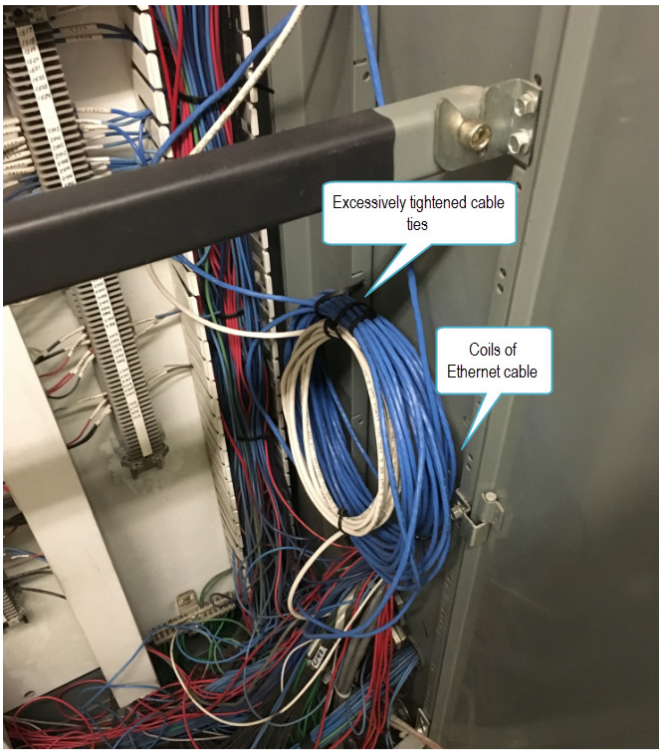


**Figure 5:8 - Slitter #4 Drives Panel**

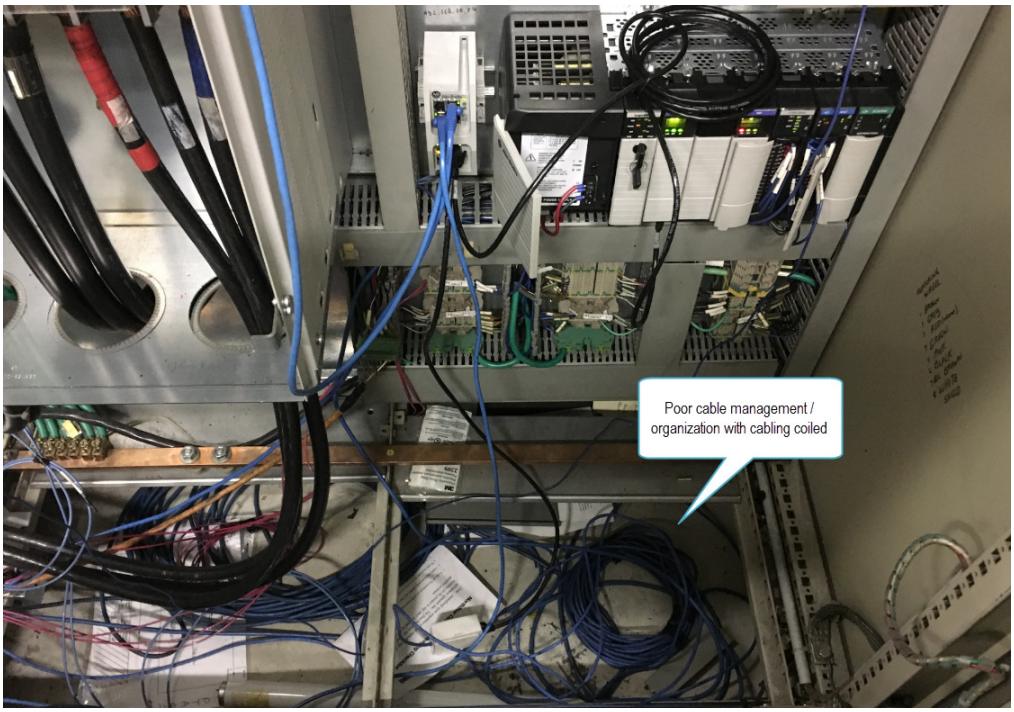


**Figure 5:9 - Mill #2 Saw Carriage**

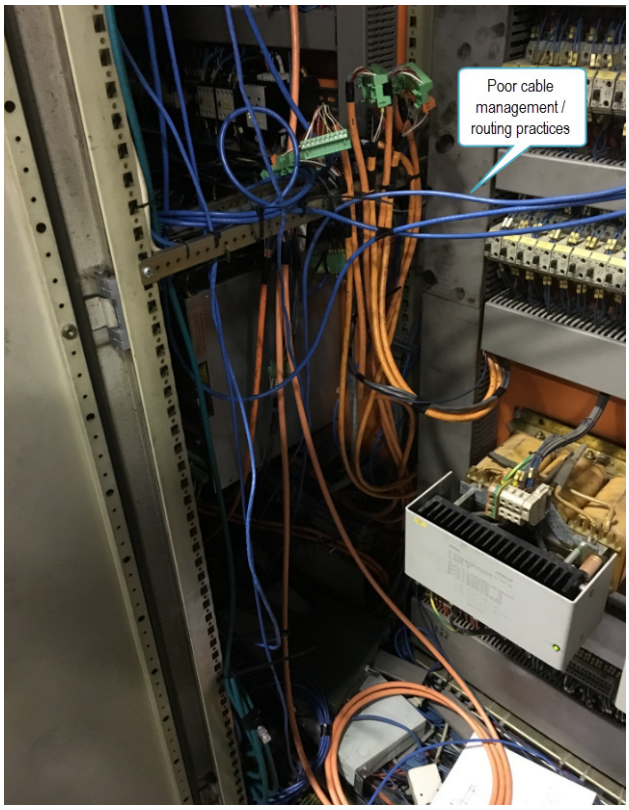


**Figure 5:10 - Mill #1 Bundler**

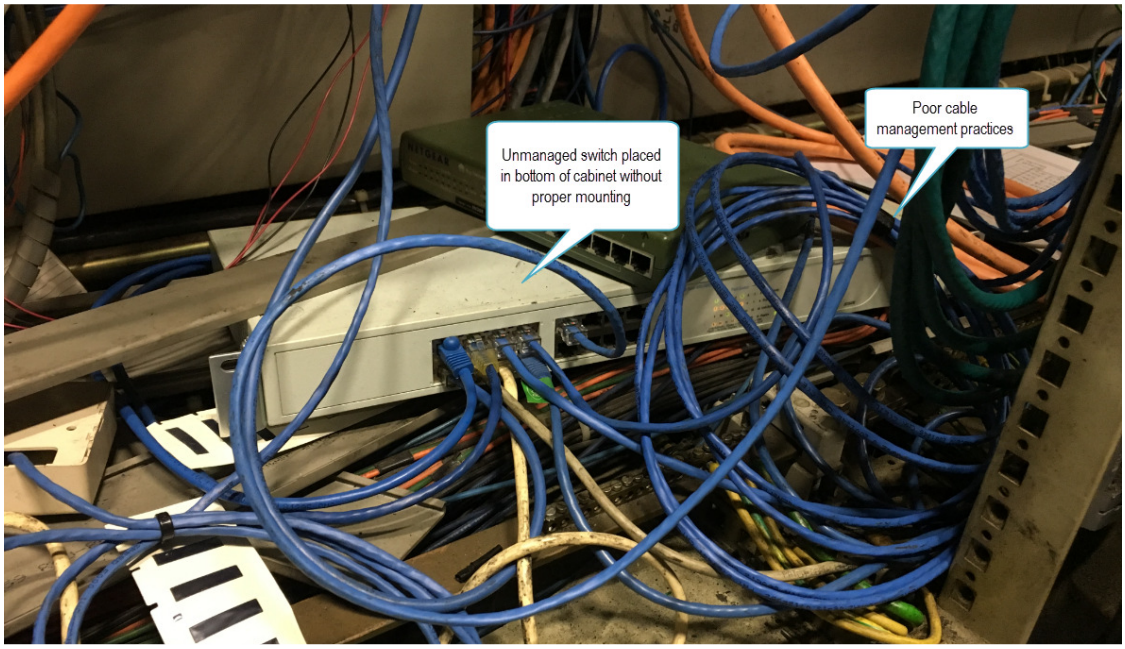


**Figure 5:11 - Mill #1 Bundler Unmanaged Switch Mounting / Cable Routing**

## 5.9 Conduit & Routing

Routing of cables is predominantly completed via the use of conduits within the Customer A, Location A facility. Multiple instances of concerns were seen as Ethernet cables are often added after the initial conduit installation and routed external to the conduit. This can pose issues as the cabling can become susceptible to Electro-Magnetic Interference (EMI) caused by fluorescent lighting / high power sources and should be addressed to provide a highly reliable physical infrastructure.

**Table 5:9 – Conduit and Routing Observation Results**

| *Conduit & Routing* | | *Section Rating:* | *LOW* |
|---|---|---|---|
| ***Observation*** | ***Comments*** | ***Recommendation*** | ***Criticality*** |
| Permanent link copper cables enter enclosures near a 3-phase power source. | Multiple instances of Ethernet cabling being routed near high voltage lines were seen. These should be addressed to ensure that intermittent communication issues do not occur. | The allowable proximity to power lines is determined by the voltage/current in the power lines and the type of network cable used. Verify that cable proximity to power lines is compliant with recommended distances based on the installation. (ODVA Ethernet/IP Media Planning & Install Guide ) | LOW |
| Copper cabling is routed near fluorescent lighting. | | Fluorescent lighting generates electrical noise that can be coupled into copper cabling if the cable is too close to the light fixture. (ODVA Ethernet/IP Media Planning & Install Guide ) | LOW |
| Conduit fill capacity exceeds TIA-569 (60% filled) standard. | A few instances where recommendations regarding maximum conduit fill capacity were seen | Run additional conduit or redesign the conduit run so that conduits are less than 60% filled. | LOW |
| Copper cabling is routed through the IACS environment in an inner duct. | | Information Purposes Only | ACCEPTABLE |
| Copper cable runs exceed 30 meters. | | In under-floor systems or conduit systems ensure that a pull-box is used when runs exceed 30m (100ft). Center-pull and/or back-feeding methods are recommended to reduce cable loading. | LOW |
| More than two 90 degree bends exist in the copper cable run. | | In under-floor systems or conduit systems ensure that a pull-box is used when there are more than two 90 degree bends in the conduit. Center-pull and/or back-feeding methods are recommended to reduce cable | LOW |

| | | | |
|---|---|---|---|
| | | loading. | |
| Fiber optic cable is routed through the IACS environment in an inner duct. | | Information Purposes Only | ACCEPTABLE |
| It is unknown if more than two 90 degree bends exist in a fiber cable run. | | In under-floor systems or conduit systems, install a pull-box when there are more than two 90-degree bends. Center-pull and/or back-feeding methods are recommended to reduce cable loading. | LOW |
| Fiber optic cables are not exposed to environmental conditions. | This was not explicitly validated throughout the entire facility and should be verified to ensure a robust fiber infrastructure | Information Purposes Only | ACCEPTABLE |
| Fiber optic cable environmental exposure does not include chemicals. | This was not explicitly validated throughout the entire facility and should be verified to ensure a robust fiber infrastructure | Information Purposes Only | ACCEPTABLE |
| Fiber optic cable environmental exposure does not include moisture. | This was not explicitly validated throughout the entire facility and should be verified to ensure a robust fiber infrastructure | Information Purposes Only | ACCEPTABLE |
| Fiber optic cable environmental exposure does not include sunlight. | This was not explicitly validated throughout the entire facility and should be verified to ensure a robust fiber infrastructure | Information Purposes Only | ACCEPTABLE |
| Fiber optic cable environmental exposure does not include fire hazard. | This was not explicitly validated throughout the entire facility and should be verified to ensure a robust fiber infrastructure | Information Purposes Only | ACCEPTABLE |
| Fiber optic cable environmental exposure does not include extreme temperatures. | This was not explicitly validated throughout the entire facility and should be verified to ensure a robust fiber infrastructure | Information Purposes Only | ACCEPTABLE |

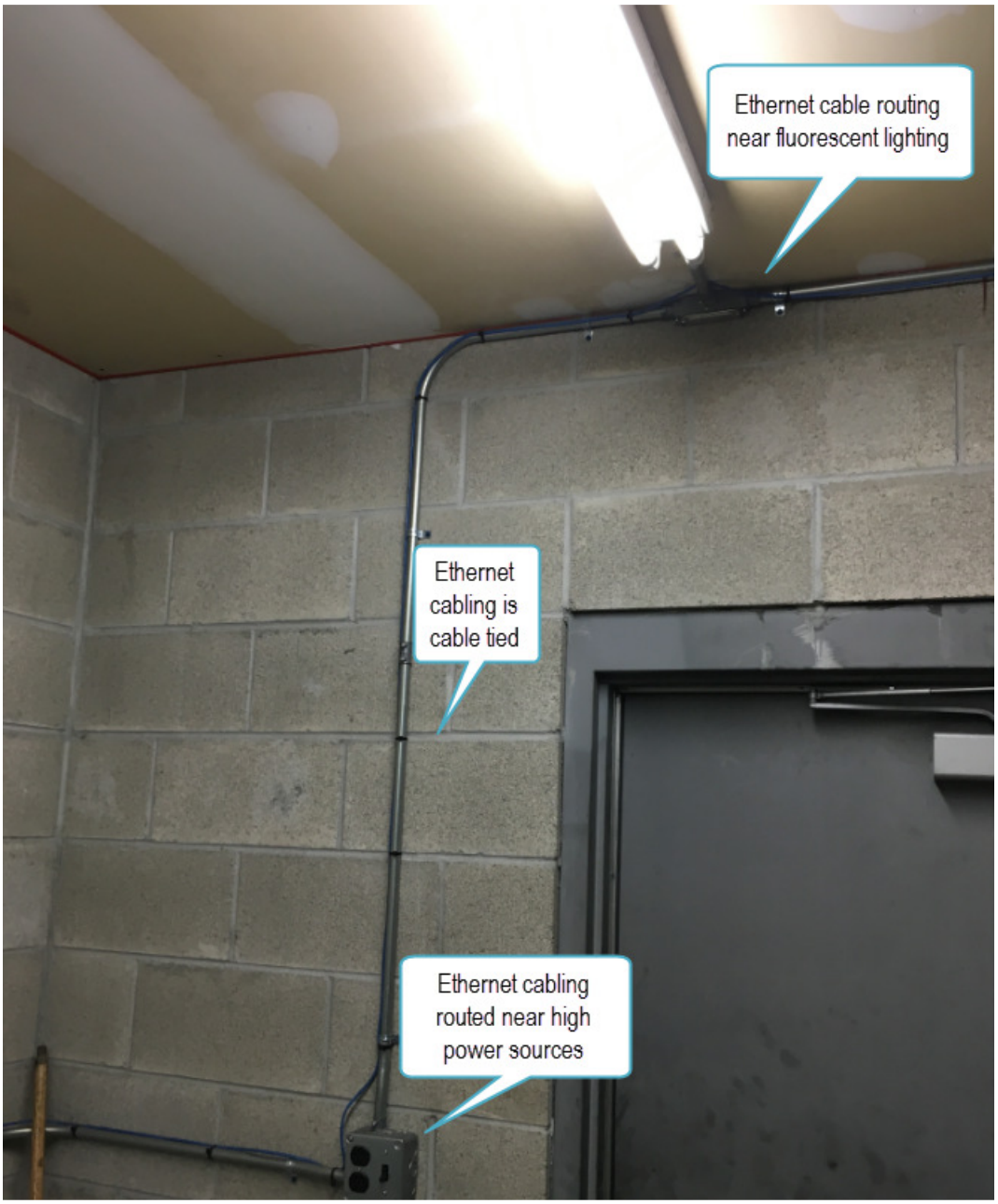


**Figure 5:12 - Slitter #4 Drives Room Cable Routing Near Fluorescent Lighting / High Power Source**

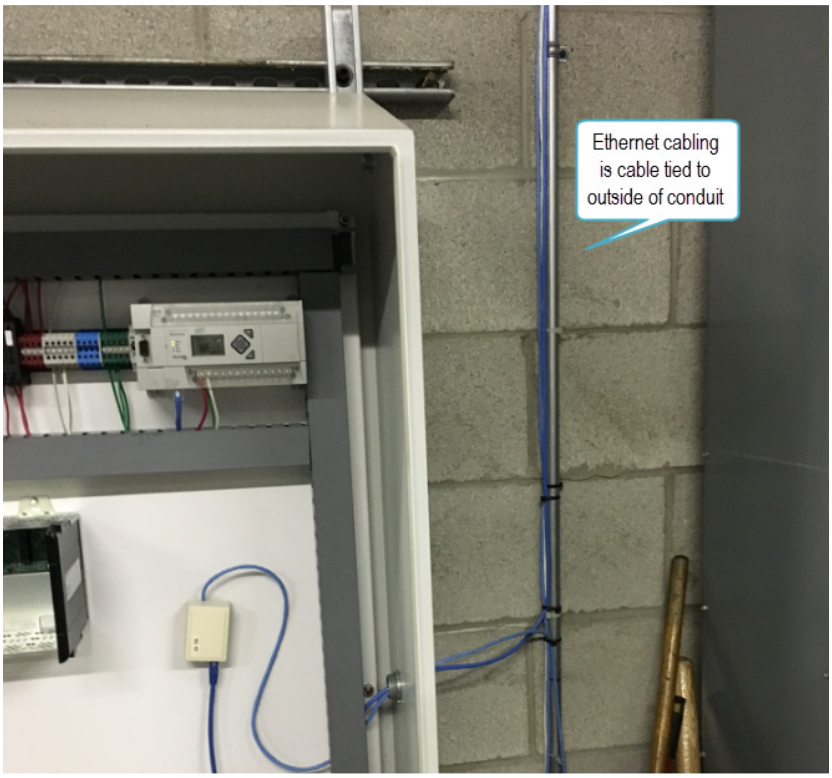


**Figure 5:13 - Mill #1 Quick Settings (QS) Panel**


**Figure 5:14 - Slitter #4 Drives Room**

## 5.10 Cable Labeling

Cable labelling standards are not consistently deployed in the production environment. This can lead to issues in network troubleshooting as termination points for each of the cables are not clearly outlined.

Please refer to Section 8.11 for recommendations on cable labelling practices.

**Table 5:10 – Cable Labeling Observation Results**

| *Cable Labeling* | | *Section Rating:* | *LOW* |
|---|---|---|---|
| ***Observation*** | ***Comments*** | ***Recommendation*** | ***Criticality*** |
| There is not a site standard for cable labeling. | | TIA-606B is the internationally accepted standard for labeling communication cables. This standard can be implemented in whole or in part to suit the needs of the site. (ANSI/TIA-606-B) | LOW |
| The labeling standard is not implemented consistently on site. | Various different methods are used to label cables from printed methods to hand written markings | Implement labeling standards consistently across the plant for increased ease in identifying cables and troubleshooting. (ANSI/TIA-606-B) | LOW |
| The label does not identify both end locations of the cable. | | Label all Ethernet cabling so that both end locations of the cable are identified as this can significantly aid in troubleshooting. (ANSI/TIA-606-B) | LOW |
| Documentation does not exist for cable labels on the IACS network. | | All outlet and cable labels should be included in the design documentation for the network and should be verified during a network validation process. (ODVA Media Planning and Installation Manual) | LOW |
| A change management procedure does not exist for updating cable labeling when changes are made on the IACS network. | | A change management process should exist for documenting changes that occur to the cable labeling scheme which include updating network drawings. | LOW |

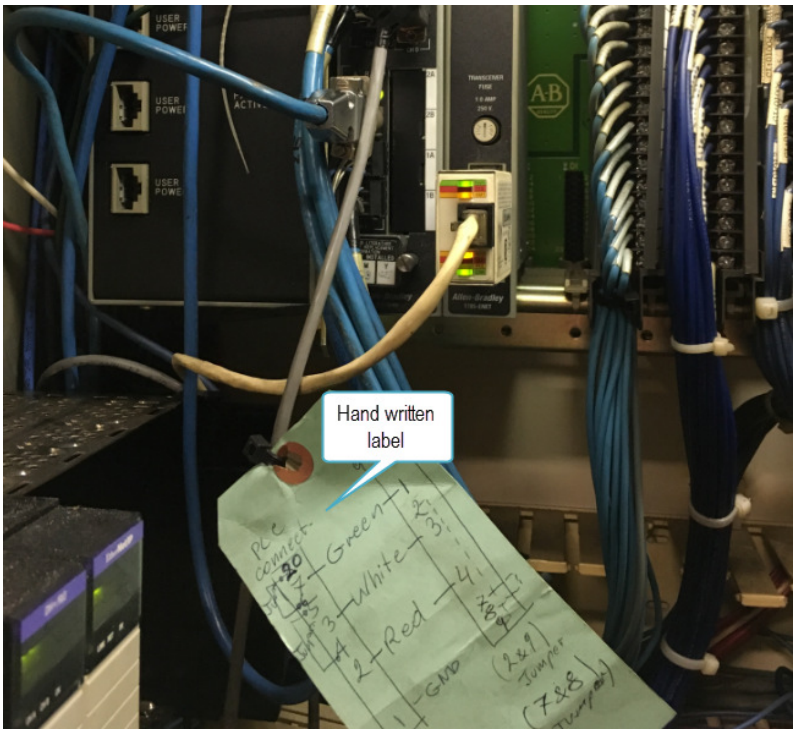


**Figure 5:15 - Mill #1 Travelling Cut-off Saw (TCOS)**

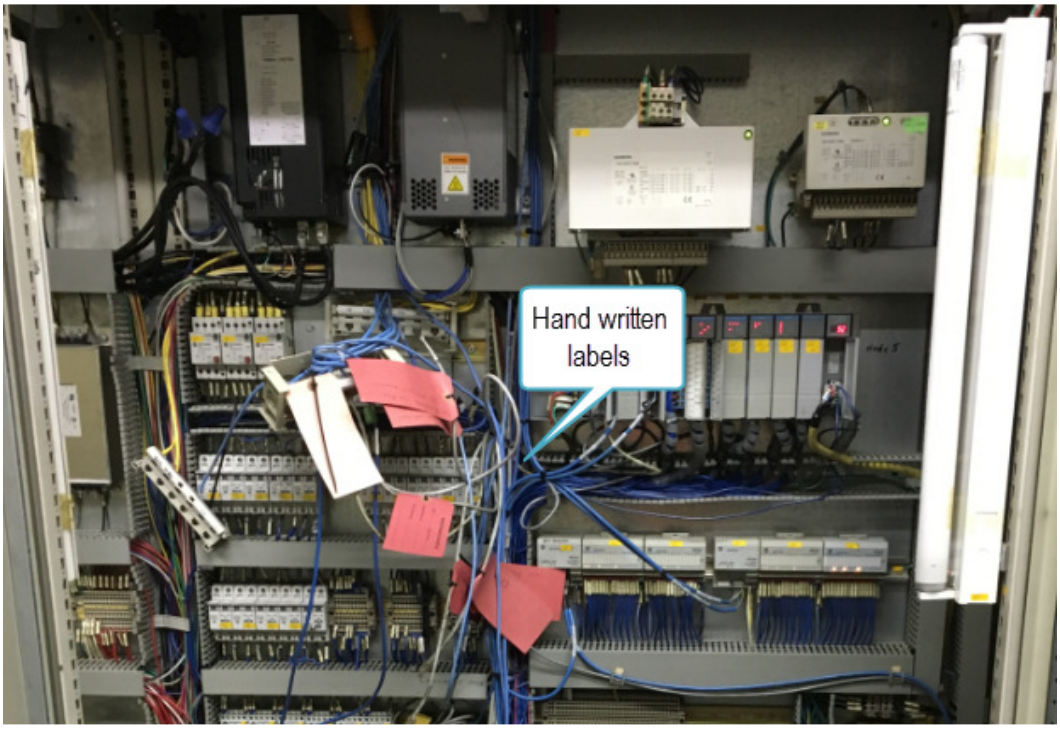


**Figure 5:16 - Mill #2 PTA**

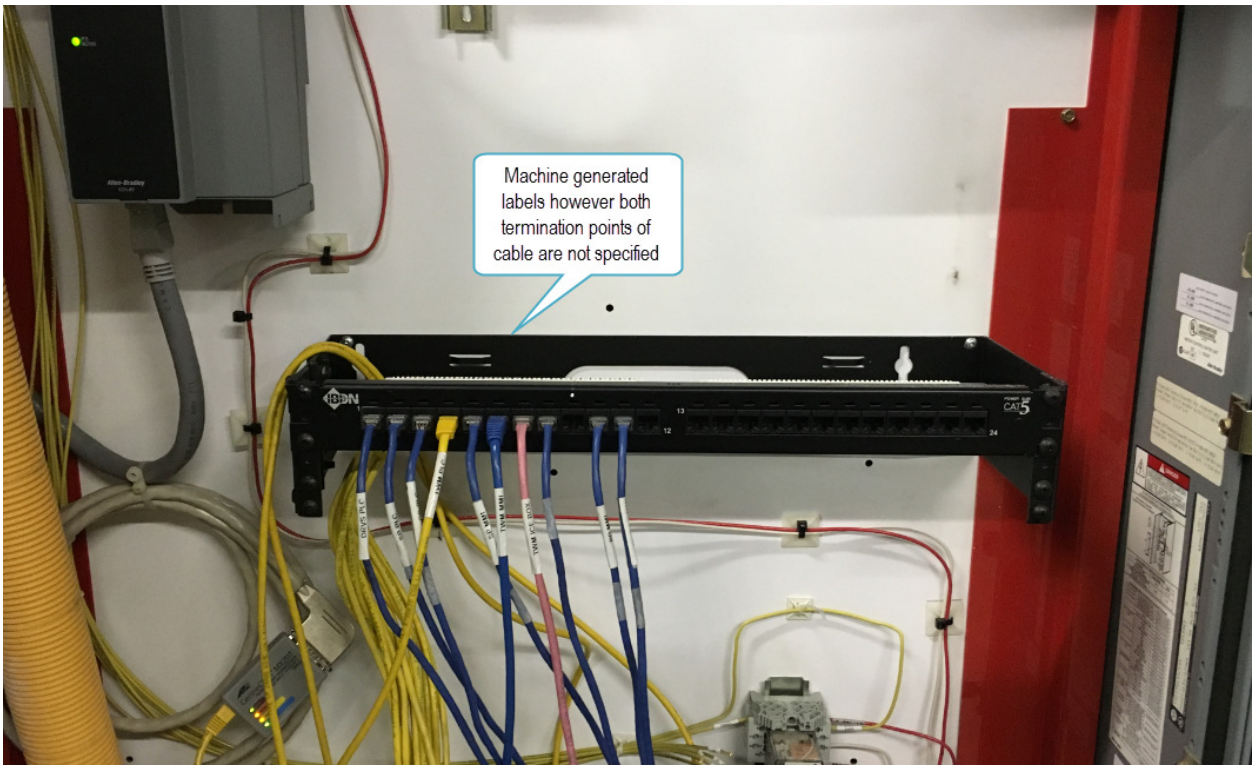


**Figure 5:17 - Mill #2 TWM Panel Cable Labeling**

## 5.11 Power Redundancy System

Uninterruptable Power Supplies (UPS) are used in various locations within the production environment (eg: Mill IT panels) however are not consistently applied to critical infrastructure equipment. Some situations may have switch infrastructure connected whereas others do not. This can pose significant issues during production in coming back from a power outage as various switch platforms can take in excess of 5 minutes to reboot.

Customer A, Location A should review the critical infrastructure components and come up with a plan to provide power redundancy for these items as required.

**Table 5:11 – Power Redundancy System Observation Results**

| ***Power Redundancy System*** | | ***Section Rating:*** | ***MODERATE*** |
|---|---|---|---|
| ***Observation*** | ***Comments*** | ***Recommendation*** | ***Criticality*** |
| There is a power redundancy strategy for network equipment. | Although there is a power redundancy strategy it is not deployed consistently throughout the design | Information Purposes Only | ACCEPTABLE |
| The strategy is not implemented across all network infrastructure components. | Only IT switch infrastructure has UPS backup at this point | Network infrastructure components are key to the overall operation of the IACS network, application or process. | MODERATE |

| | | | |
|---|---|---|---|
| | | A loss of power to these components could seriously impact the application or process, and with the long restart time (several minutes) of many of these devices, it could impact the restarting of the application or process. A risk analysis and / or a requirements analysis should be completed to determine the impact on the loss of the network infrastructure components. | |

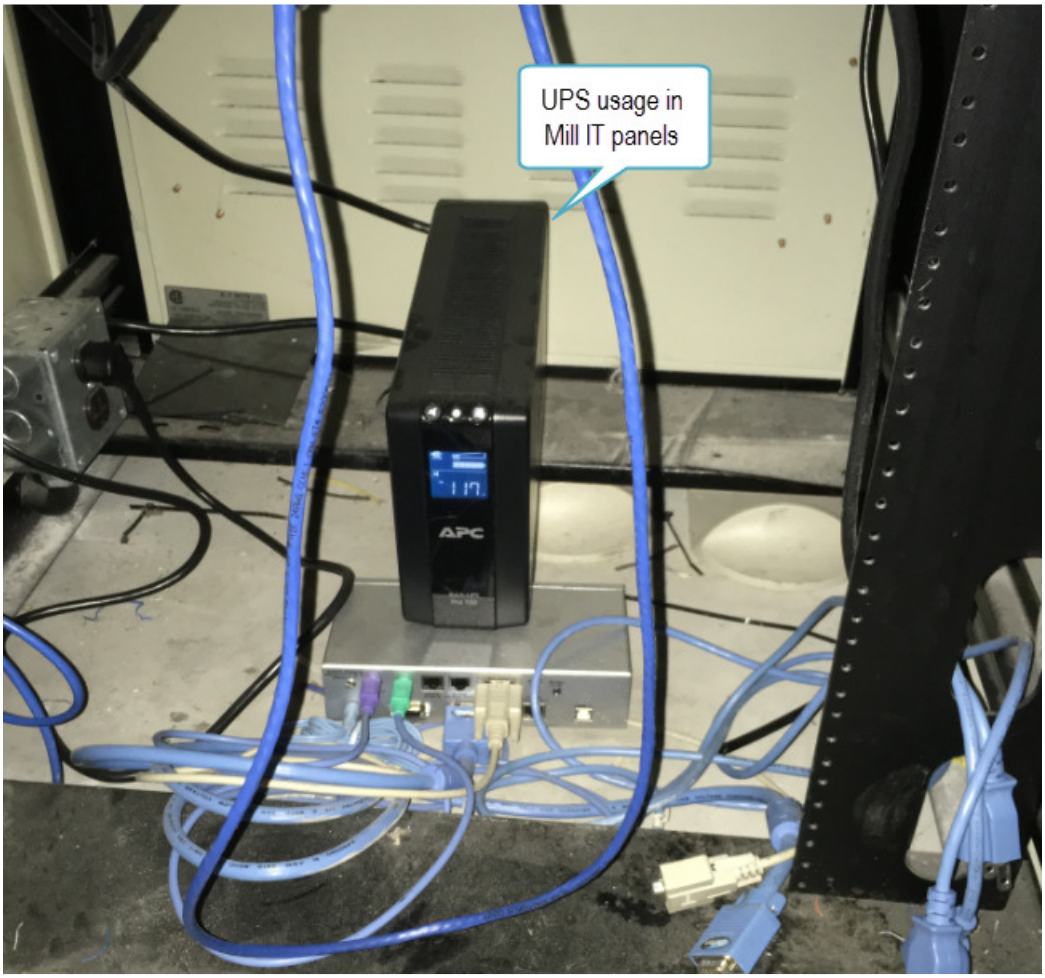


**Figure 5:18 - Mill 2 Drives Room #1 IT Cabinet**

## 5.12 Grounding

Grounding and bonding was seen to be done consistently within the production environment at Customer A, Location A.

**Table 5:12 – Grounding Observation Results**

| *Grounding* | | *Section Rating:* | *ACCEPTABLE* |
|---|---|---|---|
| ***Observation*** | ***Comments*** | ***Recommendation*** | ***Criticality*** |
| Control/network equipment is bonded to racks/cabinets. | This was not explicitly validated throughout the entire facility and should be verified to ensure proper grounding techniques are applied | Information Purposes Only | ACCEPTABLE |
| Control/network equipment is bonded to common ground. | This was not explicitly validated throughout the entire facility and should be verified to ensure proper grounding techniques are applied | Information Purposes Only | ACCEPTABLE |
| Metal conduit/wire way sections are bonded to adjacent sections. | This was not explicitly validated throughout the entire facility and should be verified to ensure proper grounding techniques are applied | Information Purposes Only | ACCEPTABLE |
| Metal conduit/wire way sections are bonded to termination points. | This was not explicitly validated throughout the entire facility and should be verified to ensure proper grounding techniques are applied | Information Purposes Only | ACCEPTABLE |

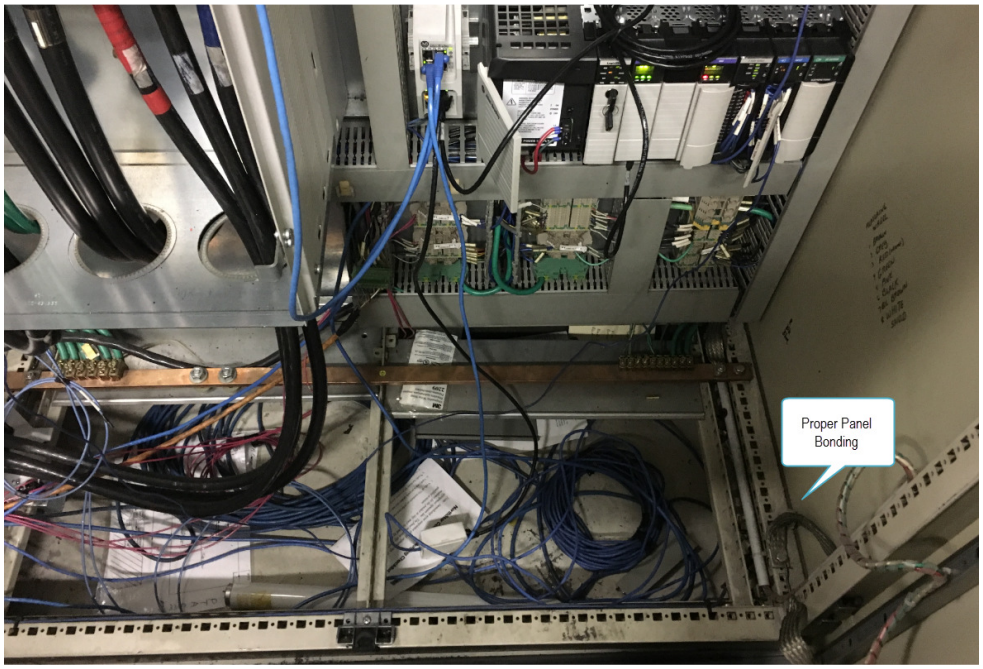


**Figure 5:19 - Mill #2 Saw Carriage Proper Panel Grounding / Bonding**

# 6 NETWORK LOGICAL INFRASTRUCTURE

The logical architecture at Customer A, Location A is based on a single flat subnet for all plant level communications. Although this approach may initially provide ease of connectivity as routing between various is not required, using a single subnet does not provide a future ready, scalable solution. As more production environment end device hardware (ie: drives, I/O, starters, etc.) becomes Ethernet communication capable the need to have a properly designed infrastructure to handle communications becomes critical.

A key challenge with the single subnet approach to the production environment is that it produces a single broadcast domain and single fault domain. These become critical items as any network event that occurs in Mill #1 can easily impact Mill #2 / Slitter #2 / Slitter #4 and could potentially bring production in the facility to a stop. Additionally, a single broadcast domain can start to overwhelm end devices as the network becomes larger. Finally, determinism of the network can be greatly impacted by larger broadcast domains and can significantly affect the performance of the industrial Ethernet control system.

To provide a method of obtaining a future ready, scalable network that reduces broadcast and fault domains, VLAN segmentation can be deployed. By developing an industrial networking plan as recommended in Section 2.1.3, the various aspects of using VLAN segmentation within the production environment can be explored. It is highly recommended to engage a professional network design resource to help in the design of a highly reliable, high performance, scalable and future ready network.

## 6.1 Logical Topology

VLAN segmentation is not currently used in the production environment. The currently allocated IP address range allows for 254 devices using a 192.168.10.0 /24 subnet.

**Table 6:1 – Logical Topology Observation Results**

| *Logical Topology* | | *Section Rating:* | *HIGH* |
|---|---|---|---|
| ***Observation*** | ***Comments*** | ***Recommendation*** | ***Criticality*** |
| Logical flow maps do not exist for the IACS network. | Only rudimentary physical network topological maps exist at this point | Logical flow maps should exist for the IACS network and show detailed information of traffic flow between all devices on the IACS network. | LOW |
| The production environment network is not segmented into subnets. | | Information Purposes Only | HIGH |
| Subnets are not separated logically. | | IP networks are divided into smaller network called subnets. Each subnet represents a group of hosts on the network. Hosts on the same subnet communicate directly with each other over the Layer 2 network. Hosts on different subnets communicate with each other via their default gateways. Subnets divide the IP network into smaller, more manageable | HIGH |

| | | | |
|---|---|---|---|
| | | networks. In the CPwE architecture, it is recommended to use VLAN segmentation wherever possible. Additionally, each VLAN in the Manufacturing zone should have a unique subnet assigned to it. | |
| Additional subnets are separated physically. | Although the production environment is on a single subnet, there are 2 other subnets in use for the HMI network and encoder network in Mill #1. These are currently segmented via the ControlLogix backplane. | Information Purposes Only | ACCEPTABLE |
| A thorough specification guide is not provided to OEMs for network compliance | At this point, preliminary specifications are outlined to OEMs when the project team is involved however this is not included as a portion of the project bid package. | A specification guide should be created that provides OEMs with requirements to meet plant network compliance. (CPwE DIG) | LOW |
| Critical IACS devices are not redundant and are not on redundant networks. | | IACS components or networks that are classified as critical to the organization have high availability requirements. One method of achieving high availability is through the use of redundancy. Lack of redundancy in critical components could provide single point of failure possibilities. (800-82) | HIGH |
| Critical IACS devices are not designed for graceful degradation to prevent catastrophic cascading evenings. | Currently there are linear segments of switches within the network topology that could be affected based on a single failure point | If a component fails, it should fail in a manner that does not generate unnecessary traffic on the IACS, or does not cause another problem elsewhere, such as a cascading event. (800-82) | HIGH |

## 6.2 Security Zone

Separation from the enterprise network is currently being done via a single Juniper Networks firewall. Although this is a suitable method for small scale control systems, the magnitude of the production Ethernet network is increasing with new equipment slated to be added. This approach should be evaluated in regards to its acceptability within the production environment at Customer A, Location A.

To provide a scalable architecture, the use of an Industrial De-Militarized Zone (IDMZ) that includes active / backup firewalls between the production and enterprise allows for increased segmentation, secure data flow, and added security on the production network. Rockwell Automation recommends that IDMZs are deployed over traditional firewalls as IDMZs ensure that no data directly traverses from the production environment to the enterprise. For further information on the approach of deploying an IDMZ, please reference our joint Rockwell Automation / Cisco document "Securely Traversing Data across the Industrial De-Militarized Zone" outlined in Section 1.2.

**Table 6:2 – Security Zone Observation Results**

| ***Security Zone*** | | ***Section Rating:*** | ***MODERATE*** |
|---|---|---|---|
| ***Observation*** | ***Comments*** | ***Recommendation*** | ***Criticality*** |
| The IACS network is isolated from the Enterprise network. A firewall currently provides the isolation. | Isolated currently via a singular firewall without the use of replication servers as recommended within our standardized approach using an IDMZ. | Information Purposes Only | ACCEPTABLE |
| Security appliances are not used on the network. | | Information Purposes Only | MODERATE |
| The IACS is not configured to maximize use of vendor supplied security features. | Although most of the IACS switches do have an IP address allocated, they are not optimized for the application via configuration to benefit from the various security features available. | Switches have been susceptible to attacks such as MAC spoofing, table overflows, and attacks against the spanning tree protocols, depending on the device and its configuration. A variety of features such as MAC address filtering, port-based authentication using IEEE 802.1x, and specific vendor recommended practices can be used to mitigate these attacks, depending on the device and implementation. (800-82) | MODERATE |
| The IACS network has not become disabled during adverse conditions. | | Information Purposes Only | ACCEPTABLE |

## 6.3 Manufacturing Zone

The current architecture follows a segmented distribution switching architecture (via the Cisco 2960-S switches in each Mill) and does not have a dedicated router as all plant level devices communicate via a single subnet. To allow for recommended segmentation of traffic dedicated VLANs for the production environment are recommended.

Using the approach of having dedicated VLANs for the production environment creates the need for routing. It is highly recommended that inter-VLAN routing take place on a dedicated router (or router pair) within the production environment. Using a dedicated router in the production environment ensures that the plant operations can be completely disconnected from the enterprise in the event of a network issue thus allowing for communications on the production network to continue.

**Table 6:3 – Manufacturing Zone Observation Results**

| *Manufacturing Zone* | | *Section Rating:* | *HIGH* |
|---|---|---|---|
| ***Observation*** | ***Comments*** | ***Recommendation*** | ***Criticality*** |
| Core network devices are not dedicated to the IACS network. | Routing is not currently completed in the production environment | The converged resource model forces two different asset types, the Enterprise and the IACS networks, to share the same physical and logical network infrastructure. They have different and often conflicting requirements regarding uptime, management, end user requirements, critically ratings, and Quality of Service (QoS) settings. It is recommended that they be separate devices when multiple VLANs are present in the production environment. When that cannot occur, a complete requirements and risk analysis should be completed. | MODERATE |
| A router is not installed on the IACS network. | | Information Purposes Only | ACCEPTABLE |
| The logical framework for the IACS network does not follow a hierarchal or campus model design methodology. | Although somewhat of a hierarchical approach is taken within the topology, an implementation with integrated routing in the production environment via a Core router is not present | The Converged Plantwide Ethernet (CPwE) network logical framework is the foundation of an IACS. It is based on the Purdue Reference model, ISA99, and the Cisco Hierarchy or Campus network design. The Cisco Hierarchy defines 3 levels of networking infrastructure functionality as follows:<br>• Access – Provides connectivity to end devices. OSI Layer 2 | LOW |

| | | | |
|---|---|---|---|
| | | switching; security; and QoS<br>• Distribution – Aggregates the Access mode switches; Uses OSI Layer 3 protocols; Provides additional security; policy enforcement; load balancing; fast convergence; and scalability.<br>• Core – Network backbone – Fast convergence; Highly reliable; Stable; aggregates the Distribution Switches; and provides connectivity to the IDMZ.<br>On a smaller network the Core and Distribution levels may be combined in a collapsed core / distribution configuration. In the CPwE network framework, the core and distribution levels (either separate or collapsed) are part of the Manufacturing Level. It is recommended that this hierarchy approach be implemented within the IACS network regardless of the size of the network infrastructure being deployed. | |
| Managed switches are employed at the Core / Distribution level. | | Managed switches are recommended throughout the IACS Network. This requirement is for the following but not limited to:<br>• Network Performance<br>• Troubleshooting.<br>• Monitoring. | ACCEPTABLE |
| The Core / Distribution level managed switches have not been configured. | Although managed switches are used in the Cisco 2960-S distribution level switches, they have not been configured and optimized for the application | Managed switches that are not configured will not maintain the proper level of network performance required for the IACS. Managed switches should be configured. The specific details on how the switches should be configured are application specific and a requirements analysis should be done to gather the data to properly configure the switches. | LOW |

| | | | |
|---|---|---|---|
| The Core / Distribution level switch configurations have not been verified for accuracy. | Discussions with both the operations group as well as the IT department revealed minimal configuration in both the distribution and access level switches | The end configuration of the switch is the important part of ensuring high performance operation of the network. Regardless of the process used to configure the network infrastructure assets, a machine by machine validation of the configuration should be performed by on-site personnel. | LOW |
| A company standard or policy does not exist for the configuration and operation of Core / Distribution level IACS switches. | | A separate and unique set of policies should be available for the IACS network. It is common place to have a policy or a set of polices for the enterprise network infrastructure regarding the configuration and operation of the networking assets. The IACS network infrastructure should also have a set of policies regarding the network infrastructure that will address the specific needs and requirements of the IACS network. It is recommended that these documents are created and kept up to date as changes occur with the IACS Network. To create the document a requirements analysis is be required. | LOW |
| An Ethernet/IP I/O network using MSG instructions is employed on the IACS network. | MSG instructions are used to communicate between various processors containing information on their status and any required interlocks | Information Purposes Only | ACCEPTABLE |
| The Ethernet/IP I/O network is connected employing a shared switch. | | Location of how I/O devices are connected to the network depends on requirements of the control system. Intercommunication requirements on types of communication and the speed (device RPI) at which they communicate need to be understood before a recommendation can be made. | ACCEPTABLE |
| VLANs are not employed for network segmentation. | A single subnet is used for the production environment | Information Purposes Only | HIGH |

| | | | |
|---|---|---|---|
| A dedicated management VLAN does not exist on the IACS network. | | By default, the management VLAN is VLAN1 and should not be used. A separate VLAN should be created for the use of switch management. | LOW |
| Dedicated VLANs do not exist for managing all of the different IACS network operations. | | The IACS network should include logical segmentation of traffic throughout the manufacturing zone. A complete requirements analysis and risk analysis should be completed to determine proper logical segmentation. | LOW |
| Open switchports on Core / Distribution level switches have not been administratively shutdown (disabled). | | Unused switch ports (interfaces or ports) on the switch pose a security risk to the network. When not in use, they should be disabled (or placed in a shutdown state). On Cisco devices and Allen-Bradley Stratix 6000, 8000, 8300, & 5700 switches, the state of the switch ports (interfaces or ports) can be controlled from the manufacturing applications to allow the interface state to be changed to allow temporary network access for maintenance connectivity. | ACCEPTABLE |
| The Manufacturing Zone is connected to the Cell / Area Zone via switch to switch. | | Method utilized to uplink to Manufacturing Zone depends on the requirements of the cell / area zone and supervisory systems. Chassis based uplinks will limit the type of traffic allowed across the backplane and to remaining devices below the chassis. A complete requirements analysis and risk analysis should be completed to determine proper method to uplink cell / area zone networks. | ACCEPTABLE |
| There is only a single path connecting the Core / Distribution level switches to the Access level switches. | Resilient / redundant paths are not currently used | Multiple communication paths (especially diverse paths) improve the resiliency of the network and may improve performance. | LOW |
| The IPv4 address schema is | IP addresses of the plant connected | Information Purposes Only | ACCEPTABLE |

| | | | |
|---|---|---|---|
| documented for IACS network. | IACS devices are documented in an Excel sheet however the information was not verified as to its accuracy | | |
| The IACS network IP address schema is employing a private IPv4 address range. | | Information Purposes Only | ACCEPTABLE |
| Procedures exist for the replacement and configuration of IACS devices. | | Information Purposes Only | ACCEPTABLE |
| IP address segmentation exists between the Enterprise network and the IACS network. | The production environment is isolated from the enterprise via the use of Network Address Translation (NAT) techniques within the Juniper Networks firewall (as per Customer A IT personnel) | Information Purposes Only | ACCEPTABLE |

## 6.4 Cell/Area Zone

The use of managed switches within the production environment is predominant with most being either the Stratix 6000 or Stratix 5700 variants (approximately 95% of switches within the production environment are managed). Managed switches provide advanced functionalities when compared to unmanaged switches as follows:

- Multicast traffic management to effectively direct traffic to the intended recipients
- Built-in prioritization of certain traffic types based on configuration
- Traffic segmentation to limit broadcast domains (ie: VLAN's)
- Loop prevention
- Ease of troubleshooting through physical connection diagnostics
- Configurable port security (ie: MAC address monitoring / blocking, port shutdown, etc.)

Due to the advanced functionality available within managed switches, a continued approach that includes the use of managed switches as much as possible (if not exclusively) within the production environment should be taken.

It is important to note that managed switches can only provide optimal performance on the network when they are configured with special considerations as to the requirements of each application. Most switches in the production environment at Customer A, Location A have minimal configuration (most are only supplied with an IP address enabling managed features) as optimized configuration has not been completed. Each switch should be evaluated and configured to allow for enhanced performance of the production network.

**Table 6:4 – Cell/Area Zone Observation Results**

| *Cell/Area Zone* | | *Section Rating:* | *HIGH* |
|---|---|---|---|
| ***Observation*** | ***Comments*** | ***Recommendation*** | ***Criticality*** |
| The access level switches within the Cell/Area zones of the IACS network are a combination of managed and unmanaged switches. | Although the use of managed switches is predominant, there are still a few unmanaged switches in use | Use of unmanaged switches in combination with managed switches may leave the IACS exposed to security risks, degrade the performance, and degrade the quality of the network services. This may cause various issues including network and system outages. | MODERATE |
| Managed access level switches within the Cell/Area zones have been configured. | Although they have been configured, minimal optimization has been completed to tailor the configuration for each application | Information Purposes Only | ACCEPTABLE |
| The Device Manager (Web Interface) was used to configure the access level switches with the Cell/Area zones. | | Information Purposes Only | ACCEPTABLE |
| The managed access level switch configurations have not been verified for accuracy. | Managed switch configurations were not validated however they were discussed with IT and operations personnel to obtain a thorough understanding of the approach | The end configuration of the switch is the important part of ensuring the proper configuration and operation of the network. Regardless of the | LOW |

| | | | |
|---|---|---|---|
| | completed. | process used to configure the network infrastructure assets, a machine by machine validation of the configuration should be performed. | |
| A company standard or policy does not exist for the configuration and operation of IACS switches | | A separate and unique set of policies should be available for the IACS network.<br>It is common place to have a policy or a set of polices for the enterprise network infrastructure regarding the configuration and operation of the networking assets. The IACS network infrastructure should also have a set of policies regarding the network infrastructure that will address the specific needs and requirements of the IACS network.<br>It is recommended that these documents are created and kept up to date as changes occur with the IACS network. To create the document a requirements analysis may be required. | HIGH |
| Access level switches are managed by a PLC (PAC). | Many of the Stratix 6000 / Stratix 5700 managed switches in use have been brought into the I/O tree within Logix 5000 for monitoring | Information Purposes Only | ACCEPTABLE |
| Access level switches do not support more than one Cell/Area zone. | | Consolidating the number of switches within the overall IACS network infrastructure reduces the configuration time, and simplifies deployment. A risk and requirements analysis should be done to determine the best architecture for a given application. | MODERATE |
| Open switch ports exist on access level switches. | | Information Purposes Only | ACCEPTABLE |
| Open switch ports on access level switches have not been administratively shutdown (disabled). | | Unused switch ports (interfaces or ports) on the switch pose a security risk to the network. When not in use, they should be disabled or placed in a shutdown state. On Rockwell | MODERATE |

| | | | |
|---|---|---|---|
| | | Automation Stratix 6000, 8000, 8300, & 5700 switches, the state of the switch ports (interfaces or ports) can be controlled from the manufacturing applications to allow the interface state to be changed to allow temporary network access for maintenance connectivity. | |

# 7 INDUSTRIAL SECURITY & SAFETY

At Customer A, Location A security within the network architecture of the production environment is primarily handled via the use of Access Control Lists (ACLs) style of scripts within a dedicated firewall separating the enterprise and production environments. Other methods of security enforcement are also evident including local PC hardening on the maintenance laptops through the use of anti-virus software.

It is important to note that hardening of the network infrastructure and end devices in the production environment was often not completed. This includes the following:

- Hardening of the switches via configuration of various security aspects (ie: port security, MAC address tracking per port, Access Control Lists (ACLs), etc.)
- Enforcement of standards regarding the use of portable media storage devices
- Instituting a Defense in Depth approach as outlined within multiple standards such as those developed by the National Institute of Standards and Technology (NIST).

Please note that cyber-attacks on production facilities are becoming more common and therefore security should be a major topic of consideration moving forward. Rockwell Automation treats security within the production environment very seriously and recommends a thorough evaluation be completed to minimize the effect of potential threats.

Please note that all aspects dealing with safety in the production environment are handled via procedures and physical guarding on the various machines. The one exception is the Mill #2 Safety Prep panel as it has a single CompactLogix L43S safety processor that uses managed switches for network infrastructure to carry the CIP Safety traffic to the various end devices.

## 7.1 Asset Management

Assets are centrally managed through an Enterprise Resource Planning (ERP) system within the Customer A, Location A facility. All devices stocked are outlined within the ERP system and are updated upon removal.

Currently manual processes are in place to ensure backup copies of programs are available and stored on local maintenance laptops as well as network drives upon changes. To provide an automated method of achieving this backup please refer to FactoryTalk® AssetCenter literature on the Rockwell Automation website or via contacting your local Rockwell Automation representative

**Table 7:1 – Asset Management Observation Results**

| *Asset Management* | | *Section Rating:* | *MODERATE* |
|---|---|---|---|
| ***Observation*** | ***Comments*** | ***Recommendation*** | ***Criticality*** |
| A policy exists requiring an accurate inventory be established and maintained for IACS assets. | | Information Purposes Only | ACCEPTABLE |
| A procedure exists for maintaining an accurate inventory of IACS hardware assets. | | Information Purposes Only | ACCEPTABLE |
| A procedure exists for maintaining an accurate inventory of IACS software assets. | | Information Purposes Only | ACCEPTABLE |

| | | | |
|---|---|---|---|
| A procedure does not exist to address unauthorized software and hardware. | | All components in the IACS should be verified within the authorization boundary and either inventoried as a part of the system or recognized by another system as a component within that system. (800-53) | MODERATE |
| The IACS inventory is updated to reflect installations, removals, and updates. | | Information Purposes Only | ACCEPTABLE |
| A policy exists to ensure IACS device configurations can be restored to their last known operable state. | Completed via stored copies of the latest programs on maintenance laptops / network drives | Information Purposes Only | ACCEPTABLE |
| A procedure exists to ensure modified device configuration files are updated and stored off-line. | The procedure may or may not be officially documented however is understood among the maintenance personnel | Information Purposes Only | ACCEPTABLE |
| A Bill of Materials (BOM) does not exist for parts used in critical infrastructure. | | Establish an accurate BOM for the IACS. Without a BOM, material planning and replenishment are often made in an information vacuum, resulting in excess inventory levels, stock outages, significant expediting charges, and expensive downtime. | LOW |
| Accurate product lifecycle information does not exist for all IACS physical assets. | | Product lifecycle information should be available and managed for all IACS assets. Please see Section 4 of this document for further details | LOW |
| Accurate product lifecycle information does not exist for all IACS critical infrastructure. | | Accurate product lifecycle information should be required for all IACS critical infrastructure which if not available, could result in downtime in parts becoming discontinued. | LOW |
| An exchange service contract does not exist providing 24-hour turn around on replacement inventory for critical components. | Due to the fact that service contracts don't exist for the network infrastructure equipment, spares are held locally on site. This is seen as an acceptable method by plant personnel. | A 24-hour turn around on replacement inventory for critical IACS components is advised, even if spares are available at the site. | LOW |
| A procedure does not exist for identifying discontinued physical assets. | | A procedure should be established for identifying and documenting discontinued physical assets so a | LOW |

| | | | |
|---|---|---|---|
| | | replacement asset can be identified and tested. | |
| A procedure exists for migrating discontinued physical assets. | | Information Purposes Only | ACCEPTABLE |
| A procedure exists for accurately documenting installed software. | | Information Purposes Only | ACCEPTABLE |
| A procedure does not exist for accurately tracking software licenses. | Various versions of Rockwell software are installed on the maintenance laptops however are not synchronized to ensure compatibility | A procedure should exist for accurately tracking software licenses to eliminate potential downtime resulting from software license complications. | LOW |
| A procedure does not exist for performing an internal software audit. | | A procedure should be developed for identifying and testing all software installed on IACS devices. Software not vital to the IACS should be eliminated. | LOW |

## 7.2 Governance

**Table 7:2 – Governance Observation Results**

| Governance | | Section Rating: | LOW |
|---|---|---|---|
| **Observation** | **Comments** | **Recommendation** | **Criticality** |
| Security policies have not been developed specific to the IACS. | Although policies exist for the enterprise, these are not transferred over to the production environment. | Security policies specific to the IACS should be developed taking into consideration performance, availability, and risk management requirements. (800-82) | LOW |
| Policies do not exist requiring the auditing of specific processes on the IACS. | | Independent audits should review and examine records and activities to determine the adequacy of system controls and ensure compliance with established IACS processes. Audits should also be used to detect breaches in IACS security services and recommend changes, which may include making existing security controls more robust and/or adding new security controls. (800-82) | LOW |
| A policy exists requiring suppliers to be vetted prior to initiating contractual agreements. | | Information Purposes Only | ACCEPTABLE |
| A policy exists requiring IACS products to be vetted prior to purchasing. | | Information Purposes Only | ACCEPTABLE |
| A policy exists pertaining to the use of IACS re-manufactured or refurbished products. | | Information Purposes Only | ACCEPTABLE |
| A policy exists requiring the use of approved shipping vendors for the shipping and receiving of IACS network devices. | | Information Purposes Only | ACCEPTABLE |
| A policy does not exist stating the information security responsibilities for vendors. | | Specific security policies should be developed and state the security responsibilities for vendors. Training should be included as required. (800-82) | LOW |
| A policy does not exist stating the information security responsibilities for contractors. | | Specific security policies should be developed and state the security responsibilities for | LOW |

| | | | |
|---|---|---|---|
| | | contractors. Training should be included as required. (800-82) | |
| A response plan exists stating the procedure if the IACS network communication is interrupted. | All communications should be disrupted at the firewall connection to the production environment | Information Purposes Only | ACCEPTABLE |
| A response plan exists stating the procedure if there is a critical physical asset failure. | | Information Purposes Only | ACCEPTABLE |
| A policy exists requiring IACS data to be backed up. | All changes to configurations / programs are to be backed up by maintenance personnel | Information Purposes Only | ACCEPTABLE |
| Critical IACS backup data is not stored at a facility separate from the live environment. | All data is stored locally within maintenance laptops or available network drives | Identify an alternate storage site that is separated from the primary storage site so as not to be susceptible to the same hazards. Configure the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives. Identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline explicit mitigation actions. (800-53) | LOW |
| Backup media and data is not tested for reliability and integrity. | | Test backup information to verify media reliability and information integrity. Use a sample of backup information in the restoration of selected IACS functions as part of contingency plan testing. (800-53) | LOW |

## 7.3 Risk Assessment & Management

As of this point, many risk assessment processes are not employed within the production environment to mitigate potential threats. These should be evaluated based on critical processes to ensure that production uptime is maximized.

**Table 7:3 – Risk Assessment and Management Observation Results**

| *Risk Assessment & Management* | | *Section Rating:* | *HIGH* |
|---|---|---|---|
| ***Observation*** | ***Comments*** | ***Recommendation*** | ***Criticality*** |
| There have been no security incidents reported to the DHS IACS Cyber Emergency Response Team. | | The goal of the DHS National Cyber Security Division's CSSP is to reduce industrial control system risks within and across all critical infrastructure and key resource sectors by coordinating efforts among federal, state, local, and tribal governments. This also spans industrial control systems owners, operators and vendors. The CSSP coordinates activities to reduce the likelihood of success and severity of impact of a cyber-attack against critical infrastructure control systems through risk-mitigation activities. (800-82) | LOW |
| A risk assessment has not been performed specific to the IACS network. | | An IACS network risk assessment should be performed and is intended as a common basis and practical guideline for developing organizational security standards and effective security management practices, and to help build confidence in inter-organizational activities. (800-82) | LOW |
| A vulnerability assessment has not been executed on the IACS environment. | | Include as part of security control assessments in-depth monitoring, malicious user testing, and penetration testing. Testing on a live production environment should be evaluated before executing. (800-53) | LOW |
| Scanning tools are not used to identify vulnerabilities. | | Employ vulnerability scanning tools that include the capability | LOW |

| | | | |
|---|---|---|---|
| | | to readily update the list of IACS vulnerabilities scanned. (800-53) | |
| Procedures do not exist for vulnerability validation and mitigation. | | A method for assessing and rating the risk of a possible vulnerability at a specific facility is needed. The risk is a function of the likelihood (probability) that a defined threat agent (adversary) can exploit a specific vulnerability and create an impact (consequence). The risk induced by any given vulnerability is influenced by a number of related indicators including, Network and computer architecture and conditions, Installed countermeasures, Technical difficulty of the attack, Probability of detection (e.g., amount of time the adversary can remain in contact with the target system/network without detection), Consequences of the incident, and Cost of the incident. These are considering factors when developing a vulnerability mitigation procedure. | LOW |
| A procedure does not exist to evaluate the impact to assets as a result of a security compromise. | | A method for assessing and rating the risk of a possible vulnerability at a specific facility is needed. The risk is a function of the likelihood (probability) that a defined threat agent (adversary) can exploit a specific vulnerability and create an impact (consequence). The risk induced by any given vulnerability is influenced by Consequences of the incident and Cost of the incident. These include the impact to IACS assets which could include downtime. | LOW |
| Vendor documentation does not exist regarding security controls and features employed in the IACS environment. | Although documentation does exist from the IACS device manufacturer regarding various security features, it is not updated on-site to reflect the use | Obtain, protect as required, and make available to authorized personnel, vendor/manufacturer documentation that describes | LOW |

| | | | |
|---|---|---|---|
| | of specific items. | the functional properties of the security controls employed within the IACS with sufficient detail to permit analysis and testing. (800-53) | |
| A policy does not exist requiring updates to software when updates are released by vendors. | Many new features are available for the controllers and network infrastructure devices currently in use and should be evaluated for their applicability | Centrally manage the flaw remediation process and install software updates only after testing in an isolated test environment. Due to IACS integrity and availability concerns, give careful consideration to the methodology used to carry out automatic updates. (800-53) | LOW |
| A procedure does not exist to test software in an isolated environment before being installed on the live IACS. | | OS and application security patches deployed without testing could compromise normal operation of the IACS. Documented procedures should be developed for testing new security patches. | HIGH |

## 7.4 Access Controls

Corporate policies are in place to restrict the access to the Industrial Automation Control System (IACS) devices via the use of specific laptops that are password protected. In saying this, there are areas where potential improvements can be made to increase security and should be reviewed to ensure their applicability to the production environment.

**Table 7:4 – Access Controls Observation Results**

| *Access Controls* | | *Section Rating:* | *HIGH* |
|---|---|---|---|
| ***Observation*** | ***Comments*** | ***Recommendation*** | ***Criticality*** |
| Logical access is restricted to the IACS network. | Access is restricted via password protected maintenance laptops however it is important to note that other laptops may also connect to the production network | Information Purposes Only | ACCEPTABLE |
| Unused ports and services on IACS devices are not disabled. | | Disable unused ports and services on IACS devices after testing to assure this will not impact IACS operation. (800-82) | MODERATE |
| IACS user privileges are restricted to only those that are required to perform each person's job. | Only applicable maintenance personnel are given the password to the laptops | Information Purposes Only | ACCEPTABLE |
| Separate authentication mechanisms and credentials for users of the IACS network and the Enterprise network are in place and operational. | | Information Purposes Only | ACCEPTABLE |
| Password policies do not exist defining when passwords must be used, how strong they must be, and how they must be maintained. | | The length, strength, and complexity of passwords should balance security and operational ease of access within the capabilities of the software and underlying OS. Passwords should have appropriate length and complexity for the required security. In particular, they should not be able to be found in a dictionary or contain predictable sequences of numbers or letters. (800-82) | LOW |
| A policy exists defining protection of attended and unattended workstations. | | Information Purposes Only | ACCEPTABLE |
| IACS passwords are not always required for system login. | A specific example are the Panelview terminals used around the facility | Passwords should be implemented on IACS components to prevent | MODERATE |

| | | | |
|---|---|---|---|
| | | unauthorized access. Password-related vulnerabilities include not having a password for system login (if the system has user accounts). (800-82) | |
| IACS passwords are not always required for system power-on. | | Passwords should be implemented on IACS components to prevent unauthorized access. Password-related vulnerabilities include not having a password for system power-on (if the system does not have user accounts). (800-82) | LOW |
| ICS passwords are not posted or observable in plain sight. | | Information Purposes Only | ACCEPTABLE |
| Sharing of passwords is permitted. | Maintenance personnel share the same access credentials for the maintenance laptops | Passwords should be kept confidential to prevent unauthorized access. Passwords should not be shared and should be unique to individual user accounts with associates. (800-82) | LOW |
| Passwords are not changed every 30 days for systems that do not support strong password configurations. | | Security awareness is a critical part of IACS incident prevention, particularly when it comes to social engineering threats. Social engineering is a technique used to manipulate individuals into giving away private information, such as passwords. This information can then be used to compromise otherwise secure systems. Passwords should be changed periodically in case a password has become compromised and should be changed with increased frequency for systems that do not support strong password credentials. (800-82) | MODERATE |
| It is unknown if vendor default passwords are in use on the IACS. | Although this was not verified on all IACS devices, it is important that default passwords are changed through configuration. | Control system suppliers often supply systems with default passwords. These passwords are factory set and are often easy to guess or are changed infrequently, which creates additional security risks. Default passwords should not be used | MODERATE |

| | | | |
|---|---|---|---|
| | | on the IACS. (800-82) | |
| IACS passwords are not changed a minimum of every 120 days. | | Security awareness is a critical part of IACS incident prevention, particularly when it comes to social engineering threats. Social engineering is a technique used to manipulate individuals into giving away private information, such as passwords. This information can then be used to compromise otherwise secure systems. Passwords should be changed periodically in case a password has become compromised. (800-82) | MODERATE |
| Policies do not exist requiring the management of IACS network system accounts. | | Develop policy and employ automated mechanisms to support the management of IACS accounts. (800-53) | LOW |
| A procedure does not exist for deleting temporary accounts after a pre-defined time period. | | IACS should automatically terminate temporary and emergency accounts after a pre-determined time period which should not exceed a reasonable amount of time that the account is required. (800-53) | LOW |
| A procedure does not exist for identifying user accounts that have been inactive for a pre-defined time period. | | IACS should automatically disable inactive accounts after a pre-defined time period which should not exceed a reasonable amount of time that an account could be inactive. (800-53) | LOW |
| A procedure does not exist for removing inactive user accounts. | | IACS should automatically disable inactive accounts after a pre-defined time period which should not exceed a reasonable amount of time that an account could be inactive. (800-53) | LOW |
| Account privileges are assigned in accordance with a role-based access scheme. | | Information Purposes Only | ACCEPTABLE |
| Users are required to authenticate to the IACS network. | | Information Purposes Only | ACCEPTABLE |
| User are not uniquely identifiable. | | ICS should use multifactor authentication for network access to IACS accounts and all | MODERATE |

| | | | |
|---|---|---|---|
| | | accounts should be unique to the user. (800-53) | |
| Multifactor authentication is not used. | | ICS should use multifactor authentication for network access to IACS accounts. (800-53) | MODERATE |
| Authentication is not required for devices attempting to physically interface to the IACS network. | | ICS should uniquely identify and authenticate IACS devices before establishing a connection. This should be evaluated against process requirements. (800-53) | HIGH |
| A policy does not exist governing the use of wireless access points on the IACS network. | Although wireless devices are not currently in use to transmit IACS traffic, ports are not explicitly configured to minimize access based on specific MAC addresses or the number of MAC addresses | A wireless policy should be established dictating strong mutual authentication between wireless clients and access points is needed to ensure that clients do not connect to a rogue access point deployed by an adversary, and also to ensure that adversaries do not connect to any of the IACS's wireless networks. (800-82) | MODERATE |
| Devices are not configured to ensure authentication information is encrypted in configuration scripts and memory locations. | | Ensure that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys. (800-53) | LOW |
| Remote access is not used to gain access to the IACS network. | Remote access is not currently supported for troubleshooting / diagnostics – all access is only allowed while at the facility | Information Purposes Only | ACCEPTABLE |
| Explicit security configurations ensure IACS data is controlled according to data type, source, and destination. | Via the use of the firewall currently separating the production and enterprise environments, ACLs are put in place to only allow connection via the ERP system to the controllers | Information Purposes Only | ACCEPTABLE |
| Host-based boundary protection configurations exist on IACS servers. | | Information Purposes Only | ACCEPTABLE |
| Boundary protection devices are configured to fail securely. | The firewall between the production and enterprise environment will fail to a secure state | Information Purposes Only | ACCEPTABLE |
| A policy does not exist requiring the IACS environment to be scanned for unauthorized network devices, | | Monitoring for unauthorized wireless connections to the IACS should be deployed, | LOW |

| | | | |
|---|---|---|---|
| including wireless access points. | | including scanning for unauthorized wireless access points and an action plan if an unauthorized connection is discovered. (800-53) | |

## 7.5 Awareness & Training

**Table 7:5 – Awareness and Training Observation Results**

| *Awareness & Training* | | *Section Rating:* | *LOW* |
|---|---|---|---|
| ***Observation*** | ***Comments*** | ***Recommendation*** | ***Criticality*** |
| Training and educational materials have been developed specific to the IACS. | | Information Purposes Only | ACCEPTABLE |
| Computer security awareness training is not provided for all employees. | | The organization should provide basic security awareness training to all IACS users (including managers, senior executives, and contractors) as part of initial training for new users, when required by system changes, and on pre-defined reoccurring interval thereafter. (800-53) | LOW |
| Computer security awareness training is not provided as part of the on-boarding process for new employees. | | The organization should provide basic security awareness training to all IACS users (including managers, senior executives, and contractors) as part of initial training for new users. (800-53) | LOW |
| A computer security awareness training refresher is not provided annually. | | The organization should provide basic security awareness training to all IACS users (including managers, senior executives, and contractors) on pre-defined reoccurring interval, usually on an annual basis. (800-53) | LOW |
| Computer security awareness training is not provided to 3rd party contractors before accessing the IACS. | | The organization should provide basic security awareness training to all IACS users including 3rd party contractors before accessing the IACS. (800-53) | LOW |
| Physical security and safety training is provided for all employees. | | Information Purposes Only | ACCEPTABLE |
| Physical security and safety training is provided as part of the on-boarding process for new employees. | | Information Purposes Only | ACCEPTABLE |

| | | | |
|---|---|---|---|
| A physical security and safety training refresher is provided annually. | | Information Purposes Only | ACCEPTABLE |
| Physical security and safety training is provided to 3rd party contractors before accessing the IACS. | | Information Purposes Only | ACCEPTABLE |

## 7.6 Data Security

**Table 7:6 – Data Security Observation Results**

| Data Security | | Section Rating: | HIGH |
|---|---|---|---|
| **Observation** | **Comments** | **Recommendation** | **Criticality** |
| Encryption and/or cryptographic hashes are not used to protect IACS data in transit. | | Access links not protected with authentication and/or encryption have the increased risk of adversaries using these unsecured connections to access remotely controlled systems. This could lead to an adversary compromising the integrity of the data in transit as well as the availability of the system, both of which can result in an impact to public and plant safety. Before deploying encryption, first determine if encryption is an appropriate solution for the specific IACS application. (800-82) | LOW |
| Encryption and/or cryptographic hashes are not used to protect IACS data at rest. | | Before deploying encryption, first determine if encryption is an appropriate solution for the specific IACS application, because authentication and integrity are generally the key security issues for IACS applications. Other cryptographic solutions such as cryptographic hashes should also be considered. (800-82) | LOW |
| A testing environment does not exist to facilitate secure testing and impact assessment of changes prior to implementation on the live IACS. | | Many IACS processes are continuous in nature. Unexpected outages of systems that control industrial processes are not acceptable. Outages often must be planned and scheduled days/weeks in advance. Exhaustive pre-deployment testing is essential to ensure high availability for the IACS. (800-82) | HIGH |
| A policy does not exist to restrict the use of portable media. | | Policy should be developed restricting the use of portable media devices on the IACS. | LOW |

| | | | |
|---|---|---|---|
| | | Enforcement should take into consideration that it may not be feasible to physically monitor them. (800-82) | |
| All external physical system interfaces to the IACS are documented. | The firewall between the production and enterprise environments limits ingress to specific ERP clients | Information Purposes Only | ACCEPTABLE |
| All external physical system interfaces to the IACS are regularly scanned for vulnerabilities. | The firewall between the production and enterprise environments limits ingress to specific ERP clients | Information Purposes Only | ACCEPTABLE |
| Anti-virus detection software is present in the IACS environment. | | Information Purposes Only | ACCEPTABLE |
| Virus signatures are deployed to the IACS environment a minimum of every 30 days. | | Information Purposes Only | ACCEPTABLE |
| A policy does not exist prohibiting the use of personally owned portable storage media on the IACS network. | For example, USB thumb drives are allowed | Policy should be developed prohibiting the use of personally owned, removable media in the IACS. (800-53) | LOW |
| Portable media devices are not encrypted. | | If sensitive data (e.g., passwords, dial-up numbers) is stored in the clear on portable devices such as laptops and PDAs and these devices are lost or stolen, system security could be compromised. Policy, procedures, and mechanisms are required for protection. (800-82) | LOW |
| A policy does not exist requiring secure sanitization and disposal of hardware. | For example, failed controllers are not required by policy to be wiped before disposal | A policy should be developed for tracking, documenting, and verifying media sanitization and disposal actions. (800-53) | LOW |
| A change control / configuration management procedure does not exist for the IACS. | | A Change Control / Configuration Management procedure should be established which ensures the IACS environment can be returned to a known state and all changes are documented. This information should be updated whenever changes occur and periodically at pre-defined intervals. (800-53) | LOW |
| A change control / configuration management procedure does not | Although this is something that is done by the various maintenance | A Change Control / Configuration Management | LOW |

| | | | |
|---|---|---|---|
| exist for ensuring backups of software, firmware, and configurations representing the as-is environment are available prior to initiating changes within the IACS. | electricians, a formally documented procedure does not exist | procedure should be developed and should include backups of software, firmware and configurations representing the As-Is environment are available prior to initiating changes within the IACS. (800-53) | |
| A change control / configuration management procedure does not exist to detect unauthorized changes to the IACS. | | The Change Control / Configuration Management procedure should include testing, validation, and documenting changes to the IACS before implementing the changes on the operational system. (800-53) | HIGH |
| A policy exists prohibiting unauthorized software use. | | Information Purposes Only | ACCEPTABLE |
| Games are not allowed on IACS equipment. | | Information Purposes Only | ACCEPTABLE |
| Peer-to-Peer chat is not allowed on IACS equipment. | | Information Purposes Only | ACCEPTABLE |
| The internet is not accessible on IACS equipment. | | Information Purposes Only | ACCEPTABLE |
| Streaming video is not allowed on IACS equipment. | | Information Purposes Only | ACCEPTABLE |
| Unauthorized executable downloads are not allowed on IACS equipment. | | Information Purposes Only | ACCEPTABLE |
| Unauthorized file transfers are not allowed on IACS equipment. | | Information Purposes Only | ACCEPTABLE |

## 7.7 Maintenance

**Table 7:7 – Maintenance Observation Results**

| *Maintenance* | | *Section Rating:* | *LOW* |
|---|---|---|---|
| ***Observation*** | ***Comments*** | ***Recommendation*** | ***Criticality*** |
| A procedure exists for collecting maintenance records for the IACS. | | Information Purposes Only | ACCEPTABLE |
| Maintenance records include date and time of maintenance. | | Information Purposes Only | ACCEPTABLE |
| Maintenance records identify the individual performing the maintenance. | | Information Purposes Only | ACCEPTABLE |
| Maintenance tools are restricted to authorized personnel only. | | Information Purposes Only | ACCEPTABLE |
| A policy does not exist requiring diagnostic tools to be tested for malicious code before they are allowed on the IACS network. | | All media containing diagnostic and test programs should be checked for malicious code before the media is used in the IACS. (800-53) | LOW |
| Remote sessions for maintenance are not employed on the IACS. | Remote access for troubleshooting is not currently allowed | Information Purposes Only | ACCEPTABLE |

## 7.8 Incident Detection

Incident detection is becoming an important part of an Industrial Automation Control System (IACS). Further evaluation should be completed to understand the security vulnerabilities present.

**Table 7:8 – Incident Detection Observation Results**

| *Incident Detection* | | *Section Rating:* | *MODERATE* |
|---|---|---|---|
| ***Observation*** | ***Comments*** | ***Recommendation*** | ***Criticality*** |
| Network-based intrusion detection sensors are not implemented on the IACS network. | | Individual intrusion detection tools should be interconnected and configured into a system wide intrusion detection system using common protocols. (800-53) | MODERATE |
| Host-based intrusion detection sensors are not implemented on the IACS network. | | A host-based intrusion detection tool should be implemented as the line of defense into a system wide intrusion detection system. (800-53) | MODERATE |
| Policy requires security incidents to be documented. | | Information Purposes Only | ACCEPTABLE |

## 7.9 Physical Security & Safety

**Table 7:9 – Physical Security and Safety Observation Results**

| *Physical Security & Safety* | | *Section Rating:* | *ACCEPTABLE* |
|---|---|---|---|
| ***Observation*** | ***Comments*** | ***Recommendation*** | ***Criticality*** |
| Employee access is auditable. | | Information Purposes Only | ACCEPTABLE |
| Visitor access is auditable. | | Information Purposes Only | ACCEPTABLE |
| All facility ingress and egress demarcations are monitored (24x7/365). | | Information Purposes Only | ACCEPTABLE |
| The entire facility perimeter is secured by fencing or equivalent. | | Information Purposes Only | ACCEPTABLE |
| The locations within the production area(s) where IACS and devices operate are protected by access control mechanisms. | | Information Purposes Only | ACCEPTABLE |
| Policy exists prohibiting tailgating via badge access. | | Information Purposes Only | ACCEPTABLE |
| Signage complies with OSHA regulations. | | Information Purposes Only | ACCEPTABLE |
| PPE requirements are specified prior to production building ingress. | | Information Purposes Only | ACCEPTABLE |
| Signs managing vehicle traffic flow are present at all on-site roadway intersections. | | Information Purposes Only | ACCEPTABLE |

# 8 REFERENCE INFORMATION

## 8.1 Methodology Additional Information

The Logical Manufacturing Framework, provides a template for IT and IACS convergence based on standards and generally accepted practices. Both ISA-95 and the Purdue Model for Control Hierarchy segment industrial control devices into hierarchical "levels" of operation within a manufacturing facility. Using levels as common terminology helps in understanding the flow of information plant-wide from the device level to the Enterprise. For enhanced security and traffic management, ISA-99 segments levels into "zones." Zones establish domains of trust for security access and smaller LANs to shape and manage network traffic.

The first generally accepted practice calls for establishing a Demilitarized Zone (DMZ) between the Enterprise Zone and the Manufacturing Zone. The DMZ is a buffer zone providing a barrier between the Enterprise and Manufacturing Zones, but allows for data and services to be shared securely. All network traffic from either side of the DMZ terminates in the DMZ. No traffic traverses the DMZ; that is, no traffic directly travels between the Enterprise and Manufacturing Zones. All services required for manufacturing operations, such as FactoryTalk®, should remain in the Manufacturing Zone.

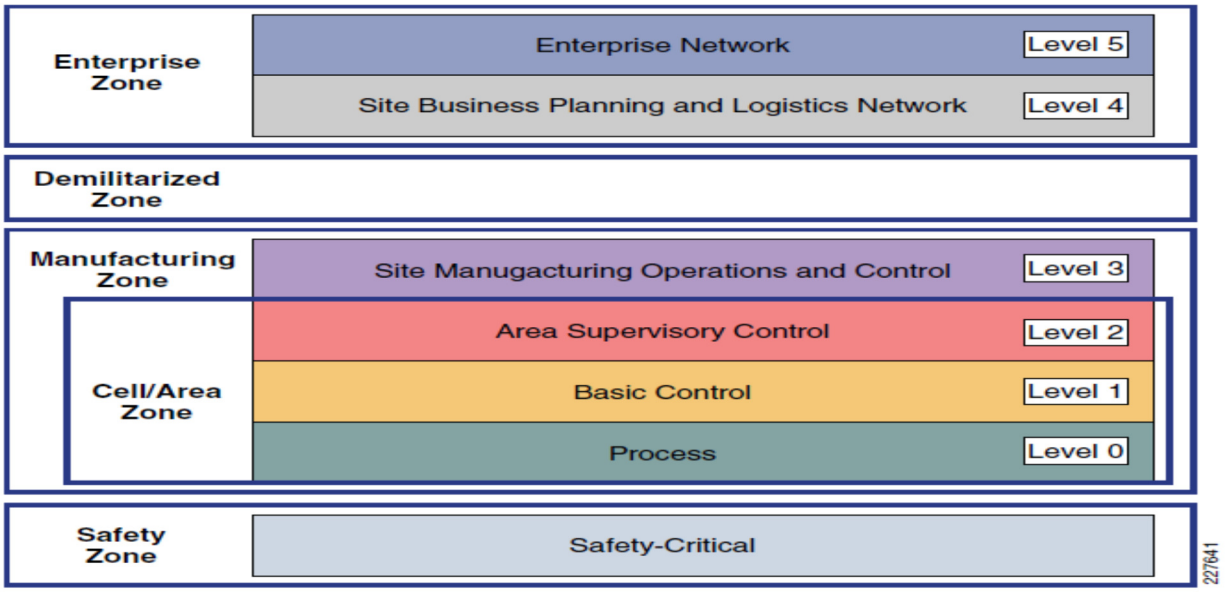


**Figure 8:1 – Logical Framework for IT and IACS Convergence**

To maintain these generally accepted practices while enabling information convergence between the Enterprise and Manufacturing Zones, Manufacturing Zone applications should replicate data to an application mirror within the DMZ. Users should then replicate the data from this application mirror to an application within the Enterprise Zone. This replication can be either unidirectional or bidirectional.

The DMZ is also a demarcation line for segmenting network traffic and security policies between the Enterprise and Manufacturing Zones, including segmenting network services such as Quality of Service (QoS), Virtual LANs (VLANs), VRF (Virtual Routing Forwarding) and multicast traffic. These services exist in both the Enterprise and Manufacturing Zones, but not necessarily implemented using the same policies, and should be segmented.

Converged Plantwide Ethernet Architectures provide recommendations, design guidance, generally accepted practices, methodology, and documented configuration settings. This helps establish a robust and secure network infrastructure for control and information data availability, integrity, and confidentiality. Built on industry standards and a future-ready network foundation, these manufacturing-focused reference architectures address today's applications, like safety through CIP Safety, and tomorrow's applications, like motion through CIP Motion, time synchronization through IEEE 1588 precision time protocol (PTP) with CIP Sync, and incorporation of voice over IP (VoIP) and video on demand (VOD).

The NIST Cybersecurity Framework is based on several existing global standards, guidelines, and practices which were developed within the industry. The goal is to acknowledge the nature of cybersecurity risks so practices can be developed that effectively meet business requirements. The framework follows a risk-based approach to managing cybersecurity by providing a mechanism to:

- Describe their current cybersecurity posture;
- Describe their target state for cybersecurity;
- Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process;
- Assess progress toward the target state;
- Communicate among internal and external stakeholders about cybersecurity risk.

To provide an overview of the key aspects that should be addressed in all plantwide Ethernet integration efforts, Cisco and Rockwell Automation have put together a document outlining the "Top 10 Key Considerations for EtherNet/IP Plantwide Implementations". For further reference on this topic please consult the References section of this document listed in Section 1.2.

## *8.2 Physical Topology Additional Information*

A large variety of network topologies must be considered to address a wide range of industrial applications. Topology starts with considering how devices are connected to the IACS network. In many industrial applications, the IACS devices themselves support only single network connections and therefore are connected via only a single connection to a single access switch. Where availability is critical and the devices support multiple connections, they should be connected to multiple switches to avoid single points of failure. The information below provides details on a redundant star topology, a ring topology, and a linear topology.

**Table 8:1 – Physical Topology Types**

| Type | Advantages | Disadvantages |
|---|---|---|
| Redundant Star | - Resiliency from multiple connection failures<br>- Faster Convergence to connection loss<br>- Consistent number of hops (typically two in flat design) provides predictable and consistent performance and real-time<br>- Fewer bottlenecks in the design reduces changes of segment over-subscription | - Additional wiring (and relevant costs) required to connect layer 2 access switches directly to a layer 3 distribution switch<br>- Additional configuration complexity |
| Ring | - Resiliency from loss of one network connection<br>- Less cabling complexity in certain plant floor layouts<br>- Multiple paths reduces potential for over-subscription and bottlenecks | - Additional configuration complexity<br>- Longer convergence times<br>- Variable number of hops makes designing predictable performance more complex |
| Linear | - Easy to design, configure, and implement<br>- Least amount of cabling (and associated cost) | - Loss of network service in case of connection failure (no resiliency)<br>- Creates bottlenecks on the links closest to layer 3 device, and varying number of hops make it more difficult to produce reliable performance |

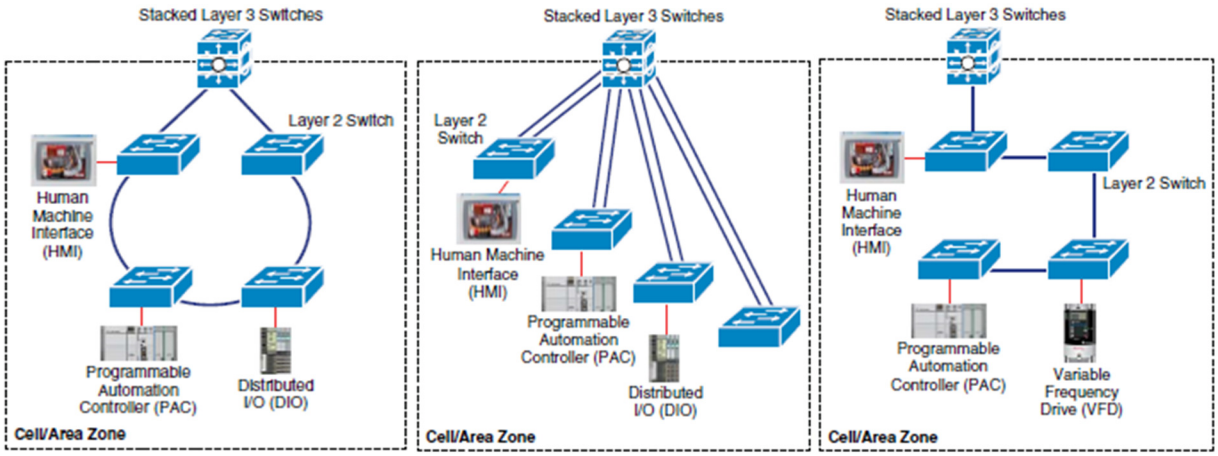


**Figure 8:2 – Physical Topologies Drawings**

## *8.3 Switch Selection Additional Information*

- All switches should be managed. No unmanaged switches or hubs should be authorized on the production network, or in the network infrastructure.
- All Access switches mounted in non-office type of locations (shop floor, hazardous climate areas, etc.) should be IP65 rated industrialized and hardened equipment OR be mounted in NEMA rated rack enclosures with environmental controlled measures, such as air conditioning, filtering and cooling.
- All Access switches should support the following:
    - IEEE 802.1D Spanning-Tree Protocol
    - IEEE 802.1w Rapid Spanning-Tree Protocol (RSTP)
    - IEEE 802.1s Multiple Spanning-Tree Protocol (MSTP)
    - Per VLAN Spanning-Tree Plus (PVST+)
    - VLAN Trunking Protocol (VTP)
    - IGMPv2 snooping and querying
    - SSHv2 (optional – for remote configuration)
    - SNMP (optional – for remove configuration and statistical analysis)
    - NTP (optional – to synchronize time across the network infrastructure)
    - IEEE 802.1x Port Based Access Control (Optional – if used by the enterprise)
    - Port Mirroring
- Core and Distribution switches should be Layer 3 functioning devices
- Core and Distribution switches should support the following:
    - IEEE 802.1D Spanning-Tree Protocol
    - IEEE 802.1w Rapid Spanning-Tree Protocol (RSTP)
    - IEEE 802.1s Multiple Spanning-Tree Protocol (MSTP)
    - Per VLAN Spanning-Tree Plus (PVST+)
    - VLAN Trunking Protocol (VTP)
    - IGMPv2 snooping and querying
    - SSHv2 (optional – for remote configuration)
    - SNMP (optional – for remove configuration and statistical analysis)
    - NTP (optional – to synchronize time across the network infrastructure)

- IEEE 802.1x Port Based Access Control (Optional – if used by the enterprise)
- Port Mirroring
- Advanced IP unicast routing protocols (OSPF, Interior Gateway Routing Protocol (IGRP), EIGRP, and Border Gateway Protocol Version 4 (BGPv4))
- Policy-Based Routing (PBR)
- Inter-VLAN routing provides for full Layer 3 routing between two or more VLANs

## 8.4 Router Selection Additional Information

Routing is the process of finding a path to a destination host. Routers or Layer-3 switches forward packets from one network (sub-network or VLAN) to another IP based network. To do this, routers send each other information about the networks they know about by using various types of routing protocols. Routers use this information to build a routing table that consists of the available networks, the cost associated with reaching the available networks, and the path to the next hop. Routing is the process of finding a path to a destination host. Routers or Layer-3 switches forward packets from one network (sub-network or VLAN) to another based IP layer information. To do this, routers send each other information about the networks they know about by using various types of routing protocols. Routers use this information to build a routing table that consists of the available networks, the cost associated with reaching the available networks, and the path to the next hop. The correct routing protocol should be selected based on the characteristics and needs of the network.

**Table 8:2 – Routing Protocol Comparison**

| Name | Type | Proprietary | Function | Updates | Metric | VLSM | Summarization |
|---|---|---|---|---|---|---|---|
| RIP | Distance Vector | No | Interior | 30 sec | Hops | No | Auto |
| RIPv2 | Distance Vector | No | Interior | 30 sec | Hops | Yes | Auto |
| IGRP | Distance Vector | Yes | Interior | 90 sec | Composite | No | Auto |
| EIGRP | Adv. Distance Vector | Yes | Interior | Trig | Composite | Yes | Both |
| OSPF | Link-State | No | Interior | Trig | Cost | Yes | Manual |
| IS-IS | Link-State | No | Interior | Trig | Cost | Yes | Auto |
| BGP | Path Vector | No | Exterior | Incr | N/A | Yes | Auto |

## 8.5 Ethernet Communication Module Additional Information

All Ethernet/IP modules must have a unique IP address on the network. The network mask is used to determine which subnet the Ethernet/IP module is on. The gateway address is used when the Ethernet/IP module needs to communicate with a TCP/IP device that is located on another subnet. The network mask is used to determine if the destination host is on the local or a remote subnet. If the destination is on the local subnet, the Ethernet/IP module sends the packet directly to the destination. If the destination is on a remote subnet, the Ethernet/IP module forwards the packet to the gateway. The gateway then forwards the packet to the appropriate subnet.

Most Ethernet/IP network implementations require that the gateway address is statically configured on the module. Some implementations may choose to use DNS name resolution. If your Ethernet/IP network implementation requires the use of DNS, the primary name server, secondary name server, domain name, and hostname field should be completed.

In most applications, the IP addresses of Ethernet/IP I/O devices are statically entered into the application. Because of this, it is important that the module's address always matches the address entered in the application.

**Table 8:3 – Ethernet/IP Module Configuration Parameters**

| Parameter | Description | Required | Recommended | Optional |
|---|---|---|---|---|
| IP Address | The IP address of the Ethernet/IP module | Yes | | |
| Network Mask | The network mask of the Ethernet/IP module | Yes | | |
| Gateway Address | The default gateway address of the Ethernet/IP module | | Yes | |
| Primary Name Server | The IP address of the primary DNS server | | | Yes |
| Secondary Name Server | The IP address of the secondary DNS server | | | Yes |
| Domain Name | THE DNS domain name of the Ethernet/IP module | | | Yes |
| Host Name | The host name of the Ethernet/IP module | | | Yes |

## 8.6 Environmental Conditions Additional Information

MICE is a method of categorizing the environment into three classifications that are mapped to severity levels 1=Office, 2=Light Industrial, and 3=Industrial. Each increasing severity level is harsher. The industrial areas can be generalized into four typical areas: factory floor, work area, machine area, and control, equipment, telecommunications room with each having their own classification.

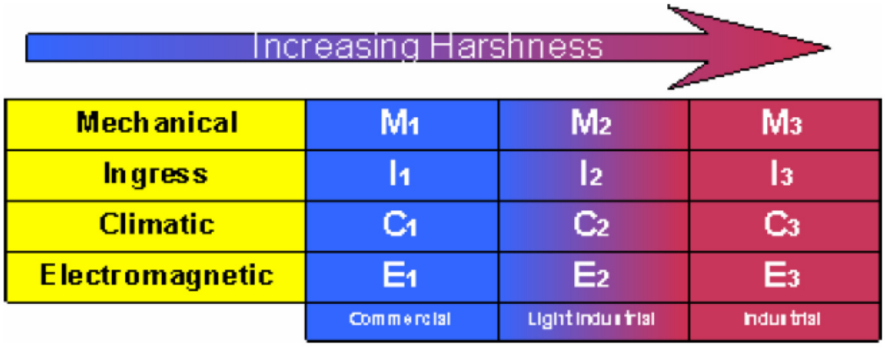


**Figure 8:3 – M.I.C.E. Chart**

Generally an area does not have the same level for all categories (Mechanical, Ingress, Climatic/Chemical and Electromagnetic). For example, a machine maybe in an area where the vibration is very high, hence M3, the area may be free of dust and liquids, hence I1, the temperatures may be high, hence C3, and the electromagnetic levels are low, hence E1.

## 8.7 Enclosures Additional Information

Rockwell Automation recommends switches mounted in non-office type of locations (shop floor, hazardous climate areas, electrical rooms, and so forth) be environmentally rated with no internal cooling fans and mounted in NEMA 4X or IP65 enclosures. Switch temperature rating should meet or exceed 140°F, and the temperature inside the enclosure cannot exceed the switch's temperature rating. The goal is to avoid using environmental control measures, such as air conditioning, filtering, and cooling measures, that would otherwise require regular maintenance.

Cabinet selection should allow environmental control measures to be added if necessary to maintain switch operational temperatures. The use of environmental control measures should be an exception and only be used if required. Switch temperatures should be monitored during operation to ensure temperature ratings are not being exceeded.

Type 4X enclosures constructed for either indoor or outdoor use are: to provide a degree of protection to personnel against access to hazardous parts; to provide a degree of protection of the equipment inside the enclosure against ingress of solid foreign objects (windblown dust); to provide a degree of protection with respect to harmful effects on the equipment due to the ingress of water (rain, sleet, snow, splashing water, and hose-directed water); to provide an additional level of protection against corrosion; and to be undamaged by the external formation of ice on the enclosure.

## *8.8 Cable Selection Additional Information*

Copper cabling must follow the EIA/TIA standard for Category-6 Twisted Pair (Cat-6). All cable connectors, patch panels, and jacks must also follow the Cat-6 specification. Patch cables should be pre-manufactured and certified by the vendor.

Singlemode/multimode fiber optic cable and connectors must comply with the ANSI/TIA/EIA 568-B.3 Fiber Optic Cabling Components Standard.

Observe the following guidelines when handling excess cable:

- Do not coil excess cable of different types (i.e. motor power and feedback) together. An efficient transformer is formed at HF which can add noise to the network.
- Cable lengths should ideally be trimmed to fit the application.
- If excess cable cannot be trimmed, it should be laid in an 'S' or figure eight pattern (refer to the figure below).

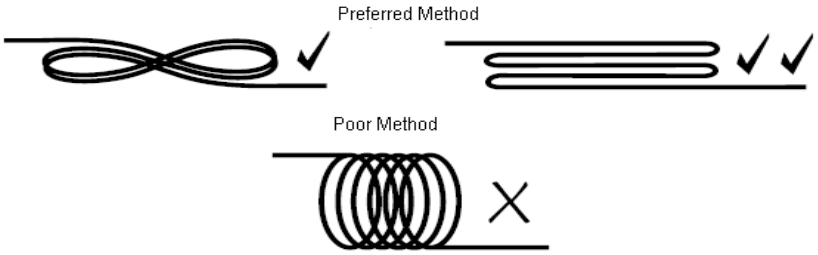


**Figure 8:4 – Handling Excess Cable**

## *8.9 Cable Management Additional Information*

Cable management from a network perspective is often an afterthought, or is entirely overlooked, during an IACS design. First, horizontal network cables should be installed and left undisturbed. Then moves, additions, and changes to the physical topology of the network should be done by means of patch cables at patch panels or jack outlets. This is known as the patch field and should be the focus for all moves, additions, or changes.

Cable management should be designed to support the goals of manageability, reliability, security, and scalability. 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.

## 8.10 Conduit and Routing Additional Information

Category-6 (Cat-6) UTP copper and fiber optic Ethernet media must be routed in rigid galvanized conduit to minimize the potential for incidental damage. Rigid conduit and media installation must meet or exceed the following requirements:

- TIA-569-B, Commercial Building Standard for Telecommunications Pathways and Spaces
- Conduit should be run in the most direct route possible.
- Maximum conduit segment length shall be 280 ft.
- Maximum conduit length between pull boxes shall be 100 ft.
- Minimum conduit bend radius is 6x the internal diameter of the conduit.
- A pull point shall be provided if there are more than two (2) 90° degree bends or equivalent in a conduit segment.
- A conduit run shall serve no more than 3 network outlet boxes.
- 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.
- Each section of the wire way or conduit must be bonded to each adjacent section and panels so that it has electrical continuity along its entire length, and must be bonded to the enclosure at the entry point.
- Copper cabling selected for installation must be approved by the cable manufacturer for routing in conduit.
- Cable runs in conduit shall not exceed 60% fill rate or conduit fill capacities specified by the cable manufacturer.

As listed in the following table, External Enclosure-to-Enclosure Routing Requirements defines cable routing external to enclosures. This is to minimize cross talk from nearby cables.

**Table 8:4 – External Enclosure-to-Enclosure Routing Requirements**

| Cable in contiguous metal wire way or conduit? | Route Cable at this Minimum Distance | From Noise Source of this Strength |
|---|---|---|
| YES | 0.08m (3 inches) | Category 1 conductors less than 20 amps |
| | 0.15m (6 inches) | AC power lines of 20 amps or more, up to 100 kVA |
| | 0.3m (12 inches) | AC power lines greater than 100kVA |
| NO | 0.15m (6 inches) | Category 1 conductors less than 20 amps |
| | 0.3m (12 inches) | AC power lines of 20 amps or more, up to 100 kVA |
| | 0.6m (24 inches) | AC power lines greater than 100kVA |

As listed in the following table, Routing Requirements Internal to Enclosures defines cable routing internal to enclosures.

**Table 8:5 – Routing Requirements Internal to Enclosures**

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

## 8.11 Cable Labeling Additional Information

The following figure shows an example of how to build a labeling standard for your facility.

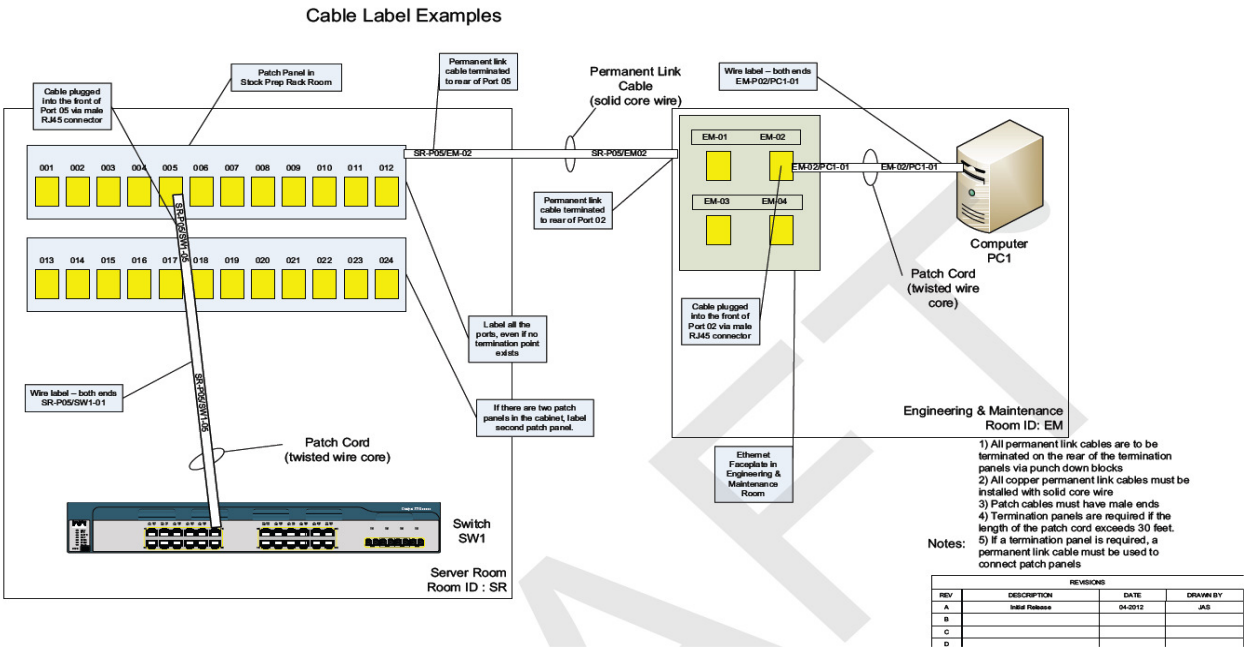


**Figure 8:5 – Cable Labeling Example**

## 8.12 Power Redundancy Additional Information

Power supply failures are the second leading cause of switch failure. All switches utilized in the Process Control network should be required to support redundant power supplies. The redundant power supply requirement is necessary to reduce the risk that a single power supply could impact the normal Process Control network operation. All power supplies should be monitored for failure and a corrective action plan must be developed to replace failing or failed power supplies. Network hardware that supports hot swapping of power supplies is required.

Access level switches should be required to utilize external redundant power supplies. The external power supplies allow the power supplies to be replaced without powering down the switch.

Network hardware that support redundant power supplies should be required to have separate power sources feeding the individual power supplies. Power circuits should be supplied from separate power sub panels to reduce the risk that a single circuit breaker could disrupt the power to both power supplies.

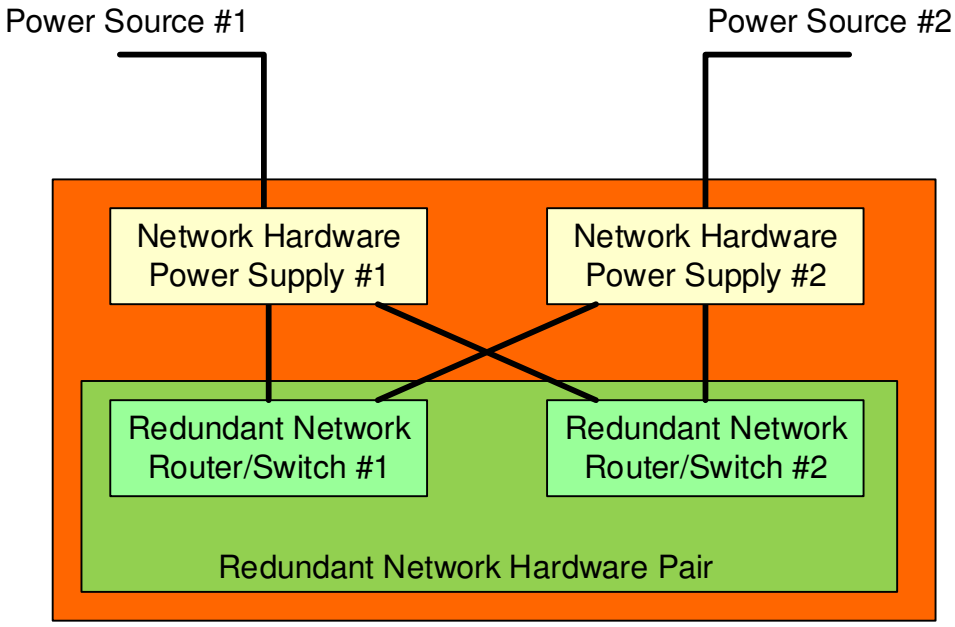


**Figure 8:6 – Redundant Power Source**

## 8.13 Grounding Additional Information

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

A properly implemented Grounding and Bonding system should be intentional, visually verifiable, and properly sized. It should be sized properly per TIA-607-B standards. Mechanical connections should be replaced with compression style, two-hole lugs (Optional: use lugs qualified to NEBS Level 3 testing). 6 AWG TGC (Telecommunications Grounding Conductor) should be utilized from the TGB to each Rack. Multiple TGCs can be run from each rack to the TGB or a Tap/Run structure can be utilized based on customer preference. To ensure continuity, it is recommended to add grounding bars for each rack and grounding strips along the full RU. Equipment should be bonded via manufacturer's bonding screws w/ 6AWG jumpers or, if not present, via mounting holes utilizing grounding hardware. For consistency and to meet the visually verifiability standards of TIA-607-B, it is also recommended to include proper grounding of control panels and end devices within them.

## 8.14 Logical Topology Additional Information

The following information is from the Converged Plantwide Ethernet (CPwE) Design and Implementation Guide published by Cisco and Rockwell Automation, and is provided for reference purposes only.

Availability of the IACS has a direct correlation to the plant uptime and OEE of a manufacturing facility. Because the network is a key aspect of the overall system, these requirements translate directly to the IACS network. Key considerations for high availability include the following:

- Creating alternative data communication paths, regardless of physical layout. Risk profile, opportunity cost, culture, and other variables determine how much and to what level redundant paths are required.
- Eliminating single points of failure with critical operations, including such items as dual-power supplies, alternate power routes for redundant media, and redundant IACS network infrastructure, such as routers, switches, and firewalls.
- Using advanced network resiliency and convergence techniques to improve availability, such as EtherChannel/LACP, Spanning Tree Protocol, Flex Links, and Hot Standby Routing Protocol (HSRP).
- Although a redundant star topology offers the best convergence capabilities, consider alternative ring recovery techniques when configured in a physical ring topology.
- Using routing protocols such as EIGRP or OSPF to achieve high availability.
- Integrating the network device into the IACS application to better identify and diagnose issues when they do occur.
- Incorporating features and services to allow the quick replacement of failed devices with minimal or no configuration of the replacement device.

The following table is provided for reference only. The first step to having a network that has high availability and is resilient is to determine the network's required availability. The table below shows the downtime per week based on network availability requirements. The key considerations outlined above are used in combination to create a network with high availability.

**Table 8:6 – Network Availability Requirements**

| Network Availability | Downtime per year | Downtime per Week |
|---|---|---|
| 95% | 438 hours | 8.4 hours |
| 99% | 87.6 hours | 101 minutes |
| 99.9% | 8.8 hours | 10 minutes |
| 99.99% | 52.6 hours | 1 minute |
| 99.999% | 5.3 minutes | 6 seconds |

## *8.15 Security Zone Additional Information*

A DMZ and firewalls are an essential aspect of protecting an IACS network and its applications. The combination of firewalls and a DMZ zone concept are key aspects of the defense-in-depth approach for IACS network security. The key security zone features include the following:

- Deploy plant firewalls to manage traffic between the Enterprise network and the IACS. A firewall supplies the following:
  - Establishing traffic patterns between the network zones via assigned security levels, for example establishing a DMZ
  - Stateful packet inspection of all traffic between the various zones, if allowed by the above
  - Enforce Authentication of users from one zone trying to access resources in another, for example from the Enterprise accessing DMZ services
  - Intrusion Protection Services (IPS) inspecting traffic between the zones designed to identify and potentially stop a variety of attacks
- A DMZ zone where data and services between the zones can be securely shared

The firewall and DMZ concept also play an important role in allowing remote access to the IACS network.

## 8.16 Manufacturing Zone Additional Information

The manufacturing zone contains all IACS networks, devices, and controllers that are critical to controlling and monitoring plantwide operations. Hierarchically, the manufacturing zone includes site manufacturing operations and control functions as well as multiple cell/area zones.

To preserve smooth plant wide operations and functioning of the IACS application and IACS network, this zone requires clear isolation and protection from the Enterprise network via security devices within the DMZ. This insulation not only enhances security segmentation between the enterprise and manufacturing zones, but often represents an organizational boundary where IT and Control Engineers responsibilities interface.

This approach permits the manufacturing zone to function entirely on its own, irrespective of the connectivity status to the higher levels. A methodology and procedure should be deployed to buffer IACS data to and from the Enterprise network. Key features of the manufacturing zone include the following:

- Interconnecting the various Cell/Area IACS networks
- Interconnecting the Level 3 Site Manufacturing Systems
- Providing network management and security services to all IACS systems and devices
- Endpoint protection

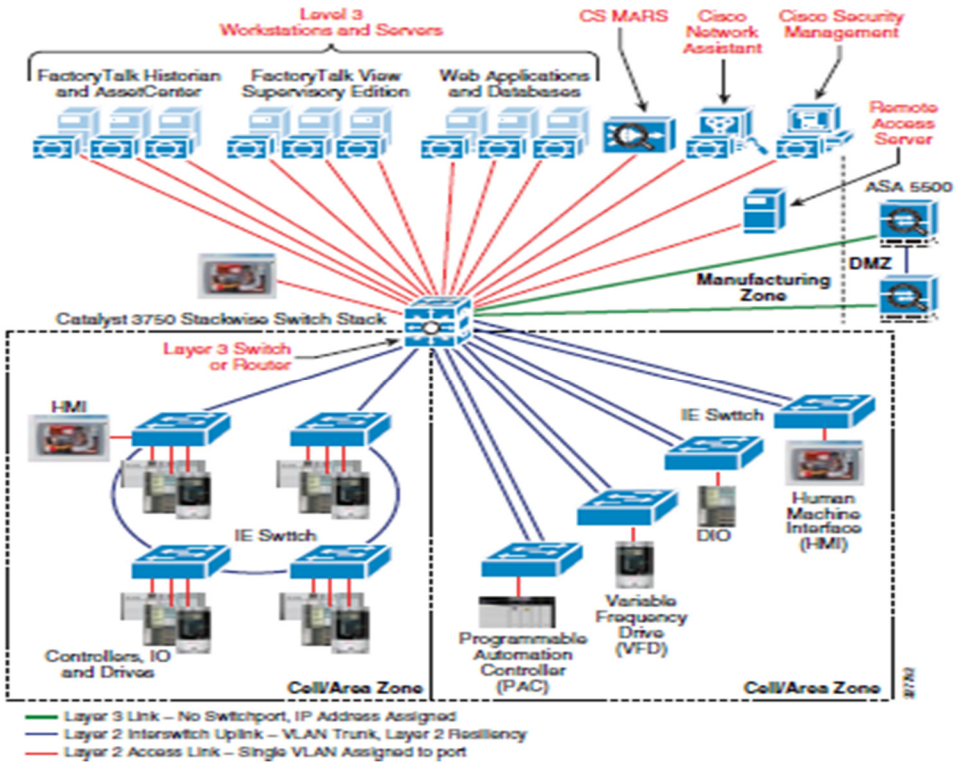


**Figure 8:7 – Example of Manufacturing Zone**

## 8.17 Cell/Area Zone Additional Information

The cell/area zones are the networks that connect sensors, actuators, drives, controllers, and other IACS device that needs to communicate in real-time. The availability and performance requirements are most distinct in the cell/area zone. The key design considerations are as follows:

- *Industrial Characteristics* - The environmental conditions of the plant floor must be taken into consideration because the equipment must be able to perform in these conditions. This drives the industrial characteristics of all the equipment, including the network infrastructure. The network topology must be shaped to fit appropriately into the plant floor environment.
- *Interconnectivity and Interoperability* - Standardization on a single vendor's IACS or industrial Ethernet network equipment within the cell/area zone may not be practical. Consideration and evaluation should be performed so the technologies which provide the greatest opportunity for interconnectivity and interoperability within a mixed-vendor IACS environment will be utilized.
- *Real-time communications and network performance* - Cell/Area IACS networks must be designed to meet the latency and jitter requirements of the IACS it supports. This can impact the size of the LAN, the number of routing hops, and the VLAN configuration.
- *Availability* - The availability of the cell/area zone is critical to the manufacturing process. Without a properly functioning cell/area IACS network, some or all of the plant operations may come to a halt. This can severely impact plant efficiency. Availability itself is a function of equipment, infrastructure, configuration and software. The network must also be able to recover from network impacting events, such as a connection break, to avoid the system automatically shutting down.
- *Manageability* - The plant floor maintenance personnel tend not to have the same networking experience as IT. The setup and configuration of network equipment must take into consideration the experience level of the plant floor maintenance personnel.
- *Security* - IACS and Enterprise network convergence require evolved security policies. IACS assets have become susceptible to the same security vulnerabilities as the Enterprise assets. Protecting IACS assets requires a defense-in-depth security approach to assure the availability, confidentiality, and integrity of the IACS data.
- *Unmanaged vs. Managed* - Although the cost of the network infrastructure may not represent a large portion of the plant floor, the same cost reduction mentality is often applied as to other aspects of the manufacturing facility. Without clear understanding of the qualities of a managed, intelligent network, the additional hardware costs they represent may lead network developers to choose less intelligent solutions based purely on initial cost considerations; only late do they determine that the cheaper, unmanaged infrastructure cannot scale, perform, integrate, or be as easily maintained as an intelligent, managed network.

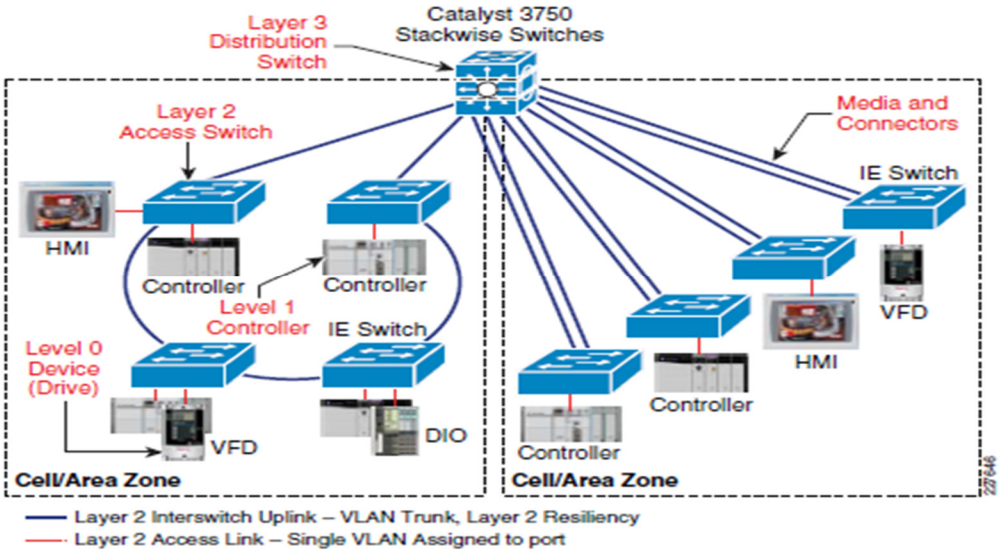


**Figure 8:8 – Example of Cell/Area Zone**

# 9 ABBREVIATIONS & REFERENCE DOCUMENTATION

## 9.1 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 |
| FTA | 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 |
| 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 |

**Table 9:1 – Commonly Accepted Industrial Automation Abbreviations**

## *9.2 Reference Documentation*

The following are references to standards and generally accepted practices documentation:

- ANSI/ISA-TR99.00.01-2007, Security Technologies for Manufacturing and Control Systems
- ANSI/ISA-99.00.01-2007, Security for Industrial Automation and Control Systems: Concepts, Terminology and Models
- ANSI/ISA-99.02.01-2009, Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program
- ISA-95.01, Models & Terminology
- SA-95.02, Object Model Attributes
- ISA-95.03, Activity Models
- ISA-95.04, Object Models & Attributes
- ISA-95.05, B2M Transactions
- ODVA EtherNet/IP Specification
- PUB00035R0, ODVA Network Infrastructure for EtherNet/IP: Introduction and Considerations
- PUB00148R0, ODVA EtherNet/IP Media Planning and Installation Manual
- ANSI/TIA 1005, Cabling Telecommunications Standards for Industrial Premises
- ANSI/TIA-568-C.n, Commercial Copper and Fiber Cabling
- 090818_IA_IEPIRA, Panduit Industrial Ethernet Physical Infrastructure Reference Architecture Design Guide
- TIA-569-B, Commercial Building Standard for Telecommunications Pathways and Spaces
- TIA-942, Telecommunication Infrastructure Standard for Data Centers