

STANDARD NETWORK ASSESSMENT

Prepared for



**Spacely Sprockets
Orbit City, Wisconsin**

**RA Document: RA DRAFT
Project Number: 7000555123
6/22/2020**

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

CONTENTS

1	DOCUMENT CONTROL.....	5
1.1	Document Approval.....	5
1.2	Revision History.....	5
1.3	Interview Participants.....	5
1.4	Disclaimer.....	6
2	BACKGROUND & OVERVIEW.....	7
2.1	Executive Summary.....	7
2.2	Scope.....	14
3	CUSTOMER NETWORK DEVICES.....	15
4	NETWORK PHYSICAL INFRASTRUCTURE.....	17
4.1	Physical Topology.....	18
4.2	Switch Selection.....	19
4.3	Router Selection.....	20
4.4	Ethernet Communication Modules.....	21
4.5	Environmental Conditions & Enclosures.....	22
4.6	Cable Selection.....	24
4.7	Cable Management.....	27
4.8	Conduit & Routing.....	32
4.9	Cable Labeling.....	36
4.10	Power Redundancy System.....	36
4.11	Grounding.....	37
5	NETWORK LOGICAL INFORMATION.....	38
5.1	Logical Topology.....	38
5.2	Security Zone.....	39
5.3	Manufacturing Zone.....	40
5.4	Cell/Area Zone.....	42
6	INDUSTRIAL SECURITY & SAFETY.....	45
6.1	Asset Management.....	45
6.2	Governance.....	47
6.3	Risk Assessment & Management.....	48
6.4	Access Controls.....	49
6.5	Awareness & Training.....	54
6.6	Data Security.....	55
6.7	Maintenance.....	57
6.8	Incident Detection.....	58
6.9	Physical Security & Safety.....	58
7	REFERENCE INFORMATION.....	60
7.1	Methodology Additional Information.....	60
7.2	Reference Documents.....	62
7.3	Physical Topology Additional Information.....	62
7.4	Switch Selection Additional Information.....	64
7.5	Router Selection Additional Information.....	65
7.6	Ethernet Communication Module Additional Information.....	65
7.7	Environmental Conditions Additional Information.....	66
7.8	Enclosures Additional Information.....	66
7.9	Cable Selection Additional Information.....	67
7.10	Cable Management Additional Information.....	67
7.11	Conduit & Routing Additional Information.....	68
7.12	Cable Labeling Additional Information.....	69
7.13	Power Redundancy Additional Information.....	70
7.14	Grounding Additional Information.....	71

DRAFT or FINAL

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

7.15	Topology Additional Information.....	71
7.16	Security Zone Additional Information.....	72
7.17	Manufacturing Zone Additional Information	72
7.18	Cell/Area Zone Additional Information.....	74
8	ABBREVIATIONS & STANDARDS	76
8.1	Commonly Accepted Industrial Abbreviations	76
8.2	Additional References.....	77

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

FIGURES & TABLES

Table 1:1 – Document Approval.....	5
Table 1:2 – Revision History	5
Table 1:3 – Interview Participants	5
Table 2:1 – Key Issues	7
Table 2:2 – Key Issue Related Causes.....	8
Table 2:3 – Key Findings.....	9
Table 2:4 – Summary of Observations.....	12
Table 3:1 – Network Asset Evaluation.....	15
Figure 4:1 – Spacely Sprockets Production Network Topology.....	17
Table 4:1 – Physical Topology Observation Results.....	18
Table 4:2 – Switch Selection Observation Results.....	19
Figure 4:2 – Mill #1 Bundler Unmanaged Switch Mounting.....	20
Table 4:3 – Router Selection Observation Results	20
Table 4:4 – Ethernet Communication Modules Observation Results	21
Table 4:5 – Environmental Conditions Observation Results.....	22
Table 4:6 – Enclosures Observation Results.....	22
Figure 4:3 – Mill #2 Rea JET Cabinet Filter	23
Table 4:7 – Cable Selection Observation Results	24
Figure 4:4 – Mill #2 PTA Panel Cable Terminations.....	26
Figure 4:5 – Mill #2 TWM Cable Routing.....	26
Table 4:8 – Cable Management Observation Results	27
Figure 4:6 – Mill #2 TWM Panel Cable Routing.....	28
Figure 4:7 – Mill #2 Drives Room #1 IT Cabinet.....	29
Figure 4:8 – Mill #1 Travelling Cutoff Saw	30
Figure 4:9 – Slitter #4 Drives Panel.....	31
Figure 4:10 – Mill #2 Saw Carriage.....	31
Table 4:9 – Conduit & Routing Observation Results	32
Figure 4:11 – Mill #1 Bundler.....	33
Figure 4:12 – Slitter #4 Drives Room Cable Routing	34
Figure 4:13 – Mill #1 Quick Settings Panel.....	35
Figure 4:14 – Slitter #4 Drives Room.....	35
Table 4:10 – Cable Labeling Observation Results.....	36
Table 4:11 – Power Redundancy System Observation Results	36
Table 4:12 – Grounding Observation Results.....	37
Table 5:1 – Logical Topology Observation Results	38
Table 5:2 – Security Zone Observation Results	39
Table 5:3 – Manufacturing Zone Observation Results.....	40
Table 5:4 – Cell/Area Zone Observation Results	42
Table 6:1 – Asset Management Observation Results	45
Table 6:2 – Governance Observation Results.....	47
Table 6:3 – Risk Assessment & Management Observation Results	48
Table 6:4 – Access Controls Observation Results.....	49
Table 6:5 – Awareness & Training Observation Results	54
Table 6:6 – Data Security Observation Results.....	55
Table 6:7 – Maintenance Observation Results.....	57
Table 6:8 – Incident Detection Observation Results	58
Table 6:9 – Physical Security & Safety Observation Results	58
Figure 7:1 – Logical Framework for IT and IACS Convergence.....	60
Table 7:1 – Reference Documents	62
Table 7:2 – Physical Topology Types	62
Figure 7:2 – Physical Topologies Drawings.....	63
Table 7:3 – Routing Protocol Comparison	65

DRAFT or FINAL

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

Table 7:4 – Ethernet/IP Module Configuration Parameters.....	65
Figure 7:3 – M.I.C.E. Chart	66
Figure 7:4 – Handling Excess Copper Cabling	67
Table 7:5 – External Enclosure-to-Enclosure Routing Requirements.....	68
Table 7:6 – Routing Requirements Internal to Enclosures.....	68
Figure 7:5 – A representative model of typical telecommunication infrastructure elements for administration	69
Figure 7:6 – Redundant Power Source	70
Table 7:7 – Network Availability Requirements	71
Figure 7:7 – Example of Manufacturing Zone.....	73
Figure 7:8 – Example of Cell/Area Zone	75

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

1 DOCUMENT CONTROL

1.1 Document Approval

Table 1:1 – Document Approval

Date	Organization	Name - Title

1.2 Revision History

Table 1:2 – Revision History

Date	Version	Description	Author
6/22/2020	1.0	1 st Draft Created	Rockwell Automation Authorized Service Provider Program

1.3 Interview Participants

Table 1:3 – Interview Participants

Date	Name	Title	Company
6/01/2020	Consultant A	Senior Network Consultant	Happy Springs Electric
6/01/2020	Consultant B	Networks & Security Consultant	Happy Springs Electric
6/01/2020	Interviewee A	Information Technology Security Lead	Spacely Sprockets
6/01/2020	Interviewee B	Information Technology MRP Lead	Spacely Sprockets
6/01/2020	Interviewee C	Maintenance Electrician	Spacely Sprockets
6/01/2020	Interviewee D	Strategic Maintenance Lead	Spacely Sprockets
6/01/2020	Interviewee E	Operations Technology Security Lead	Spacely Sprockets
6/01/2020	Interviewee F	Systems Analyst	Spacely Sprockets

DRAFT or FINAL

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

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 Spacely Sprockets environment. This information is to be considered as preliminary and informative, and is subject to review and revision at any time by Spacely Sprockets or Rockwell Automation. This document further includes information that may be proprietary, confidential, or otherwise sensitive from both Spacely Sprockets and Rockwell Automation. Prior to any dissemination outside of Spacely Sprockets 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.

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

2 BACKGROUND & OVERVIEW

2.1 Executive Summary

In June 2020, Spacely Sprockets has approved the Rockwell Automation Authorized Service Provider Happy Springs Electric to provide consulting services at their Widget Springs Foundry site in Orbit City in the form of a Standard Network Assessment. This assessment has been developed to evaluate the physical and logical design and implementation of the industrial automation control system (IACS) network (WSOT Network) and relies on information collected during a physical inspection process and an interview process with key stakeholders. This assessment does not make use of Ethernet analyzer tools and does not include any modification or remediation actions. Additional services including a comprehensive network assessment, network design, security survey, security design, and remediation can be provided in separate engagements.

The network at the Widget Springs Foundry site will be assessed and measured against industry leading standards for IACS networks and the analyzed data provide a summary of identified issues, criticality ratings, and recommendations for remediation where possible.

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.

ACCEPTABLE = Indicates an item that is acceptable and is listed for informational purposes only.

This document constitutes the complete standard network assessment deliverable and should be used as a roadmap for Spacely Sprockets to achieve their network reliability, performance, and security goals at their Widget Springs Foundry site in Orbit City, Wisconsin.

The subsections below provide the background and overview of the consultation services performed, with key findings and a high-level summary of the assessment results that are provided in detail within the remaining sections of this report.

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 8](#).

2.1.1 Specific Network Related Issues

The main network related items outlined by Spacely Sprockets as current issues within the production environment at their Widget Springs Foundry site in Orbit City were as follows:

Table 2:1 – Key Issues

Issue #	Impact Rating	Issue Description
1	LOW	Slow uploading time from some PLCs on-site
2	MODERATE	Slow times in transferring data between specific PLCs via message instructions
3	HIGH	Production downtime has been experienced without specific related causes being determined and may point to a network related issue
4	HIGH	Frequent communications loss between PLC and AC Drives causing drive fault and downtime

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

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 above, an evaluation of all aspects of the network equipment was completed. During this time key items relating to the main issues identified were noted as follows:

Table 2:2 – Key Issue Related Causes

Issue #	Impact Rating	Identified Cause
1	LOW	Several switches in the network are unmanaged. Coupled with a "flat" (single subnet) network topology creates a large broadcast domain and increases propagation time and potential collisions across the network.
2	MODERATE	Several switches in the network are unmanaged. Coupled with a "flat" (single subnet) network topology creates a large broadcast domain and increases propagation time and potential collisions across the network. Message traffic was also being routing across several ControlLogix backplanes with legacy 1756-ENET modules. These modules are discontinued and should be migrated to newer 1756-EN2T / EN2TR modules to support more modern production network requirements.
3	HIGH	A single subnet with 254 available IP addresses is used to communicate between all PLCs on the production network. Additionally, multiple ethernet end devices are also placed in this subnet that are communicating directly with their associated PAC/PLC. The broadcast and fault domains in this flat network are too large and do not provide adequate segmentation to keep issues in one area of the plant from propagating and affecting other areas.
4	HIGH	Cable installation and management issues are causing cables and connectors to sustain damage. Running Ethernet cables too close to high power sources may be introducing excessive noise on the link causing disruptions.

2.1.3 Key Findings

Based on the information obtained during the network assessment and with special focus being given to addressing the issues presented by Spacely Sprockets at the Widget Springs Foundry site in Orbit City, it was observed that some key areas within the production environment could benefit from targeted improvements to the network. These improvements look to increase performance, stability, resiliency, and security while focusing on the importance of realizing operating efficiencies.

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 Spacely Sprockets 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 or its distributor and partner networks 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 table lists items that Rockwell Automation believes should be evaluated in the near future to improve specific functional aspects of the network installation at the Widget Springs Foundry site.

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

Table 2:3 – Key Findings

Key Observations		Rating Filter:	HIGH
Access Controls Observation: A procedure does not exist for deleting temporary accounts after a pre-defined time period.	Comment: Recommendation: ICS 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)		HIGH
Access Controls Observation: A procedure does not exist for removing inactive user accounts.	Comment: Recommendation: ICS 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)		HIGH
Access Controls Observation: Wireless communications are not limited to a designated physical boundary.	Comment: Recommendation: Confine wireless communications to the IACS boundaries. Actions that may be taken to confine wireless communications to IACS boundaries including reducing the power of the wireless transmission such that it cannot transit the physical perimeter, employ measures such as TEMPEST to control wireless emanations, and configuring the wireless access such that it is point to point in nature. (800-53) Prior to installation, a wireless survey should be performed to determine antenna location and strength to minimize exposure of the wireless network. The survey should take into account the fact that attackers can use powerful directional antennas, which extend the effective range of a wireless LAN beyond the expected standard range. Faraday cages and other methods are also available to minimize exposure of the wireless network outside of the designated areas. (800-82)		HIGH
Access Controls Observation: Multi-factor authentication is not required to initiate a remote access session.	Comment: Recommendation: Remote access capabilities that enable control engineers and vendors to gain remote access to systems should be deployed with multifactor security controls to prevent unauthorized individuals from gaining access to the IACS. (800-82)		HIGH
Access Controls Observation: It is unknown if IACS devices have been modified to ensure default configurations are not in place.	Comment: Recommendation: Using default configurations often leads to insecure and unnecessary open ports and exploitable network services running on hosts. Improperly configured firewall rules and router ACLs can allow unnecessary traffic. (800-82)		HIGH
Cable Management Observation: Cable bend radius is tighter than 4x cable diameter.	Comment: Recommendation: Maximum bend radius is 4 x cable diameter.		HIGH
Cable Selection Observation: The maximum length of the permanent link cables do not allow for the use of patch cables so that total length does not exceed 100m (328ft).	Comment: Permanent link cables were observed running close to 100m with additional 5m patch cables at either end Recommendation: Re-terminate the permanent link cables to a shorter length when possible. (ODVA Ethernet/IP Media Planning & Install Guide)		HIGH
Cell Area Zone Observation: All access level switches within the Cell/Area zones of the IACS network are unmanaged switches.	Comment: asdf Recommendation: Use of unmanaged switches may leave the IACS exposed to security risks, degrade the performance, and quality of the network services and may cause problems including network and system outages.		HIGH

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

Key Observations		Rating Filter:	HIGH
Data Security Observation: Portable media devices are not encrypted.	Comment: Recommendation: 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)		HIGH
Data Security Observation: A change control / configuration management procedure does not exist for ensuring backups of software, firmware, and configurations representing the as-is environment are available prior to initiating changes within the IACS.	Comment: Recommendation: A Change Control / Configuration Management 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)		HIGH
Data Security Observation: A change control / configuration management procedure does not exist to audit changes to the IACS.	Comment: Recommendation: The Change Control /Configuration Management procedure should include auditing of IACS changes and indications of changes to determine whether unauthorized changes have occurred. Automated mechanisms may be used to enforce access restrictions and support auditing of the enforcement actions. (800-53)		HIGH
Data Security Observation: A change control / configuration management procedure does not exist to detect unauthorized changes to the IACS.	Comment: Recommendation: The Change Control / Configuration Management procedure should incorporate detection of unauthorized, security-relevant configuration changes into the organization's incident response capability to ensure that such detected events are tracked, monitored, corrected, and available for historical purposes. (800-53)		HIGH
Data Security Observation: A testing environment does not exist to facilitate secure testing and impact assessment of changes prior to implementation on the live IACS.	Comment: Recommendation: 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
Data Security Observation: A policy does not exist to restrict the use of portable media.	Comment: Recommendation: Policy should be developed restricting the use of portable media devices on the IACS. Enforcement should take into consideration that it may not be feasible to physically monitor them. (800-82)		HIGH
Data Security Observation: Virus signatures are not deployed to the IACS environment a minimum of every 30 days.	Comment: Recommendation: Antivirus tools only function effectively when installed, configured, running full-time, and maintained properly against the state of known attack methods and payloads. (800-82)		HIGH
Governance Observation: A response plan does not exist stating the procedure if the IACS network communication is interrupted.	Comment: Recommendation: Include a full recovery and reconstitution of the IACS to a known state as part of contingency plan. (800-53)		HIGH
Governance Observation: Critical IACS backup data is not stored at a facility separate from the live environment.	Comment: Recommendation: 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 outlines explicit mitigation actions. (800-53)		HIGH

DRAFT or FINAL

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

Key Observations		Rating Filter:	HIGH
Governance Observation: Audit logs are not tamper proof.	Comment: Recommendation: Audit logs should be stored in a secure location to reduce the opportunity for intrusion. (800-82)		HIGH
Logical Topology Observation: Critical IACS are not redundant and are not on redundant networks.	Comment: Recommendation: 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
Power Redundancy System Observation: The strategy is not implemented on critical network components.	Comment: Recommendation: A risk analysis and / or a requirements analysis should be completed to determine the impact on the loss of the network infrastructure components. Network infrastructure components are key to the overall operation of the IACS network, application or process. 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.		HIGH
Risk Management Observation: A risk assessment has not been performed specific to the IACS network.	Comment: Recommendation: 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)		HIGH
Risk Management Observation: A procedure does not exist to test software in an isolated environment before being installed on the live IACS.	Comment: Recommendation: 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
Switch Selection Observation: Unmanaged switches are used throughout the IACS network.	Comment: There are a few Stratix 2000 switches used in some machine cells Recommendation: Use of unmanaged switches should be avoided. If they cannot be avoided, then they should be severely restricted. Managed switches provide network traffic control and improved maintenance and troubleshooting capability. Managed switches are preferred over unmanaged switches. (CPwE DIG)		HIGH
Cell Area Zone Observation: Only a minimal configuration has been performed on the access level switches (i.e. Setting the IP address for management or using an express setup)	Comment: Recommendation: Managed switches can only provide optimal performance on the network when they are configured with special considerations as to the requirements of each application they will support. Each switch should be evaluated and configured with a more complete configuration.		HIGH

2.1.4 Summary of Physical, Logical, & Security Ratings

This report will provide an overview of the network architecture along with the potential recommended actions. The following table summarizes the observations made during the network assessment. Each observation has a recommendation and a criticality rating, along with a reference to a section of this report for more detail.

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

DRAFT or FINAL

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

Documentation in Table 7-1, 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.

The following table summarizes the observations made during the network assessment. Each observation has a recommendation and a criticality rating, along with a reference to a section of this report for more detail.

Table 2:4 – Summary of Observations

Network Physical Infrastructure		Total Rating:	MODERATE
Section	Section Name	Impact Rating	Recommended Action
4.1	Physical Topology	MODERATE	It is recommended that NICs are not connected to different networks. A server or end device bridging two networks makes it a target for those trying to bypass a firewall or other security measures. (CPwE DIG)
4.2	Switch Selection	HIGH	Use of unmanaged switches should be avoided. If they cannot be avoided, then they should be severely restricted. Managed switches provide network traffic control and improved maintenance and troubleshooting capability. Managed switches are preferred over unmanaged switches. (CPwE DIG)
4.3	Router Selection	MODERATE	Use a layer 3 device that is capable of acting as the gateway for the network. Using a device that is not capable of handling the level of network gateway traffic for the IACS could introduce communication delays and may result in poor performance of the network and IACS.
4.4	Ethernet Communication Modules	LOW	Consider standardizing firmware versions across similar controller interfaces. Consistent firmware revisions improve interoperability, troubleshooting and maintenance. (CPwE DIG)
4.5	Environmental Conditions	ACCEPTABLE	
4.6	Enclosures	MODERATE	Replace enclosures with ones that are suitable for the environment they are being placed into. Using improperly rated enclosures can lead to premature device failure and downtime.
4.7	Cable Selection	MODERATE	Re-terminate the permanent link cables to a shorter length when possible. (ODVA Ethernet/IP Media Planning & Install Guide)
4.8	Cable Management	HIGH	Maximum bend radius is 4 x cable diameter.
4.9	Conduit & Routing	LOW	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)
4.10	Cable Labeling	LOW	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)

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

Network Physical Infrastructure		Total Rating:	MODERATE
Section	Section Name	Impact Rating	Recommended Action
4.11	Power Redundancy System	HIGH	A risk analysis and / or a requirements analysis should be completed to determine the impact on the loss of the network infrastructure components. Network infrastructure components are key to the overall operation of the IACS network, application or process. 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.
4.12	Grounding	MODERATE	Each section of the conduit or metal pathway should be grounded to the section adjacent to it to maintain the electrical continuity along the entire length. Follow IEEE 1100, ANSI-J-STD-607-A, or other local and national codes for the grounding and bonding requirements.

Network Logical Information		Total Rating:	MODERATE
Section	Section Name	Impact Rating	Recommended Action
5.1	Logical Topology	MODERATE	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)
5.2	Security Zone	MODERATE	Develop security appliance standards that meet the requirements of the IACS.
5.3	Manufacturing Zone	LOW	Multiple communication paths (especially diverse paths) improve the resiliency of the network and may improve the performance.
5.4	Cell/Area Zone	HIGH	Use of unmanaged switches may leave the IACS exposed to security risks, degrade the performance, and quality of the network services and may cause problems including network and system outages.

Industrial Security & Safety		Total Rating:	HIGH
Section	Section Name	Impact Rating	Recommended Action
6.1	Asset Management	LOW	Update inventory of complete IACS system and all components as an integral part of component installations, removals, and system updates. (800-53)
6.2	Governance	HIGH	Audit logs should be stored in a secure location to reduce the opportunity for intrusion. (800-82)
6.3	Risk Assessment & Management	HIGH	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)

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

Industrial Security & Safety		Total Rating:	HIGH
Section	Section Name	Impact Rating	Recommended Action
6.4	Access Controls	HIGH	Using default configurations often leads to insecure and unnecessary open ports and exploitable network services running on hosts. Improperly configured firewall rules and router ACLs can allow unnecessary traffic. (800-82)
6.5	Awareness & Training	MODERATE	The organization should develop basic training and education materials specific to the IACS. Subjects should include but are not limited to, security and safety. (800-53)
6.6	Data Security	HIGH	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)

2.2 Scope

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

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

3 CUSTOMER NETWORK DEVICES

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 the documentation of these devices relevant to the scope of this section.

The following Device and Environmental Ratings are used as a guide for assessment at each location:

Device Condition	Rating Criteria
Good	<ul style="list-style-type: none"> Network device properly mounted in a clean cabinet Stress not placed interfaces due to Ethernet Cable strain or weight Temperature, vibration, moisture, and air quality is office grade
Fair	<ul style="list-style-type: none"> Slight dust accumulation Properly mounted device with satisfactory temperature, vibration, moisture, and air quality
Poor	<ul style="list-style-type: none"> Extremely high dust or particle content within device vents and interfaces Device not mounted properly or according the vendor installation recommendation Temperature, vibration, moisture, and/or air quality is excessive or may be harmful to the MTBF of the device

Table 3:1 – Network Asset Evaluation

Allen-Bradley	1785-ENET	PAC	Mill #1-TWS	Good	Fair	Discontinued
Allen-Bradley	1756-ENBT	PAC	Mill #1-QS Main	Good	Good	Active Mature
Allen-Bradley	1756-ENBT	PAC	Mill #1-QS Main	Good	Good	Active Mature
Allen-Bradley	1756-ENBT	PAC	Mill #1-QS Main	Good	Good	Active Mature
Allen-Bradley	1783-EMS08T	Access Switch	Mill #1-QS Main	Good	Good	Active
Allen-Bradley	1783-EMS08T	Access Switch	Mill #1-QS Main	Good	Good	Active
Allen-Bradley	1783-EMS08T	Access Switch	Mill #1-QS Main	Good	Good	Active
Allen-Bradley	1756-ENBT	PAC	Mill #1-DRC Drives	Good	Good	Active Mature
Allen-Bradley	1785-ENET	PAC	Mill #1-TCOS	Good	Fair	Discontinued
Allen-Bradley	1756-ENBT	PAC	Mill #1-TCOS	Good	Fair	Active Mature
Cisco	2960-S	Distribution Switch	Mill #1-IT Cabinet	Good	Fair	Active Mature
Cisco	2960-S1	Distribution Switch	Mill #1-IT Cabinet	Good	Fair	Active Mature
Allen-Bradley	1756-ENBT	PAC	Mill #1-Canada Stamp	Good	Good	Active Mature
Allen-Bradley	1756-ENBT	PAC	Mill #1-Bundler	Good	Fair	Active Mature
3-COM	Baseline 2016-3C16470	Access Switch	Mill #1-Bundler	Good	Fair	Active
Allen-Bradley	MicroLogix 1400	PAC	Mill #1-Bundler	N/A	N/A	Active
Allen-Bradley	MicroLogix 1400	PAC	Mill #1-Bundler	N/A	N/A	Active
Allen-Bradley	1756-ENBT	PAC	Slitter #2	Good	Fair	Active Mature
Allen-Bradley	1756-ENBT	PAC	Slitter #4-Main	Good	Good	Active Mature
Allen-Bradley	1756-ENBT	PAC	Slitter #4-Main	Good	Good	Active Mature
Allen-Bradley	9300-RADES	Other	Slitter #4-Main	Good	Good	Active Mature
Hirschmann	Spider 8TX	Access Switch	Slitter #4-Main	Good	Good	Active
Allen-Bradley	1785-ENET	PAC	Mill #2-TWM	Good	Good	Discontinued
Allen-Bradley	1785-ENET	PAC	Mill #2-Strip Prep	Good	Good	Discontinued
Allen-Bradley	1756-ENBT	PAC	Mill #2-Drives PLC	Good	Good	Active Mature
Allen-Bradley	1756-ENBT	PAC	Mill #2-QS	Good	Good	Active Mature
Allen-Bradley	MicroLogix 1400	PAC	Mill #2-QS	N/A	N/A	Active
Allen-Bradley	MicroLogix 1400	PAC	Mill #2-QS	N/A	N/A	Active
Cisco	2960-S	Distribution Switch	Mill #2-IT Cabinet (Drives Room #1)	Good	Good	Active Mature
Cisco	3550	Core Switch/Router	Mill #2-IT Cabinet (Drives Room #1)	Good	Good	Active

DRAFT or FINAL

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

Allen-Bradley	1785-ENET	PAC	Mill #1-TWS	Good	Fair	Discontinued
Cisco	2960-S	Distribution Switch	Mill #2-IT Cabinet (Drives Room #2)	Good	Good	Active Mature
Cisco	2960-S	Distribution Switch	Mill #2-IT Cabinet (Drives Room #2)	Good	Good	Active Mature
Cisco	3550	Core Switch/Router	Mill #2-IT Cabinet (Drives Room #2)	Good	Good	Active
Allen-Bradley	SLC-5/05	PAC	Mill #2-PTA	Good	Good	Active Mature
Allen-Bradley	SLC-5/05	PAC	Mill #2-Bundler	Good	Good	Active Mature
Allen-Bradley	1756-ENBT	PAC	Mill #2-Bundler (Remote)	Good	Fair	Active Mature
Allen-Bradley	1783-EMS08T	Access Switch	Mill #2-Bundler (Remote)	Good	Fair	Active
Allen-Bradley	MicroLogix 1400	PAC	Mill #2-Bundler (Remote)	Good	Fair	Active
Allen-Bradley	MicroLogix 1400	PAC	Mill #2-Bundler (Remote)	Good	Fair	Active
Allen-Bradley	1756-ENBT	PAC	Mill #2-E-Line	Good	Good	Active Mature
Allen-Bradley	1756-ENBT	PAC	Mill #2-Saw/Cutoff/Blade	N/A	N/A	Active Mature
Allen-Bradley	1756-ENBT	PAC	Mill #2-Saw Carriage	Good	Good	Active Mature
Allen-Bradley	1783-EMS08T	Access Switch	Mill #2-Saw Carriage	Good	Good	Active
Allen-Bradley	1783-EMS08T	Access Switch	Mill #2-Saw Operator (Panel)	Good	Fair	Active
Allen-Bradley	1783-BMS20CGL	Access Switch	Mill #1-QS Encoder (Panel #1)	Good	Good	Active
Allen-Bradley	1783-BMS20CGL	Access Switch	Mill #1-QS Encoder (Panel #2)	Good	Good	Active
Allen-Bradley	1783-EMS08T	Access Switch	Mill #1-QS Encoder (Panel #3)	Good	Good	Active
Allen-Bradley	1768-ENBT / L43S	Safety PAC	Mill #2-Safety Prep	Good	Good	Active
Allen-Bradley	1783-ETAP	Other	Mill #2-Safety Prep	Good	Good	Active
Allen-Bradley	1783-BMS10CGA	Access Switch	Mill #2-Safety Prep	Good	Good	Active

DRAFT or FINAL

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

4 NETWORK PHYSICAL INFRASTRUCTURE

The current architecture at Spacely Sprockets, Orbit City employs a star topology for switch connections. Resilient connections may be used within the production network environment. Plant level connections to access switches are using primarily device level ring (DLR) topology. In saying this, some panels are using unmanaged switches to aggregate local machine connections. Cells/Areas are connected to the Manufacturing Zone using switch to switch connections. Primarily copper cabling is present in the IACS network.

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

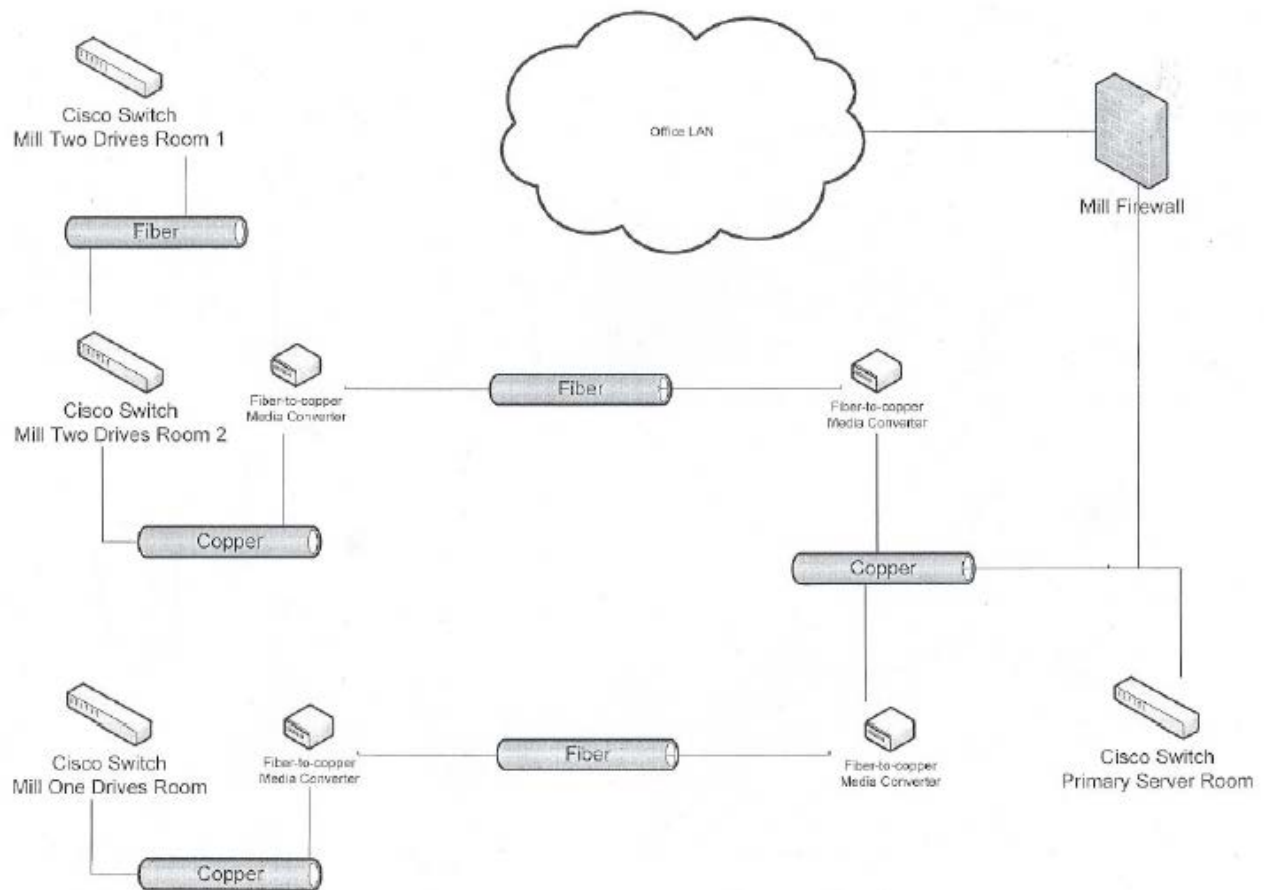


Figure 4:1 – Spacely Sprockets Production Network Topology

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

4.1 Physical Topology

The network infrastructure is arranged in a star topology at Spacely Sprockets, Orbit City.

The topology could be improved with switch redundancy and the use of Etherchannels. REP could also be implemented to provide a more fault tolerant topology.

Table 4:1 – Physical Topology Observation Results

Physical Topology		Section Rating:	MODERATE
Observation: The physical topology of the IACS network is a star.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: The IACS network was designed to meet a specific availability rating.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: Fault tolerance has been incorporated into the IACS network design.	Comment: Minimal fault tolerance is incorporated, primarily in redundant media paths Recommendation: Information Purposes Only		ACCEPTABLE
Observation: Fault tolerance does not incorporate redundancy of end devices.	Comment: Recommendation: Determine if the redundancy of end devices is required to meet uptime requirements and implement accordingly. (CPwE DIG)		LOW
Observation: Fault tolerance does not incorporate redundancy of switches.	Comment: Recommendation: Determine if the redundancy of switches is required to meet uptime requirements and implement accordingly. (CPwE DIG)		MODERATE
Observation: Fault tolerance does not incorporate redundancy of routers.	Comment: Recommendation: Determine if the redundancy of routers is required to meet uptime requirements and implement accordingly. (CPwE DIG)		MODERATE
Observation: Fault tolerance does not incorporate redundancy of firewalls.	Comment: Recommendation: Determine if the redundancy of firewalls is required to meet uptime requirements and implement accordingly. (CPwE DIG)		MODERATE
Observation: Fault tolerance incorporates redundancy of links.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: A virtual infrastructure is used to support manufacturing applications.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: Dual NICs are employed in devices on the IACS network.	Comment: 1756-EN2TR modules with dual nics are present Recommendation: It is recommended that NICs are not connected to different networks. A server or end device bridging two networks makes it a target for those trying to bypass a firewall or other security measures. (CPwE DIG)		MODERATE

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

4.2 Switch Selection

The use of managed switches allows for advanced network functionality in the production environment at the Widget Springs Foundry site. However, the presence of unmanaged switches creates the potential of having larger broadcast domains and increased latency on the network as well as the possibility of network loops and broadcast storms if connections are routed incorrectly.

Table 4:2 – Switch Selection Observation Results

Switch Selection		Section Rating:	HIGH
Observation: A single switch vendor is used consistently throughout the network.	Comment: Cisco switches are used throughout the plant		ACCEPTABLE
	Recommendation: Information Purposes Only		
Observation: Managed switches are used throughout the IACS network.	Comment:		ACCEPTABLE
	Recommendation: Information Purposes Only		
Observation: Unmanaged switches are used throughout the IACS network.	Comment: There are a few Stratix 2000 switches used in some machine cells		HIGH
	Recommendation: Use of unmanaged switches should be avoided. If they cannot be avoided, then they should be severely restricted. Managed switches provide network traffic control and improved maintenance and troubleshooting capability. Managed switches are preferred over unmanaged switches. (CPwE DIG)		
Observation: Switches in the IACS network are currently out of support (End-of-Life).	Comment:		MODERATE
	Recommendation: Upgrade switch hardware that is no longer supported by the vendor. Out or support hardware presents a risk if a failure occurs that requires a replacement, which if not available, could result in downtime.		
Observation: Switches are designed for the environment in which they are used.	Comment:		ACCEPTABLE
	Recommendation: Information Purposes Only		
Observation: Switches are not under a maintenance/support agreement.	Comment:		MODERATE
	Recommendation: Determine if placing switches under a maintenance/support agreement is necessary to maintain plant uptime requirements. (CPwE DIG)		
Observation: It is unknown if spare switches are stocked on site.	Comment:		MODERATE
	Recommendation: Determine if stocking spares on site is needed to meet availability requirements. (CPwE DIG)		

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

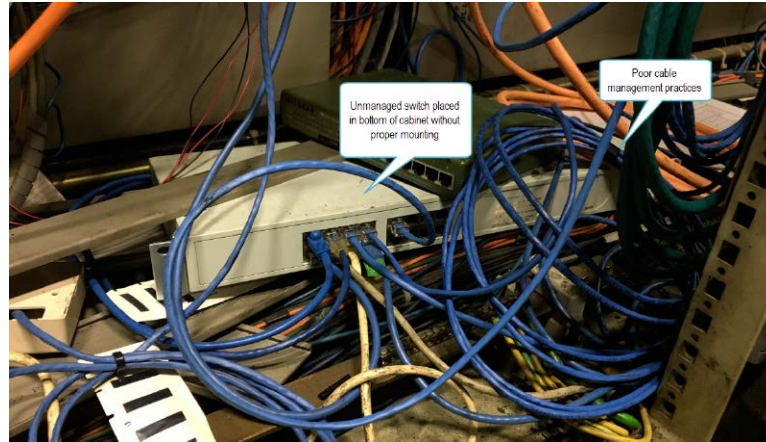


Figure 4:2 - Mill #1 Bundler Unmanaged Switch Mounting

4.3 Router Selection

Since there are multiple subnets on the production network, routing is required for communication between subnets to occur and there is an identified router that handles this task.

Table 4:3 – Router Selection Observation Results

Router Selection		Section Rating:	MODERATE
Observation: A router is installed in the network.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: There is only one router in the network.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: A single router vendor is used consistently throughout the network or no router is currently in use.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: A PLC is acting as the gateway for the network.	Comment: Recommendation: Use a layer 3 device that is capable of acting as the gateway for the network. Using a device that is not capable of handling the level of network gateway traffic for the IACS could introduce communication delays and may result in poor performance of the network and IACS.		MODERATE
Observation: Routers are designed for the environment in which they are used or no router is currently in use.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: Routers are not under a maintenance/support agreement.	Comment: Recommendation: Determine if placing routers under a maintenance/support agreement is necessary to maintain plant uptime requirements. (CPwE DIG)		MODERATE
Observation: Spare routers are not stocked on site.	Comment: Recommendation: Determine if stocking spares on site is needed to meet availability requirements. (CPwE DIG)		MODERATE

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

Router Selection		Section Rating:	MODERATE
Observation: There are no available expansion slots.	Comment: Recommendation: Information Purposes Only		LOW
Observation: There are available ports or no router is currently in use.	Comment: There are 2 available ports on the router Recommendation: Information Purposes Only		ACCEPTABLE

4.4 Ethernet Communication Modules

A single controller platform is currently in use within the production environment at the Widget Springs Foundry site. This results in a common set of communication cards being employed across systems in the production environment.

Table 4:4 – Ethernet Communication Modules Observation Results

Ethernet Communication Modules		Section Rating:	LOW
Observation: Switch port speed/duplex settings are configured correctly for the controller interface.	Comment: Auto speed and duplex is being used on most switchports Recommendation: Information Purposes Only		ACCEPTABLE
Observation: Firmware revisions of similar controller interfaces are not consistent with each other.	Comment: Recommendation: Consider standardizing firmware versions across similar controller interfaces. Consistent firmware revisions improve interoperability, troubleshooting and maintenance. (CPwE DIG)		LOW
Observation: Non-Rockwell controllers/interfaces are not used.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: Spare controller interface modules are stocked on site.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

4.5 Environmental Conditions & Enclosures

Assessment of the environmental conditions found no evidence of corrosion or material degradation on the network hardware however the enclosures may not provide suitable protection for the network equipment.

Table 4:5 – Environmental Conditions Observation Results

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

Table 4:6 – Enclosures Observation Results

Enclosures		Section Rating:	MODERATE
Observation: The network equipment is mounted in enclosures.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: The enclosures are not properly rated for the environment.	Comment: Enclosures in washdown areas are not rated for washdown Recommendation: Replace enclosures with ones that are suitable for the environment they are being placed into. Using improperly rated enclosures can lead to premature device failure and downtime.		MODERATE
Observation: Open post networking cabinets do not exist outside of protective environments on the IACS network.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE

Spacely Sprockets – Orbit City STANDARD NETWORK ASSESSMENT



Figure 4:3 - Mill #2 Rea JET Cabinet Filter

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

4.6 Cable Selection

Current cable standards are not consistently followed for cable and connector usage within the production environment at Spacely Sprockets, Orbit City. Shielded copper cable is installed with over-molded termination types.

Fiber optic cable and connectors do not appear to be standardized within the production environment for long distance communications.

Table 4:7 – Cable Selection Observation Results

Cable Selection		Section Rating:	MODERATE
Observation: There is a specification for cable/connectors to be used.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: It is unknown if cables are certified to perform to TIA/EIA-568 specifications.	Comment: Recommendation: 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
Observation: Certification testing is not performed as part of a regular maintenance program.	Comment: Recommendation: 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
Observation: CAT5e Cable is installed.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: Cables have been in use for 10 years or more.	Comment: Recommendation: 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.		LOW
Observation: Shielded cables are installed.	Comment: Recommendation: If the potential difference is less than or equal to 1 volt, root-mean-square (RMS), the shield of the cable should be connected to the shielded jack at both ends of the horizontal cable and shielded patch cords used to connect from jacks on the horizontal cable to equipment. Since the switch / active equipment in the zone enclosure is grounded, the jack on the horizontal cable does not have to be grounded itself. As an option, depending on user preference, it can be grounded to the enclosure. If the potential difference is greater than 1 volt RMS, the use of a Potential Equalizing Conductor (PEC) should be evaluated. The PEC is used to connect spatially separated devices to ensure that they are at the same potential. If the potential difference is greater than 1 volt RMS, a measurement of the potential difference has not been made or a PEC is not deployed, the shield of the horizontal cable should not be connected to the local ground at the end farthest away from the zone enclosure switch. In the event that a shielded jack is used at this remote end, it has to be isolated from the local ground. This can be accomplished by mounting the jack in a patch panel similar to the one described above, or by using another isolating device, for example a DIN rail mount adaptor. The shield should be connected to the jack at the end that is located in the enclosure.		ACCEPTABLE

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

Cable Selection		Section Rating:	MODERATE
Observation: High-flex cables are installed.	Comment: Recommendation: High-flex cable should only be used where needed. Signal propagation characteristics of high-flex cable are not as good as standard cable so its use should be restricted. (ODVA Ethernet/IP Media Planning & Install Guide)		LOW
Observation: Over-molded cable terminations are used.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: There are no cable runs longer than 100m.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: The maximum length of the permanent link cables do not allow for the use of patch cables so that total length does not exceed 100m (328ft).	Comment: Permanent link cables were observed running close to 100m with additional 5m patch cables at either end Recommendation: Re-terminate the permanent link cables to a shorter length when possible. (ODVA Ethernet/IP Media Planning & Install Guide)		HIGH
Observation: Manufacturer certified patch cables are used.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: Fiber optic cables are not used in the network.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: There is no specification for cable/connectors to be used.	Comment: Recommendation: Specifying cable and connectors ensures they are suited to the installation and perform within expectations. (ODVA Ethernet/IP Media Planning & Install Guide)		LOW
Observation: It is unknown if the installed cable/connectors comply with specification.	Comment: Recommendation: Re-terminate or re-run cables so that the cables and/or connectors comply with specifications. (ODVA Ethernet/IP Media Planning & Install Guide)		LOW
Observation: Certification testing is not performed as part of a regular maintenance program.	Comment: Recommendation: 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
Observation: Cables have been in use for less than 15 years.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: Backbone links between switches are 1 Gbps.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: It is unknown if MTRJ connectors are used.	Comment: Recommendation: MTRJ connectors have been unreliable in industrial applications. ST, SC or LC connectors are preferred. (ODVA Ethernet/IP Media Planning & Install Guide)		LOW
Observation: There are no cable runs longer than 1000 ft.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: Media converters are not used.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE

DRAFT or FINAL

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

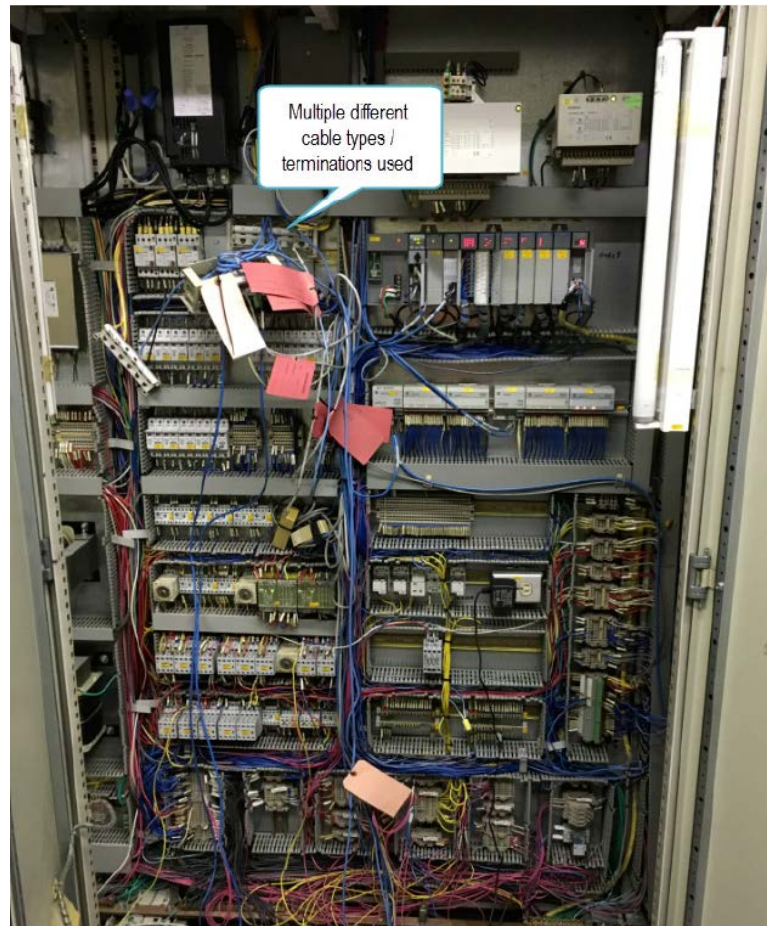


Figure 4:4 - Mill #2 PTA Panel Cable Terminations

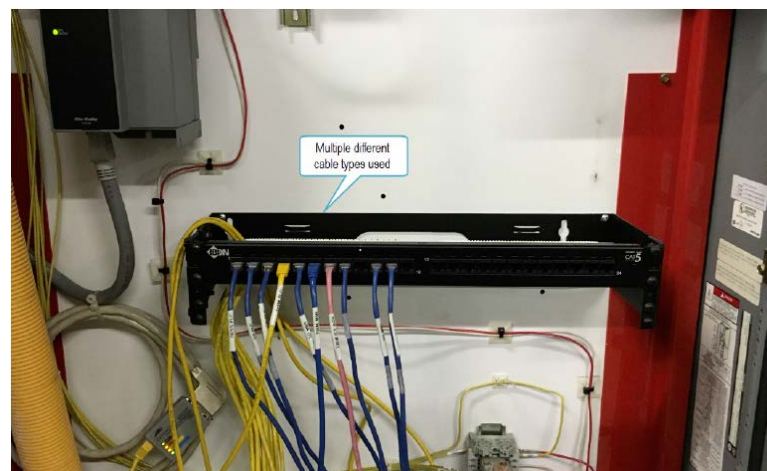


Figure 4:5 - Mill #2 TWM Cable Routing

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

4.7 Cable Management

The lack of use of proper cable management practices was noted in the production environment at the Widget Springs Foundry site. Improper cable management is seen as a significant potential risk for the production environment as it can be a contributor to cable damage and/or premature failure, potentially leading to network downtime and lost production.

There were significant issues noted for the cable installation at various locations throughout the plant.

- 1) Zip ties were over tightened and were cutting into cable jacket at several locations
- 2) Excess cable length in some cases was coiled and secured with zip ties however this caused the cable to exceed the allowable bend radius

Table 4:8 – Cable Management Observation Results

Cable Management		Section Rating:	HIGH
Observation: Cable management practices are not used in areas containing network equipment.	Comment: Recommendation: Cable management refers to dressing and routing cables, in the vicinity of network equipment, in a manner that protects the cable and alleviates strain on connections.		MODERATE
Observation: Cables are not contained in wire ways inside enclosures.	Comment: Loose cabling was observed hanging in network cabinets Recommendation: Cables should be secured physically to prevent damage to the cables, prevent movement of the cable to prevent damage to the connectors and the cable. If not within a wire way, then secured using recommended best practices for the securing of communication cables in an IACS network.		MODERATE
Observation: Cables are not secured with plastic cable ties.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: Cables are not susceptible to damage from doors opening/closing.	Comment: Recommendation: Re-route cables within cabinets/enclosures away from doors to prevent pinching.		ACCEPTABLE
Observation: Cables are not stretched or dangling in a manner than places strain on cable connectors.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: Cables are not stretched or dangling in a manner than places strain on device connectors.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: There is at least 12 inches of slack in the cable.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: Cable bend radius is tighter than 4x cable diameter.	Comment: Recommendation: Maximum bend radius is 4 x cable diameter.		HIGH
Observation: Large coils of excess cable are present.	Comment: Recommendation: 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.		MODERATE
Observation: Permanent link cables terminate in patch panels.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

Cable Management		Section Rating:	HIGH
Observation: Cable bend radius is not tighter than 15x cable diameter.	Comment:	ACCEPTABLE	
	No fiber cabling is installed		
	Recommendation: Information Purposes Only		



Figure 4:6 - Mill #2 TWM Panel Cable Routing

Spacely Sprockets – Orbit City STANDARD NETWORK ASSESSMENT



Figure 4:7 - Mill #2 Drives Room #1 IT Cabinet

Spacely Sprockets – Orbit City STANDARD NETWORK ASSESSMENT

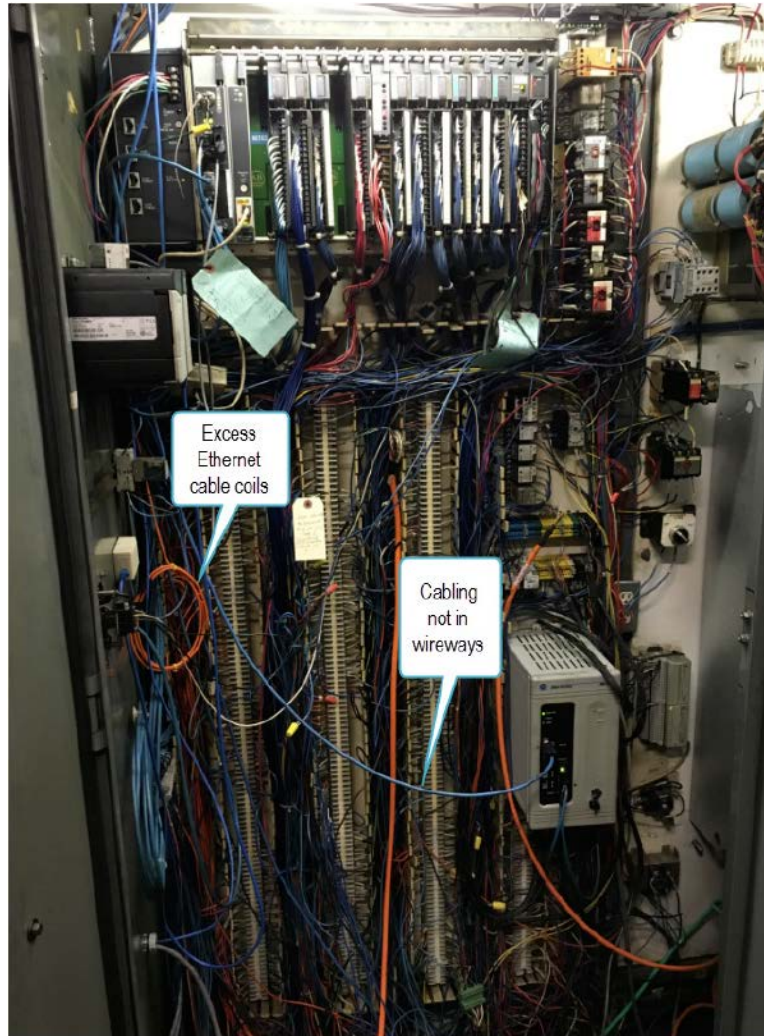


Figure 4:8 - Mill #1 Travelling Cutoff Saw

Spacely Sprockets – Orbit City STANDARD NETWORK ASSESSMENT

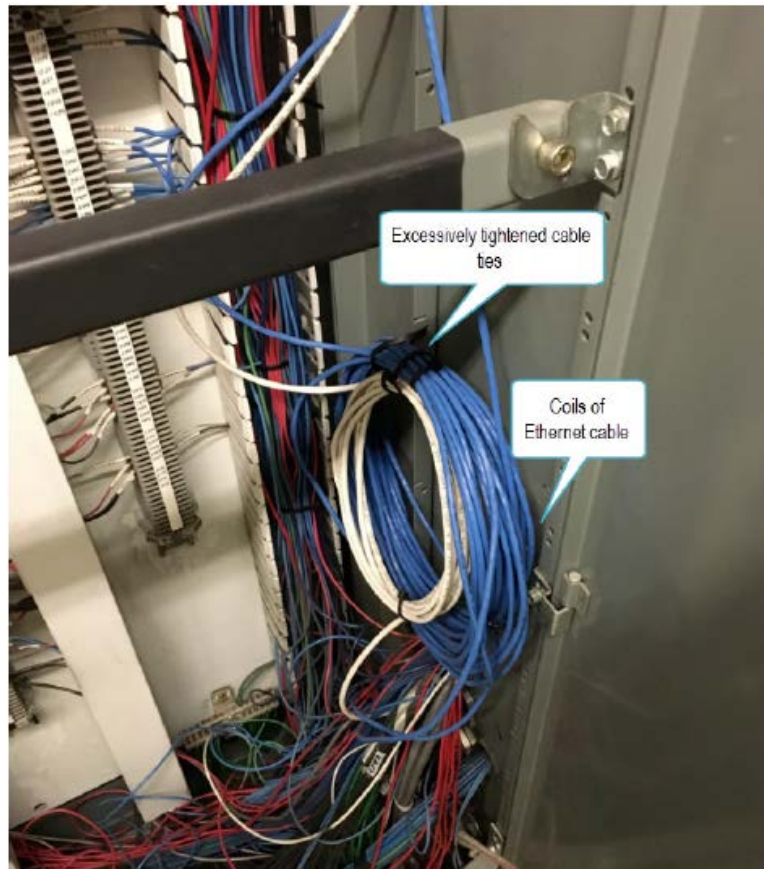


Figure 4:9 - Slitter #4 Drives Panel

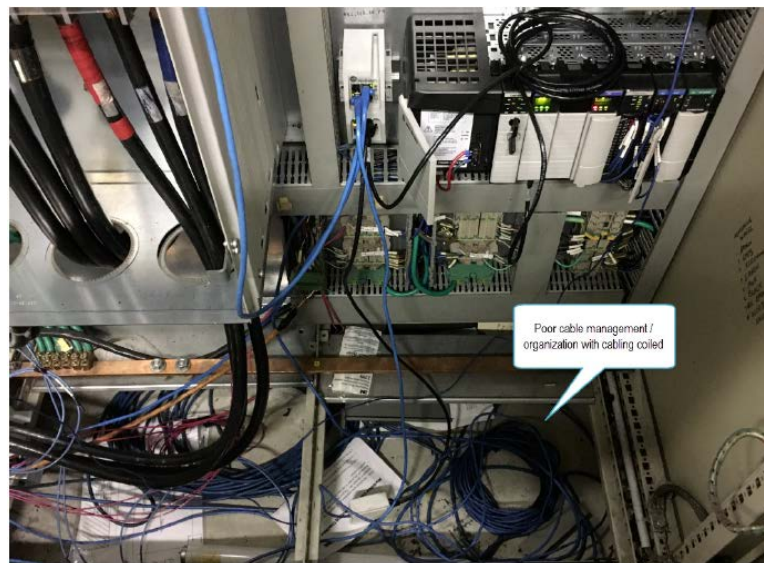


Figure 4:10 - Mill #2 Saw Carriage

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

4.8 Conduit & Routing

Cables are routed predominantly via innerduct pathways within the Widget Springs Foundry site. Exposure to sources of Electro-Magnetic Interference (EMI) such as fluorescent lighting or high-power sources were noted and could cause the cabling to be susceptible to electrical noise from EMI.

Table 4:9 – Conduit & Routing Observation Results

Conduit & Routing		Section Rating:	LOW
Observation: Permanent link copper cables do not enter enclosures near a 3-phase power source.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: Copper cabling is routed near fluorescent lighting.	Comment: Recommendation: 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)		MODERATE
Observation: Conduit fill capacity meets TIA-569 (60% filled) standard.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: Copper cable runs do not exceed 30 meters or is not routed in a conduit system.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: More than two 90 degree bends exist in the copper cable run.	Comment: Recommendation: 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

Spacely Sprockets – Orbit City STANDARD NETWORK ASSESSMENT

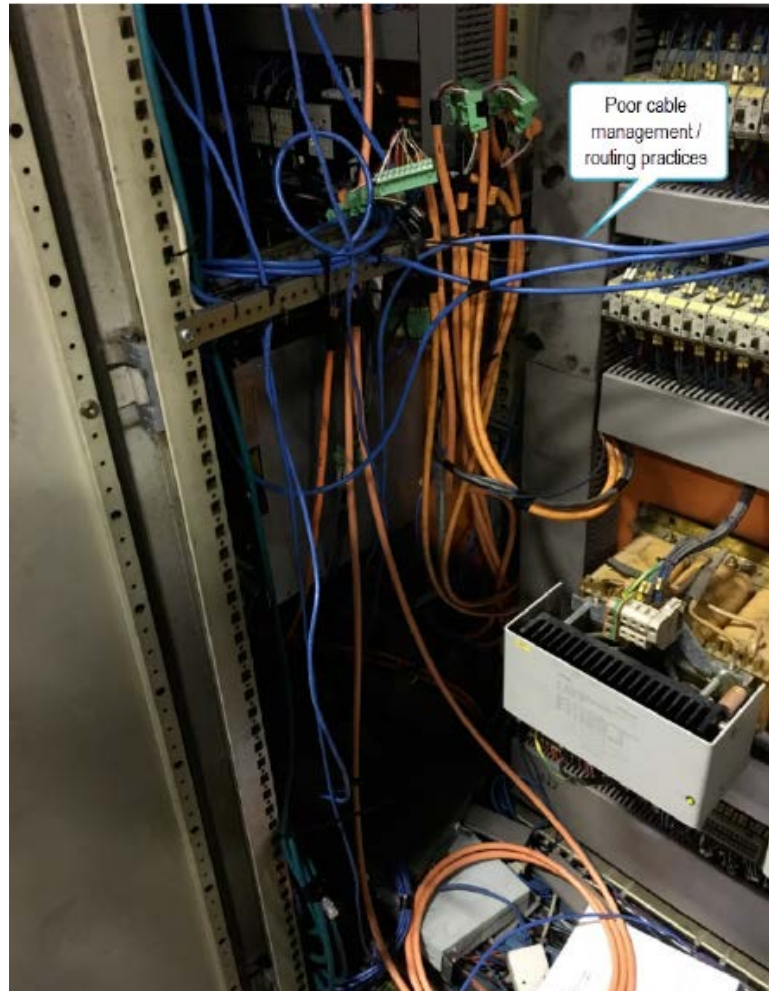


Figure 4:11 - Mill #1 Bundler

Spacely Sprockets – Orbit City STANDARD NETWORK ASSESSMENT



Figure 4:12 - Slitter #4 Drives Room Cable Routing

Spacely Sprockets – Orbit City STANDARD NETWORK ASSESSMENT



Figure 4:13 - Mill #1 Quick Settings Panel



Figure 4:14 - Slitter #4 Drives Room

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

4.9 Cable Labeling

Cable labeling standards may not be consistently deployed in the production environment. If the cable labeling scheme is not properly documented, it may be a factor in the inconsistent application of labeling standards throughout the production environment. Documentation for the labeling scheme should be created and should be reviewed and updated periodically or as required to support the network installation within the environment.

Table 4:10 – Cable Labeling Observation Results

Cable Labeling		Section Rating:	LOW
Observation: There is a site standard for cable labeling.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: All cable labels are legible.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: It is unknown if documentation exist for cable labels on the IACS network.	Comment: Recommendation: 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

4.10 Power Redundancy System

A power redundancy strategy exists for the network at the Widget Springs Foundry site however it does not provide coverage for critical components.

Table 4:11 – Power Redundancy System Observation Results

Power Redundancy System		Section Rating:	HIGH
Observation: There is a power redundancy strategy for network equipment.	Comment: UPS power supplies are used on critical equipment Recommendation: Information Purposes Only		ACCEPTABLE
Observation: The strategy is not implemented on critical network components.	Comment: Recommendation: A risk analysis and / or a requirements analysis should be completed to determine the impact on the loss of the network infrastructure components. Network infrastructure components are key to the overall operation of the IACS network, application or process. 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.		HIGH
Observation: The strategy is implemented across all network infrastructure components.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

Power Redundancy System		Section Rating:	HIGH
Observation: Uninterruptible power supplies (UPS) are used as part of the power redundancy strategy.	Comment: Recommendation: Information Only.		ACCEPTABLE
Observation: UPS units are monitored or testing regularly to confirm operating status.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: Dual power supplies are used for critical network hardware.	Comment: Recommendation: Information Only.		ACCEPTABLE
Observation: Separate power circuits are used for critical network hardware.	Comment: Recommendation: Information Only.		ACCEPTABLE

4.11 Grounding

Proper electrical grounding of all network equipment in the IACS network is important as it helps reduce / limit the amount of electrical noise present in the network which could cause errors in network transmissions and reduce the available bandwidth in heavily affected segments of the network.

Table 4:12 – Grounding Observation Results

Grounding		Section Rating:	MODERATE
Observation: A single ground system is used on site.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: Control/network equipment is bonded to racks/cabinets.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: Control/network equipment is bonded to common ground.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: Metal conduit/wire way sections are not bonded to adjacent sections.	Comment: Recommendation: Each section of the conduit or metal pathway should be grounded to the section adjacent to it to maintain the electrical continuity along the entire length. Follow IEEE 1100, ANSI-J-STD-607-A, or other local and national codes for the grounding and bonding requirements.		MODERATE
Observation: Metal conduit/wire way sections are not bonded to termination points.	Comment: Recommendation: The cabinets or other termination point of the conduit would be considered to be part of the continuous pathway of the conduit or metal wire way, and therefore should be bonded to the conduit or wire way. Follow IEEE 1100, ANSI-J-STD-607-A, or other local and national codes for the grounding and bonding requirements.		MODERATE

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

5 NETWORK LOGICAL INFORMATION

The logical architecture at Spacely Sprockets, Orbit City consists of multiple subnets using VLAN segmentation with no routing between subnets. Deploying subnets with no routing does provide a higher level of isolation and may be appropriate for highly critical systems however this may also lead to the over-expansion of the isolated subnets (and consequently expansion of the broadcast and fault domains) as new equipment or devices are added in those areas. Routing traffic between subnets/VLANs provides administrative controls over network traffic, allows broadcast and fault domains to be well defined and controlled, and allows for scalable network designs to be implemented within the production environment.

5.1 Logical Topology

Logical segmentation is used in the production environment. The typical subnet configuration in use allows for 255 - 1022 devices. It was also noted that critical systems were either not redundant or were not connected to redundant networks. Implementing redundancy in critical systems limits the single point of failure possibilities which could be present and helps achieve the high availability requirements of the system. These requirements should be understood and re-assessed as needed to ensure that the IACS network is able to meet the needs of critical production systems.

Table 5:1 – Logical Topology Observation Results

Logical Topology		Section Rating:	MODERATE
Observation: Logical flow maps exist for the IACS network.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: Logical flow maps are not updated when changes to the IACS occur.	Comment: Recommendation: Logical flow maps should be updated according to a change management procedure when any changes are made to the IACS network.		MODERATE
Observation: The IACS network is segmented into subnets.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: Subnets are separated logically.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: Subnets are not separated physically.	Comment: Recommendation: 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 networks. In the CPwE architecture, each VLAN in the Manufacturing zone has a unique subnet assigned to it.		MODERATE
Observation: A specification guide is not provided to OEMs for network compliance	Comment: Recommendation: A specification guide should be created that provides OEMs with requirements to meet plant network compliance. (CPwE DIG)		MODERATE

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

Logical Topology		Section Rating:	MODERATE
Observation: Critical IACS are not redundant and are not on redundant networks.	Comment: Recommendation: 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
Observation: Critical IACS are not designed for graceful degradation to prevent catastrophic cascading evenings.	Comment: Recommendation: 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)		MODERATE
Observation: ICS are prioritized based on criticality to production.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE

5.2 Security Zone

The noted lack of isolation between production and enterprise networks places the security, stability, and performance of the production network at risk. To provide a scalable architecture, the use of an Industrial De-Militarized Zone (IDMZ) that includes active / backup firewalls between the production and enterprise networks allows for increased segmentation, secure data flow, and added security on the production network.

Table 5:2 – Security Zone Observation Results

Security Zone		Section Rating:	MODERATE
Observation: The IACS network is isolated from the Enterprise network.	Comment: asd Recommendation: Information Purposes Only		ACCEPTABLE
Observation: Security appliances are used on the network.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: It is unknown if a set of standards exist defining security appliance/firewall infrastructure.	Comment: Recommendation: Develop security appliance standards that meet the requirements of the IACS.		MODERATE
Observation: The IACS is not configured to maximize use of vendor supplied security features.	Comment: Recommendation: 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. VLAN hopping, the ability for an attack to inject frames to unauthorized ports, has been demonstrated using switch spoofing or double-encapsulated frames. These attacks cannot be conducted remotely and require local physical access to the switch. 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
Observation: The IACS network has not become disabled during adverse conditions.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE

DRAFT or FINAL

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

5.3 Manufacturing Zone

The current architecture uses network devices that are dedicated to the IACS network. VLANs are used for network segmentation however there is no router installed on the IACS network. 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.

Table 5:3 – Manufacturing Zone Observation Results

Manufacturing Zone		Section Rating:	LOW
Observation: Core network devices are dedicated to the IACS network.	Comment: asdf		ACCEPTABLE
	Recommendation: Information Purposes Only		
Observation: The logical framework for the IACS network follows a hierarchal or campus model design methodology.	Comment:		ACCEPTABLE
	Recommendation: Information Purposes Only		
Observation: The IACS network infrastructure design employs Core/Distribution level switches.	Comment:		ACCEPTABLE
	Recommendation: Information Purposes Only		
Observation: Managed switches are employed at the Core / Distribution level.	Comment:		ACCEPTABLE
	Recommendation: Information Purposes Only		
Observation: The Core / Distribution level managed switches have been configured.	Comment:		ACCEPTABLE
	Recommendation: Information Purposes Only		
Observation: The Device Manager (Web Interface) was used to configure the Core / Distribution level switches with the Cell/Area zones.	Comment:		ACCEPTABLE
	Recommendation: Information Purposes Only		
Observation: The Core / Distribution level switch configurations have not been verified for accuracy.	Comment:		LOW
	Recommendation: The end configuration of the switch is the important part of ensuring the proper configuration and operation of the network. Regardless of the process used to configure the network infrastructure assets, a line by line validation of the configuration should be performed.		
Observation: A company standard or policy does exist for the configuration and operation of Core / Distribution level IACS switches.	Comment:		ACCEPTABLE
	Recommendation: Information Purposes Only		
Observation: A company policy or stand was used to configure the Core / Distribution level IACS switches.	Comment:		ACCEPTABLE
	Recommendation: Information Purposes Only		
Observation: An Ethernet/IP I/O network using produce / consume tags is employed on the IACS network.	Comment:		ACCEPTABLE
	Recommendation: Information Purposes Only		

DRAFT or FINAL

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

Manufacturing Zone		Section Rating:	LOW
Observation: The Ethernet/IP I/O network is connected employing a DLR.	Comment: Recommendation: 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 (RPI) at which they communicate need to be understood before a recommendation can be made.		ACCEPTABLE
Observation: VLANs are employed for network segmentation.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: Switches are not configured to use the default VLAN.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: A dedicated management VLAN exist on the IACS network.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: Dedicated VLANs do not exist for managing all of the different IACS network operations.	Comment: Recommendation: 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
Observation: Open switchports exist on Core / Distribution level switches.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: Open switchports on Core / Distribution level switches have been administratively shutdown (disabled).	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: The Manufacturing Zone is connected to the Cell / Area Zone via switch to switch.	Comment: Recommendation: 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. Dual homed computers pose a security risk. A complete requirements analysis and risk analysis should be completed to determine proper method to uplink cell / area zone networks.		ACCEPTABLE
Observation: It is unknown if there are redundant paths connecting the Core / Distribution level switches to the Access level switches.	Comment: Recommendation: Multiple communication paths (especially diverse paths) improve the resiliency of the network and may improve the performance.		MODERATE
Observation: The IPv4 address schema is documented for IACS network.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: The IACS network IP address schema is employing a private IPv4 address range.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: Each VLAN on the IACS network has a unique IPv4 subnet.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: Procedures exist for the replacement and configuration of IACS devices.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

Manufacturing Zone		Section Rating:	LOW
Observation: IP address segmentation does not exist between the Enterprise network and the IACS network.	Comment: Recommendation: The IACS and Enterprise networks have different functions and have different requirements. To help facilitate the transfer of information between the two networks, separate IP addresses or complete IP address scheme should be created and used.		MODERATE
Observation: A router is not installed on the IACS network.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE

5.4 Cell/Area Zone

The use of unmanaged access switches within the Cell/Area zones of the IACS network is not recommended as it 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. 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, configuration of the switch needs to be done with special considerations as to the requirements of each application that the switch will handle. Most switches in the production environment at Spacely Sprockets, Orbit City 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 5:4 – Cell/Area Zone Observation Results

Cell/Area Zone		Section Rating:	HIGH
Observation: All access level switches within the Cell/Area zones of the IACS network are unmanaged switches.	Comment: asdf Recommendation: Use of unmanaged switches may leave the IACS exposed to security risks, degrade the performance, and quality of the network services and may cause problems including network and system outages.		HIGH
Observation: Managed access level switches within the Cell/Area zones have been configured.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: Cisco Network Assistant (CAN) was used to configure the access level switches with the Cell/Area zones.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: The managed access level switch configurations have not been verified for accuracy.	Comment: Recommendation: The end configuration of the switch is the important part of ensuring the proper configuration and operation of the network. Regardless of the process used to configure the network infrastructure assets, a line by line validation of the configuration should be performed.		LOW

DRAFT or FINAL

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

Cell/Area Zone	Section Rating:	HIGH HIGH
Observation: Only a minimal configuration has been performed on the access level switches (i.e. Setting the IP address for management or using an express setup)	Comment: Recommendation: Managed switches can only provide optimal performance on the network when they are configured with special considerations as to the requirements of each application they will support. Each switch should be evaluated and configured with a more complete configuration.	
Observation: A company standard or policy does not exist for the configuration and operation of IACS switches?	Comment: Recommendation: 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 policies 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 may be required.	MODERATE
Observation: Access level switches are not managed by a PLC (PAC).	Comment: Recommendation: Configuring the Access (Cell / Area Zone) switches in the I/O tree of your applications allows some configuration and maintenance functionality from your project. The backing up, restoring, importing, and exporting of configuration data can be done from that controller A requirements analysis should be done or this as part of the overall analysis to determine if this option would have any impact on the performance and if the switches in the Cell / Area Zone support this option. This option should be configured when it does not impact the overall performance of the network.	ACCEPTABLE
Observation: Unmanaged access level switches are not employed on the IACS network.	Comment: Recommendation: Information Purposes Only	ACCEPTABLE
Observation: Access level switches support more than one Cell/Area zone.	Comment: Recommendation: Information Purposes Only	ACCEPTABLE
Observation: Cell/Area Zones follow the same VLAN scheme as the Manufacturing Zone.	Comment: Recommendation: Information Purposes Only	ACCEPTABLE
Observation: Open switchports exist on access level switches.	Comment: Recommendation: Information Purposes Only	ACCEPTABLE
Observation: Open switchports on access level switches have not been administratively shutdown (disabled).	Comment: Recommendation: Unused switchports (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 Automation Stratix 8000, 8300, & 5700 switches, the state of the switchports (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.	MODERATE

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

Cell/Area Zone	Section Rating: HIGH
Observation: Resilient Ethernet Protocol (REP) is not being employed in Cell/Area Zones.	Comment: Recommendation: A ring physical topology is a topology used in an IACS network for a variety of reasons, the most common is for network resiliency and it accomplishes this by providing multiple communication paths. REP provides the logical management of the network connections to prevent the multiple communication paths from disrupting the network. It also provides the mechanisms required for fast convergence of the network in the event of a single network failure. It is recommended that if a ring topology is to be used among the switches within the Cell / Area Zone, that: <ul style="list-style-type: none"> • A ring management protocol be used • The switches being deployed should be from the same manufacturer • The switches should be the same model and firmware / IOS • Should be configured and enabled on all the switches within the ring

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

6 INDUSTRIAL SECURITY & SAFETY

At Spacely Sprockets, Orbit City, security within the network architecture of the production environment is handled via the use of security appliances within the production network. Security policies have been developed specifically for the IACS and these should be reviewed periodically as part of a holistic cyber defense program to ensure they continue to guard against current cyber threats.

It is important to note that hardening of the network infrastructure and end devices in the production environment may not have been completed. Areas that need improvement include:

- Enforcement of standards regarding the use of portable media devices
- Hardening of switches via configuration of various security aspects (ie: port security, MAC address tracking per port, Access Control Lists (ACLs), etc.)

Cyber-attacks on production facilities are becoming more common and therefore security should be a major topic of consideration. Rockwell Automation treats security within the production environment very seriously and is ready to assist Spacely Sprockets in securing their environment through cyber security services for assessing, remediating, and managing security risks.

6.1 Asset Management

Procedures exist for maintaining an accurate inventory of hardware assets within the production environment.

Critical infrastructure parts BOMs (Bill of Material) do not exist or may need to be updated. This presents a risk to production in the event of a failure requiring replacement parts on critical infrastructure as the failure to identify and procure the correct replacement part could significantly extend production downtime.

Table 6:1 – Asset Management Observation Results

Asset Management		Section Rating:	LOW
Observation: A policy exist requiring an accurate inventory be established and maintained for IACS assets.	Comment: asf		ACCEPTABLE
	Recommendation: Information Purposes Only		
Observation: A procedure exist for maintaining an accurate inventory of IACS hardware assets.	Comment:		ACCEPTABLE
	Recommendation: Information Purposes Only		
Observation: A procedure does not exist for maintaining an accurate inventory of IACS software assets.	Comment:		LOW
	Recommendation: Update inventory of software components as an integral part of component installations, removals, and system updates. (800-53)		
Observation: A procedure exist to address unauthorized software and hardware.	Comment:		ACCEPTABLE
	Recommendation: Information Purposes Only		
Observation: The IACS inventory is not updated to reflect installations, removals, and updates.	Comment:		MODERATE
	Recommendation: Update inventory of complete IACS system and all components as an integral part of component installations, removals, and system updates. (800-53)		
Observation: A policy exist to ensure IACS device configurations can be restored to their last known operable state.	Comment:		ACCEPTABLE
	Recommendation: Information Purposes Only		

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

Asset Management		Section Rating:	LOW
Observation: A procedure does not exist to ensure modified device configuration files are updated and stored off-line.	Comment: Recommendation: Assessed component configurations and any approved deviations to current deployed configurations in the IACS be backed up or stored off-line in a secure location. (800-53)		MODERATE
Observation: A Bill of Materials (BOM) does not exist for parts used in critical infrastructure.	Comment: Recommendation: 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 outs, significant expediting charges and expensive downtime.		LOW
Observation: Accurate product lifecycle information does not exist for all IACS physical assets.	Comment: Recommendation: Product lifecycle information should be available and managed for all IACS assets.		MODERATE
Observation: Accurate product lifecycle information exists for all IACS critical infrastructure.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: An exchange service contract does not exist providing 24-hour turn around on replacement inventory for critical components.	Comment: Recommendation: A 24-hour turn around on replacement inventory for critical IACS components is advised, even if spares are available at the site.		MODERATE
Observation: A procedure exist for identifying discontinued physical assets.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: A procedure does not exist for migrating discontinued physical assets.	Comment: Recommendation: A procedure should be established for migrating discontinued physical assets. If asset discontinuation is monitored frequently, chances increase that a migration can be performed during a planned downtime.		MODERATE
Observation: A procedure exist for accurately documenting installed software.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: A procedure does not exist for accurately tracking software licenses.	Comment: Recommendation: A procedure should exist for accurately track software licenses to eliminate potential downtime resulting from software license complications.		MODERATE
Observation: A procedure exist for performing an internal software audit.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

6.2 Governance

IACS governance is foundation of a proper risk management strategy. The governance policies and response plans define how risks may be managed within the IACS and contributes to effective decision making regarding IACS assets.

Table 6:2 – Governance Observation Results

Governance		Section Rating:	HIGH
Observation: Security policies have been developed specific to the IACS.	Comment: asd		ACCEPTABLE
	Recommendation: Information Purposes Only		
Observation: Policies exist requiring the auditing of specific process on the IACS.	Comment:		ACCEPTABLE
	Recommendation: Information Purposes Only		
Observation: Audit logs are not tramper proof.	Comment:		HIGH
	Recommendation: Audit logs should be stored in a secure location to reduce the opportunity for intrusion. (800-82)		
Observation: Audit logs are not collaborated and reviewed.	Comment:		MODERATE
	Recommendation: Audit logs should be monitored and analyzed for intrusion attempts. (800-82)		
Observation: A policy does not exist requiring suppliers to be vetted prior to initiating contractual agreements.	Comment:		MODERATE
	Recommendation: Perform a due diligence review of suppliers prior to entering into contractual agreements to acquire IACS hardware, software, firmware, or services. (800-53)		
Observation: A policy does not exist requiring IACS products to be vetted prior to purchasing.	Comment:		MODERATE
	Recommendation: Perform a due diligence review of suppliers and their products prior to entering into contractual agreements to acquire IACS hardware, software, firmware. (800-53)		
Observation: A policy exist pertaining to the use of IACS re-manufactured or refurbished products.	Comment:		ACCEPTABLE
	Recommendation: Information Purposes Only		
Observation: A policy does not exist requiring the use of approved shipping vendors for the shipping and receiving of IACS network devices.	Comment:		LOW
	Recommendation: Use trusted shipping and warehousing for all IACS components. Trusted shipping and warehousing reduces opportunities for subversive activities or interception during transit. (800-53)		
Observation: The IACS network architecture employs a diverse set of suppliers for security appliances.	Comment:		ACCEPTABLE
	Recommendation: Information Purposes Only		
Observation: A policy exist stating the information security responsibilities for employees.	Comment:		ACCEPTABLE
	Recommendation: Information Purposes Only		
Observation: A policy exist stating the information security responsibilities for customers.	Comment:		ACCEPTABLE
	Recommendation: Information Purposes Only		
Observation: A policy exist stating the information security responsibilities for vendors.	Comment:		ACCEPTABLE
	Recommendation: Information Purposes Only		

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

Governance		Section Rating:	HIGH
Observation: A policy exist stating the information security responsibilities for contractors.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: A response plan does not exist stating the procedure if the IACS network communication is interrupted.	Comment: Recommendation: Include a full recovery and reconstitution of the IACS to a known state as part of contingency plan. (800-53)		HIGH
Observation: A response plan exists stating the procedure if there is a critical physical asset failure.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: A policy exists requiring IACS data to be backed up.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: Critical IACS backup data is not stored at a facility separate from the live environment.	Comment: Recommendation: 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 outlines explicit mitigation actions. (800-53)		HIGH
Observation: Backup media and data is not tested for reliability and integrity.	Comment: Recommendation: 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)		MODERATE

6.3 Risk Assessment & Management

Without having a good understanding of the risks present within the IACS network it may be challenging to properly define and implement effective security management policies and practices. Performing an IACS network risk assessment is a key step in establishing a comprehensive organizational security standard.

Table 6:3 – Risk Assessment & Management Observation Results

Risk Assessment & Management		Section Rating:	HIGH
Observation: A risk assessment has not been performed specific to the IACS network.	Comment: Recommendation: 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)		HIGH
Observation: A vulnerability assessment has been executed on the IACS environment.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: Scanning tools are used to identify vulnerabilities.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

Risk Assessment & Management		Section Rating:	HIGH
Observation: Procedures exist for vulnerability validation and mitigation.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: A procedure do not exist to evaluate the impact to assets as a result of a security compromise.	Comment: Recommendation: 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.		MODERATE
Observation: Vendor documentation does not exist regarding security controls and features employed in the IACS environment.	Comment: Recommendation: Obtain, protect as required, and make available to authorized personnel, vendor/manufacturer documentation that describes the functional properties of the security controls employed within the IACS with sufficient detail to permit analysis and testing. (800-53)		MODERATE
Observation: A policy exist requiring updates to software when updates are released by vendors.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: A procedure does not exist to test software in an isolated environment before being installed on the live IACS.	Comment: Recommendation: 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

6.4 Access Controls

An architecture that includes an industrial demilitarized zone (IDMZ) with firewalls is an important component in any IACS network as it provides the ability to manage traffic and prevent unwanted traffic from reaching the production network.

Table 6:4 – Access Controls Observation Results

Access Controls		Section Rating:	HIGH
Observation: Logical access is restricted to the IACS network.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: Unused ports and services on IACS devices are not disabled.	Comment: Recommendation: Disable unused ports and services on IACS devices after testing to assure this will not impact IACS operation. (800-82)		MODERATE

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

Access Controls		Section Rating:	HIGH
Observation: ICS user privileges are not restricted to only those that are required to perform each person's job.	Comment: Recommendation: Poorly specified access controls can result in giving an IACS user too many or too few privileges. The following exemplify each case: • System configured with default access control settings gives an operator administrative privileges • System improperly configured results in an operator being unable to take corrective actions in an emergency situation Access control policies should be developed as part of an IACS security program. (800-82)		MODERATE
Observation: Separate authentication mechanisms and credentials for users of the IACS network and the Enterprise network are in place and operational.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: It is unknown if IACS devices have been modified to ensure default configurations are not in place.	Comment: Recommendation: Using default configurations often leads to insecure and unnecessary open ports and exploitable network services running on hosts. Improperly configured firewall rules and router ACLs can allow unnecessary traffic. (800-82)		HIGH
Observation: Password policies exist defining when passwords must be used, how strong they must e, and how they must be maintained.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: A policy exist defining protection of attended and unattended workstations.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: ICS passwords are always required for system login.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: ICS passwords are always required for system power-on.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: It is unknown if IACS password authentication hampers and interferes with emergency actions for the IACS.	Comment: Recommendation: Passwords should be implemented on IACS components to prevent unauthorized access. Password authentication should not hamper or interfere with emergency actions for IACS. (800-82)		MODERATE
Observation: ICS passwords are not posted or observable in plain sight.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: Sharing of passwords is not permitted.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: Passwords are not changed every 30 days for systems that do not support strong password configurations.	Comment: Recommendation: 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

DRAFT or FINAL

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

Access Controls		Section Rating:	HIGH
Observation: Vendor default passwords are not in use on the IACS.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: ICS passwords are changed a minimum of every 120 days.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: Policy exists requiring the management of IACS network system accounts.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: A procedure does not exist for deleting temporary accounts after a pre-defined time period.	Comment: Recommendation: ICS 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)		HIGH
Observation: A procedure exists for identifying user accounts that have been inactive for a pre-defined time period.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: A procedure does not exist for removing inactive user accounts.	Comment: Recommendation: ICS 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)		HIGH
Observation: Account privileges are assigned in accordance with a role-based access scheme.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: Users are required to authenticate to the IACS network.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: User are uniquely identifiable.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: Multifactor authentication is not used.	Comment: Recommendation: ICS should use multifactor authentication for network access to IACS accounts. (800-53)		LOW
Observation: Authentication is not required for devices attempting to physically interface to the IACS network.	Comment: Recommendation: ICS uniquely identifies and authenticates IACS devices before establishing a connection. This should be evaluated against process requirements. (800-53)		MODERATE
Observation: A policy exists governing the use of wireless access points on the IACS network.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: Device configurations enforce the use of authentication and encryption for users of wireless networks.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

Access Controls		Section Rating:	HIGH
Observation: Wireless communications are not limited to a designated physical boundary.	Comment: Recommendation: Confine wireless communications to the IACS boundaries. Actions that may be taken to confine wireless communications to IACS boundaries including reducing the power of the wireless transmission such that it cannot transit the physical perimeter, employ measures such as TEMPEST to control wireless emanations, and configuring the wireless access such that it is point to point in nature. (800-53) Prior to installation, a wireless survey should be performed to determine antenna location and strength to minimize exposure of the wireless network. The survey should take into account the fact that attackers can use powerful directional antennas, which extend the effective range of a wireless LAN beyond the expected standard range. Faraday cages and other methods are also available to minimize exposure of the wireless network outside of the designated areas. (800-82)		HIGH
Observation: Wireless communications are restricted logically to a specified demarcation device.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: Default authentication credentials are not used to access devices on the IACS network.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: It is unknown if devices are configured to ensure authentication information is encrypted in configuration scripts and memory locations.	Comment: Recommendation: Ensure that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys. (800-53)		MODERATE
Observation: Remote access is used to gain access to the IACS network.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: Remote access sessions are monitored.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: Encryption methods are used to protect data in motion during remote access sessions.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: Policy exists preventing the disclosure of remote access credentials.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: Multi-factor authentication is not required to initiate a remote access session.	Comment: Recommendation: Remote access capabilities that enable control engineers and vendors to gain remote access to systems should be deployed with multifactor security controls to prevent unauthorized individuals from gaining access to the IACS. (800-82)		HIGH
Observation: Explicit security configurations do not ensure IACS data is controlled according to data type, source, and destination.	Comment: Recommendation: ICS should enforce information flow control using explicit security attributes on data type, source, and destination objects as a basis for flow control decisions. (800-53)		MODERATE
Observation: Information flow control is not enforced using hardware mechanisms.	Comment: Recommendation: ICS should dictate data flow by using but not limited to, hardware mechanisms. (800-53)		MODERATE
Observation: Information flow control is enforced using security policy filters.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE

DRAFT or FINAL

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

Access Controls		Section Rating:	HIGH
Observation: Information flow control is enforced through human review.	Comment: Recommendation: ICS should enforce the use of human review for security policy filters when the system is not capable of making an information flow control decision. (800-53)		ACCEPTABLE
Observation: Host-based boundary protection configurations do not exist on IACS servers.	Comment: Recommendation: ICS servers should prevent remote devices that have established a non-remote connection with the system from communicating outside of that communications path with resources in external networks. (800-53)		MODERATE
Observation: Host-based boundary protection configurations do not exist on IACS workstations.	Comment: Recommendation: ICS workstations should prevent remote devices that have established a non-remote connection with the system from communicating outside of that communications path with resources in external networks. (800-53)		MODERATE
Observation: Host-based boundary protection configurations do not exist on IACS mobile devices.	Comment: Recommendation: ICS mobile devices should prevent remote devices that have established a non-remote connection with the system from communicating outside of that communications path with resources in external networks. (800-53)		MODERATE
Observation: A policy exists requiring boundary protection devices to fail securely in the event of a failure.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: A specification does not exist defining fail-secure constructs for boundary protection devices.	Comment: Recommendation: In the event of a failure of a boundary protection device, a fail secure would reduce the risk of a security vulnerability during the failure. A specification should be developed regarding fail secure configurations and should take into consideration communication requirements for the IACS.		MODERATE
Observation: Boundary protection devices are configured to fail securely.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: A policy exists requiring the IACS environment to be scanned for unauthorized network devices, including wireless access points.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: Wireless networking capabilities are disabled on devices where wireless capabilities are not permitted.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: Internet browsing capabilities are disabled on devices where Internet browsing is not permitted.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

6.5 Awareness & Training

Training materials for the IACS should be developed in order to ensure that proper procedures are being followed for all activities that may impact the production system or worker safety. Failure to properly understand or follow procedures may result in accidental interruption to production, unintended exposure of the production network to a malicious actor, or in extreme cases, physical harm to employees.

Table 6:5 – Awareness & Training Observation Results

Awareness & Training		Section Rating:	MODERATE
Observation: Training and educational materials have not been developed specific to the IACS.	Comment: Recommendation: The organization should develop basic training and education materials specific to the IACS. Subjects should include but are not limited to, security and safety. (800-53)		MODERATE
Observation: Computer security awareness training is provided for all employees.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: Computer security awareness training is provided as part of the on-boarding process for new employees.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: A computer security awareness training refresher is provided annually.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: Computer security awareness training is not provided to 3rd party contractors before accessing the IACS.	Comment: Recommendation: The organization should provide basic security awareness training to all IACS users including 3rd party contractors before accessing the IACS. (800-53)		MODERATE
Observation: Physical security and safety training is provided for all employees.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: Physical security and safety training is provided as part of the on-boarding process for new employees.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: A physical security and safety training refresher is provided annually.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: Physical security and safety training is provided to 3rd party contractors before accessing the IACS.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE

DRAFT or FINAL

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

6.6 Data Security

Data security within the IACS employs encryption or other means to secure data in transit as well as data at rest within the IACS.

There was no logically separated testing/development environment noted at the Widget Springs Foundry site. Since many IACS processes are continuous in nature, unexpected outages of systems in the IACS is unacceptable. Pre-deployment testing and validation of planned changes is essential to ensure high availability of the production systems.

Table 6:6 – Data Security Observation Results

Data Security		Section Rating:	HIGH
Observation: Encryption and/or cryptographic hashes are used to protect IACS data in transit.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: Encryption and/or cryptographic hashes are used to protect IACS data at rest.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: A testing environment does not exist to facilitate secure testing and impact assessment of changes prior to implementation on the live IACS.	Comment: Recommendation: 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
Observation: A policy does not exist to restrict the use of portable media.	Comment: Recommendation: Policy should be developed restricting the use of portable media devices on the IACS. Enforcement should take into consideration that it may not be feasible to physically monitor them. (800-82)		HIGH
Observation: All external physical system interfaces to the IACS are documented.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: All external physical system interfaces to the IACS are regularly scanned for vulnerabilities.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: All external physical system interfaces to the IACS are secure by encryption.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: Anti-virus detection software is present in the IACS environment.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: Virus signatures are not deployed to the IACS environment a minimum of every 30 days.	Comment: Recommendation: Antivirus tools only function effectively when installed, configured, running full-time, and maintained properly against the state of known attack methods and payloads. (800-82)		HIGH
Observation: A policy exists prohibiting the use of personally owned portable storage media on the IACS network.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE

DRAFT or FINAL

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

Data Security		Section Rating:	HIGH
Observation: Portable media devices are not encrypted.	Comment: Recommendation: 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)		HIGH
Observation: A policy does not exist requiring secure sanitization and disposal of hardware.	Comment: Recommendation: A policy should be developed for tracking, documenting, and verifying media sanitization and disposal actions. (800-53)		MODERATE
Observation: A change control / configuration management procedure exists for the IACS.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: A change control / configuration management procedure does not exist for ensuring backups of software, firmware, and configurations representing the as-is environment are available prior to initiating changes within the IACS.	Comment: Recommendation: A Change Control / Configuration Management 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)		HIGH
Observation: A change control / configuration management procedure exists to document changes to the IACS.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: A change control / configuration management procedure exists to test and validate proposed changes to the IACS.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: A change control / configuration management procedure does not exist to audit changes to the IACS.	Comment: Recommendation: The Change Control / Configuration Management procedure should include auditing of IACS changes and indications of changes to determine whether unauthorized changes have occurred. Automated mechanisms may be used to enforce access restrictions and support auditing of the enforcement actions. (800-53)		HIGH
Observation: A change control / configuration management procedure does not exist to detect unauthorized changes to the IACS.	Comment: Recommendation: The Change Control / Configuration Management procedure should incorporate detection of unauthorized, security-relevant configuration changes into the organization's incident response capability to ensure that such detected events are tracked, monitored, corrected, and available for historical purposes. (800-53)		HIGH
Observation: A policy exists prohibiting unauthorized software use.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: Games are not allowed on IACS equipment.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: Peer-to-Peer chat is not allowed on IACS equipment.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: The internet is not accessible on IACS equipment.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: Streaming video is not allowed on IACS equipment.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE

DRAFT or FINAL

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

Data Security	Section Rating:	HIGH
Observation: Unauthorized executable downloads are not allowed on IACS equipment.	Comment: Recommendation: Information Purposes Only	ACCEPTABLE

6.7 Maintenance

There is currently no policy which requires diagnostic tools capable of running test programs to be tested for malicious code prior to use in the IACS. Diagnostic tools that are capable of communicating on IACS networks and/or storing and executing program code, have the potential to carry malicious code undetected through physical security boundaries and should be tested and/or properly updated with appropriate security patches prior to allowing them to be used in the IACS.

Table 6:7 – Maintenance Observation Results

Maintenance	Section Rating:	MODERATE
Observation: A procedure exists for collecting maintenance records for the IACS.	Comment: Recommendation: Information Purposes Only	ACCEPTABLE
Observation: Maintenance records include date and time of maintenance.	Comment: Recommendation: Information Purposes Only	ACCEPTABLE
Observation: Maintenance records identify the individual performing the maintenance.	Comment: Recommendation: Information Purposes Only	ACCEPTABLE
Observation: Maintenance records do not identify the employee escort.	Comment: Recommendation: Maintenance records should include the name of the escort if applicable. (800-53)	MODERATE
Observation: Maintenance tools are restricted to authorized personnel only.	Comment: Recommendation: Information Purposes Only	ACCEPTABLE
Observation: A policy does not exist requiring diagnostic tools to be tested for malicious code before they are allowed on the IACS network.	Comment: Recommendation: All media containing diagnostic and test programs should be checked for malicious code before the media is used in the IACS. (800-53)	MODERATE
Observation: Remote sessions for maintenance are employed on the IACS.	Comment: Recommendation: Remote maintenance sessions should be monitored and audited to ensure the IACS has not been compromised during a remote session. (800-53)	MODERATE
Observation: Remote sessions for maintenance are not audited.	Comment: Recommendation: Remote maintenance sessions should be monitored and audited to ensure the IACS has not been compromised during a remote session. Information available for the audit should include but is not limited to the name and credentials of the remote maintenance personnel, time, date, action being performed, system being performed on, and the outcome. (800-53)	MODERATE

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

6.8 Incident Detection

Incident detection plays an important role in any holistic cyber security program. Network-based and host-based sensors allow malicious activity to be detected and contained faster and with less impact to production systems. Host-based intrusion detection sensors are not currently in use but should be implemented as they play a vital role and act as the first line of defense in a system-wide intrusion detection system.

Table 6:8 – Incident Detection Observation Results

Incident Detection		Section Rating:	MODERATE
Observation: Network-based intrusion detection sensors are implemented on the IACS network.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: Host-based intrusion detection sensors are not implemented on the IACS network.	Comment: Recommendation: A host-based intrusion detection tool should be implemented as the line of defense into a system wide intrusion detection system. (800-53)		MODERATE
Observation: Policy requires security incidents to be documented.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE

6.9 Physical Security & Safety

Table 6:9 – Physical Security & Safety Observation Results

Physical Security & Safety		Section Rating:	MODERATE
Observation: Employee access is auditable.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: Visitor access is auditable.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: All facility ingress and egress demarcations are monitored (24x7/365).	Comment: Recommendation: Information Purposes Only		ACCEPTABLE
Observation: The entire facility perimeter is not secured by fencing or equivalent.	Comment: Recommendation: Classic physical security considerations typically refer to a ringed architecture of layered security measures. Creating several physical barriers, both active and passive, around buildings, facilities, rooms, equipment, or other informational assets, establishes these physical security perimeters. Physical security controls meant to protect physical locations include fences, anti-vehicle ditches, earthen mounds, walls, reinforced barricades, gates, or other measures. Most organizations include this layered model by preventing access to the plant first by the use of fences, guard shacks, gates, and locked doors. (800-82)		MODERATE
Observation: The locations within the production area(s) where IACS and devices operate are protected by access control mechanisms.	Comment: Recommendation: Information Purposes Only		ACCEPTABLE

DRAFT or FINAL

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

Physical Security & Safety		Section Rating:	MODERATE
Observation: Policy exists prohibiting tailgating via badge access.	Comment:		ACCEPTABLE
	Recommendation: Information Purposes Only		
Observation: Signage complies with OSHA regulations.	Comment:		ACCEPTABLE
	Recommendation: Information Purposes Only		
Observation: PPE requirements are specified prior to production building ingress.	Comment:		ACCEPTABLE
	Recommendation: Information Purposes Only		
Observation: Signs managing vehicle traffic flow are present at all on-site roadway intersections.	Comment:		ACCEPTABLE
	Recommendation: Information Purposes Only		
Observation: Signs managing vehicle traffic flow are present at all on-site railroad crossings.	Comment:		ACCEPTABLE
	Recommendation: Information Purposes Only		
Observation: The site Emergency Action Plan complies with OSHA regulation.	Comment:		ACCEPTABLE
	Recommendation: Information Purposes Only		
Observation: Hazardous materials are not stored on site.	Comment:		ACCEPTABLE
	Recommendation: Chemical manufacturers or importers are required to classify the hazards of chemicals which they produce or import, and all employers to provide information to their employees about the hazardous chemicals to which they are exposed, by means of a hazard communication program, labels and other forms of warning, safety data sheets, and information and training. In addition, this section requires distributors to transmit the required information to employers. (OSHA Standards 29 CFR 1910.1200(b)(1))		
Observation: Material Safety Data Sheets (MSDS) or Workplace Hazardous Materials Information Systems (WHMIS) are maintained as required by OSHA or Health Canada.	Comment:		ACCEPTABLE
	Recommendation: Information Purposes Only		
Observation: Policy exists prohibiting weapons on site property.	Comment:		ACCEPTABLE
	Recommendation: Information Purposes Only		

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

7 REFERENCE INFORMATION

7.1 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 breaks down and determines plant-wide information flow. 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.

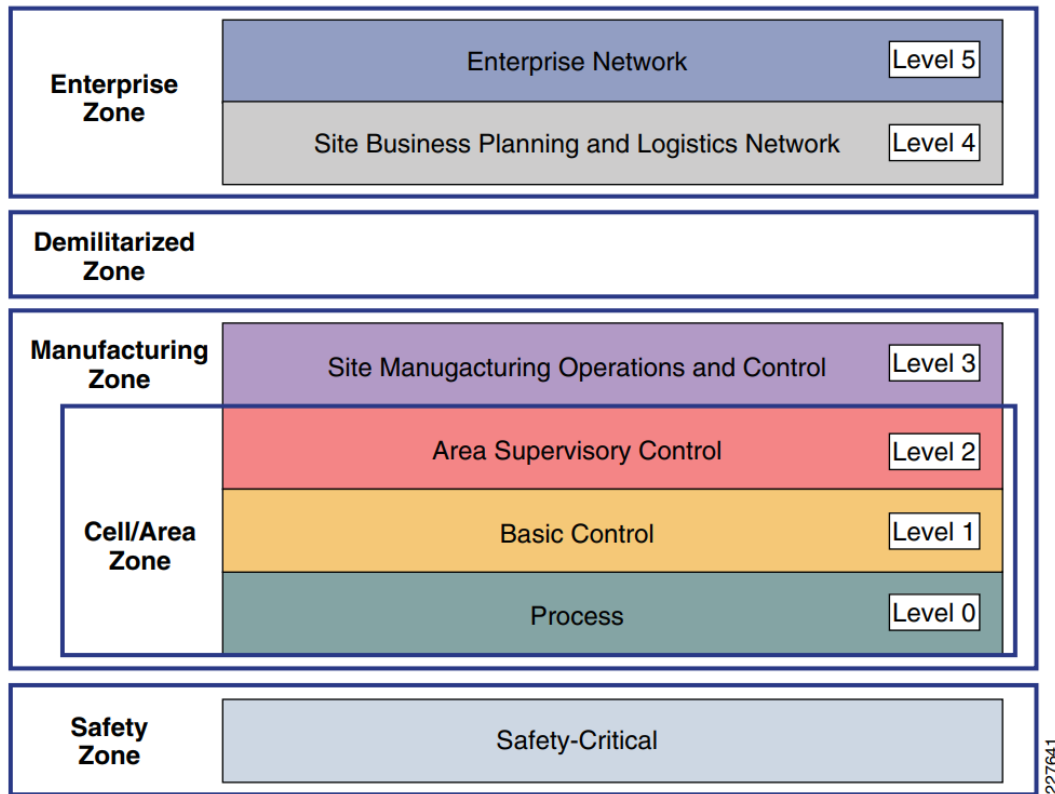


Figure 7:1 – Logical Framework for IT and IACS Convergence

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.

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

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 provides 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 meets 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, Rockwell Automation has partnered with Cisco, Panduit, and other industry leaders to produce a series of white papers and design guides that outline the design, deployment, and integration of various components within a Connected Enterprise. These documents are all available from Rockwell Automation's website and can be accessed by using the following links:

Design Guides:

https://www.rockwellautomation.com/en_NA/capabilities/industrial-networks/technical-data/overview.page?

Network Whitepapers:

https://www.rockwellautomation.com/en_NA/capabilities/industrial-networks/whitepapers/overview.page?

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

7.2 Reference Documents

Table 7:1 – Reference Documents

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-09	-	Guidance for Selecting Cables for Ethernet/IP Networks	Rockwell Automation
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

7.3 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 7:2 – Physical Topology Types

Type	Advantages	Disadvantages	CPwE Reference Guide
Redundant Star	<ul style="list-style-type: none"> Resiliency from multiple connection failures Faster Convergence to connection loss Consistent number of hops (typically two in flat design) provides predictable and consistent performance and real-time Fewer bottlenecks in the design reduces changes of segment over-subscription 	<ul style="list-style-type: none"> Additional wiring (and relevant costs) required to connect layer 2 access switches directly to a layer 3 distribution switch Additional configuration complexity 	<ul style="list-style-type: none"> Deploying a Resilient CPwE Architecture ENET-TD010¹ Deploying Parallel Redundancy Protocol ENET-TD021²
Ring	<ul style="list-style-type: none"> Resiliency from loss of one network connection Less cabling complexity in certain plant floor layouts Multiple paths reduce potential for over-subscription and bottlenecks 	<ul style="list-style-type: none"> Additional configuration complexity Longer convergence times 	<ul style="list-style-type: none"> Deploying Resilient Ethernet Protocol ENET-TD005³ Deploying Device Level Ring (DLR) ENET-TD015⁴

¹ https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td010_-en-p.pdf

² https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td021_-en-p.pdf

³ https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td005_-en-p.pdf

⁴ https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td015_-en-p.pdf

DRAFT or FINAL

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

- Variable number of hops makes designing predictable performance more complex

Linear

- Easy to design, configure, and implement
- Least amount of cabling (and associated cost)
- Loss of network service in case of connection failure (no resiliency)
- Creates bottlenecks on the links closest to layer 3 device, and varying number of hops make it more difficult to produce reliable performance

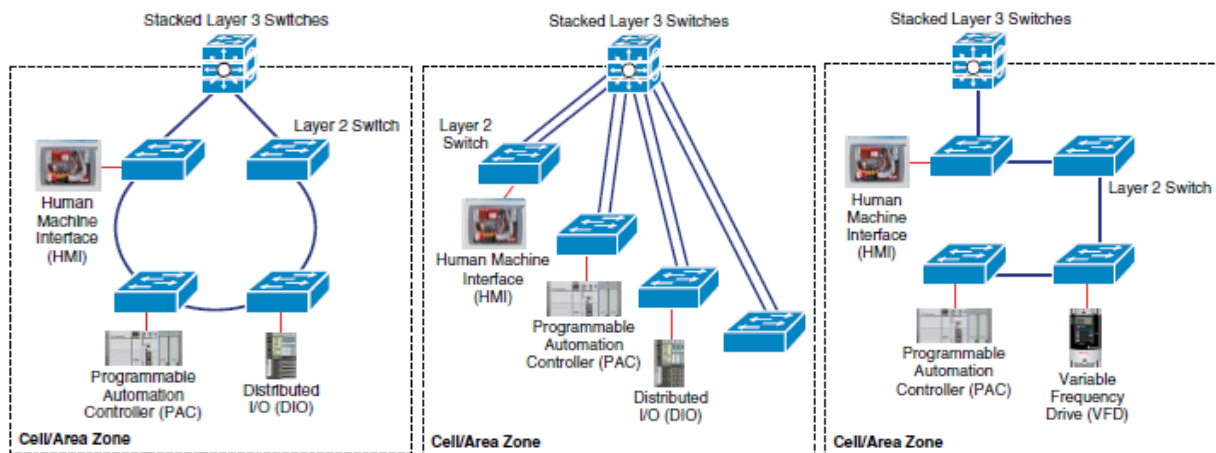


Figure 7:2 – Physical Topologies Drawings

DRAFT or FINAL

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

7.4 Switch Selection Additional Information

Recommendations on switch selection minimum requirements are as follows:

- All switches should be managed. No unmanaged switches or hubs should be authorized on the 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 mount 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 (OSFP, 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

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

7.5 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 based on 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. 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 on 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 7:3 – Routing Protocol Comparison

Type	Advantages	Dis-Advantages	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

7.6 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 7:4 – 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


DRAFT or FINAL

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

7.7 Environmental Conditions Additional Information

MICE is a method of categorizing the environment that supports three levels called classifications: M1I1C1E1, M2I2C2E2, and M3I3C3E3. The three classifications can be 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 as shown below.



	M ₁	M ₂	M ₃
Mechanical	M ₁	M ₂	M ₃
Ingress	I ₁	I ₂	I ₃
Climatic	C ₁	C ₂	C ₃
Electromagnetic	E ₁	E ₂	E ₃
	Commercial	Light Industrial	Industrial

Figure 7:3 – 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.

7.8 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 IP56 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.

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

7.9 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. See the CPwE design guide [ENET-TD003⁵](#) for additional information about deploying fiber optic physical infrastructure.

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).

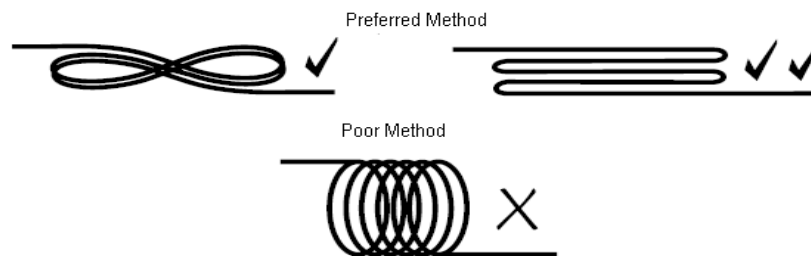


Figure 7:4 – Handling Excess Copper Cabling

7.10 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. The following table lists the generally accepted practices for network cable management.

⁵ https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td003_-en-p.pdf

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

7.11 Conduit & 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 wireway 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 40% 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 7:5 – External Enclosure-to-Enclosure Routing Requirements

Cable in contiguous metal wireway or conduit?	Route Cable at this Minimum Distance	From Noise Source of this Strength
YES	0.08m (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 7:6 – 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

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

7.12 Cable Labeling Additional Information

The identifying text on all labels should follow TIA-606 standards. For clarity, there is usually a breakdown from the enclosure/rack, rack unit (RU), port, etc. that is consistent throughout the facility. For example, CP1.PP1.02 could signify control panel 1, patch panel 1, and port 2 and can identify VLANs, manufacturing process, location, network traffic type, etc. Color coding can identify VLANs, manufacturing process, location, network traffic type, etc. Color coding can be achieved with labels, hook & loop cable ties, and color bands when cables themselves are colored for other reasons (e.g. Fiber cable colors indicate cable type).

The following figure from the TIA-606-C standard shows an example of typical telecommunications infrastructure elements that require labeling.

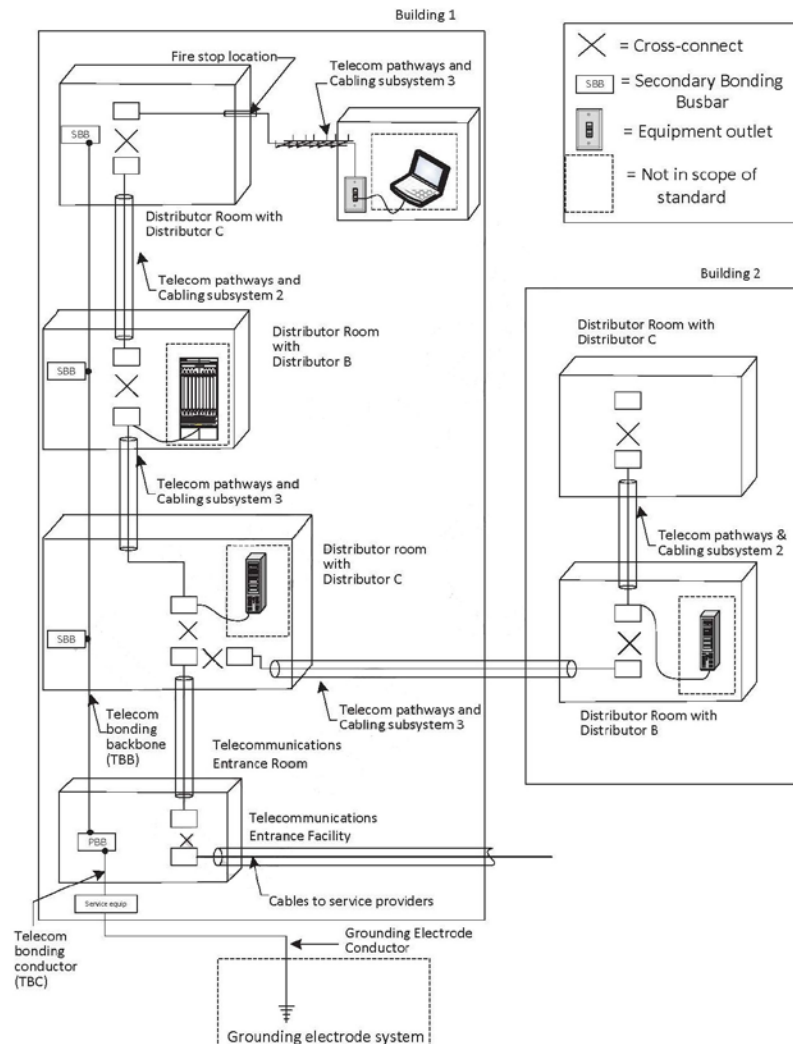


Figure 7:5 – A representative model of typical telecommunication infrastructure elements for administration

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

7.13 Power Redundancy Additional Information

Power supply failures are the second leading cause for switch failure. All switches utilized in the Process Control network are 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 are 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 are 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.

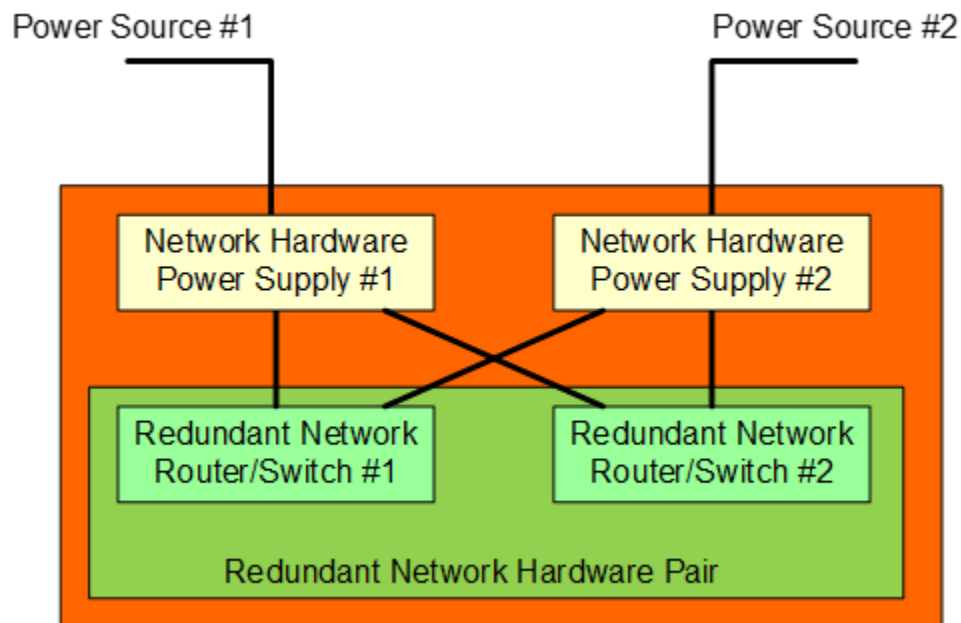


Figure 7:6 – Redundant Power Source

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

7.14 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 NEC. 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.

7.15 Topology Additional Information

The following information is from the Converged Plantwide Ethernet (CPwE) Design and Implementation Guide ([ENET-TD001](#)⁶) 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 redundancy star topology offers the best convergence capabilities, consider alternative ring recovery techniques when configured in a 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 outlines above are used in combination to create a network with high availability.

Table 7:7 – Network Availability Requirements

Network Availability	Downtime per Year	Downtime per Week
----------------------	-------------------	-------------------

⁶ https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td001_-en-p.pdf

DRAFT or FINAL

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

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

7.16 Security Zone Additional Information

An Industrial Demilitarized Zone (IDMZ) and firewalls are an essential aspect of protecting an IACS network and its applications. The combination of firewalls and an IDMZ 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 an IDMZ
 - 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 IDMZ services
 - Intrusion Protection Services (IPS) inspecting traffic between the zones designed to identify and potentially stop a variety of attacks
- Deploy an IDMZ where data and services between the zones can be securely shared. Like a traditional IT Demilitarized Zone (DMZ) the OT-oriented IDMZ provides a managed separation layer between the Enterprise network and IACS where broker services reside to forward traffic between networks.

The firewall and IDMZ concept also play an important role in allowing remote access to the IACS network. See the CPwE design guide [ENET-TD019](#)⁷ for additional information about deploying network security and [ENET-TD002](#)⁸ for additional information about deploying firewalls.

7.17 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 plantwide 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

⁷ https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td019_-en-p.pdf

⁸ https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td002_-en-p.pdf

DRAFT or FINAL

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

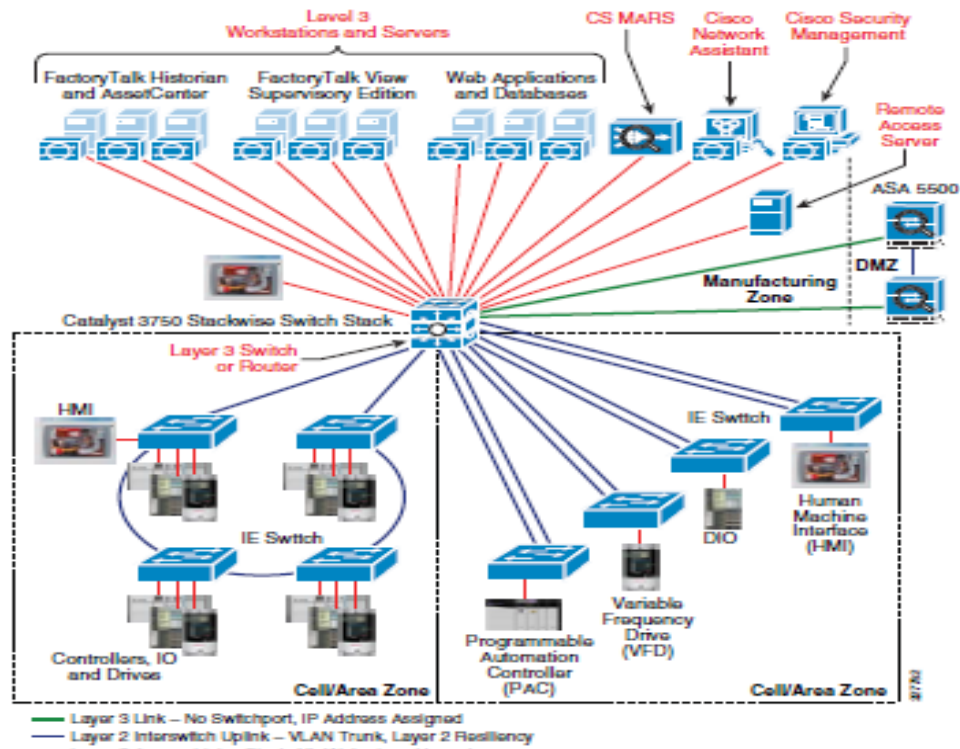


Figure 7:7 – Example of Manufacturing Zone

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

7.18 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. Deploying technologies such as Network-Address-Translation (NAT) can help simplify management of cell/area zone networks for plant floor personnel while maintaining scalability and compliance with IACS network policies. See the CPwE design guide [ENET-TD007](#)⁹ for additional information about deploying NAT inside cell/area zones.
- *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 later do they determine that the cheaper, unmanaged infrastructure cannot scale, perform, integrate, or be as easily maintained as an intelligent, managed network.

⁹ https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td007_-en-p.pdf

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

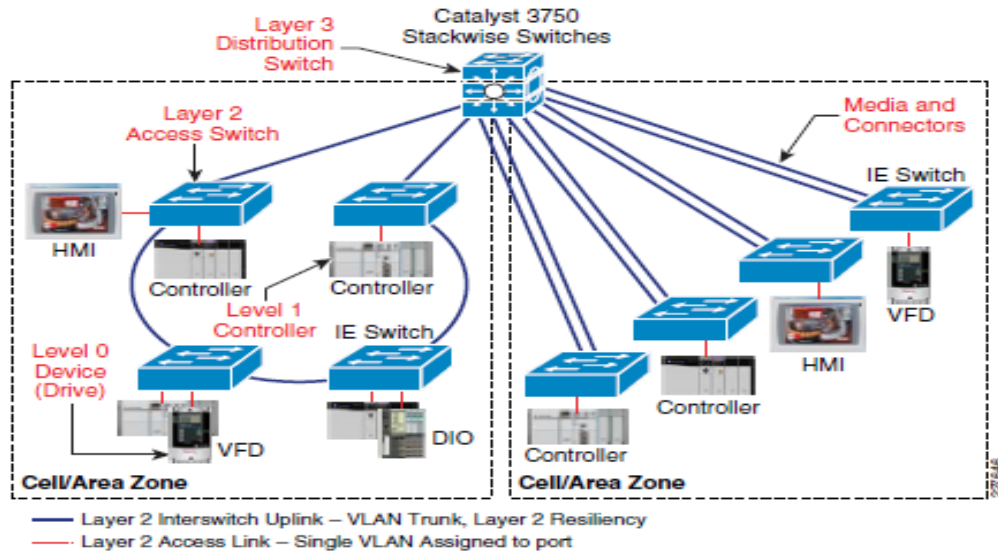


Figure 7:8 – Example of Cell/Area Zone

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

8 ABBREVIATIONS & STANDARDS

8.1 Commonly Accepted Industrial 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 Electrotechnical 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	ODVA, Inc. (Formerly Open DeviceNet Vendors Association, Inc)
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

DRAFT or FINAL

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

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

8.2 Additional References

8.2.1 Recommended References for Policy Generation

- ISO 17799 (properly interpreted and revised for a control environment)
- NIST SP-800 Documents (freely available)
- NIST PCSRF activities (contact NIST PCSRF for more information)
- Internal IT policies and standards
- Internal corporate information management policies
- ODVA EtherNet/IP Specification
- PUB00035R0, ODVA Network Infrastructure for EtherNet/IP: Introduction and Considerations
- PUB00148R0, ODVA EtherNet/IP Media Planning and Installation Manual
- 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

8.2.2 ISA

- ISA SP-99 TR99.00.01 (Technical Report 1)
- ISA SP-99 TR99.00.02 (Technical Report 2)
- ISA SP-99 d99.00.01 (Models, Definitions, and Terminologies)
- ISA SP-99 d99.00.02 (Security Program Considerations)
- 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
- ISA-95.02, Object Model Attributes
- ISA-95.03, Activity Models
- ISA-95.04, Object Models & Attributes
- ISA-95.05, B2M Transactions
- ANSI/TIA 1005, Cabling Telecommunications Standards for Industrial Premises
- ANSI/TIA-606-C, Administration Standard for Telecommunications Infrastructure
- ANSI/TIA-568-C.n, Commercial Copper and Fiber Cabling
- ISA-TR99.00.01-2007, Security Technologies for Industrial Automation and Control Systems
- ISA-TR99.00.02-2007, Integrating Electronic Security into Manufacturing and Control ISA SP-99 Security, in draft form

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

8.2.3 *Governmental*

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

8.2.4 *NIST*

- NIST SP 800-12 The NIST Handbook
- NIST SP 800-14 Generally Accepted Principles and Practices for Securing Information Technology Systems
- NIST SP 800-18 Guide for Developing Security Plans for Information Technology Systems
- NIST SP 800-26 Security Self-Assessment Guide for Information Technology Systems
- NIST SP 800-27 Rev A Engineering Principles for Information Technology Security (Baseline for Achieving Security)
- NIST SP 800-30 Rev A Risk Management Guide for Information Technology Systems
- NIST SP 800-37 Guide for the Security Certification and Accreditation of Federal Information Systems
- NIST SP 800-53 Recommended Security Controls for Federal Information Systems
- NIST SP 800-55 Security Metrics Guide for Information Technology Systems
- NIST SP 800-60 Guide for Mapping Types of Information and Information Systems to Security Categories
- NIST SP 800-65 Integrating IT Security into Capital Planning and Investment Control Process
- NIST SP 800-70 Security Configuration Checklists Program for IT Products
- NIST SP 800-72 Guidelines on PDA Forensics
- NIST SP 800-82 Guide to Industrial Control Systems (ICS) Security
- FIPS 199 Standards for Security Categorization of Federal Information and Information Systems

Spacely Sprockets – Orbit City

STANDARD NETWORK ASSESSMENT

8.2.5 *The Institute Of Electrical And Electronics Engineers*

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