Mining Architecture Guide
Important User Information

Read this document and the documents listed in the additional resources section about installation, configuration, and operation of this equipment before you install, configure, operate, or maintain this product. Users are required to familiarize themselves with installation and wiring instructions in addition to requirements of all applicable codes, laws, and standards.

Activities including installation, adjustments, putting into service, use, assembly, disassembly, and maintenance are required to be carried out by suitably trained personnel in accordance with applicable code of practice.

If this equipment is used in a manner not specified by the manufacturer, the protection provided by the equipment may be impaired.

In no event will Rockwell Automation, Inc. be responsible or liable for indirect or consequential damages resulting from the use or application of this equipment.

The examples and diagrams in this manual are included solely for illustrative purposes. Because of the many variables and requirements associated with any particular installation, Rockwell Automation, Inc. cannot assume responsibility or liability for actual use based on the examples and diagrams.

No patent liability is assumed by Rockwell Automation, Inc. with respect to use of information, circuits, equipment, or software described in this manual.

Reproduction of the contents of this manual, in whole or in part, without written permission of Rockwell Automation, Inc., is prohibited.

Throughout this manual, when necessary, we use notes to make you aware of safety considerations.

---

**WARNING**: Identifies information about practices or circumstances that can cause an explosion in a hazardous environment, which may lead to personal injury or death, property damage, or economic loss.

**ATTENTION**: Identifies information about practices or circumstances that can lead to personal injury or death, property damage, or economic loss. Attentions help you identify a hazard, avoid a hazard, and recognize the consequence.

**IMPORTANT** Identifies information that is critical for successful application and understanding of the product.

Labels may also be on or inside the equipment to provide specific precautions.

**SHOCK HAZARD**: Labels may be on or inside the equipment, for example, a drive or motor, to alert people that dangerous voltage may be present.

**BURN HAZARD**: Labels may be on or inside the equipment, for example, a drive or motor, to alert people that surfaces may reach dangerous temperatures.

**ARC FLASH HAZARD**: Labels may be on or inside the equipment, for example, a motor control center, to alert people to potential Arc Flash. Arc Flash will cause severe injury or death. Wear proper Personal Protective Equipment (PPE). Follow ALL Regulatory requirements for safe work practices and for Personal Protective Equipment (PPE).
# Table of Contents

## Preface
- Additional Resources .................................................. 7

## Chapter 1
- Overview for the Mining Smart Industry Architecture
  - Introduction ............................................................. 9
  - Documented Assumptions ........................................... 10
    - Standards of Design .............................................. 10
    - Intended Testing Target ......................................... 10
  - Application Selection ............................................... 11
    - Functional Overview Surface Mining .......................... 11
    - Table of Assets .................................................. 14
  - Testing ......................................................................... 15
    - Tests performed .................................................... 15

## Chapter 2
- Design Considerations for the Mining Smart Industry Architecture
  - Overview ................................................................. 17
  - Reference Architecture ............................................. 17
    - Industrial IoT Network Technology ............................ 20
    - Network Zoning ..................................................... 21
  - Network Resiliency .................................................. 24
    - Ring Topologies ..................................................... 25
    - Redundant Star Topology Technologies ........................ 26
    - Parallel Redundancy Protocol .................................... 27
  - Time Synchronization ............................................... 28
  - Selection of IES and Smart IIoT Devices ....................... 30
    - Convergence-Ready OEM Applications .......................... 31
  - Instrumentation ........................................................ 32
    - Asset Management .................................................. 33
    - Field Network Infrastructure ..................................... 33
  - PlantPAx System Considerations .................................. 34
  - Level 3 Sitewide considerations .................................. 34
    - Physical Infrastructure Deployment .............................. 34
    - Industrial Network Building Block Systems .................... 37
  - Cellular Considerations and Designs ............................. 41
  - Cybersecurity .......................................................... 42
    - OT Persona - Holistic and Diverse Site-wide Cybersecurity . 46
    - Industrial IT Persona - Holistic and Diverse Site-wide Security 47
    - IT Persona - Holistic and Diverse Site-wide Cybersecurity .... 48

## Chapter 3
- Configuration Considerations for the Mining Smart Industry Architecture
  - End Device Configuration Considerations ....................... 49
    - Network Switches ................................................... 49
    - Programmable Automation Controller .......................... 50
    - E300 Electronic Overload Relays .................................. 50
Table of Contents

PowerFlex 755T Variable Frequency Drives .......................... 50
Process Instrumentation and Linking Devices ..................... 50
Flex 5000 I/O ................................................................. 51
Integrated Display Thin Client ............................................. 51
Premier Integration ......................................................... 51
Automatic Device Configuration (ADC) .............................. 52
Controller Level Configuration Considerations ..................... 52
Controller Characterization ............................................... 53
Process Control Response Time ......................................... 54
Specifying Devices to be Controlled per Controller ............... 60
States of Operation, Command Sources, and Areas of Control 61
Additional Tips .............................................................. 65
HMI Configuration Considerations ..................................... 67
Application and Infrastructure .......................................... 68
Designing the HMI ........................................................ 74
Security Configuration Considerations ............................... 75
What to Integrate into DCS ............................................. 76
Project Layout .............................................................. 76
Historian Configuration Considerations ............................. 79
Overview ................................................................. 79
FactoryTalk Historian Components .................................. 79
Configurations .............................................................. 79
FactoryTalk LiveData Interface ........................................ 81
Failover ................................................................. 82
Other Interfaces ........................................................ 82
Derived Tags .............................................................. 83
Advanced Server Components ......................................... 84
Configuration Considerations ......................................... 84
Disaster Recovery ......................................................... 85
Process Device Items ..................................................... 86
Maintaining Proper Revision Control ................................. 87

Chapter 4

Test Bed Configuration and Test Results
Test Bed Configuration ..................................................... 89
Overview ................................................................. 89
Zone Setup ............................................................. 91
Scaling the Test Bed .................................................... 93
HMI Application ........................................................ 99
Traffic Flows ............................................................ 101
Test Results ............................................................. 102
Results Summary ....................................................... 102
Performance Metrics Definition .................................... 103

Chapter 5

Mining Smart Industry Architecture Specific Use Cases
Conveyance ............................................................. 105
What is Conveyance ..................................................... 105
Major Challenges .................................................. 105
Maintenance .......................................................... 106
Rockwell Automation Benefits in Conveyance ............. 107
Popular Configuration Drawing - Conveyance ............. 107
Compression ............................................................ 108
  Compressors and Compressed Air Systems ............... 108
  Major Challenges ................................................ 109
  Rockwell Automation Benefits in Compressors .......... 109
  Popular Configuration Drawing - Compressor Systems .. 110
Flotation ................................................................. 110
  What is Flotation? ............................................... 110
  Major Challenges ................................................ 110
  Rockwell Automation Benefits in Flotation .............. 111
Stacker Reclaimers .................................................. 111
  What is a stacker-reclaimer? .................................. 111
  Major Challenges ................................................ 111
  Rockwell Automation Benefits for Stacker-Reclaimers ... 111
  Popular Configuration Drawing - Stacker-Reclaimer ..... 112
Pumping ................................................................. 112
  What is a pump system? ........................................ 112
  Major Challenges ................................................ 112
  Rockwell Automation Benefits for pump systems ....... 113
  Popular Configuration Drawing pump systems .......... 113

Appendix A
Hardware / Software Used in Testing
  Hardware .................................................................. 115
  Software .................................................................. 117

Appendix B
References
  Converged Plantwide Ethernet (CPwE) Reference Architectures. 119
  ODVA References .................................................. 120
  Rockwell Automation References .......................... 120
  Cisco References .................................................. 121
  Panduit References ............................................... 122
  Endress+Hauser References ................................. 122
These documents contain additional information concerning related products from Rockwell Automation.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Industrial Automation Wiring and Grounding Guidelines, publication 1770-4.1</td>
<td>Provides general guidelines for installing a Rockwell Automation industrial system.</td>
</tr>
</tbody>
</table>


To order paper copies of technical documentation, contact your local Allen-Bradley distributor or Rockwell Automation sales representative.

A list of resources, including links from our partners, is located in Appendix B.
Notes:
Chapter 1

Overview for the Mining Smart Industry Architecture

Introduction

Coordination of large industrial automation and control systems (IACS), like process automation systems (PAS) and supervisory control and data acquisition (SCADA) systems, requires robust networks that connect thousands of distributed IACS devices. Modern site-wide mining requirements are increasing the demands on network infrastructure. The expectation is that networks can handle network and security services and deliver a full spectrum of real-time control and monitoring capabilities within a mining site-wide operations environment. One of the main challenges with the Industrial Internet of Things (IIoT) is the lack of design considerations that are placed on IACS. The lack of architectured, tested, and validated network and IACS design considerations results in higher risk in project execution and site-wide operation.

As technology continues to drive innovations, the mining industry must continue to keep pace to remain competitive in an ever-changing marketplace. The technology trend is to replace systems of yesterday with higher-performance, low-cost, option-rich devices that shorten the return on investment and offer more flexibility. As IACS technology evolves, systems migrate to functions that are being increasingly distributed to smarter, more granular, IACS components capable of performing localized operations. Within the IIoT, data must be reliably and securely accessible to anyone who needs it, anywhere in the globe. As a result, enterprise-wide systems must be able to provide a robust, scalable backbone that will meet the reliability and throughput needs of the mining industry.

Mining sites are under increasing pressure to reduce overall costs, boost productivity and quality, and improve personnel safety. One systematic approach for reaching these goals is automating and integrating site-wide architectures through the management of process information. Device-level integration through digital communication is the key to unlocking the full potential of the electronic controls being installed in industrial sites today. Choosing a communication platform that is versatile is key in defining an infrastructure that will allow support for various types and priorities of communication. Defining network policy and infrastructure allows enterprise owners to create a reliable and secure infrastructure for integrating the many kinds of IACS applications within mining sites.
This Mining Smart Industry Architecture (SIA) will provide a set of best practices, design, configuration, and troubleshooting considerations for mining applications by focusing both on general architecture and specific applications. The recommendations that are provided in this document have been tested and validated (by Rockwell Automation, Panduit, Endress+Hauser, and Cisco) in a laboratory environment and provide statistical accuracy of system performance.

**Documented Assumptions**

**Standards of Design**

The following standards and guidelines were utilized in accordance with best industry practices:

1. PlantPAx® 4.6 Guidelines
2. Application Code Manager Modular Equipment Guidelines
3. ISA 101 for HMI development
4. ISA 18.2 for Alarm Management

**Intended Testing Target**

The focus of this validation is meant to provide the user guidelines of deploying the PlantPAx Distributed Control System with the Rockwell Automation Mining Solution.
Application Selection

Functional Overview Surface Mining

The following process circuit use case is intended to provide a high-level overview of a surface mine system that is used for testing and validation of the Mining SIA. This process is geared at a hard rock, open quarry mining operation, but many parallels can be drawn to other functions of surface mining. Furthermore, the following extraction and concentration circuit is modeled after the Society of Mining Engineering 15-step process.

Following the flow circuit will be the assumptions made for size of equipment and representation within testing.
**Primary Crusher**

The primary crusher will serve as the asset to enable the deconstruction of raw material to smaller consumable feeds of material for usage later within the refining, concentration, and agglomeration processes. This asset will be represented as a 13.8 [kV], 15 000 [HP], 11.2 [MW] synchronous machine run via a soft starter.

**Secondary Crusher**

The secondary crusher will serve as the asset to take the out feed from primary crusher whose feed diameter size was rejected via the vibrating screen. As a result, this ore feed is further pulverized to a consumable size for further downstream processes. This asset will be represented as 4.16 [kV], 5 000 [HP], 3.72 [MW] synchronous machine a soft starter or constant torque variable-speed drive (VSD).

**Vibrating Screens**

The vibrating screens will serve to size and separate crushed and pulverized feeds of ore. This process will be used to confirm that the correct size of feed is correctly delivered to the rest of the concentration and agglomeration circuits. This asset will be represented as a 480 [VAC], 150 [HP], 112 [kW] induction motor driven by a VSD.

**Conveyance Systems**

Conveyance systems are the transportation artery of the Mining SIA use cases. The goal is to effectively transport ore through various stages of the operation, reliably, and effective rate of speed. Transfer belts within this application will be represented by 4.16 [kV] 5 000 [HP], 3.72 [MW] twin induction motors mounted at the head of the conveyor driven by VSDs. Other belts within the system will be represented as single induction motors 4.16 [kV], 3 000 [HP], 2.24 [MW] driven by VSDs. Low voltage belts will be represented as 480 [VAC], 200 [HP], 149 [kW] driven by VSDs.

**Rod Mills**

Rod mills provide a first pass milling capability of ore. These assets will be represented as 4.16 [kV], 2600 [HP], 1939 [kW] synchronous machines run by VSDs.

**Ball Mills**

Ball mills provide a secondary pass milling of ore. The discharge flow of the ball mill will be a gravity fed trough systems instrumented with load cells to determine flows, loading, and operation of the mill. These assets will be represented as 4.16 [kV], 2600 [HP], 1939 [kW] synchronous machines run by VSDs.
Flotation Cells

Flotation cells are a step within the concentration circuit that is used to remove impurities via the injection of chemicals and air bubbles within a solution. The concept is, by chemically altering the solution process owners have the capability to “float” good quality material over the top of the cell, while impurities would sink to the bottom. In certain instances, float cells are often cascaded to improve the purity and concentration of the final product. These assets will be modeled as 480 [VAC], 100 [HP], 75 [kW] induction motors drive by VSDs.

Thickeners

A thickener is an asset that essentially de-waters slurry and other waste material before pumping tailings to tailings ponds and other storage locations. These devices will be represented as 480 [VAC], 50 [HP], 37.3 [kW] induction motors drive by VSDs.

Pump Stations

Tailings pumps are used to transfer waste to tailings ponds. These assets will be represented by 4.16 [kV] 1000 [HP], 746 [kW] induction motors directly coupled to centrifugal pumps. These devices will be driven by VSDs. Low voltage pumping assets will be induction motors driven by VSDs at 480 [VAC] and range in size from 50 [HP], 37.3 [kW] to 500 [HP], 373 [kW].

Stacker Reclaimers

Stacker Reclaimers are mobile pieces of surface equipment that are used to move processed ore to stockpiles, or reclaim the processed ore from stockpiles for loading on vessels for shipment, for example, trucks, rail cars, boats, etc. The conveyor belts on these devices will be driven by VSDs. Low voltage conveyor assets will be induction motors driven by VSDs at 480 [VAC] and range in size from 50 [HP], 37.3 [kW] to 500 [HP], 373 [kW].
### Table of Assets

The following is a table of the electrical assets that are listed previously.

<table>
<thead>
<tr>
<th>Asset Number</th>
<th>Asset Name</th>
<th>Device Type</th>
<th>Size [HP] / [kW]</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Primary Crusher</td>
<td>Synchronous Motor / Soft Starter</td>
<td>15000 / 11.2 [MW]</td>
</tr>
<tr>
<td>2</td>
<td>Secondary Crusher</td>
<td>Synchronous Motor / Soft Starter</td>
<td>5000 / 3.72 [MW]</td>
</tr>
<tr>
<td>3</td>
<td>Vibrating Screener</td>
<td>Induction Motor / VSD</td>
<td>150 / 112</td>
</tr>
<tr>
<td>4</td>
<td>Transfer Belt Crusher</td>
<td>Induction Motor / VSD</td>
<td>5000 / 2.74 [MW]</td>
</tr>
<tr>
<td>5</td>
<td>Transfer Belt Screener</td>
<td>Induction Motor / VSD</td>
<td>3000 / 2.74 [MW]</td>
</tr>
<tr>
<td>6</td>
<td>Transfer Belt Concentration Plant</td>
<td>Induction Motor / VSD</td>
<td>200 / 149</td>
</tr>
<tr>
<td>7</td>
<td>Rod Mill 1</td>
<td>Synchronous Motor / VSD</td>
<td>2600 / 1939</td>
</tr>
<tr>
<td>8</td>
<td>Rod Mill 2</td>
<td>Synchronous Motor / VSD</td>
<td>2600 / 1939</td>
</tr>
<tr>
<td>9</td>
<td>Ball Mill 1</td>
<td>Synchronous Motor / VSD</td>
<td>2600 / 1939</td>
</tr>
<tr>
<td>10</td>
<td>Ball Mill 2</td>
<td>Synchronous Motor / VSD</td>
<td>2600 / 1939</td>
</tr>
<tr>
<td>11</td>
<td>Ball Mill 3</td>
<td>Synchronous Motor / VSD</td>
<td>2600 / 1939</td>
</tr>
<tr>
<td>12</td>
<td>Ball Mill 4</td>
<td>Synchronous Motor / VSD</td>
<td>2600 / 1939</td>
</tr>
<tr>
<td>13</td>
<td>Flotation Cell 1</td>
<td>Induction Motor / VSD</td>
<td>100 / 75</td>
</tr>
<tr>
<td>14</td>
<td>Flotation Cell 2</td>
<td>Induction Motor / VSD</td>
<td>100 / 75</td>
</tr>
<tr>
<td>15</td>
<td>Thickener 1</td>
<td>Induction Motor / VSD</td>
<td>50 / 37.3</td>
</tr>
<tr>
<td>16</td>
<td>Tailings Pump 1</td>
<td>Induction Motor / VSD</td>
<td>1000 / 746</td>
</tr>
<tr>
<td>17</td>
<td>Pump 1</td>
<td>Induction Motor / VSD</td>
<td>50 / 37.3</td>
</tr>
<tr>
<td>18</td>
<td>Pump 2</td>
<td>Induction Motor / VSD</td>
<td>500 / 373</td>
</tr>
<tr>
<td>19</td>
<td>Stacker-Reclaimer 1</td>
<td>Induction Motor / VSD</td>
<td>50 / 37.3</td>
</tr>
<tr>
<td>20</td>
<td>Stacker-Reclaimer 2</td>
<td>Induction Motor / VSD</td>
<td>50 / 37.3</td>
</tr>
</tbody>
</table>
Testing

Validation of the Mining SIA was performed in a lab environment that closely simulates a real-world installation. This testing included the actual hardware and software that is deployed in an IACS. In total, nine different tests were conducted to represent three different scales of network traffic (small, medium, and large), each was tested with three levels of network traffic. Details of the test bed setup and resulting output data is explained in chapter 4.

Tests performed

- Small-scale mining architecture network with 3 levels of traffic flow identified as low, moderate, and high.
- Medium-scale mining architecture network with 3 levels of traffic flow identified as low, moderate, and high.
- Large-scale mining architecture network with 3 levels of traffic flow identified as low, moderate, and high.

TIP The remainder of this document will discuss architecture and control strategy best practices on how to size and implement a system to represent a typical extraction and concentration circuit.
Chapter 1  Overview for the Mining Smart Industry Architecture

Notes:
Chapter 2

Design Considerations for the Mining Smart Industry Architecture

Overview

The prevailing trend in Industrial Automation and Control System (IACS) networking is the convergence of technology. Specifically IACS operational technology (OT) with information technology (IT). The Mining Smart Industry Architecture (SIA) design considerations help to enable IACS network and security technology convergence. This convergence includes OT-IT persona convergence, through the use of standard Ethernet, Internet Protocol (IP), network services, security services, and EtherNet/IP™. A reliable and secure converged site-wide IACS architecture helps to enable the Industrial Internet of Things (IIoT).

This chapter describes the primary design considerations for the Mining SIA use cases. These use cases were architected, tested, and validated by Rockwell Automation, Panduit, Endress+Hauser, and Cisco.

Reference Architecture

The foundation for the reliable and secure Mining SIA is Converged Plantwide Ethernet (CPwE) reference architectures. CPwE (see Figure 1 on page 19) is a collection of architected, tested, and validated designs. The content of CPwE, which is relevant to both operational technology and informational technology disciplines, consists of documented architectures, best practices, guidance, and configuration settings. This content helps industrial operations and original equipment manufacturers (OEMs) achieve the design and deployment of a scalable, reliable, secure, and future-ready site-wide industrial network infrastructure. CPwE can also help industrial operations and OEMs achieve cost reduction benefits. By using proven designs, you can facilitate quicker deployment while helping to minimize the deployment risk of new technology. CPwE is brought to market through an ecosystem consisting of industry thought leaders Rockwell Automation, Cisco Systems, and Panduit.

IACS applications are composed of multiple control and information disciplines such as continuous process, batch, discrete, and hybrid combinations. To take advantage of the business benefits associated with IIoT, industrial operations must face the challenges of industrial hardening of standard Ethernet and IP-converged IACS networking technologies. CPwE is the underlying architecture that provides standard network and security services for control and information disciplines, devices, and equipment found in modern IACS applications.
CPwE key tenets include:

- Smart IIoT devices
  - Controllers, I/O, drives, instrumentation, actuators, analytics, and single IIoT network technology (EtherNet/IP)
- Zoning (segmentation)
  - Smaller connected LANs, functional areas, and security groups
- Managed infrastructure
  - Managed Allen-Bradley® Stratix® industrial Ethernet switches (IES), Cisco® Catalyst® distribution/core switches, FactoryTalk® Network Manager™ software, and Stratix industrial firewalls
- Resiliency
  - Robust physical layer and resilient or redundant topologies with resiliency protocols
- Time-critical data
  - Data prioritization and time synchronization via CIP Sync™ protocol and IEEE-1588 Precision Time Protocol (PTP)
- Wireless
  - Unified wireless LAN (WLAN) to enable mobility for personnel and equipment
- Holistic defense-in-depth security
  - Multiple layers of diverse technologies for threat detection and prevention, which is implemented by different persona (for example, OT and IT) and applied at different levels of the site-wide IACS architecture
- Convergence-ready
  - Seamless site-wide integration by trusted partner applications
Figure 1 - CPwE Architectures

For more information on CPwE, see
Industrial IoT Network Technology

EtherNet/IP is the IIoT network technology for the Mining SIA. EtherNet/IP uses the ODVA, Inc. Common Industrial Protocol (CIP™), and is ready for the Industrial Internet of Things. EtherNet/IP offers the following benefits:

- Single industrial network technology for:
  - Multi-discipline Network Convergence - Discrete, Continuous Process, Batch, Motor, Safety, Motion, Power, Time Synchronization, Supervisory Information, Asset Configuration/Diagnostics

- Established
  - Risk reduction – broad availability of products, applications, and vendor support
  - ODVA: Cisco Systems, Panduit, Endress+Hauser, and Rockwell Automation are principal members
  - Supported – Conformance testing, defined QoS priority values for EtherNet/IP devices
  - Standard – IEEE 802.3 Ethernet and IETF TCP/IP Protocol Suite
  - Enables convergence of OT and IT – common toolsets (assets for design, deployment, and troubleshooting) and skills/training (human assets)
  - Topology and media independence – flexibility and choice
  - Device-level and switch-level topologies; copper - fiber - wireless
  - Portability and routability – seamless site-wide information sharing
  - No data mapping – simplifies design, speeds deployment, and reduces risk

For more information on EtherNet/IP, CIP Sync, and DLR, see odva.org: http://www.odva.org/Technology-Standards/EtherNet-IP/Overview.
Network Zoning

Zoning is a key CPwE tenet that is utilized within the Mining SIA. Zoning is a practice of segmenting the IACS network to create smaller domains of trust to help protect the IACS network from risks in the network. As shown in Figure 2, CPwE segments the IACS site-wide architecture into different zones: Area Zone, Industrial Zone, Industrial Demilitarized Zone (IDMZ), and Enterprise Zone. OT/IT teams control the communication between the Enterprise and Industrial zones through the IDMZ. This zoning creates strong boundaries and helps to reduce the risk of unauthorized communications.

The segmentation between Area Zones is commonly done using virtual local area networks (VLANs) with access control lists (ACLs) at the Layer 3 distribution switch. A group of IACS assets that are part of the same functional Area Zone and need to communicate with each other are put in the same VLAN. When IACS assets need to communicate with IACS assets in another functional Area Zone, communication occurs via the Layer 3 distribution switch that uses ACLs to either permit or deny traffic.

There are many benefits that are associated with zoning, such as creating functional areas (building block approach for scalability and future-ready architectures), creating smaller connected LANs for smaller broadcast/fault domains, segmenting disparate IIoT network traffic types, and creating smaller domains of trust (security groups) to help contain any security incidents. For example, if there is a security group access policy to restrict the communication between the VLANs (Area Zones), traffic from an infected host is contained within the VLAN. However, as the size of the ACL increases, the complexity of managing the ACL also increases.

The CPwE logical zoning model employs commonly used industry standards to organize the site-wide functions into Levels and functional/security Area Zones:

- **Levels:**
  - Purdue Model for Control Hierarchy
  - ISA 95 Enterprise-Control System Integration

- **Zones:**
  - IEC-62443 (formerly ISA99) Industrial Automation and Control Systems (IACS) Security
  - NIST 800-82 Industrial Control System (ICS) Security
  - DHS/INL/ICS-CERT Recommended Practices
The Area Zones

Contains Levels 0...2 of IACS devices. One or more Area Zones actually reside within the Industrial Zone, as depicted in Figure 2.

- **Level 0 Process**
  - Industrial sensors, drives, actuators, and similar devices that interact with the physical environment by taking measurements or performing actions such as starting a motor.

- **Level 1 Basic Control**
  - Controllers, such as programmable logic controllers, distributed control system (for example, PlantPAx®), and programmable automation controllers (for example, ControlLogix®) that communicate directly with the Level 0 devices, other controllers, and higher-level IACS applications.

- **Level 2 Area Supervisory Control**
  - Operator interfaces including human machine interface (HMI), and thin clients (for example, ThinManager®).
The Industrial Zone

(Levels 0...3) contains the Area Zones and the Level 3 IACS applications that maintain site-wide control of the lower-level IACS applications. The Level 3 applications include PlantPAx, FactoryTalk applications (for example, Historian, AssetCentre and Network Manager), and an industrial data center (IDC) for servers and network infrastructure devices. The IDC commonly contains network services such as Network Time Protocol (NTP), Domain Name Server (DNS), Dynamic Host Configuration Protocol (DHCP). The IDC also contains security services such as Active Directory, remote access, and identity services (authentication, authorization and accounting.)

Industrial Demilitarized Zone

CPwE includes an additional zone, that is based on IEC-62443, that resides between the Industrial and Enterprise Zones, called the Industrial Demilitarized Zone. The IDMZ provides a layer of separation between the traditional IT and OT operated areas of the network, allowing only traffic that is required to traverse the zone securely.

The Enterprise Zone

Contains Level 4 and Level 5, provides access to the internet and higher-order network applications such as email, database, business-to-business (B2B), and business-to-consumer (B2C) applications and other non-critical resources. This zone, which is often seen as a source of security threats to the Industrial Zone resources, is typically managed by the IT department.

For more information on zoning, see:

Network Resiliency

Business practices, corporate standards, policies, industry standards, and tolerance to risk are key factors in determining the degree of resiliency and application availability that is required within an IACS site-wide architecture. A resilient network architecture within an IACS application plays a pivotal role to help minimize the risk of IACS application shutdowns while helping to maximize overall uptime for the Mining SIA use cases.

A holistic, resilient, and site-wide network architecture is composed of multiple technologies (logical and physical.) These technologies utilize a defense-in-depth approach where different solutions are required address various network resiliency requirements, which are deployed at different levels within the site-wide architecture. When selecting a resiliency technology, evaluate various site application factors, including the physical layout of IACS devices (geographic dispersion), resiliency performance, media type (copper, fiber, wireless), tolerance to data latency and jitter, and future-ready requirements.

Resiliency technologies are typically single-fault tolerant, are a single LAN, and utilize redundant path topologies (for example, ring and redundant star.) A resiliency protocol (for example, Device Level Ring Protocol) is used to block one physical path while forwarding Ethernet frames along the other physical path. This configuration helps to avoid Layer 2 loops. Network convergence (recovery, healing) times vary across resiliency technologies. Convergence time disruption is defined as the time it takes to discover a failure (for example, link or device) along a path, unblock the blocked path, then start forwarding Ethernet frames along that unblocked path.

The Mining SIA (Figure 3) uses a diverse defense-in-depth approach, utilizing a hybrid of device-level ring (DLR), switch-level ring (DLR and REP), and redundant star topologies (Flex Links and EtherChannel) to achieve the availability required in modern Mining SIA use cases.

**Figure 3 - Mining Smart Industry Architecture**
Ring Topologies

For single or dual media rings, all IES are connected in a linear fashion, with each end of the linear topology connected together to form a ring. A resiliency protocol (for example, DLR) is required to avoid Layer 2 loops within the ring. Network convergence times vary across resiliency technologies.

Device Level Ring technology is optimized to provide ring topology resiliency for time critical IACS applications. DLR supports fast ring convergence (single-fault tolerant) in the event of an IACS device or link failure. DLR also supports flexible topologies such as IACS device-level (embedded switch), switch-level (Layer 2, IES only), and mixed device/switch-level ring hybrid topologies (Figure 4) for OEM (equipment, skid, machine) and site-wide IACS deployments. DLR is standard Ethernet (OT-IT convergence) with standard network services such as quality of service (QoS) and IEEE 1588 PTP (Precision Time Protocol).

![Figure 4 - Device Level Ring Protocol, Device-level, and Switch-level Topology Examples](image)

The Deploying Device Level Ring within a Converged Plantwide Ethernet Architecture Design Guide outlines several use cases for designing and deploying the DLR technology throughout a site-wide IACS network infrastructure. The CPwE DLR Design Guide highlights the key IACS application requirements, technology, and supporting design considerations to help with the successful design and deployment of these specific use cases within the CPwE framework.

For more information on Device Level Ring, see:
- Deploying Device Level Ring within a Converged Plantwide Ethernet Architecture Design Guide, publication ENET-TD015.
- EtherNet/IP Device Level Ring Application Technique, publication ENET-AT007.

Resilient Ethernet Protocol (REP) is a Cisco resiliency technology that is implemented on IES and Cisco distribution switch-level rings. REP is designed to provide network and application convergence if there is a media or network
failure, without a negative impact on most network IACS applications. REP is a segment protocol that integrates easily into Mining SIA Area Zone LANs. REP is a distributed and secure control plane protocol that does not rely on a master switch controlling the status of the ring. Therefore, failures can be detected locally, either through loss of signal (LOS) or loss of connectivity to a neighboring switch. By default, REP automatically elects an alternate port (the IES port being blocked.) Any REP port within the REP topology can initiate a switchover to unblock the alternate port.

The Deploying a Resilient Converged Plantwide Ethernet Architecture Design and Implementation Guide (DIG) outlines several use cases for designing and deploying a holistic, diverse, and resilient site-wide IACS network infrastructure. This DIG highlights the key IACS application requirements, technology, and supporting design considerations to help with the successful design and deployment of these specific use cases within the framework of CPwE.

For more information on REP, see:


Redundant Star Topology Technologies

Redundant star topologies utilize point-to-point redundant paths between Layer 2 IES and Layer 3 distribution switches (Figure 5 on page 27). A resiliency protocol (for example, Flex Links) is used to block one physical path while forwarding Ethernet frames along the other physical path. This configuration helps to avoid Layer 2 loops. Network convergence times vary across resiliency technologies. Convergence time disruption is defined as the time it takes to discover a failure (for example, link or device) along a path, unblock the blocked path, then start forwarding Ethernet frames along that unblocked path. The Mining SIA, based on CPwE design consideration best practices, utilizes both Flex Links and EtherChannel.

Flex Links is a Cisco resiliency protocol that is an alternative to Rapid Spanning Tree Protocol (RSTP) and EtherChannel in redundant star topologies. It is used to connect Layer 2 IES to a Layer 3 distribution switch. With Flex Links, an active uplink interface and a backup uplink interface are defined. To begin, the active interface is in the up condition. The interface that is up sends and receives frames just like any other Ethernet port. The backup interface begins in the standby state. The standby interface establishes a link to the other side of the connection (that is, it is up/up by both switches). However, the interface in the standby state does not send or receive any packets. Only the interface that is up sends and receives the traffic to and from the switch. When a failure is detected on the forwarding link, the MAC address and multicast entries are transferred to the standby link. When the failed interface is restored, it becomes the standby link.

EtherChannel and Link Aggregation Control Protocol (LACP) are not resiliency protocols. They are designed to provide additional bandwidth between
switches by aggregating multiple Ethernet connections into a higher bandwidth virtual connection. However, these protocols need to quickly recover from the loss of one or more channel members. This fast recovery from a failure of an individual channel member can be used to provide link redundancy between Layer 2 IES and Layer 3 distribution. EtherChannel bundles multiple Ethernet links between two switches into a single logical link and balances the traffic load across the physical links. When a physical link is lost, the EtherChannel load-balancing algorithm stops using the lost link and uses the other available links. When the link is restored, EtherChannel resumes balancing the load across the available link. In this way, EtherChannel can be used as a resiliency protocol when multiple links exist between two switches. To be used as a resiliency protocol, the switches must have redundant links between each other, such as in the redundant star topology.

Figure 5 - Redundant Star Topology Examples

Parallel Redundancy Protocol

Parallel Redundancy Protocol (PRP) is a multiple-fault tolerant (depending on topology) standard defined in IEC 62439-3 and is adopted in the ODVA, Inc. EtherNet/IP specification. PRP technology creates seamless network redundancy by allowing PRP enabled IACS devices to send duplicate Ethernet frames over two independent Local Area Networks (LANs). If a failure occurs in one of the LANs, traffic continues to flow through the other LAN uninterrupted with zero recovery time.
Although not part of the Mining SIA, if the site-wide architecture availability requirements necessitate a redundant network technology (vs. a resilient network technology), Parallel Redundancy Protocol could be used.

**Figure 6 - Parallel Redundancy Protocol Example**

The Deploying Parallel Redundancy Protocol within a Converged Plantwide Ethernet Architecture Design and Implementation Guide (DIG) outlines several use cases for designing and deploying PRP technology and topologies throughout a mining site-wide IACS network infrastructure.

The CPwE PRP DIG highlights the key IACS application requirements, technology, and supporting design considerations to help with the successful design and deployment of these specific use cases within the CPwE framework.

For more information, see:
- EtherNet/IP Parallel Redundancy Protocol Application Technique, publication ENET-AT006.

**Time Synchronization**

CIP Sync technology uses the CIP application layer protocol and the IEEE 1588-2008 Precision Time Protocol (PTP) standard for time synchronization. CIP Sync and IEEE 1588-2008 are designed for local and site-wide IACS applications requiring high accuracies beyond those attainable with Network Time Protocol (NTP.) CIP Sync uses IEEE 1588 Precision Time Protocol (PTP) to synchronize clocks in the IACS application. In the PTP architecture, all clocks are synchronized to a single grandmaster clock. In turn, this clock must be synchronized to Coordinated Universal Time (UTC) to represent the time of day in the system.

CIP Sync is used across a broad range of IACS applications to synchronize IACS clocks (**Figure 7**) and helps enable applications such as event time stamping, sequencing, and logging. For example:
• A sequence of events (SOE) or first fault detection system can use timestamps to determine the order in which faults occurred in the system. These timestamps allow for the tracking of faults to establish the first in a chain of faults. These types of applications use dedicated alarm instructions in the Programmable Automation Controller (PAC) to record events or time stamping inputs in order to log the change of state for a point.

• An in-PAC chassis historian module logs historical data at Level 1 (skid/machine).

• High-speed applications can use timestamps to process inputs and outputs asynchronously from the control loop. For example, an application can use time-synchronized inputs and outputs to trigger a diverter without the application scan time matching the part cycle time.

Figure 7 - Time Synchronization Example

The Deploying Scalable Time Distribution within a Converged Plantwide Ethernet Architecture Design Guide (DG) outlines several use cases for designing, deploying, and managing time synchronization technology throughout a site-wide IACS network infrastructure. CPwE Time Design Guide highlights the key IACS application requirements, technology, and supporting design considerations to help with the successful design and deployment of these specific use cases within the CPwE framework.

For more information on time synchronization, see:

• Deploying Scalable Time Distribution within a Converged Plantwide Ethernet Architecture Design Guide, publication ENET-TD016.
Chapter 2  Design Considerations for the Mining Smart Industry Architecture

Selection of IES and Smart IIoT Devices

Whether an end user, OEM, or system integrator, reliable and secure network infrastructure is critical for IACS design and deployment considerations. IACS applications requirements vary, so scalable and flexible choices in Smart IACS and IES devices are key to supporting the type of network and security services that are required for specific IACS applications.

With modern Smart IACS devices, open does not mean easy, and standard does not mean foolproof. The end user, OEM, or system integrator have more responsibility to select and test the Smart IACS devices to ensure they meet the IACS application requirements. The choice of Smart IACS devices is driven by the following business and technology aspects:

- Product conformance testing, with declaration of conformity, by the technology governing body (for example, ODVA).
- Controllers (Level 1) selection considerations:
  - Number of EtherNet/IP ports, media (for example, copper, fiber), topology (for example, DLR, PRP)
  - Environment: on-machine / in-panel
  - Communication speed: 100 Mbps, 1 Gbps
  - Maximum # of connected IACS devices
  - Minimum requested packet interval (RPI) for PACs (how fast)
  - Maximum I/O data size per RPI
- Sensors/Actuators (Level 0) selection considerations:
  - Application Requirements
  - Environment: on-machine / in-panel
  - Number of EtherNet/IP ports, media (for example, Copper, fiber), topology (for example, DLR, PRP)
  - Communication speed: 100 Mbps, 1 Gbps
  - Minimum RPI (how fast)
  - Maximum I/O data size per RPI

For more information on Smart IACS device selection, see:
- Integrated Architecture Builder

The choice of IES infrastructure devices is driven by the following business and technology aspects:

- Fully managed industrial Ethernet switches (IES) may provide too many reliability and security capabilities for specific IACS application criteria.
- Unmanaged IES reliability and security capabilities may be too limited for specific IACS application criteria.
- Lightly managed IES reliability and security capabilities may provide the right balance of business and technology aspects to meet specific IACS application criteria—for example, segmentation, data prioritization, resiliency, and security.
For more information on IES device selection, see:

- Integrated Architecture Builder
- Stratix Managed Switches User Manual, publication 1783-UM007.

**Convergence-Ready OEM Applications**

To help simplify seamless integration into the end-user site-wide network infrastructure, OEMs (skids, machines, and equipment) should take into account the following design and deployment considerations when selecting network and security services:

- Manageability by an industrial Ethernet protocol that fully uses standard Ethernet and IP (such as EtherNet/IP) as the multi-discipline IIoT technology:
  - Common network infrastructure devices - optimized asset utilization
  - Scalable and future-ready - better sustainability
- IP addressing schema:
  - Who manages? End User (OT/IT) or OEM?
  - Address range (class), subnet, default gateway (routability)
  - Implementation conventions - static/dynamic, hardware/software configurable, network address translation (NAT), and domain name services (DNS)
- Use of Common Layer 2 and Layer 3 Network Services:
  - Segmentation, data prioritization
  - Topologies - Switch-level, device-level, and hybrid
  - Availability - Loop prevention and redundant path topologies with resiliency protocols
- Use of Common Layer 1, Layer 2, and Layer 3 Security Services:
  - Physical access, port security, access control lists, and application security (for example, FactoryTalk Security)
  - Alignment with emerging IACS security standards such as IEC-62443 (formerly ISA 99) and NIST 800-82
- Time Synchronization Services:
  - IEEE 1588 Precision Time Protocol (PTP)
  - CIP Sync applications – time stamping, first fault, and SOE

The OEM Networking within a Converged Plantwide Ethernet Architecture Design Guide outlines several use cases for designing and deploying lightly managed IES for OEM applications (skid, machine, equipment) and throughout the Area Zone within a site-wide IACS network infrastructure. The Design Guide highlights the key IACS application requirements, technology, and supporting design considerations to help with the successful design and deployment of these specific use cases within the framework of CPwE.
For more information on convergence-ready, see:


**Instrumentation**

Robust integration of field instrumentation into an IACS enables users to have accurate information and better control of variables. This integration affects process performance, maintenance, online configuration, and diagnostics. The integration of these instruments allows for faster troubleshooting and replacement if there is a failure. In a connected environment, instrumentation also increases asset uptime, reduces process variability, and provides key insights for cost savings across process areas.

Successful process control requires the selection of appropriate instrumentation and correct design for a quick integration to the IACS. Intelligent device utilization and appropriate integration to the IACS bring the following benefits to site operation:

- Remote diagnostic and configuration
- Real-time data integration for Advanced Analytics
- Smart Spares Parts Management
- Device traceability
- Plug and Play replacement
- Measurement Accuracy
- Process Simulation enablement

Figure 8 provides an overview of the joint integration tools and benefits that are provided by Endress+Hauser and Rockwell Automation within the PlantPAx DCS.

**Figure 8 - Joint Integration Tools and Benefits.**

**FASTER TIME TO MARKET**

- Suite of control and HMI objects to accelerate project engineering, commissioning and start-up
- Seamless integration and “Internet of Things” ready
- Decreased risk

**KEY DELIVERABLES**

- Integration Documents - Comprehensive and easy guidance to system design and setup
- Customized Add-On Profiles
- Pre-engineered Add-On Instructions, Global Objects and Faceplates
- Pre-defined diagnostic tables
- Endress+Hauser Heartbeat Technology integration
Asset Management

FDT® Technology holds the key to integrating any device, system or network in today's complex industrial automation architecture. It consists of two major software components: FRAME™ Application (FDT/FRAME™) and Device Type Manager™ (FDT/DTM™). Together, an FDT/FRAME and a DTM or a collection of DTMs create an FDT-enabled application, which can be scaled from a single device to tens of thousands of devices controlled by a single FRAME throughout the automation communication pyramid.

Rockwell Automation provides various communication and module DTMs for EtherNet/IP, HART remote I/O's and Foundation Fieldbus. The FDT frame application FieldCare SFE500 from Endress+Hauser is a universal tool for field device configuration and parameterization including a comprehensive library of certified DTMs.

For more information, see Integrate Endress+Hauser Instruments in a PlantPAx Distributed Control System, publication PROCES-SG003.

Field Network Infrastructure

EtherNet/IP I/O Network

The EtherNet/IP I/O Network is mandatory for these reference topologies, with relevant impact to integration tests.

The EtherNet/IP I/O Network may be built in a star, linear bus, or device level ring topology, and in a hybrid network topology composed of those configurations. For increased site availability, this topology assumes applying DLR as the backbone and the preferred option to connect all DLR capable EtherNet/IP devices that do not support DLR may be connected in star topology via managed Stratix switches. HART devices can be connected either via HART capable 1756 ControlLogix I/O or 1794 FLEX™ I/O.

For more information, see Rockwell Automation Library of Process Objects: EtherNet/IP Instrumentation for PlantPAx DCS, publication PROCES-RM012.

HART I/O

HART I/O is necessary to connect complementary HART devices, as required if EtherNet/IP options are not reasonable to be used.

For more information, see Rockwell Automation Library of Process Objects: HART Modules for PlantPAx DCS, publication PROCES-RM010.
Foundation Fieldbus

Field Device Tool / Device Type Manager (FDT / DTM) technology is supported, which allows direct access to device configuration and diagnostics via FDT frames.

Rockwell Automation Linking Device supports as many as 16 field devices on one H1 segment. The linking devices have full FOUNDATION Fieldbus Host capability including Link Active Scheduler (LAS) capability. The H1 segment is divided between two physical ports with individual protection.

Multiple levels of device and media redundancy are supported including: ring, split, and redundant trunk, also adding devices online is allowed.

For more information, see FOUNDATION Fieldbus Design Considerations, publication PROCES-RM005.

PlantPAx System Considerations

The PlantPAx system uses standard Rockwell Automation Integrated Architecture (IA) products to build a distributed control system (DCS). Our modern DCS is scalable, flexible, and open while still providing the reliability, functionality, and performance expected from a DCS. Depending upon the scale of the system, the PlantPAx architecture can meet the needs for many applications.

For a more detailed system configuration and sizing and scaling option please consult: PlantPAx Distributed Control System, publication PROCES-RM001.

Level 3 Sitewide considerations

Physical Infrastructure Deployment

The Level 3 Site Operations Area provides the switching, compute, and storage resources that are needed to operate a site-wide IACS architecture efficiently, including the PlantPAx DCS. This area is the foundation for data collection and application hosting in the industrial setting. Level 3 equipment may be physically housed in an industrial data center, in a rack in the control room, or several other locations on the premise. Level 3 Site Operations applications range from manufacturing execution systems (MES) measures such as Overall Equipment Effectiveness (OEE), lot traceability preventive maintenance schedules, process monitoring/management, safety/security dashboards, and productivity key performance indicators (KPIs). Continuity of service is imperative as these functions are used for daily decision-making on an ever-increasing basis. Mining downtime, and other site-wide processes, is readily measured in minutes and in thousands of dollars from missed customer commitments. Reliable and secure network support for these applications keeps operations and business communication running smoothly.
The Level 3 Site Operations Area is a model for integrating a scalable, modular, logical network and compute systems into the physical infrastructure. Some benefits of this approach are:

- Improves network availability, agility, scalability, and security
- Reduces operational costs, including energy costs, with improved efficiencies
- Can help to simplify resource provisioning
- Lays the foundation for consolidation and virtualization
- Helps to create a path to future technology requirements

**Key Requirements and Considerations**

Industrial network deployments have evolved over the years from a network gateway layout to a converged site-wide architecture. This evolution applies to manufacturing plants and mining facilities. CPwE architecture provides standard network services to the applications, devices, and equipment that is found in modern IACS applications and integrates them into the wider enterprise network. The CPwE architecture provides design and implementation guidance to achieve the real-time communication and deterministic requirements of the IACS and to help provide the scalability, reliability, and resiliency required by those systems.

In support of industrial network performance, many physical infrastructure aspects of the Level 3 Site Operations serve an important role, and must be considered in the design and implementation of the network.

- **Industrial Characteristics**
  - Site networking assets and cabling that is used in Level 3 Site Operations are not environmentally hardened but are almost exclusively installed in IP20 or better environments. Environmental risks at Level 3 Site Operations involve thermal management of heat that is dissipated by equipment and power quality considerations.

- **Physical Network Infrastructure Life Span**
  - IACS and site-wide backbone can be in service as long as 20 years or more. Hardware that is used in Level 3 Site Operations has a much shorter life span, generally three to five years. The infrastructure used to connect and house the hardware such as cabinets, cabling, connectivity, and enclosures has a much longer life span, generally 10...15 years. Consideration of higher performance cabling enables current and future data communications needs to be fully met. Choices between copper and fiber-optic cabling assure higher data rate transport requirements.

- **Maintainability**
  - MACs at Level 3 have dependencies that affect many Area Zones. Also, changes must be planned and executed correctly to avoid bringing down the IACS process. Proper cable management such as bundling, identification, and access is vital for proper Level 3 Site Operations maintenance.
• Scalability
  • The high growth of EtherNet/IP connections can strain network performance and cause network sprawl that threatens uptime and security. A strong physical building block design accounts for traffic growth and management of additional cabling to support designed network growth. Use a physical zone topology together with structured copper and fiber-optic cabling that is chosen for high data throughput. Choose building-block pre-configured solutions to enable a network infrastructure that is comprised of modular components that scale to meet increasing industrial Ethernet communications needs in the IACS network.

• Designing for High Availability
  • A robust, reliable physical infrastructure achieves the service levels that are required of present and future IACS networks. The use of standards-based cabling together with measured, validated performance confirms reliable data throughput. Use of redundant logical and physical networks assures highest availability. Properly designed and deployed pathways should be employed to ensure redundant cable paths are also resilient.

• Network Compatibility and Performance
  • Cable selection is the key to optimal physical network performance. Network performance is governed by the poorest performing element in any link. Network compatibility and optimal performance are essential from port to port, including port data rate and cabling bandwidth.

• Grounding and Bonding
  • A well architected grounding/bonding system is crucial for industrial network performance at every level whether internal to control panels, across sites, or between structures. A single, verifiable grounding network avoids ground loops that can degrade data and have equipment uptime and safety implications.

• Security
  • Network security is a critical element of network uptime and availability. Physical layer security measures, such as logical security measures, should follow a defense-in-depth hierarchy. The Level 3 Site Operations physical defense in-depth strategy could take the form of locked access to industrial data center/control room spaces and cabinet key card access to help limit access, use of lock-in-block-out (LIBO) devices to control port usage, and keyed patch cords to avoid inadvertent cross patching. Using a physical strategy in concert with your logical strategy prevents inadvertent or malicious damage to equipment and connectivity achieving service level goals.
Industrial Network Building Block Systems

Industrial network building block systems, such as the industrial distribution frame (IDF), industrial data center (IDC), and physical network zone system (PNZS), are purpose-built for various architecture needs. Applications for the building block approach are diverse and include different types of locations such as warehouses, manufacturing plants, and mining. The building block system approach speeds deployment and reduces deployment risk because the building block system design is pre-engineered and validated for thermal, cable management, identification, and grounding. For the IACS site-wide backbone, which is part of the Industrial Zone, specific physical network building block systems include the PNZS and the IDF. These building block systems are described in the following sections.

PNZS

The Physical Network Zone System is a network building block of the IACS industrial Ethernet network following a physical zone topology. The PNZS allows for rapid deployment of the industrial networking equipment that is required to connect the site-wide IACS architecture. It includes copper and fiber connectivity, patching for the uplinks and downlinks, and a steel enclosure for reliability and improved security. It also includes power features to minimize engineering and installation time for faster implementation.

The PNZS serves as a consolidation point in the architecture, providing communications to a localized group of control panels in the Area Zone. DIN-mount IES should be protected using an appropriately specified PNZS. This protection includes physical and electrical, including UPS backup power when needed. In most cases, external cooling may not be required, reducing cost and minimizing A/C maintenance when compared to an Enterprise switch deployment. Cabling and connectors are the same as those used with Enterprise switches. Cable management and connectivity include DIN mount patch panel, DIN adapter for RJ45 jacks, and slack and strain relief features mounted to backplane or DIN. In addition, a barrier may be included to separate higher voltages from the DC power to the switches.

Figure 9 - Example PNZS
Chapter 2  Design Considerations for the Mining Smart Industry Architecture

The Industrial Data Center

The successful deployment of Level 3 Site Operations depends on a robust network infrastructure that is built on a rock-solid physical layer that addresses the environmental, performance, and security challenges present when deploying IT assets (servers, storage arrays, and switching) in industrial settings. The Level 3 Site Operations is a key convergence point for IT and OT. Many businesses obtain these functions in a pre-engineered package, Industrial Data Center (IDC). IDC systems include the proper IT assets that are housed in an appropriate cabinet with patching, power, grounding/bonding, identification, and physical security considerations already addressed a plug and play solution. IDC is often the host of the PlantPAx Distributed Control System virtual machines.

The IDC from Rockwell Automation (Figure 10 on page 39) can help your business realize the cost savings of virtualization in an operations environment through a pre-engineered, scalable infrastructure offering. All hardware required to run multiple operating systems and multiple applications on virtualized servers is included in the cost. Industry-leading collaborators including Cisco, Panduit, Dell EMC, and VMware collaborating with Rockwell Automation to help your business realize the benefits of virtualization through this integrated offering.

Features and Benefits:

- Reduced Cost of Ownership
  - Decrease the server footprint in your facility and realize savings over the lifetime of your assets
- Uptime Reliability
  - Deliver high availability and fault tolerance
- Designed for Your Industry
  - Engineered specifically for use in industrial operations environments including mining. Commonly deployed for PlantPAx DCS
- Ease of Ordering and Commissioning
  - Pre-assembled solution that includes configuration service. No need to place multiple equipment orders
- One Number for Technical Support
  - Includes TechConnectSM support so you have one phone number to call. Additional support levels include 24x7 support and remote monitoring
Industrial Distribution Frame

A cabinet with a Rack Unit (RU) frame is preferred when network designs include rack-mount gear. Deployment of Enterprise-grade computer or network cabinets leads to premature network switch failure because cabinets are typically open to the environment, accumulating dusts, liquids, and other contaminants over time. The predominant enclosure choice is a double-hinged 26 RU design which is commonly referred to as an IDF (Figure 11 on page 40). An IDF is designed for 19-inch RU style switches and other gear, such as a UPS, and is typically wall or column mounted. An IDF may come pre-configured with cabling, duct, cable ties, and so on, leading to consistent equipment deployment, minimizing engineering effort and reducing installation time. The advantage of a pre-configured IDF is best-in-class cable management, thermal performance, and proven installation.

Often, an IDF has both access and distribution switching. Combining access and distribution switches consolidates sensitive network equipment in a protective and cooled enclosure in a cost-effective manner, controlling security access and simplifying mounting. An IDF contains many switches but is sized for two Cisco distribution switches (for example, Catalyst 9300 fiber-based) and up to three Cisco access switches (for example, Catalyst 2960 copper-based) along with a UPS.
Physical Network Design Considerations

The Industrial Network Building Block system provides modularity and simplifies the overall setup and configuration. Connecting the building blocks with a properly designed physical infrastructure will increase the network reliability. Figure 10 illustrates a simplified Industrial Zone physical deployment between Levels 0...3. This provides an example of the network building blocks that are connected with physical connections. Depending on the mining network size, the Level 3 Site Operations could connect to the Area Zones through Core Switches. The links between the core switches in the Level 3 Site Operations and the distribution switch in the IDF use fiber-optic cabling. The distribution layer also connects to control panels that have IES with fiber network cabling. Longer runs for remote applications may require single mode fiber.
Cellular Considerations and Designs

As cellular continues to advance in technology, considerations for cellular usage in an industrial environment is on the rise. The fifth generation (5G) cellular network is beginning to emerge and with it brings potential for new applications. Latency time and reliability are improving with each generation. Currently cellular is not common among mining applications but due to the locale of components needing network connections it may be considered in future designs. Although cellular applications remain a small market for industrial applications, including mining, here are some basic things to consider when implementing a cellular system.

- Secure Connection: Data security is important when designing a cellular system. Sending data over the public air is susceptible to unauthorized users seeking to access the data. Encrypting the data at the sending end and decrypting at the receiving end is one method of securing the data. Often this is accomplished using a virtual private network (VPN.) VPN has several types of protocols available and there are different types of VPNs.
Antenna location: Upon installation of a cellular system an antenna will be utilized for signal transmission. This antenna can be mounted directly on a device or a remote antenna can be used to provide a better signal. Locating the antenna has a direct impact on performance and therefore should be thoroughly researched before installation. Installation of the antenna in an area with fewer obstructions and potential areas of interference will improve overall reliability.

Installation: Often the cellular appliances are mounted up high for optimizing antenna performance, but this can lead to a more challenging thermal location. Cooling may be needed if the ambient temperature exceeds the recommended values of the cellular appliance. Physical location of the network connection and remote antenna connection should also be designed to avoid high EMI areas or other types of interference.

Cellular plan: Selecting a cellular plan can be challenging due to the number of providers and different types of plans. Many providers have developed plans that focus on end points that provide IoT type data. The volume of data being collected will have an impact on the way the billing is structured.

Cellular provider and coverage area: Coverage can vary based on carrier and location. It is best to research what is the best setup for the area of deployment and the types of networks available (CDMA, GSM, 4G, 5G, etc.). Some of these networks have carrier-specific characteristics and there are limitations on coexistence of networks. Reliability is the key performance indication for cellular coverage in a production environment. Industrial environments are more challenging due to obstruction with metal objects and remote locations.

Bandwidth: Industrial applications often require availability to be the top priority therefore bandwidth is less of an issue in comparison. Small critical packets (motion control application for example) sent frequently is more common than moving high volumes of data at a faster speed. However, bandwidth and the network setup will affect the overall performance and thereby ties into availability. Determining the required bandwidth that fulfills the need of the network while maintaining high availability is the ideal setup.

Cybersecurity

Industrial IoT offers the promise of business outcomes by using innovative technology. The challenge for industrial operations is to develop a balanced security stance to take advantage of IoT innovation while maintaining the integrity of industrial security and safety best practices. Business practices, corporate standards, security policies and procedures, application requirements, industry security standards, regulatory compliance, risk management policies, and overall tolerance to risk are all key factors in determining the appropriate security stance.

Although not part of the Mining SIA, if the site-wide architecture requirements necessitate cybersecurity, the CPwE industrial security framework (Figure 14 on page 45) could be overlaid on the Mining SIA network infrastructure. Although
industrial cybersecurity should be holistic for Greenfield IIoT projects, there are many solutions available to help industrial operations incrementally improve the security stance for their legacy IIoT architectures.

No single product, technology, or methodology can fully secure IIoT applications. Protecting IIoT assets requires a holistic security approach to help address different types of threats. This approach uses multiple layers of diverse technologies for protection and detection, which is applied at different levels of IIoT architectures, while being implemented by different personas.

One size does not fit all when it comes to risk tolerance and stance on availability, safety, and security. What is acceptable by one industrial operator may be unacceptable to another and vice versa. IIoT architectures should support scalability, which includes the degree of holistic and diverse industrial cybersecurity technologies that are applied at different levels of a site-wide cybersecurity architecture. Scalable cybersecurity comes in many forms. Based on risk mitigation requirements, several diverse technology options are available for threat detection and prevention to help industrial operations meet their tolerance to risk.

Multiple layers of defense-in-depth (Figure 13 on page 44) for IIoT architectures include, but are not limited to:

- Education and Awareness Programs - training of OT personnel on established industrial security/safety policies and procedures including how to respond to a security incident.
- Physical – limit physical access to authorized personnel only: control room, areas, control panels, IACS devices – for example, locks, gates, biometrics.
- Network – restrictive access, hardening, traffic flow analysis, and traffic inspection.
- Computer Hardening – patch management program, white listing of IACS applications, restrict admin privileges, removal of unused applications/protocols/services, closing unnecessary logical ports, and protecting physical ports.
- Application – restrictive access, trusted communications, hardening, and monitoring.
- Device Hardening – trusted communications, change management with disaster recovery, data encryption, and restrictive access.
Defense-in-Depth

The CPwE Industrial Security Framework (Figure 14 on page 45) helps to provide a holistic, scalable, diverse, and incremental architectural best practices:

- Defense-in-Depth - architectural best practices for holistic and diverse threat detection and protection
- Alignment with industrial security standards
  - IEC 62443 - zones and conduits, availability, integrity, confidentiality.
  - NIST 800-82 - cybersecurity framework, identify, protect, detect, respond, and recover.
  - ICS-CERT - recommended practices for secure network architectures.
- Different Personas
  - OT - for example, Control System Engineers
  - Industrial IT - Control System Engineers (OT) in collaboration with IT Network Engineers, OT Engineers with IT skills, or IT with knowledge of OT requirements.
  - IT - for example, security architects in collaboration with OT.
- Scalability – IIoT smart device to IACS application, IIoT smart device to Level 3 Site Operations, IIoT smart device to on-premise analytics in the enterprise, and IIoT smart device to cloud-based applications.
Figure 14 - Holistic and Diverse Site-wide Cybersecurity - CPwE Industrial Security Framework
OT Persona - Holistic and Diverse Site-wide Cybersecurity

The information in this section corresponds to the items highlighted in tan in Figure 14 on page 45.

Industrial cybersecurity should be holistic and not treated as a bolt-on afterthought for new IIoT architectures. However, there are many solutions available to help industrial operations incrementally improve the cybersecurity stance for their legacy IIoT architectures.

- Hardening for Level 0...2 IACS devices - policies and procedures, physical measures, electronic measures, encrypted communications, trusted communications (CIP Security™).
- Zoning – segmenting devices and applications into functional and security zones, CPwE Logical Model, Layer 2/3 switch hierarchy with access control lists (ACLs), virtual local area networks (VLANs) for Layer 2 networks, Layer 3 network address translation (NAT) devices, and industrial firewalls.
- Port Security – network and IACS devices, both physical and electronic.
- Application Hardening – application access control, trusted communications with possible whitelisting.
- Industrial Firewall – zoning (access control for protection) of OEM skids/equipment/machines, zoning (access control for protection) of legacy networks with legacy IACS devices that have little to no security capabilities, and inspection of both IIoT and non-IIoT traffic.
- Status and Monitoring – inventory and asset management of both IACS and network devices.
Industrial IT Persona - Holistic and Diverse Site-wide Security

The information in this section corresponds to the items highlighted in blue in Figure 14 on page 45.

Multiple layers of defense-in-depth for IIoT architectures threat detection and prevention should include, but not limited to:

- **Computer Hardening** – patch management program, white listing of IACS applications, restrict admin privileges, removal of unused applications/protocols/services, closing unnecessary logical ports, and protecting physical ports.
- **Network Infrastructure** – hardening, access control (physical and electronic), and resiliency.
- **Wireless LAN (WLAN)**
  - Access Policy
    - Equipment SSID
    - Site Personnel SSID
    - Trusted Partners SSID
  - WPA2 with AES Encryption
  - Autonomous WLAN
    - Pre-Shared Key
    - 802.1X - (EAP-FAST)
  - Unified WLAN
    - 802.1X - (EAP-TLS)
    - CAPWAP DTLS
- **Remote Access Server** – for central policy enforcement for site, enterprise, and remote access.
- **Status and Monitoring** – health status of IACS and network devices.
IT Persona - Holistic and Diverse Site-wide Cybersecurity

The information in this section corresponds to the items highlighted in purple in Figure 14 on page 45.

Multiple layers of defense-in-depth for IIoT architectures threat detection and prevention should include, but not limited to:

- Network Access Control – centralized authentication, authorization and accounting (AAA), identity and mobility services, and software-defined segmentation.
- Site-wide Firewall Management – industrial firewalls and firewalls within Industrial Demilitarized Zone (IDMZ).
- Active Directory – genesis of identity and access control policy.
- Status and Monitoring – traffic flow analysis and traffic inspection.
- Site Firewalls - active/standby, inter-zone traffic segmentation, ACLS, IPS and IDS, VPN services, portal and remote desktop services proxy.
- IDMZ best practices – data brokers for reliable and secure communications, TLS proxy, application mirror, reverse proxy, remote desktop gateway server.

For more information on cybersecurity, see:

- Deploying Identity and Mobility Services within a Converged Plantwide Ethernet Architecture Design and Implementation Guide, publication ENET-TD008.
- Cloud Connectivity to a Converged Plantwide Ethernet Architecture Application Guide, publication ENET-TD017.
- Securely Traversing IACS Data Across the Industrial Demilitarized Zone Design and Implementation Guide, publication ENET-TD009.
- Deploying Industrial Firewalls within a Converged Plantwide Ethernet Architecture Design and Implementation Guide, publication ENET-TD002.
- Securing your PlantPAx system in The Connected Enterprise, publication PROCES-WP024.
- CIP Security with Rockwell Automation Products Application Technique, publication SECURE-AT001.
Chapter 3

Configuration Considerations for the Mining Smart Industry Architecture

This chapter describes the primary configuration considerations for the Mining Smart Industry Architecture (SIA) use cases. These use cases were architected, tested, and validated by Rockwell Automation, Panduit, Endress+Hauser, and Cisco.

End Device Configuration Considerations

The end devices in the Mining SIA are key components to the overall process. Each end device is critical for motor control, field I/O, and network connectivity. Programmable Automation Controllers (PAC) execute logic to control the process and continuously monitor the state of the end devices.

Rockwell Automation intelligent motor control portfolio consists of variable-frequency drives (VFDs) such as the PowerFlex 755, direct online starters (DOLs) such as the E300 Electronic Overload Relay.

The assets that are deployed in the Mining SIA test environment consist of network switches, PACs, PlantPAx Distributed Control System (DCS), Overload Relays, variable-frequency drives, Process Instrumentation, and Linking Devices.

Network Switches

Mine sites require reliable and robust network infrastructure to connect industrial automation and control system (IACS) processes and communicate to remote areas. To address this, the Mining SIA test environment design incorporated multiple EtherNet/IP topologies using the Stratix family of managed switches as the backbone. The Stratix 5400 Industrial-Managed Ethernet Switches were connected in a Redundant Star topology, while the Stratix 5700 Industrial-Managed Ethernet Switches are connected in a switch-level ring leveraging the DLR protocol. The Stratix 5700 switches provide Network Address Translation (NAT) capabilities to map IP addresses from the equipment-level to the higher-level site-wide network. The Stratix 5400 switches in the IACS provide Layer 2 and Layer 3 routing for multi-layer site-wide IACS network architecture and all-Gigabit ports for high network performance. The Stratix 5400 and 5700 also integrate into the Studio 5000 Logix Designer environment in order for the Logix controller to retain switch configuration as part of Automatic Device Configuration.
Programmable Automation Controller

The Programmable Automation Controller (PAC) is a powerful component in the architecture. The PAC is responsible for executing the program (ladder logic, function block, structured text, or sequential function charts) to control the processes. The PAC is also responsible for decisions based on the outputs of field devices such as level transmitters, flow transmitters, or weigh scales. ControlLogix® 5570 and 5580 Controllers offer increased capacity. This increase in capacity decreases the overall number of controllers in the IACS by consolidating more control strategies into one task.

In Mine applications, the ControlLogix 5570 controller can be used to deploy a Model Predictive Control (MPC) algorithm for a Ball Mill. The ControlLogix 5580 can be leveraged to introduce redundant control applications to improve the overall process efficiency. In addition, the ControlLogix 5580 Controllers offer an improved data exchange between the Levels 0...2 control and Level 3 Mine Site Operations layers of the Mining SIA.

E300 Electronic Overload Relays

Direct online starters (DOL) are used to control smaller ancillary loads that do not require the starting precision of a VFD on a conveyor or do not have the high system inertia that is exhibited in a crushing application. The E300 Electronic Overload Relay is responsible for starting and stopping the motor and to help protect it from thermal wear while providing meaningful diagnostics throughout the starting and run sequence.

PowerFlex 755T Variable Frequency Drives

The PowerFlex 755T portfolio of Variable Frequency Drives provides harmonic mitigation (PowerFlex 755TL), regeneration (PowerFlex 755TR), and a common bus solution (PowerFlex 755TM.) This portfolio helps customers increase IACS performance and decrease overall energy costs that are associated with a mining application. The PowerFlex 755T provides predictive maintenance to enhance the lifecycle and performance of the drive.

Process Instrumentation and Linking Devices

Process instrumentation and the associated protocol linking devices play an integral role in the overall mining process. Instrumentation from Endress+Hauser includes digital pressure transmitters, electromagnetic flowmeters, non-contact level transmitters, temperature transmitters, and Coriolis flowmeters. The process instrumentation use EtherNet/IP and several different linking devices such as HART, Foundation Fieldbus, and PROFIBUS PA to integrate into the overall Mining SIA test environment.
**Flex 5000 I/O**

The FLEX 5000™ I/O architecture allows for the integration of field wiring into the IACS. The FLEX 5000 I/O architecture has versatile input and output modules and spans many types of applications. The FLEX 5000 I/O architecture is also enabled with 1 Gb EtherNet/IP for high performance and multiple options for network connections. These options include Copper or Fiber media in a Linear, Star, DLR, or PRP topology.

Mining applications include vast amounts of field I/O from sensors and switches that are embedded within the concentration circuit. These types of connections, whether digital or analog, are easily terminated at the Flex 5000 module and integrated into the IACS.

**Integrated Display Thin Client**

To distribute and serve content through a plant or mine site, the VersaView® 5200 ThinManager® Thin Clients with integrated display are deployed. These Thin Clients are used for convenient access to information in remote mine operations and multiple clients throughout the site. Mine Operations can use the thin clients to view KPIs or shadow HMI applications.

**Premier Integration**

The use of pre-engineered and tested Add-on Profiles (AOPs) allows you to integrate motor control devices, network switches, and field I/O into the Logix controller more quickly and use common software to configure and program. The use of common software allows for easier configuration, device management, and increased availability of equipment.

In addition to the AOPs and Add-On Instructions (AOIs), a portion of Premier Integration that can be unlocked by the Logix controller is the concept of Automatic Device Configuration (ADC). ADC is the process of automatically uploading the end device configuration into the Logix controller and organizing the information based on device type and IP address. In case the end device (for example, E300 Overload Relay) fails, it can be replaced with a new unit. Once the controller sends a Forward Open request, it downloads the configuration data to the new E300 Overload Relay.
Automatic Device Configuration (ADC)

Mine site Operations teams are continuously looking for ways to increase equipment availability and improve machine/skid efficiency. Unscheduled downtime is a contributing factor to loss of productivity and decreased efficiency.

When a motor control device, such as a PowerFlex variable-frequency drive (VFD) is connected to a Logix processor on an EtherNet/IP network, the overall time that it takes to get the motor running again is reduced when leveraging Automatic Device Configuration (ADC). The Logix processor automatically updates the firmware and sends the configuration data to the PowerFlex VFD when it establishes a connection, saving valuable maintenance time. This update minimizes downtime and simplifies maintenance, allowing for quicker device replacement without extensive knowledge of the device required.

Controller Level Configuration Considerations

The controller is one of the key sources of all operational data within an IACS. The controller contains all device control, configuration, diagnostic, and information data associated to each controlled device. A typical solution that is deployed to a mining site contains multiple controllers that are distributed across the vast operational environment. Different minerals, environmental factors, recovery processes, and operations lead to numerous variations on the IACS requirements, which vary the requirements on the controller level of configurations.

This section raises several key items that must be evaluated during design, delivery, and maintenance of controller configurations of an IACS. These items are evaluated through the phases of a production lifecycle to maximize the site-wide mining capabilities.
Controller Characterization

The size of a controller required, in terms of memory and processing power, is defined by several items. Key items to note:

- Magnitude of the processing facility.
  - For example, 100,000 TPA versus 100,000,000 TPA.
- Complexity of process control.
  - For example, Discrete versus Continuous versus Batching Control.
- Amount of flexibility and configuration.
  - For example, application with fixed configuration versus application with significant configuration.
- Required speed of response.
  - For example, required IACS response time of 1 second versus 10 ms.
- Required availability of the IACS.
  - For example, high availability with multiple IACS component failures versus no fault tolerance IACS.
- Frequency and volume of communications.
  - For example, hundreds of remote devices, disparate

The larger, faster and more complicated the control required; the more processing power that is required, hence more controllers are required to meet the site operations. Determining the sizing requirements of not only the controller but also the PlantPAx® system is important. Not doing so can result in suboptimal performance and user experience.

The requirements that are identified determine the amount of equipment that can be safely and repeatably controlled by the controller. Using modular validated and tested standards that have been characterized to determine the sizing requirements makes this is a simple task. This process is simplified further when using the Integrated Architecture® Builder System Estimator Tool. This tool can essentially be used during proposal, design, and development stages to characterize the IACS correctly according to the required process.
Process Control Response Time

Determining the response time that is required for each process is a key design decision that must be made as part of the IACS operation. Different mining processes have different speeds of response that is required for control. Generally the control is discrete and relatively slow, for example, processes require a controlled response within 500 ms. There are faster acting speeds of responses that are required in certain applications, such as:

- PID loop Control for Control Valves, VSD Speed Control, etc.
- Coordinated Drive control, such as Master Follower Drive Torque applications and Multiple Coordinated Drive Positioning Control.
- Relatively fast digital processing devices, such as discrete motor positioning control with the use of a brake applications, resistor banks, and dynamic clutch control.

Failure to meet the required speed of response repeatably could be catastrophic. It is important to be aware of various configurations, from process input to process output, which could lead to delays or for the IACS to respond in another way than initially designed. Design decisions must be made to deliver repeatable scan time. The remainder of this section covers configuration options available to the control system engineer. Configuration options are summarized in the following figure.

Figure 15 - Potential Process Response Time Considerations
Device Response

Instrumentation monitoring and controlling the process has various capabilities, functions, and performance. Multiple factors could influence the designed operation and affect the instruments accuracy and reliability. Examples are factors such as process, environmental, and installation. Assuming the instrument has been installed and commissioned correctly with professional consultation, what could influence the devices response?

- Physical measuring capabilities of the instrument
- Filtering applied at the instrument
- Internal processing time, from process measurement to making the information available to the IACS
  - This could be on a control loop, such as 4-20mA, or available through networked communications such as EtherNet/IP.

The items that are listed previously are some of the potential delays that could influence the speed of response. Selection of the correct instrument to meet the requirements is critical. Fortunately, the current capabilities within the market more than meet the requirements of the mining industry and with technology constantly improving, these capabilities can only be expected to continue to improve. The item to be aware of is, as technological advancement progresses and more configuration is available to address multiple use cases, there could be delays that are introduced in certain configurations that have a negative impact on the overall operations. Make sure that you are aware of your requirements and can maintain them through the configuration of the thousands of assets across the enterprise.

Communicated to/from the Controller

Communication with the controller can be done in several ways. If we had a hardwired setup, communication would go through an input module with the input module being polled by the controller. The controller could either be polling through the backplane (if local IO) or polling through a communication device through the network. If we had a networked communication to the device, the controller would be polling through a communication device.

The Input/Output (I/O) Hardware Module (for example, 1756-IF16H or 1756-OF8H) would have various configurations that could be useful for the implementation. These configuration options are similar to the items discussed in the previous section, Device Response on page 55. The difference is that typically the Module applies to multiple process signals, for example, 16 inputs or 8 outputs from the previous example, where typically instrumentation is focused on one or specific processes that it is monitoring.
The size and frequency of the information that is periodically communicated between the device and the controller has an impact on utilization of all components that are involved in this data exchange. See Figure 16 for a setup example. By changing the Request Packet Interval (RPI) of the information that is required from the Instrument by halving the time, this change doubles the required information that is transferred, requiring the controller, switch, and device to transfer the same amount of data twice as often as it initially required.

**Figure 16 - Controller, Industrial Ethernet Switch, Endress+Hauser Device**

By setting data collection to as fast as physically possible, all information signals get back to the controller as fast as possible. For example, if the RPI is set to 10 ms but is only used every 500 ms, we are providing 50 updates before it is used in the code, this is an overdesign. The best fit depends on the operation and IACS. The recommendation is that the RPI is set twice as fast as the task that is logically required, this applies to all inputs/outputs of the module not just one.

For more information, see PlantPAx Distributed Control System, publication PROCES-RM001-EN-P.

There are exceptions to this configuration, for example, the PID instruction recommends that the input is updated 10 times faster than the loop update time but working with the RPI being set to the preceding recommendation carries for 99% of applications.

More information can be found in Knowledgebase article 57174 for this example.

Changing the RPI could influence the throughput of your operation. The ideal state to be in for achieving safe and repeatable logical execution is to set the RPI with primary consideration for optimal control and maximized network throughput with no wasted communications or dropped packets.
Selecting between Direct and Optimized connections can also impact operations. Direct connection messaging occurs at a cyclic rate that is specified by the RPI during configuration. A rack-optimized connection is a grouping of data from multiple I/O modules into one block of data that is sent over one connection at the same data rate.

Integrated Architecture Builder (IAB) is an excellent tool to verify the ideal IACS state by loading in the configuration of the entire IACS. By applying the application software devices, control strategies, and software versions, IAB confirms utilization of each component within the IACS, providing guidance where required. Within the tool, there are assumptions that are made to ensure an estimate can be achieved. For more information, see Integrated Architecture Builder.

**Controller Tasks**

A Logix 5000™ controller supports multiple tasks to schedule and prioritize the running of your programs, which are based on specific criteria. These tasks balance the processing time of the controller and provide flexibility in structuring the controller execution to suit the application.

With the flexibility comes large amounts of design decisions to be made to create a control that has excellent reliability, is safe, and repeatable. Correct design structures the execution in such a way that provides a more predictable scan time of logic. The logic still must be written in such a way that will achieve the required speed to response. No matter how well the logic is written, if the tasks are being called and executed in a manner that does not enable the logic to perform as required then the IACS will fail.

Key items to note about Controller Tasks:
- The controller runs only one task at one time.
- Another task can interrupt a task that is running and take control.
- In any given task, only one program runs at one time.

There are several different tasks, configuration options, and recommendations that are available. For more information, see these manuals:
- Logix 5000 Controllers Tasks, Programs, and Routines, publication 1756-PM005-EN-P.
- Logix5000 Controllers Design Considerations, publication 1756-RM094-EN-P.

The controller operating system is a preemptive, multitasking system that is IEC 61131-3 compliant. ControlLogix and CompactLogix™ controllers define the schedule and priority of how programs are executed by using tasks.
Although a project can contain multiple tasks, the controller executes only one task at a time. If a periodic task or event task being triggered while another task is executing, the priority of each task determines the execution order. Make sure that your periodic task priorities are unique. We recommend that the total execution time of all tasks is less than half the execution time of the lowest priority task or slowest task.

Controller Utilization

Controller Utilization has been covered from a characterization and an estimation point of view in the previous sections. This section covers real-time performance. It is expected that each controller that is deployed validates its controller utilization after development and implementation. This validation helps to verify that the controller utilization complies with PlantPAx recommendations.

There are several ways to monitor the utilization of the controller. Monitoring can be done inside the Studio 5000 Logix Designer environment, but this environment tends to be a view that focuses on one item at a time.

The Studio 5000® Task Monitor Tool provides insight into multiple components within the controller environment. The tool provides an overview of the activities that a Logix 5000 controller is executing, including:

- User Tasks
- Controller Performance
- Connections available and used
- Message communications
- Packet and Communication scan performance
- Communication Module Analysis

Figure 17 on page 59 is an example of the Performance tab that can be observed on the running controller. Each tab is full of information that can support analyzing the performance further. There are also built-in instructions that can be added for continuously monitoring controller utilization and performance within the logic if necessary.
Additional Tips

Items that are covered in this section provide insight into fundamental components of control. With typical mining applications and the power of the existing technologies in Rockwell Automation, these fundamentals aren’t apparent when an IACS is designed well. These fundamentals are important to be aware of, particularly when troubleshooting, evaluating expansion, and expanding. Incorrect configuration can lead to unnecessary IACS loading that leads to drops in expected performance and user experience.

Another important point to mention, is that some high-speed IO processing applications can be done through DeviceLogix™ on Motor Controllers, such as E300s or VSDs. The advantage is that high-speed equipment control is done on the end device without loading the network, communication devices, or the controller. Adequate design information and control must be provided to achieve simple fault finding and maintenance procedures when needed. For example, if an input sensor fails, there must be enough diagnostics and control to inform operations and for them to recover safely.

Consolidating the requirements of each process into defined requirements for each controller is one of the first steps in accurately defining the control that is required for the IACS. Loading these requirements into the PlantPAx System Estimator (PSE) allows for feedback on whether the proposed designed IACS is successful.
Specifying Devices to be Controlled per Controller

A key step that must be done during the initial stages of site design, is to determine how the site is to be zoned into areas of control and segmenting those areas into controllers. It is important to note, this segmentation is not always a physical location as utilities could be stored centrally but distributed throughout the site. These zoned areas clarify the processes that are associated within each area and in turn define the control response that is required for a proposed controller. Loading this information into the IAB PSE would confirm utilization of all system components, validating the proposed design from a performance standpoint.

It is important, as far as possible, to keep interdependent systems and subsystems within the same controller. In a Ball Mill example, Drive Control, Lubrication, Heating, Cooling, etc. are all logically located within the same controller. This simplifies logical coding throughout the controller.

If it is required to segment these systems, it is not an issue. Confirming the required tags are propagated between controllers is achievable with Controller-to-Controller Communications.

Controller-to-Controller Communications

There are two ways to configure communication between controllers:

- Produced/consumed tags
- Messages

Whichever method is used, we recommend that you use an array or user-defined tag. Also, produce/consumed tags cannot be edited online. Make sure to include extra capacity that can be populated by mapping logic so additional information can be shared as needed without requiring a download.

Usually, when critical interlocking is required to be done across Controllers, the recommendation is that Produced/Consumed Tags are used. As interlocking and protecting of equipment and process is required to respond within a certain amount of time, Produced/Consumed communications meet this requirement. Remember to consider the limitation on bandwidth for larger Produce/Consume tags, and the use of connections.

When non-critical information is required, for example, a period updating of informational data, the recommendation is usually to use Messaging.

For more information, see:

PlantPAx Distributed Control System, publication PROCES-RM001-EN-P

Logix 5000 Controllers Produced and Consumed Tags, publication 1756-PM011
**Unplanned Outages**

One thing to consider when designing a site is the maintenance procedures that are conducted. In doing these activities, it could lead to several scenarios that could affect various areas of the site. For example, isolation of electrical supply to a section of the site would drop power to a controller. If that controller contains control of critical equipment, such as Fire Water Control, it could have unforeseen consequences and cause dangerous situations.

Investigate points of failure, for example, Instrumentation, I/O Modules, Controller Hardware, Networking, Servers, and Operator Control Stations. Where high availability is required to achieve prevention of the point of failure, there are many options available to achieve this requirement across the IACS not only for high availability but also for redundancy.

**States of Operation, Command Sources, and Areas of Control**

Within any mining operation, equipment can be controlled in a few ways. Equipment could be controlled from multiple or single points of control depending on the design and operation requirements. Standardizing these terms across a site is important for achieving operations are more safe and have excellent availability. This section aims to provide some guidance for several items.

**States of Operation**

This typically refers to an operational state of the equipment. For example, a stacker/reclaimer:

- Stack - Chevron
- Stack - Cone Shell
- Reclaim
- Travel - Manual
- Travel - Autonomous
- Position

These operational states each have their limitations to be operated from certain command sources or area of control. For example, the Stacker/Reclaimer can only Travel manually when controlled locally on the equipment in operator command source.
Command Sources

A command source function is built into software library objects that control an output, this output could be a device that is interfaced through IO, fieldbus communications, or another control module within the IACS. This command source serves several functions, primarily:

- Manage the transitions between the selected sources that is based on user and application requests
- Enforce prioritization between sources
- Allow options to lock sources where applicable

This function is key to standardize where commands are being propagated from, the corresponding source could also have different operation (for example, in Hand.) The Command Source resolves where the command should be accepted from and what source is in control at a time. Typical sources that you can expect to be included with this functionality:

- Hand
- Out of Service
- Maintenance
- External
- Operator
- Program

When in Operator, commands are being issued through the SCADA. There are functions that are built into the SCADA that provide security based on Role, User Qualifications, and Workstation location. Confirming the Object can receive commands only from certain sources at a time simplifies operations, maintenance, and standardization.

Parent/Child relationships with ownership also add structure to the code and are simplified with the command source. For example, with a parent object in Operator Source and its Children are in Program Source, a command that is issued through the SCADA to the parent would, assuming this command would lead to a command being issued from the parent to the child, require the child command to be issued a program command. In this example, the parent’s source is the SCADA and the child’s source is the Program.
Areas of Control

Within the Mining SIA, there are different operator interfaces. Typically interfaces are through the SCADA and local operator stations. The SCADA would typically be a distributed system across the site where it can be controlled and restricted through role-based security and through area-based security.

Operator stations tend to vary. Historically, on existing sites, this interface may be push-button operated, or it could be a standalone HMI such as a PanelView™ terminal. Multiple interfaces active and controlling the IACS at any point in time can cause unsafe operating conditions. To help prevent this from happening, it is good to have a clear model of what location is in control at any point in time to simplify operations.

Today technology exists that simplifies this problem. Applying a consistent standard across the enterprise is critical for mitigating confusion and making operations more safe.

What You Should Expect Your Library to Have

We have covered the need for standardization, modular design, and interoperability of a system. This section covers additional requirements from the software library that modularly control the processes across your enterprise.

A software library is a predefined set of control, historization, and visualization elements that enable you to assemble large applications with proven strategies, rich functionality, and known performance. With the library, you can rapidly bring your system online in a safe, more reliable, and repeatable manor with a focus on day to day operations and the capability of simplified expansion.

These libraries should be built with consideration given to international standards such as Control System Programming, Enterprise and Control Connectivity, Human Machine Interface, Abnormal Situation Management, Alarm Management, and Life-Cycle Management at the least.

These libraries must be able to justify their value in each phase of the production lifecycle (see Figure 18 on page 64.) Aligned the value to the customer value drivers:

- Faster Time to Market
- Lower Total Cost of Ownership
- Improved asset utilization
- Enterprise Risk Management
Figure 18 - Production Lifecycle

Reducing Risk and Creating Value Throughout Your Production Lifecycle

**Faster Time to Market**
- Vast library of objects, functions, and strategies.
- Simple method to generate application software rapidly.
- Virtualization of Object and Simulation Capabilities, which leads to overall scenario-based testing.

**Lower Total Cost of Ownership**
- Upgrade and Migration Paths.
- Complete and holistic Technical Support.
- Simple path to market.

**Improved Asset Utilization**
- Simplified for you to ease fault finding.
- Insight for where to focus your efforts.
- Simple to implement changes.
- Stabilized Process that you can add Advanced Process Control and Optimization on top of.
Enterprise Risk Management

- Tested, Documented, Supported components with known performance.
- Implementation methods that have been tried and tested.

With the preceding in mind, it is important to make sure that the selected library meets not only the requirements noted, but also the requirements of your process applications. Rockwell Automation has a substantial library that meets the requirements in this document. For more information, see these manuals and your local Rockwell Automation representative.

- Rockwell Automation Library of Process Objects, publication PROCES-RM002
- Rockwell Automation Library of Electrical Protection Devices, publication PROCES-RM011
- Rockwell Automation Library of Process Objects EtherNet/IP Instrumentation, publication PROCES-RM012
- Knowledgebase article 1083826

Additional Tips

When to Use an Object

Within a device library, there are device functions that overlap with others. A simple way to decide if adding an object adds value, is to decide if adding functionality still allows the solution to meet the control objectives. Both operational and performance requirements must be considered.

For example, a Motor object has a few processing signals that it interfaces with and controls to operate effectively, such as an output for Forward, an Output for Reverse direction, and an input for Run Feedback of Forward and of Reverse. These two Digital Inputs and two Digital Outputs have the configuration, alarming, and functionality that is required to control the motor. In the motor object, there is no need to add in an additional object (2 x Digital Inputs and 2 x Digital Output Objects) as there would be no value added for a typical hardwire operation and would probably complicate the solution from an operational, maintenance, and migration point of view.

Where an Electronic Overload Relay is used, for example an E300, an additional E300 Object would provide additional diagnostics, simplified fault finding, and programmatic interoperability. In this case, adding an additional library Object is a simple decision.

With Inputs and Outputs for Digital devices that are hard wired, generally if the device is in the field then you require all functions (for example, filtering or virtualization) of a Digital Input and Output Object to integrate it into the IACS. If a device is hardwired inside a substation or MCC, then usually these additional features are not required.
Another point to note is where a signal will cause equipment not to be able to operate, whether you simulate the signal in the software or not, for example, an electrically hardwired protection on a motor starter circuit. It is important to visualize this point for the purpose of fault finding but not necessary to add an object for it.

**Considering Low Flow Conditions**

When developing the software application, it is typically designed for a throughput. It is important to consider that if the throughput setpoint were to be lowered, that the software would still be able to control as desired. There will be mechanical equipment limitations to this setpoint, and the software should reflect these limits. Low flow conditions could be experienced during startup, commissioning of refurbished equipment, or periodic maintenance activities on the equipment that will lead to low flow conditions. The more independent operations can be, the higher utilization of that equipment with a corresponding lower cost of ownership.

**Recovery Conditions**

Inevitably on every site something will go wrong and you will need to recover from this undesired state. This could be due to a power interruption from the energy supplier to a mechanical failure of equipment within the process. It is important to make sure that your control is versatile enough to recover from this type of failure.

There are two scenarios that are sometimes overlooked when developing software for the enterprise. The first is a power interruption, when power returns what do you expect to happen? Do you expect the site to resume its previous state automatically? Do you expect the process to be restarted manually by operations? These two options and anything in-between are possible currently. It is important to be aware of any hazardous operations that must be accounted for in order to ensure any form of IACS is done in a safe state.

The second is similar but probably not as catastrophic, depending on your specific external factors, but probably more likely to occur. That is a sequence, procedure, or phase failing to complete successfully. This failure could be due to numerous reasons and causes. Recovery could be required due to cost of chemicals, additives, or product that could potentially be lost if we dump it and start again, complexity of recovery process, and potentially the required speed for recovery. There are design principles that are required to be implemented that can allow for a safe, successful recovery. These principals must be well thought out and incorporated into the overall design of operation, maintenance, and expansion of the process.
Another useful component to leverage is the use of fault routines, which is a function that can be used to achieve the desired control.

For more information, see:
- Logix 5000 Controllers Major, Minor, and I/O Faults, publication 1756-PM014

**HMI Configuration Considerations**

The Supervisory Control and Data Acquisition (SCADA) system is a contextualized and visualized portal into the array of data that is collected from the operation. This data must be contextualized in such a way to verify that effective decisions can be made with that data. The level of autonomy within an operation will define the level of decision that is made from the SCADA.

High levels of autonomy with Advanced Process Control (APC) and well contextualized visualization notify centralized operations of abnormal situations that must be managed accordingly by operations. Lower levels of autonomy may not even have an HMI, status could still be indicated locally through lamps or light-emitting diodes (LEDs.)

This section focuses on important concepts that are required to confirm that the HMI is configured for effective usage for the production lifecycle of the operation. This covers three major questions:
- What Application and Infrastructure are required?
- What design choices are to be made around the HMI?
- How to correctly size, configure, and generate the HMI?

These items are addressed in the sections that follow. For more information, see:
- PlantPAx Distributed Control System Selection Guide, publication PROCES-SG001.
- FactoryTalk View SE Distributed System Design Considerations, publication AID 32549.
- FactoryTalk View Site Edition Tips and Best Practices TOC, publication AID 37110.
Chapter 3  Configuration Considerations for the Mining Smart Industry Architecture

**Application and Infrastructure**

Within FactoryTalk® View applications (part of PlantPAx), there are typically three key types of applications. Most sites and operations deploy Network Distributed Applications. These applications can be expanded to large architectures where the ability to enable server redundancy is simple through configuration. It is important to configure the initial application in such a way to enable this.

Accessing the runtime environment can be done throughout the network, using either Thick or Thin Clients. Combining the Runtime Client with ThinManager, you can tailor the contextualized data available securely by Device, User, and Location.

**Network Stability and Outages**

Regardless of the application that is selected, a stable network is required. If network interruptions are experienced or expected to occur regularly and production is required to continue with a local HMI interface, this needs to be accounted for in the design. For example, if a Stacker/Reclaimer uses wireless communications for control, when wind blows up metallic particles into the air this can cause communication interruptions and even outages. In this case, it could be required to have a local/network station that is positioned on the critical equipment to verify that an HMI is available if required by operations and that operations can continue without remote control or operations. The same protection could be required for any type of failure within the Mining SIA, make sure that there are provisions as required.

**Server Redundancy**

Another consideration is server redundancy. This consideration is a combination of software and hardware. With software, this is referring to Data and HMI server redundancy within the FactoryTalk environment. Determining if software redundancy is needed is determined by the criticality of the system. In general, every site requires it, the potential loss of production far outweighs the cost of an additional server. With the added requirement of updating your Windows operating system, this often requires a restart to apply the changes. See the next section for further information.

The location of the secondary server (Data and/or HMI) becomes the question of hardware redundancy. A common consideration is to locate the secondary server at another physical location. If the primary server location goes offline, then the secondary location could be used to run operations. There are a couple of things to consider with this decision.

- The performance of the connection between these two sites. If the connection does not meet the requirements of throughput and latency, user experience will be greatly impacted.
- The second server must stay online if the network coverage is offline at the primary location to have redundancy.
Configuration Considerations for the Mining Smart Industry Architecture

Chapter 3

• If there is a critical network switch located at the primary location and it goes offline, the secondary network switch must come online to have redundancy.

Server hardware redundancy is another consideration. Hardware redundancy is handled at or below the operating system level of the personal computer. Failover occurs when a hardware component fails, such as a motherboard, hard disk, Ethernet card, or input device. This type of redundancy is not directly related to the FactoryTalk application software. Typically, high availability and redundancy types of solutions require virtual environments in which application software would run. For more information, see The Industrial Data Center on page 38.

Incremental backups are another option to examine. Overall there are many different choices that can be made to achieve resilience of the architecture against faults. It is important to take a holistic system analysis approach to verify that the requirements are clearly defined to meet the needs of operations. Adding redundancy without considering all aspects of the system could result in limited impact of the implemented redundancy.

Rockwell Automation Qualification of Microsoft Updates

Rockwell Automation has a dedicated website for informing its customers on Microsoft® Updates that it has qualified. This section provides some background for the need. This website can be accessed through the following link:

Microsoft Patch Qualifications,
https://www.rockwellautomation.com/ms-patch-qualification/start.htm

Microsoft releases a range of security updates, operating system and other software updates. Rockwell Automation qualifies certain Microsoft updates for software that impacts Rockwell Automation software products.

It is recommended that you implement a controlled system suitable for your application and environment. It is recommended that Microsoft updates are not applied or installed until:

• The Microsoft update is Fully Qualified by Rockwell Automation
• The results of our testing have been published and reviewed.

“Fully Qualified” means that Rockwell Automation has tested the Microsoft updates with the primary functional areas of the relevant Rockwell Software® products. When completed, test results that show the areas that are tested and will be posted for your review.

Rockwell qualifies Microsoft updates for the Microsoft operating systems, Microsoft Offices Products, Internet Explorer, and Microsoft SQL Server products within a short time of the release of the Microsoft update but generally qualify Microsoft updates denoted as “Critical” with first testing priority.
Before implementing any Fully Qualified Microsoft updates, verify them on a non-production system, or when the facility is non-active, to confirm that there are no unexpected results or side effects.

**Mining Application Expansion**

Improvements in technology, expansion of equipment added to a Mining Application, or a phased approach of bringing the site online are examples of scenarios that could lead to the need for additional infrastructure components to meet the mining application requirements. If the initial requirements had not been structured to enable this expansion, then this could be a significant task.

Placement of the FactoryTalk Directory should be on an independent server with high availability. There is no redundancy configuration for a FactoryTalk Directory. Avoid placement of the directory on a Primary or Secondary server.

Each server should be placed in its own area. By doing so, every tag name on a graphic display has tag address syntax that directs FactoryTalk Live Data to the exact server containing the required data. (For example, \{/Area1::Topic1.Tag1\}) This improves IACS performance and stability.

**Figure 19 - Sample Server Structure**

Modification of this configuration at a later stage requires rework, which can be avoided if done correctly from the beginning. Additional information can be gathered from the following manual:

FactoryTalk View SE Distributed System Design Considerations, publication AID-32549.
**Network Distributed Application**

A network distributed application consists of a FactoryTalk Network Directory, one or more areas, one HMI server (could be redundant) per area, one or more data servers (could be redundant), and HMI project components such as graphic displays, HMI tags, and data log models. To develop a network distributed application, you create an application in FactoryTalk View Studio, add an HMI server to it, and then create the HMI project components.

There is no limit to the number of FactoryTalk applications that can be hosted by one FactoryTalk Directory (FTD.) The recommendation is to host no more than one running, or active, FactoryTalk View SE distributed application in a single FTD. Hosting multiple active FactoryTalk View SE distributed applications in one FTD can adversely impact the resources of the FTD itself.

This type of application allows client/server architecture (multiple client and server computers), allows you to have multiple HMI servers (local/remote), multiple clients (local/remote), and have your HMI servers be redundant. You can also have data server redundancy (local/remote) and have them on remote computers.

In short, the software programs behind a network distributed application - the FactoryTalk Network Directory, HMI servers, HMI clients, and data servers - can be on different computers on the network. However, all computers participating in a network distributed application must point at the same Network Directory.

**Figure 20 - Network Distributed Application**
Network Station Application

A network station application consists of:

- A FactoryTalk Network Directory
- Zero or multiple areas
- An HMI server
- At least one data server
- HMI project components such as graphic displays, HMI tags, and data log models.
- One HMI Client on the same computer. You cannot have a remote client.

To develop a network station application, you create an application in FactoryTalk View Studio, add an HMI server to it, and then create the HMI project components. The FactoryTalk Directory Server, the FactoryTalk Linx data server, and the OPC data servers can be on remote computers.

Up to 20 active FactoryTalk View SE network station applications are supported in a FactoryTalk directory.

This type of application allows client/server architecture as well, but you can only have one HMI server, but multiple local clients. This is a local application, but it can connect to a network directory, meaning it is a local application that can access data from remote computers, including FactoryTalk Historian, and FactoryTalk Transaction Manager.

In short, the HMI server and the HMI client are the software programs behind a network station application that must be on the same computer. The FactoryTalk Directory Server, the FactoryTalk Linx data server, and the OPC data servers can be on remote computers.

HMI redundancy is not supported in this application type, however, data server redundancy is supported. From FactoryTalk View SE 8.00, the application can be edited from any remote personal computer that is a part of the same FactoryTalk Directory with FactoryTalk View Studio Installed.
Local Station Application

In a local station application, also called a standalone application, all application components are on one computer. There is only one HMI server, which is created when you create the application, and the only area is the root area at the application icon. You cannot create additional areas.

This is a purely local application. In this application, all servers and clients run on one computer. There is no remote connectivity. In short, the software programs behind a local station application, the FactoryTalk Local Directory, the HMI server, the HMI client, and the FactoryTalk Linx data server, must be on the same computer. Only OPC data servers can reside on remote computers.

This application can be edited from the HMI server, or moved to a remote PC with FactoryTalk View Studio. Once modifications are made, it must be moved back to the HMI server.
Designing the HMI

The Mining SIA revolves, in part, around analyzing mine operations data and combining it with business data to create enterprise intelligence. This starts with focusing on the site-wide architecture by presenting operators with the information they need to effectively and efficiently keep operations moving.

Providing the right information and context to operations can aid in the ability to detect and respond to abnormal situations and simplify common tasks. A properly designed HMI can decrease downtime and improve yield, product quality, and productivity. Providing operators the information they need in the right context enables the best decision-making. For example:

- Displays designed using a specific color palette help the operator identify the most important information that may require immediate attention, such as alarms.
- Additional context on how critical parameters are changing, and whether they are within a desirable range, helps operators make better decisions.

Process HMI Style Guide, publication PROCES-WP023, provides guidelines for HMI design and implementation that are aligned with the industry standard. While it applies to general HMI development, it was written with FactoryTalk View SE and PlantPAx System applications in mind. This complements Human Machine Interfaces for Distributed Control Systems, publication PROCES-WP016, which covers important principles for designing HMI based on the industry standard ANSI/ISA-101.01-2015 (Human Machine Interfaces for Process Automation).

ISA 101.01 defines specifics of the HMI design process: an HMI philosophy, HMI style guide, and HMI toolkit.
• The HMI philosophy provides independent or platform-specific guiding principles for HMI design at your site. Clarifies the focus of the needs of the users and defines the requirements for the implementers. The focus is often not simplified Pipe and Instrumentation Diagrams (P&ID).

• The HMI style guide uses the guiding principles and concepts that are defined by the HMI philosophy to provide implementation and guidance.

• The HMI toolkit includes platform-specific graphical systems and HMI elements that can be used to implement the HMI style guide.

Process HMI Style Guide, publication PROCES.WP023, can assist you in the implementation of ISA 101.01 in your application by providing reusable guidelines that follow standards as a starting point for your own HMI Style Guide. This can be further simplified by leveraging the Rockwell Automation Mining Solution (part of the Mining SIA) as your HMI toolkit for implementation.

Within the referenced Style Guide, there is significant information that will aid in the design process. Security is also covered in this document but highlighted in the next section as it is a critical part the overall success and effectiveness of the system.

Security Configuration Considerations

Controls must be in place to enable authorized security interaction with the Mining SIA. These controls should provide a visual indication when users are restricted due to security. This visual indication may be the same as the indication used when users are restricted due to other reasons.

Role-based Security

Role-based security gives users access to controls and data based on their job role. Examples of job roles include operator, maintenance technician, and engineer; however, each site is different and may have different job roles.

In role-based security, a Maintenance Tech may have access to different controls and data that an Operator has.

Controls that are disabled because of security should have a consistent ‘disabled’ appearance that differs from the corresponding ‘enabled’ appearance. The disabled control should be grayscale and have a lighter foreground color than the enabled control.

User Qualifications

In larger sites, users may only have access to the IACS in the areas where they work. For example, operators may be allowed to operate equipment in one area of the site, but not in another area of the site. This qualification is sometimes referred to as Area-Based Security.
Workstation Location

In larger PlantPAx DCS applications with multiple HMI workstations, equipment operation can be restricted to certain workstations. An example of this is ‘Line of Sight Control’ where the operator’s workstation is within site of the equipment that the operator is controlling.

What to Integrate into DCS

Historically, the HMI has been the single source of information for operations. All information that anyone wanted to see, interact with and analyze needed to be accessible from the HMI. Real time or historical. This tended to become an engineering effort to interact with multiple standalone devices to provide the required system interaction that was needed, often the need for this information is focused on initially and then forgotten about.

This brings up two important components. First, periodically evaluate the HMI to be sure needs are being met. This enables continuous improvement of components core to operations. These incremental improvements should be simple to implement and their effect measurable on the operation.

Second, integrate components that are to be used for control or historization into the DCS. If a device, system, or platform is to be used for informational decision making only by operations and it has a portal to its contextualized data, for example a webpage, then it is probably best to leverage off that webpage. You can navigate to that webpage in a number of ways, through the HMI, through the information portal, but importantly raw data doesn’t need to be read out of the device to a controller / HMI. That data is manipulated to recreate contextualized information that serves the same function as the existing webpage. Just because something has a webpage, this doesn’t mean that it meets the requirements. The advancement of interoperability within IACS has simplified the process of integrating components, but it does not make this point redundant.

With these items discussed, the need of being able to see contextualized information for different roles within the organization is still required. The mechanism for which this information is supplied does not have to be the HMI. Each role within the organization will need to analyze the same common data for their requirements, verifying that the right information is available to the right person at the right time and in the context they require.

Project Layout

There are many design and configuration decisions that must be made to bring an IACS online. These decisions lead to a system that meets the requirements and performs at an expected performance level are vital to the systems success. Rockwell Automation has comprehensive guides, tools, and manuals to simplify this process. The system that follows this implementation technique is deemed a PlantPAx system.
PlantPAx System Scope

The PlantPAx system provides a modern approach to distributed control. The system shares common technology (Integrated Architecture system) with all other IACS disciplines in the site. This approach creates an information flow across the site for optimization opportunities and enables a Connected Enterprise.

Our scalable platform provides you with the flexibility to implement a system appropriate for your application. Figure 23 shows the documents that are available to help design and implement your system requirements. The starting point in the process can be found in this manual:

PlantPAx Distributed Control System Selection Guide, publication PROCES-SG001.

Figure 23 - PlantPAx System Implementation and Documentation Strategy

- Define and Procure - Helps you understand the elements of the PlantPAx system to make sure that you buy the proper components.
- Install - Provides direction on how to install the PlantPAx system.
- Prep - Provides guidance on how to get started and learn the best practices to follow before you develop your application.
- Develop - Describes the actions and libraries necessary to construct your application that resides on the PlantPAx system.
- Operate – Provides guidance on how to verify and maintain your systems for operation of your site.
Chapter 3  Configuration Considerations for the Mining Smart Industry Architecture

Configuring the HMI

After the establishment of the applicable infrastructure, selection of the HMI philosophy, HMI style guide, and HMI toolkit, you are now able to bring the application to life. There are starting HMI templates, combined with security, that drastically speed up development.

More information about configuring the template and common configuration considerations can be found in this manual:

- Library of Process Objects: Configuration and Usage, publication PROCES-RM002.

Once the structure of the HMI project is established, further configuration is required to achieve a usable application. This can be done through:

- Configuration of each object through the HMI, covered in the PROCES-RM002 manual.
- Bulk Code Generation out of Application Code Manager (ACM).

Both methods leverage off the same global objects contained within your library. The first one is done by hand, the second leverages off the same principles except that it can generate all objects for a project that is configured in ACM.

Application Code Manager

Application Code Manager is a tool that enables more efficient project development with libraries of reusable code. You can create modular objects with customizable configuration parameters using the reusable content, allowing you to specify the pertinent information on how the object is used in a project. Application Code Manager creates not only the coding for the modular object but also the associated visualization, historical, and alarming elements.

Make sure when selecting a software standard that it leverages off the full capabilities of ACM. This selection not only saves significant hours of development time, but also everything that is generated has a precision that cannot be achieved by hand. Achieving the structural standardized modular code that is desired on every site. Typical Features of ACM include:

- Engineering Design Tool
  - Easily create and configure objects in bulk using reusable libraries of code to increase application development, without any additional programming.
- Auto Content Generation
  - Create controller code for the modular object and the associated visualization, historical, and alarming data to help build projects more efficiently.
- Reusable Library Objects
  - Easily instantiate complex objects into a new or an existing project.
- Standardize Systems
- Use application-focused libraries of code, including PlantPAx Process Object Libraries, Machine/Skid Builder, and Rockwell Automation Mining Solution Libraries, to save time and more easily standardize your systems.

For more information on ACM, see the Library Designer and Library Object Manager User Manual, publication LOGIX-UM006.

**Historian Configuration Considerations**

**Overview**

FactoryTalk® Historian is a product that is formed by a strategic partnership with OSIsoft that started in 2006. This combined product offers Historian capability with the FactoryTalk platform. With FactoryTalk Historian the capability to collect data from any FactoryTalk enabled application and to contextualize the information into assets. These assets can have calculations that document the behavior of the asset over time.

**FactoryTalk Historian Components**

The following components constitute a FactoryTalk Historian System.

<table>
<thead>
<tr>
<th>Component</th>
<th>Quantity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network FactoryTalk Directory Server (FTD)</td>
<td>1</td>
</tr>
<tr>
<td>FactoryTalk Historian Server (FTH Data Archive DA)</td>
<td>1</td>
</tr>
<tr>
<td>FactoryTalk Asset Framework Server (FTH AF)</td>
<td>1</td>
</tr>
<tr>
<td>SQL Server (Express or Standard)</td>
<td>1</td>
</tr>
<tr>
<td>FactoryTalk Historian Live Data Interfaces (FTLD)</td>
<td>1+</td>
</tr>
<tr>
<td>FactoryTalk LiveData Servers (FTL)</td>
<td>1+</td>
</tr>
</tbody>
</table>

**Configurations**

There are three common configurations of FactoryTalk Historian. Each one has advantaged and limitations. These configurations allow for the system to grow from a small (1) system to a larger system (3).

1. All on one computer (Good)
2. Two computer configurations (Better)
3. Three computer configurations (Best)
**All on One Computer**

This configuration has all components listed installed on one computer. Typically, the FactoryTalk Directory is installed on a separate computer but for this configuration it can be installed on one computer.

This configuration has some limitations. The total number of tags is lower and it is recommended to stay at or below 5000 tags. Also, the ability to buffer data from the interface is not supported on the historian server. So, if the historian is shut down then there is no data collection thus the loss of new data.

This configuration has limitations such as resource conflicts and no client-server autonomy.

For more information on this configuration, see Knowledgebase article 62869, FactoryTalk Historian SE and FactoryTalk VantagePoint on a Single Host Computer.

**Two Computer Configuration**

Two computers would be the next best configuration. This configuration has the FactoryTalk LiveData Interface node transferred to the second computer.

A Buffer sub subsystem can be used. The configuration allows for the Historian to be taken down and data collection does not stop. The event data is buffered on the second computer and forwarded to the Historian when it is available. This feature is often call “Store and Forward”.

This brings up the ratings of the FactoryTalk LiveData Interface node. This is not a redundant interface node.

- Tag Count on Interface - 75,000
- Tags on scan - 50,000 events/sec on one Interface

This configuration does not limit or reduce the resource conflicts on client-server autonomy on the Historian server.

**Three Computer Configuration**

This configuration has the best performance and scalability. It is the easiest to scale data collection and add the capability of “minimal data loss.”

This changes the design to have the FactoryTalk Historian on one computer, the FactoryTalk LiveData Interface on a second and the remainder of the components on a third.

With this configuration the historian has no resource conflicts with any other application, and clients are all autonomous.

Data collection can be buffered allowing for updates to be done without interruption of new event data.
Backups can be done without concern for loss of data.

Ratings of the Historian:
- 100,000 Events/sec (sum all events on all interfaces)
- 500,000 Tags
- 50 Inbound Connections - this could be 50 FactoryTalk LiveData Interface (FTLD) nodes maximum or (25 Redundant pair) or 50 FactoryTalk ME modules
- 20 Clients

**FactoryTalk LiveData Interface**

The FactoryTalk LiveData Interface is a Historian component that collects tag data from FactoryTalk LiveData. There is no cost or license for this functionality and it can be configured to be redundant. There are primary and secondary interfaces. When the primary fails or is shut down, data collection is passed to the secondary. The common requirement for this behavior is “Minimal Loss of Data.” This requirement means that when one interface fails there is little or no data collection loss.

When configured as redundant interfaces both can also buffer data. The Historian SE server can be down on one of the two interfaces and there is little or no data collection loss. This configuration is valuable when doing updates to operating systems or to make changes in computer configuration that may require a restart.

Redundant interface Node ratings
- Tag Count on Interface - 75,000
- Tags on scan 40,000 events/sec on one redundant interface pair

To get the most out of this configuration, there are some considerations and recommendations.

1. Locate the FTLD interface and the Data Server (FTLinx) on the same computer. Locating them on the same computer minimizes the network traffic for the interface to collect FactoryTalk event data.

2. Locate the “Primary” Interface on the “Primary” Data Server (FTLinx). Locating it on the primary server is desirable because when the “Primary” computer is shut down, both of the “Primary” components are not available and all other FactoryTalk clients are moved to the “Secondary.”

The FTLD interface is a FactoryTalk Data Client and forwards on the data that is collected to the FactoryTalk Historian. There can be other FactoryTalk Clients such as View SE or FactoryTalk™ Analytics™ Edge clients collecting data from the Data Server.
Figure 24 - Redundant Interface Configuration

Good

Server #1
- Data Server Primary
- Interface Node Primary

Server #2
- Data Server Secondary
- Interface Node Secondary

Bad

Server #1
- Data Server Primary
- Interface Node Secondary

Server #2
- Data Server Secondary
- Interface Node Primary

Failover

Redundant interfaces determine when they are primary or secondary. This is not done using the FactoryTalk redundancy mechanism.

There are two methods available to the interface to determine failover.

1. Phase 1 - this method uses tags to interact with each interface - one requirement is that the tag location is a redundant endpoint. Meaning redundant HMI or Redundant Controllers. This method is not recommended without redundant endpoints.

2. Phase 2 - this method uses a file share and both interface nodes must access the file share. The recommendation is that the file share is placed on the FactoryTalk Directory computer.

Other Interfaces

There are other interfaces that can be used with FactoryTalk Historian. These interfaces are useful when there is relevant data that is needed in the same time context as other data in FactoryTalk Historian.

- 9518-OPCHDA - Historian Interface for OPC HDA
- 9518-HINRELDB - Historian Interface for ODBC - This interface, commonly called the RDBMS, is intended to move event data from a database to the Historian
- 9518-HINUNIFILE - Historian Interface Universal File Loader - This interface is used to get data from a file - xml, csv, and so on. This data could be exports from SAP or weather data persisted to file.
Derived Tags

Derived tags are a reference to controller tags that are the result of a calculation. The calculation can be done several ways and understanding how the calculation is done can impact the accuracy and the scalability.

There are three ways that calculations can be done.

1. Performance Equations (DA)
   a. Can be very controller CPU intensive
   b. Uses Archive Values and is influenced by Exception and Compression

2. Statistical Totalizers (DA)
   a. Less impact on resources
   b. Uses Snapshot Values - can be more accurate
   c. More complicated to configure

3. Asset Framework (AF) - Recommended
   a. Analysis - Very Similar to Performance Equations
   b. Can be applied to all Assets of the same Template
   c. Uses Archive Values and is influenced by Exception and Compression
   d. Can be back filled - meaning that a new calculation can be calculated on historical data

These methods can write the result of the calculation back to a Historian tag, allowing for trending of calculations. These calculations could be KPIs for process equipment. The tags that are used by the calculations do not count against the tag license. The tag license is only for tags that exist in controllers or external sources.
Advanced Server Components

Advanced server components are a collection of application interfaces that allow for exchange of data from FactoryTalk Historian. These components are typically used in integrate other applications with FactoryTalk Historian. There is an Advanced Server Options license that includes all Advanced Server components. There are also individual licenses for the PIOLEDB connectivity and the OPC-DA / HDA Server capability. Individual licenses can be a more cost-effective solution.

The following are available in the Advanced Server Option (ASO).

- **Advanced Computation Engine (ACE)** - a .NET component to write your own calculation. You can have standard calculations encapsulated and applied to multiple systems or assets.
- **Data Access** - allows for external application access to the FactoryTalk Historian data.
  - OLEDB, OLEDB Enterprise, ODBC
  - OPC-DA, OPC HDA
  - Web API (REST)

**Individual Data Access Licenses Available**

The following Data Access licenses are available if you want to use the Web API that requires the ASO license.

- **9518-HSEOLEDB** - OLEDB Provider Includes ODBC Driver (OLEDB allows for read and write capability to Historian tags)
- **9518-HSEOPC** - OPC DA/HDA

**Configuration Considerations**

There are several other design considerations that must be reviewed or acknowledged.

1. **Time synchronization.** Since the Data Server time stamps the event data from the controller, having time correct on all computers is important. A time differential of 10 minutes causes data collection problems.

2. **Correct use of Scan configurations.** There are three scan configurations: Advise (default), Polled, and Poll from Device. When used correctly the impact of a large set of tags can be controlled.

3. **FactoryTalk Directory Configuration.** It is recommended that you place a data server in its own area and not to place all data servers in the same area. The reason for this configuration is that it allows for better tag resolution, which is determining what data server has knowledge of the tag. If all data servers are in the same folder, then the first data server that has knowledge is resolved, whether it was intended.
4. Patches. It is recommended that post installation tasks include the review of patches for Historian, which are typically rolled up in the patch update.

5. Disconnected Start up. When an interface node may have to start without being able to connect to the Historian server. This configuration is in the interface configuration. You lose some scan classes – \((0.05, 0.1, & 0.25)\)

6. Backup. Historian has its own backup processes because there are many open files. It is recommended that this backup be used and then use commercial backup software to back up the backup. Remember that the archives can be large and copying them over a network would not be reasonable while the backup is in progress. The recommendation is to back up locally then copy the backup over the network.

7. Buffering. Buffering is not enabled by default. Enable this feature manually.

8. Activation. FactoryTalk Historian activation is done a bit differently than other Rockwell applications. You can have up to two Historians in the FactoryTalk Directory and you can activate them differently. For example, if you have a 1,000-tag and a 5,000-tag license you can assign them both to one Historian or you can assign the 1k tag license to Historian A and the 5k tag license to Historian B. You cannot assign 3k to each Historian server.


10. Performance Monitor Interface. FactoryTalk Historian installs the Full version of the PerfMon Interface. It can have tags that contain performance counters from any Windows computer. This capability is important when monitoring the infrastructure of a manufacturing solution. There are 140 preconfigured tags monitoring the Historian and its processes. If you want to monitor other equipment, it requires assigning more tags to the # point source.

**Disaster Recovery**

If there is a physical disaster such as equipment failure due to a power quality event or a cyberattack requiring recovery, it is critical that a disaster recovery plan with policies and procedures is put in place to ensure that appropriate hardware and software application backup is stored securely and kept up to date. The difference between a fast recovery, allowing for continued production, and a devastating outage can be attributed to asset-management software. FactoryTalk AssetCentre Server is used for Rockwell Automation and Endress+Hauser asset management. The software package provides a centralized tool for securing, managing, and tracking IACS related assets while increasing uptime, productivity, and quality. An IACS is regularly changing due to corrective actions, machine learning, and other continuous improvement efforts. Any amount of recovery without well-documented backups can introduce risk because a maintenance technician may not have the latest revision of an HMI application, .ACD file with specific controller code, device configuration, or even managed network switch configuration.
Process Device Items

Many types of items can be captured and placed under an asset tree. The following provides an explanation of the types of assets:

Process Device Assets

Process device assets are used with the Calibration Management capability. Process device assets are used to control or measure process variables such as temperature, level, flow, pressure, or pH. These devices are used to calibrate other process devices, are themselves calibrated, or are used to create logical groupings for calibration procedures.

Equipment Assets

Equipment assets are not calibrated and are used to group multiple instruments and loops (which are calibrated) that constitute a larger device such as a boiler or extruder. Equipment records are also used to group assets that are related, but not necessarily connected, such as a manufacturing line. By grouping all process devices for calibration under an equipment asset, calibration activity for that piece of equipment can easily be organized and managed. They can be placed under system process devices.

Instrument Assets

Instrument assets are single devices that are used in the process, control, or laboratory system that require calibration. They are standalone components that are building blocks for more complex devices. Examples are meters, calipers, sensors, oscilloscopes, transmitters, and gauges. They can be placed under system, loop, and equipment process devices.

Loop Assets

Loop assets are collections of instruments, in a specified order, which is calibrated as one device. These collections are used to group instruments that are used for a common purpose and reduce the overall number of calibrations that must be performed. For example, a temperature control loop can consist of an RTD sensor, a transmitter, and an indicator, where calibration is performed on the entire loop instead of the individual components. Loop assets can be placed under system and equipment process devices.

System Assets

System assets are the highest level grouping of calibration-related assets. Systems can be composed of all other process device types (excluding test instruments), even other systems. They can have their own calibration specifications or can be used as a container to control scheduling of the associated devices. For example, a system record can consist of all equipment, loops, and instruments that constitute a control room HVAC system. They can be placed under system process devices.
Test Instrument Assets

Test Instrument assets are used to calibrate other process devices. They are standalone devices that are never used as components of complex devices. To verify traceability and to comply with ISO and other quality control processes, test instruments themselves must also be calibrated to NIST traceable standards. They can be placed under system, loop, and equipment process devices. Process devices can be also placed in the asset tree under the root or under a container. Process device assets count toward capacity activation.

Maintaining Proper Revision Control

This recovery application with documented policies and procedures provides revision control and records of individuals accessing the files. Before modifying any file stored in Archive, you must retrieve a copy of the file to the current working folder on your computer. Retrieving a file and making it available for editing is called checking out a file. Only one user at a time can check out a file. If a file is checked out by another user, you must wait until that user checks in the file again before you can check out and edit the file. When you check out an asset, you automatically check out all files within the asset. You have the option of checking out any files that are in sub folders of the asset.

Once edits are completed to a checked-out file, it must be returned to the Archive database. Upon checking in the file, a new version is saved so that changes are backed up in the Archive database. When you are working on a file over a long period, it is good practice to check in the file daily. If you check in an asset, you automatically check in all files within the asset. You have the option of checking in any files that are in sub folders of the asset as well. You can only check in a file that someone else has checked out if you have permission.

Currently, FactoryTalk AssetCentre offers two types of scheduled operations beyond searches, Device Monitor and Disaster Recovery. The Disaster Recovery capability enables quick and accurate file recovery by verifying the program and configuration files against backed-up master files. These features maximize the IACS investment and work to manage assets effectively.
Test Bed Configuration and Test Results

Test Bed Configuration Overview

The Mining SIA test bed architecture was designed, tested, and validated to provide design and implementation guidance, test results, and documented configuration settings. This strategy can help to achieve real-time communication, reliability, scalability, and meet the requirements of a modern mining industrial automation and control system (IACS) application. The test bed configuration provides a representation of a typical network that is used in a mining extraction and concentration circuit use case. Included in the test bed are both the hardware and software components you would find in the Mining SIA use case deployment. Although this representation is only a portion of the network, the design can be used to scale to larger sizes. The architecture is based on CPwE design criteria but does not include any type of industrial security components in the test bed setup. The CPwE logical framework reflects the basic functions of an IACS, which is the model for this Mining SIA solution architecture.

Several types of traffic patterns and data sets are configured to represent closely a real-world mining operation. The programs running in the Programmable Automation Controller (PAC) are indicative of mining applications and typical deployments for PlantPAx® systems. For example, variable-frequency drives and I/O are connected to the network via EtherNet/IP™. These devices send over tag data that provides information on device configuration and current state of the live data. Although within the test bed the VFDs and I/O connections are not connected to actual working motors, they are passing the same amount of traffic on the network. In addition, process type sensors are connected to provide streams of real-time simulated data that represents Level 0 end devices. Details on the PAC programs and the function of the end devices are covered later in the chapter.

To know how much traffic the test bed configuration can accommodate, a variable amount of traffic is injected and precisely controlled. An effective way to accomplish this is by using a traffic generator. The traffic generator can inject data into any of the switches and route it to any of the connected devices. The combination of the actual IACS hardware and software, with the addition of the traffic generator, allows for a comprehensive testing platform. The following sections provide detail on how the test bed was configured and executed. An overview drawing of the test bed architecture is represented in Figure 25 on page 90 and a bill of materials is provided in Table 1 on page 91 (for a detailed version of the BOM refer to Appendix A).
## Table 1 - General Component Overview of Test Bed Architecture

<table>
<thead>
<tr>
<th>Location</th>
<th>Quantity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Level 3 Site Operations</strong> (Control room)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>Hardware - Cisco® UCS servers, distribution switch (Cisco Catalyst® 3850)</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>Industrial Data Center (IDC)</td>
</tr>
<tr>
<td></td>
<td>15</td>
<td>Software - Virtual Machines - see Appendix A for details</td>
</tr>
<tr>
<td>Zone A</td>
<td>3</td>
<td>Industrial Ethernet switches (IES) connected in redundant star configuration and linked back to distribution switch</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>ControlLogix® controllers, one for Zone A and one for Skid A</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>E300™ Electronic Overload Relays for motor control connected in a ring topology</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>E300 electronic overload relays for motor control connected in a star topology</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>PowerFlex® 755 variable-frequency drives connect in a star topology</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>Thin client for hosting ThinManager®</td>
</tr>
<tr>
<td>Zone B</td>
<td>5</td>
<td>IES connected in Device Level Ring (DLR) switch-level ring and linked back to distribution switch via REP switch-level ring</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Distribution switch connection validated with singlemode fiber for long-distance applications</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>ControlLogix controllers, one for Zone B and one for Skid B</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>FLEX 5000™ input/output blocks connected via DLR</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>Endress+Hauser EtherNet/IP sensors</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>Endress+Hauser Foundation Fieldbus sensors that are connected via Foundation Fieldbus-EtherNet/IP linking device</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>Endress+Hauser PROFIBUS PA sensor that is connected via PROFIBUS PA-EtherNet/IP linking device</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>Thin client for hosting ThinManager</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>Engineering workstation</td>
</tr>
<tr>
<td>Zone C</td>
<td>1</td>
<td>IES</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>ControlLogix controller</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>Thin client for hosting engineering workstation</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>Industrial Service Router connecting to the distribution switch</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>Industrial Service Router connecting to an IES</td>
</tr>
</tbody>
</table>

### Zone Setup

The test bed is divided up into three sections; Zone A, Zone B, and Zone C. Each zone represents a slightly different architecture with a variety of hardware. Zone A and Zone B have a fiber connection to the distribution switch. Fiber media for all links between switches is recommended. Fiber media supports greater distances, is suitable for outdoor and harsh environments, and provides faster link-loss detection and faster convergence compared to equivalent copper links. Zone A is connected via a redundant fiber Flex links connection, Zone B is connected via fiber REP ring, and Zone C represents a remote cellular zone with one copper connection. Zone C is physically connected with copper because that is the only option on the integrated service router that was used for the test.
Supplying a reliable connection between the switches in the test bed architecture is critical. Resilient topologies such as Flex links, Resilient Ethernet Protocol (REP), and Device Level Ring (DLR) are included in the zones and overall design. These three resilient topologies are commonly used today in many industries and each contains unique characteristics. Additional details on these topologies can be referenced in the design and implementation guide titled Deploying a Resilient Converged Plantwide Ethernet Architecture.

Furthermore, the fiber REP links that connect Zone B (IES21 and IES22) to the distribution switch had two different sets of physical media and SFP transceivers. One setup included multimode SFPs and five meters of fiber while the second setup included single mode SFPs and one kilometer of spooled fiber. The purpose of these two setups was to evaluate if there was any notable loss when running longer distances. Outdoor and remote applications require much longer distances that cannot be accomplished with multimode fiber connections. Specification of fiber involves different criteria such as: fiber designation (OM1, OM2, etc.), core/cladding diameter, jacket material, singlemode or multimode, etc. For more information on specifying types of fiber refer to Deploying a Fiber Optic Physical Infrastructure within a Converged Plantwide Ethernet Architecture. Performance testing validated the assumption that the singlemode fiber performed as well as the multimode fiber.

Zone A focuses on motor-control applications, which is one of the most common end devices for mining and IACS in general. Hardware that is implemented in Zone A consists of variable-frequency drives, electronic motor overload relays, access layer IES, thin client, and two PACs. Variable-frequency drives and electronic overload relays are commonly used on mining processes such as crushers, conveyors, pump stations, and reclaimers. Typically, the data from these devices are processed by a controller that resides on the local subnet, in this case it is Zone A. Each of the test zones represents an individual subnet setup on a dedicated VLAN. Traffic is routed from the motor control end devices to the PACs but can also be shared with the other zones via Layer-3 routing. The thin client residing in Zone A runs ThinManager and allows access to the data that resides on the local Zone A VLAN. This thin client connects to the distribution switch and the IDC where the server application is running.

Zone B focuses on process instrumentation and remote input/outputs. The process instrumentation consists of Endress+Hauser sensors for monitoring level, pressure, and flow. These sensors are used in common industrial environments including mining. Endress+Hauser sensors with native EtherNet/IP connect to the access-layer IES via star connection. However, legacy hardware currently residing in a site may require a linking device. Linking devices are used to translate one protocol to another. In this case, Foundation Fieldbus (FF) and PROFINET PA devices are routed through a linking device to convert to EtherNet/IP. The linking device resides on both networks and provides the appropriate translation. For the I/O, three sets of Rockwell Automation Flex 5000 are set up with a DLR connection. DLR technology is optimized to provide ring-topology resiliency for time-critical IACS applications. DLR supports fast ring convergence (single-fault tolerant) in the event of an IACS device or link failure. DLR is standard Ethernet with standard network services such as Quality of Service (QoS) and IEEE 1588 PTP (Precision Time
Protocol). Just as Zone A, Zone B consists of (2) PACs. These two controllers host the data tags of the Endress+Hauser sensors and the I/O modules.

Zone C has one controller to demonstrate a remote I/O connection over cellular. This zone was not used for testing security or scaling the Mining SIA application, only to validate a single connection over a cellular connection. Two integrated service routers (ISR) were setup with cellular connection to communicate with a remote PAC. This zone consisted of a star topology and is connected directly to the distribution switch. Connection from the distribution switch to a cellular network was chosen over a wired connection to the internet; this adds an additional performance variable that cannot be controlled. By communicating from and to the remote zone with cellular connections, the results are solely focused on cellular-link conditions.

**Scaling the Test Bed**

To fully evaluate the Mining SIA IACS performance, the test bed must be capable of increasing the amount of processed data by the PACs and varying the traffic and the speed at which data is sent across the network. Incorporating this capability into the design provides more comprehensive data that can be useful when designing network architecture. The physical hardware for this testing did not change however the scaling was achieved by loading new PAC programs that increased the required processing time and adding network traffic via the traffic generator. These two scaling factors are covered in detail over the next two sections.

**PAC Programs**

The requirement for the PAC testing programs was to create several mining processes that would act in a typical beneficiation site application. An Iron ore site was selected out of the SME Mineral Processing & Extractive Metallurgy Handbook and this process flow combined with typical Process Flow Diagrams (PFD) and Process and Instrumentation Diagrams (P&ID) that have been executed before, this created a scope for the testing code. This code was divided into 5 PACs. By segmenting these applications, a zone structure was created that would mimic a typical site not only in operation but also in a typical control and network architecture. A high-level representation of how the architecture would be represented in a mining deployment is shown in Figure 26 on page 94.
The 5 PACs are as follows:

- **Zone A - Crusher and Milling**
  - Zone Controller - MS02
  - Crushing and Milling
  - Skid Controller - MS04
  - Milling subsystem

- **Zone B - Flotation, Thickener, and Filtration**
  - Zone Controller - MS01
  - Flotation, Thickening, Filtration
  - Skid Controller - MS05
  - Flotation subsystem

- **Zone C - Stacker - Reclaimer**
  - Zone Controller - MS03
  - Stacker-Reclaimer

With each controller looking after defined processes, the associated code needed to be developed. Control modules were created for each device, interfacing with associated I/O modules. The I/O was simulated by using built in functions, within the Rockwell Automation Mining Solution, which are generated with each application. The control modules were configured and integrated into the process with associated sequencing requirements as would typically be deployed within a mining application. Communications between PACs was done through produce/consumed tags using the standard User Defined Tag (UDT) structure that is utilized during mining project deployment.
The challenge with the testing was a finite amount of hardware with a need to linearly scale the entire IACS and to run all tests against that configuration. The project sizing was done on small, medium, and large applications. Scaling the software was done by establishing the small application, and essentially doubling I/O and its associated simulation, library components, control strategies, and mining-specific application content to get the medium-sized application. The large application was double the size of the medium application, using the same scaling principle; this was scaling the amount of content that was to be controlled and simulated within the PACs. The definition of each IACS application was based on I/O count with a simple complexity. How automated an IACS is or how much procedural control is required, defines how complex an IACS is, for example, two processes can have an identical I/O count but significant differences in complexity based on the requirements of the process control.

Table 2 shows a summary on how the scaling works. The column that is labeled Total I/O is the total of analog input/outputs and digital inputs/outputs. Direct-on-line (DOL) starter and Variable Speed Drive (VSD) column represents the total number of instances of these devices that are combined in the PAC programs. Details on the I/O and device scaling, including how many devices set up per controller, is listed in Table 3.

### Table 2 - Scaling

<table>
<thead>
<tr>
<th>Scale</th>
<th>Total I/O</th>
<th>DOL and VSD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Small</td>
<td>715</td>
<td>106</td>
</tr>
<tr>
<td>Medium</td>
<td>1430</td>
<td>212</td>
</tr>
<tr>
<td>Large</td>
<td>2860</td>
<td>424</td>
</tr>
</tbody>
</table>

### Table 3 - Control Module Summary MS01

<table>
<thead>
<tr>
<th>PAC</th>
<th>Qty</th>
<th>Catalog Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MS01</td>
<td>228</td>
<td>MsAinSiS</td>
<td>Analog Input</td>
</tr>
<tr>
<td>MS01</td>
<td>2</td>
<td>MsAliasAnalog</td>
<td>Alias Analog</td>
</tr>
<tr>
<td>MS01</td>
<td>208</td>
<td>MsAliasDigital</td>
<td>Alias Digital</td>
</tr>
<tr>
<td>MS01</td>
<td>120</td>
<td>MsDinSiS</td>
<td>Digital Input</td>
</tr>
<tr>
<td>MS01</td>
<td>24</td>
<td>MsGrpM8S</td>
<td>Group Control</td>
</tr>
<tr>
<td>MS01</td>
<td>140</td>
<td>MsMtrFrS</td>
<td>Forward and Reverse Motor</td>
</tr>
<tr>
<td>MS01</td>
<td>4</td>
<td>MsMux32X</td>
<td>Multiplexer - 32x32 Inputs - Extended</td>
</tr>
<tr>
<td>MS01</td>
<td>108</td>
<td>MsPidEnS</td>
<td>PIDE Control</td>
</tr>
<tr>
<td>MS01</td>
<td>72</td>
<td>MsSeqFbS</td>
<td>Sequence Control</td>
</tr>
<tr>
<td>MS01</td>
<td>12</td>
<td>MsTrfrCs</td>
<td>Transfer Element</td>
</tr>
<tr>
<td>MS01</td>
<td>24</td>
<td>MsTrsSiS</td>
<td>Totalizer</td>
</tr>
<tr>
<td>MS01</td>
<td>232</td>
<td>MsVhv2sS</td>
<td>Valve Two State</td>
</tr>
<tr>
<td>MS01</td>
<td>88</td>
<td>MsVsdFrS</td>
<td>Variable Speed Drive</td>
</tr>
<tr>
<td>MS01</td>
<td>12</td>
<td>sArea</td>
<td>Process Area</td>
</tr>
</tbody>
</table>
Pre-existing control module classes are being used on this project. Table 4 defines which pre-existing control module classes are being used, what standard library they belong to, and a cross-reference to the design documentation. The table also lists the control module classes that must be developed specifically for this project, in this case the Library column indicates Project.

### Table 4 - Control Module Classes

<table>
<thead>
<tr>
<th>CM Class</th>
<th>CM Class Description</th>
<th>CM Class Design Documentation</th>
<th>Library</th>
</tr>
</thead>
<tbody>
<tr>
<td>MsAinSiS</td>
<td>Analog Input, Version: 2.2</td>
<td>Software Module Functional Specification - Document Number: KGEOB02001-00003,</td>
<td>(RA-LIB) RAMS 2.50</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Software Module Design Specification - Document Number: KGEOB02001-00004, User Manual -</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Document Number: 1711OB-UM02001C.</td>
<td></td>
</tr>
<tr>
<td>MsAliasAnalog</td>
<td>Alias Analog, Version: 1.0</td>
<td>Software Module Functional Specification - Document Number: XXXX00000-00000, Software Module</td>
<td>(RA-LIB) RAMS 2.50</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Design Specification - Document Number: XXXX00000-0000, User Manual - Document Number:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>XXXX00000-00000.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Design Specification - Document Number: XXXX00000-0000, User Manual - Document Number:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>XXXX00000-00000.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Design Specification - Document Number: KGEOB02002-00004, User Manual - Document Number:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1711OB-UM02002C.</td>
<td></td>
</tr>
<tr>
<td>MsGrpM8S</td>
<td>Group Control, Version: 1.6</td>
<td>Software Module Functional Specification - Document Number: KGEOB02009-00003, Software Module</td>
<td>(RA-LIB) RAMS 2.50</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Design Specification - Document Number: KGEOB02009-00004, User Manual - Document Number:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1711OB-UM02009C.</td>
<td></td>
</tr>
<tr>
<td>MsMtrFrS</td>
<td>Forward and Reverse Motor,</td>
<td>Software Module Functional Specification - Document Number: KGEOB02005-00003, Software Module</td>
<td>(RA-LIB) RAMS 2.50</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1711OB-UM02005C.</td>
<td></td>
</tr>
<tr>
<td>MsMux32X</td>
<td>Multiplexer - 32x32 Inputs -</td>
<td>Software Module Functional Specification - Document Number: KGEOB02018-00003, Software Module</td>
<td>(RA-LIB) RAMS 2.50</td>
</tr>
<tr>
<td></td>
<td>Extended, Version: 2.5</td>
<td>Design Specification - Document Number: KGEOB02018-00004, User Manual - Document Number:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1711OB-UM02018C.</td>
<td></td>
</tr>
<tr>
<td>MsPidEnS</td>
<td>PIDE Control, Version: 2.3</td>
<td>Software Module Functional Specification - Document Number: KGEOB02004-00003, Software Module</td>
<td>(RA-LIB) RAMS 2.50</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Design Specification - Document Number: KGEOB02004-00004, User Manual - Document Number:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1711OB-UM02004C.</td>
<td></td>
</tr>
<tr>
<td>MsSeqFsS</td>
<td>Sequence Control, Version: 1.8</td>
<td>Software Module Functional Specification - Document Number: KGEOB02010-00003, Software Module</td>
<td>(RA-LIB) RAMS 2.50</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Design Specification - Document Number: KGEOB02010-00004, User Manual - Document Number:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1711OB-UM02010C.</td>
<td></td>
</tr>
<tr>
<td>MsTrfCvS</td>
<td>Transfer Element, Version: 1.7</td>
<td>Software Module Functional Specification - Document Number: KGEOB02011-00003, Software Module</td>
<td>(RA-LIB) RAMS 2.50</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Design Specification - Document Number: KGEOB02011-00004, User Manual - Document Number:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1711OB-UM02011C.</td>
<td></td>
</tr>
<tr>
<td>MsTotSiS</td>
<td>Totalizer, Version: 1.7</td>
<td>Software Module Functional Specification - Document Number: KGEOB02012-00003, Software Module</td>
<td>(RA-LIB) RAMS 2.50</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Design Specification - Document Number: KGEOB02012-00004, User Manual - Document Number:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1711OB-UM02012C.</td>
<td></td>
</tr>
<tr>
<td>MsVlv2sS</td>
<td>Valve Two State, Version: 1.10</td>
<td>Software Module Functional Specification - Document Number: KGEOB02007-00003, Software Module</td>
<td>(RA-LIB) RAMS 2.50</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Design Specification - Document Number: KGEOB02007-00004, User Manual - Document Number:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1711OB-UM02007C.</td>
<td></td>
</tr>
<tr>
<td>MsVsdFrS</td>
<td>Variable Speed Drive, Version:</td>
<td>Software Module Functional Specification - Document Number: KGEOB02006-00003, Software Module</td>
<td>(RA-LIB) RAMS 2.50</td>
</tr>
<tr>
<td></td>
<td>1.9</td>
<td>Design Specification - Document Number: KGEOB02006-00004, User Manual - Document Number:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1711OB-UM02006C.</td>
<td></td>
</tr>
<tr>
<td>sfArea</td>
<td>Process Area, Version: 2.5</td>
<td>Software Module Functional Specification - Document Number: KGEOB02020-00003, Software Module</td>
<td>(RA-LIB) RAMS 2.50</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Design Specification - Document Number: KGEOB02020-00004, User Manual - Document Number:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1711OB-UM02020C.</td>
<td></td>
</tr>
</tbody>
</table>
Within the Mining SIA testing environment, certain hardware components were assigned to the processing areas and hence to certain PACs. The hardware that was physically connected for all three sized applications remained constant. This hardware was not directly coupled to a process or process control equipment. This hardware was included in the configuration of each software component, but the response of the IACS devices and IACS applications was simulated in the software to represent a real-world deployment.

The code was configured and generated out of Application Code Manager (ACM) using Rockwell Automation Mining Solution libraries, control strategies and mining-specific application content. For a detailed review of the controller organization tree structure, see Controller Organizer on page 98.

ACM generated the full feature set required for rapid software development within Rockwell Automation:

- ACD (PAC controller code file)
- Complete Code with all I/O, Diagnostics, Control Modules, Area Models, Sequences, and Application Integration Code configured.
- Complete with I/O simulation for each object to mimic device operations
- HMI
  - Pages with objects configured and placed
  - FTAE tag alarms
- Documentation
  - Factory acceptance test
  - Site acceptance test

The application was set up accordingly to PlantPAx 4.6 distributed application and was deployed on a virtual environment leveraging off the standard PlantPAx Virtual Template Images. This platform provided a distributed network application that is easily scaled and managed. The architecture is represented in Figure 27 on page 98.
Controller Organizer

Figure 28 on page 99 is the typical layout of each controller. Multiple Periodic Tasks running at different periods and priorities. Device control is divided into multiple associated Programs, this could be done in a number of ways as the structure is flexible to meet any requirement. It was done this way for simplicity and is a structure that is common for rolling projects out to some of Rockwell Automation customers.

Under Utility, there are a number of tasks, these are global functions that are used throughout the controller. The Simulation Program, provides the I/O simulation that is required to bring the application to life without a process attached. There are two modules in the I/O Tree that are inhibited, all associated modules beneath will not have their I/O updated and the Simulation Program will update them. The status of each object is monitored in the StatusMonitoring Program and for simulation, this is why it is inhibited.
HMI Application

HMI graphics were created to cover the processes of the Mining SIA use case. These covered crushing, overland, milling, flotation, thickening, tailings, stacking and reclaiming. Figure 29 on page 100 shown below illustrates an example of one of the HMI pages used. As the PAC programs double in size to create the three levels of scaling, so did the number of HMI displays. This provided a true representation of how an IACS architecture grows.
Traffic Generator

Having the ability to scale the PAC programs to the three different sizes, small, medium, and large, is effective for scaling the test, however, adding a traffic generator provides results and analysis on how much overhead is available. The traffic generator is a purpose-built hardware/software appliance that can send manually crafted packets across the network and continually monitor the performance down to the packet level. The traffic generator is set up to increase traffic in certain areas of the network to see how the overall IACS is affected. Each of the IES has a physical connection to the traffic generator. The traffic generator sends different bandwidths of data depending on the capability of the switch port being used and the aggregated amount of traffic. The IES used for the test have either 100 Mb/s or 1 Gb/s depending on the model and switch port utilized. In the test bed configuration, IES12 and IES13 consist of Stratix® 5700 and therefore are limited to 100 Mb/s for the traffic generator connection; all other IES are Stratix 5400s and provisioned 1 Gb/s interfaces.
Determining the traffic load across the network gets more complicated when factoring in the load from the other switches. Calculations were used to determine the maximum amount of traffic a switch port can handle and then three levels were established. Three different data rates, low, moderate, and high, are scaled against the maximum throughput available through end-to-end Layer 3 connectivity. Low, moderate, and high levels are 10%, 40%, and 80% respectively of this maximum throughput. This means that the high level the traffic generator for IES12 and IES13 injects traffic that takes up 80% of the maximum bandwidth available to their parents. Figure 30 provides a visual representation of the low, medium, high traffic set ups. The chart in Figure 31 shows what these values equated to in bytes per second and the loads that are listed are per switch port. Therefore the total traffic passing through a switch includes all traffic in the zone.

**Figure 30 - Network traffic Levels**

<table>
<thead>
<tr>
<th>Low</th>
<th>Total Bandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIP Traffic</td>
<td>T.G. = 10%</td>
</tr>
<tr>
<td>Moderate</td>
<td>Total Bandwidth</td>
</tr>
<tr>
<td>CIP Traffic</td>
<td>Traffic Generator = 40%</td>
</tr>
<tr>
<td>High</td>
<td>Total Bandwidth</td>
</tr>
<tr>
<td>CIP Traffic</td>
<td>Traffic Generator = 80%</td>
</tr>
</tbody>
</table>

**Figure 31 - Traffic Generator Loads**

<table>
<thead>
<tr>
<th>Source</th>
<th>IES12, IES13</th>
<th>IES11</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination</td>
<td>IES21, IES22, IES23, IES24, IES25</td>
<td>IES21, IES22, IES23, IES24, IES25</td>
</tr>
<tr>
<td>Low</td>
<td>1.0 Mb/s</td>
<td>8.4 Mb/s</td>
</tr>
<tr>
<td>Moderate</td>
<td>4.0 Mb/s</td>
<td>34.6 Mb/s</td>
</tr>
<tr>
<td>High</td>
<td>8.0 Mb/s</td>
<td>67.2 Mb/s</td>
</tr>
</tbody>
</table>

**Traffic Flows**

With the three zones setup, including the traffic generator configuration, and running their respective user application programs, the next part is to define the EtherNet/IP application layer protocol (common industrial protocol (CIP™)) traffic. This traffic consists of communications between the PACs, devices, and virtual machines. The amount of CIP traffic on the network is determined mostly by the application programs on the PACs, the data from the IACS devices, and the PlantPAx application servers. The following sections contain the details of the traffic paths and the data points that are monitored by the IES.
Common Industrial Protocol Messaging

Figure 32 represents the configured traffic paths for the test bed. Before reviewing the chart, a clear understanding of the different types of EtherNet/IP (CIP) traffic that may traverse this area of the network is required. Each of these has its own unique characteristics and impact network traffic.

Class 1 (Implicit) - Class 1 connections, time-critical traffic, sensitive to latency, jitter, and disruptions in the IACS network. Examples include I/O and produced/consumed connections. Another name for a Class 1 message is implicit messaging. Once the Class 1 connection is established, the producer sends an “implicit” message every requested packet interval (RPI).

Class 3 (Explicit) - Class 3 connections, non time-critical traffic, more tolerant to latency, jitter, and disruptions in the IACS network. Examples include MSG instructions and going online with a Programmable Automation Controller (PAC) using Studio 5000 Logix Designer®. Another name for a Class 3 message is Explicit Messaging. Explicit messages are triggered on demand, or in other terms, the data is explicitly requested.

Figure 32 - EtherNet/IP Traffic Summary (See Figure 25 on page 90 for Device Labels)

<table>
<thead>
<tr>
<th>Class 1 Implicit Traffic</th>
<th>Class 3 Explicit Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Device</td>
<td>Second Device</td>
</tr>
<tr>
<td>Motor Overloads (D101-D104)</td>
<td>PAC in Zone A Rack</td>
</tr>
<tr>
<td>VFD (D105-D107)</td>
<td>PAC in Zone A Rack</td>
</tr>
<tr>
<td>Motor Overloads (D108-D111)</td>
<td>PAC in Skid A Rack</td>
</tr>
<tr>
<td>PAC in Zone A Rack</td>
<td>PAC in Skid A Rack</td>
</tr>
<tr>
<td>PAC in Zone A Rack</td>
<td>PAC in Zone B Rack</td>
</tr>
</tbody>
</table>

Test Results

Results Summary

The results of the testing provide a relative scale that can be referenced for design architecture for mining applications. This validated Mining SIA demonstrates an efficiently designed IACS architecture that can handle large amounts of network traffic. One of the key aspects for this design, when scaling upward, is to maintain small zones (each zone consists of a single VLAN). The ‘zone’ approach allows for a simpler network that is easier to manage and provides segmentation. For the large-scale setup, even with a high level of traffic injected into the Mining SIA, there were no controller or network issues. In typical applications, it is difficult to determine how additional traffic will affect the IACS architecture. Utilizing the traffic generator for this validation supplied insight into this evaluation.
In total, 252 traffic paths were monitored and logged for the nine test levels. The nine test levels consisted of: small, medium, and large scale each with low, moderate, and high injected traffic. Figure 33 provides a summary of the data that was collected. Displayed in the chart is a summary of each test that shows average data on each interface. The data averaged on the interface represents bandwidth utilization by percentage. Averaging the bandwidth utilization data for every interface provides a holistic view. This was the method that was developed to summarize the traffic across the entire IACS architecture. The figure confirms the increase in traffic load that were achieved while not incurring any errors or packet issues. Overall, the test validated the Mining SIA and demonstrated with a traffic generator that there is enough bandwidth available for additional network traffic.

**Figure 33 - Results Summary Chart**

![Average Tx/Rx traffic per Interface](image)

**Performance Metrics Definition**

Monitoring the test bed performance was conducted using the diagnostic information available from the IES. Figure 34 on page 104 is a sample of the test results, containing the metrics.

Explanation of key performance indicators that was used in the evaluation of the network performance:

- **VLAN** – This field denotes the VLAN associated with the interface. Each zone has a unique VLAN.
- **ID** – Each of the switches in the topology are identified with an ID number, IESxy (x = VLAN number and y = IES number). DistSw0,1 refers to the stacked distribution switch that connects to each of the zones.
- **Role** – The resiliency protocols that are used in this testing consist of two interfaces working together. This field associates the interface with an A or B based on the topology.
- **Interface** – Testing was conducted per interface; this field denotes the switch interface number.
• Topology – Three types of topology are configured in the architecture: Flex Links (switch-level redundant star), DLR (device-level and switch-level rings), and REP (switch-level ring).

• Size – Three sizes, small, medium, and large, are used for scaling the PAC programs. Moving up in size essentially doubles the program size.

• Load Level – Three sizes, low, moderate, and high, are used for determining the amount of traffic generation that is injected into the Mining SIA test bed.

• Reliability – This counter is used to indicate how likely it is that a packet can be delivered or received successfully. The counter has a range of 0 to 255, with 255 being the maximum value and representing the most reliable. The lower the value the less reliable the connection is performing. Different types of errors will affect the reliability counter. The calculation is performed every five minutes and is based on this equation: reliability = number of packets / number of total frames. Reliability is converted to a percentage for the data chart.

• TxLoad – This counter is related to the reliability counter and is calculated every 5 minutes. This indicates how active the interface is with transmitting frames. A value of 255 means that the interface is completely saturated and therefore will not perform well. To convert this value to a percentage, you would use the following equation: TxLoad/255 * 100 = percent utilization. The data chart shows this value as a percentage.

• RxLoad – This counter is related to the reliability counter and is calculated every 5 minutes. This indicates how active the interface is with receiving frames. A value of 255 means that the interface is completely saturated and therefore will not perform well. To convert this value to a percentage, you would use the following equation: RxLoad/255 * 100 = percent utilization. The data chart shows this value as a percentage.

• Packet Issues – Diagnostics in the IES contain many features that determine if there is an issue with a packet. If any of these features detect an issue, it is noted here. If no problems occur, it is marked as ‘none’.

• PAC/EWS Connectivity – This data point takes into effect many different parameters and outputs a pass/fail score. Error counters are monitored on the IES and a failure on one of these counters results in a ‘fail’ score. In addition, the engineering workstation is set up with Logix5000 actively monitoring the running programs on the PACs. Any loss of communication from the EWS to the controller and reported hardware/software status is logged and specified as pass, intermittent, or fail. A value of ‘Pass’ means that the connection is maintained without any interruption and a ‘Failed’ connection results from a disconnection from the PAC. The value of intermittent means that the connection is inconsistent in its performance.

Figure 34 - Sample Test Results
Chapter 5

Mining Smart Industry Architecture Specific Use Cases

This chapter describes the extraction and concentration circuit use cases for the Mining SIA. These use cases were architected, tested, and validated by Rockwell Automation, Panduit, Endress+Hauser, and Cisco.

- Conveyance
- Compression
- Flotation
- Pumping

Conveyance

What is Conveyance

A conveyor belt is an industrial automation and control system (IACS) that carries material from one point to another. A conveyor system or material handling system consists of two key components; a loop of material that is known as the belt and two pulleys that are fixed at either end. These pulleys work in a continuous circular motion to pick up material at one end of the belt and drop off material at the other end of the belt. Since introduced in the early 20th century, conveyors have become a vital part of mine operations. Conveyor systems can be used to transport material in underground and open pit operations.

The conventional conveyor is the most common conveyor system, uses two or more pulley systems with a belt that rotates about them, and carries medium. The two pulleys can be powered for certain requirements in the conveyor system. The conventional conveyor belt is “V” shaped to hold the material better.

Major Challenges

The selection of conveyance control system is often coupled to the electrical mechanical system and desired outcomes for operation performance. The items defined by the Society of Mining Engineering as major design decisions are:

1. Determine the desired conveyor capacity.
2. Identify the material and its characteristics.
3. Choose a troughing angle.
4. Determine belt width.
5. Select belt speed.

6. Determine the idler spacing.

Conveyor Capacity

The first step in designing the capacity of the conveyor is to determine the desired capacity that is required to transport the desired amount of material. This capacity, in tons per hour (t/h), represents the peak surge volume that is expected. By determining conveyor capacity, the sizing of other conveyor parameters can be calculated. This parameter has a major impact on mechanical and electromechanical duty of equipment.

Material Characteristics

An important design consideration for a conveyor system is to characterize the material handled. Furthermore, parameters such as the over cover belt material, the maximum incline a conveyor can scale, and trough design can be identified from these material characteristics. For example, an abrasive material such as ore from an in-pit conveyor system will have many different characteristics than coal.

Maintenance

Maintenance and safety play the largest roles and problems within conveyor operation. The four types of conveyor maintenance are:

1. Preventative maintenance
2. Opportunity-based maintenance
3. Corrective maintenance
4. Condition-based maintenance

Preventative Maintenance

Preventative maintenance is time-based maintenance. Part replacements occur after certain runtimes. This type of maintenance relies solely on reliability data that is provided by the manufacturer. The manufacturer’s preventative maintenance runtimes are generally conservative.

While some parts of the conveyor system can be replaced while the conveyor system is operational, preventative maintenance often requires shutting down the IACS. This shut down results in a costly loss of processing.

Opportunity-Based Maintenance

Opportunity-based maintenance refers to the use of overall system down time to replace parts. An example would be if operations halted, the conveyor system would be shut down, and thus replacements could be made to the conveyor system.
Corrective Maintenance

Corrective maintenance, also known as run to failure maintenance, is when the system is run until components within the system undergo failure. When failure occurs, downtime is much longer and more expensive than the previously discussed maintenance types. If failure is not detected immediately, catastrophic damage can be inflicted on the system, which can amplify conveyor downtime and costs.

Condition-Based Maintenance

Condition-based maintenance involves monitoring different components of a system to predict failures. When failures can be predicted, the appropriate corrective actions can be taken to minimize the effect on operations. Condition-based maintenance interrupts processing for maintenance only when it is necessary.

Rockwell Automation Benefits in Conveyance

Rockwell Automation® conveyor system benefits include:

- Rapid development and deployment, providing excellent reliability and cost-effective solution.
- Standardized software packages that enable commonality of maintenance procedures across all sections/sites.
- Safe Remote Isolation with lockout/tagout, reduce downtime that is related to isolation, applicable to any equipment but particularly useful to long conveyors and duel company custody conveyors.
- Ease of system fault finding through unified diagnostics pulling all data into one version of the truth, allowing the executive or office personnel to see the same information that on-site operations management and equipment operators see but contextualized for their role.
- Anticipate future issues and achieve accountability through using historical data and improved diagnostics.
- Increased processing due to reduced downtime with gap control.
- Standardize your IACS and improve visibility of important system elements for monitoring and maintenance.

Popular Configuration Drawing - Conveyance

For more information, see the Mining Conveyance System Architecture, publication MIN-QR004.
Compressed Air is utilized energy source on most industries around the world, it is an important source of power in mining operations. Compressed Air has been used extensively in conventional mining in both coal and hard rock mines for decades. It is used for its reliability and safety to provide are for many applications

Compressors are turbomachinery assets within mining and beneficiation that are used as a methodology to provide compressed air for many applications. The compressors are typically a complete packaged solution where Process Control, Anti-Surge Control, and Conditional Monitoring are done in isolated systems that communicate with each other to achieve the overarching function. Their core function is to supply air reliably to a dynamic distributed system.

Mining applications where compressed air is especially useful include:

**Pneumatic Tools**

Compressed air is an excellent source of energy for power tools such as drills, wrenches, hack saws and other vital mining equipment that is used in the deep underground stretches of the mines.

**Blasting**

Compressed air systems offer safer mediums for use in blasting operations. High velocity compressed air streams can be vital in some mining situations.

**Pneumatic Control**

Pneumatic control is extensively used in multiple industries, in mining generally around loading boxes in shaft applications and in beneficiation valve control and agitation.

**Material Handling**

Materials like coal dust can be better handled when compressed air is mixed, allowing for fluidization. Compressed air can also be used in conveying material in mining.

**Cleaning**

Compressed air can also be used for purging unwanted particles from filters and other spaces amid the dirt and dust of the mining operation. It is a clean source of air and can be used effectively without the need for additional cleaning materials. This can help extend the longevity of critical mining equipment and reduce any downtime that is needed for maintenance.
**Major Challenges**

Some major challenges for mining compressors are:

1. **Isolated System**
2. **Mechanical Failure**
3. **Inefficient Operation**

**Isolated System**

A Compressor can be deployed as an isolated system with limited integration to the rest of the IACS. Limited integration can significantly impact operations when a problem occurs and the added delay of responding to the result of low air pressure. Centralized operational control rooms must be provided with enough information that they can make informed decisions; the information must be contextualized to promote abnormal situations.

Another potential key issue is the limited visualization, diagnostic, and fault-finding capabilities. Whether this information is available from remote centralized locations or not, not having the required information to fault find on a compressor can add significant operational risk.

**Mechanical Failure**

A surge condition on a centrifugal compressor can cause catastrophic damage. Prevention of this condition is fundamental to certain types of compressors to maintain their high availability criteria in delivering compressed air. Being too conservative with this anti-surge control leads to significant inefficiencies that could result in unnecessary mechanical fatigue. Mechanical failure on these critical assets can lead to significant downtime.

**Inefficient Operation**

Multiple Compressors working in isolation into the same distributed system can cause significant inefficiencies. Compressors operating at different setpoints, too many compressors being online for the required demand and unnecessary rapid response to consumption system changes are some causes of these inefficiencies. Collective control is important for optimal asset utilization without impacting operations, equipment operating in isolation without system integration is a major challenge that has to be overcome to achieve efficient operations.

**Rockwell Automation Benefits in Compressors**

You need a solution that integrates all control requirements of your compressed air network on one controller that manages your distributed system according to pressure requirements and schedule.
Our compressor solution is a standardized, single platform transparent anti-surge control. With centralized master control, multiple compressors in a distributed system are optimized with algorithms that are designed to reduce energy consumption and maximize equipment output across the system. Power management and distribution optimization provide insight into energy costs per compressor, which is based on variable rate schedules.

Our Solution:
- Is an integrated compressor control solution that operates safely and efficiently over a wide range of varying process conditions. With transparency on Process, Anti-Surge and Motor Control.
- Reduces energy costs, with optimization algorithms managing your real-time compressed air requirements
- Provides in-depth analytics as to where to make decisions
- Optimizes any compressor type, any industry
- Delivers real-time anti-surge control to help prevent surges at all times
- Provides an integrated surge test tool

Popular Configuration Drawing - Compressor Systems

For more information, see the Mining Compressor System Architecture, publication MIN-QR005.

Flotation

What is Flotation?

Flotation is the most widely used method for ore beneficiation. In ore beneficiation, flotation is a process in which valuable minerals are separated from worthless material or other valuable minerals by inducing them to gather in and on the surface of a froth layer. Sulfide minerals, non-sulfide minerals, and native metals are recovered by froth flotation.

This process is based on the ability of certain chemicals to modify the surface properties of the minerals. Other chemicals are used to generate the froth and still others are used to adjust the pH.

Major Challenges

Major challenges for flotation systems can be seen in reagent injection and concentration, level control, agitator speed, inflow and outflow rates, and densities and grades of materials. As many flotation cells are often structured in a series of banks to maximize recovery, there is often a cascade effect throughout the system. Quick response rates dampen and reject unwanted signals resulting in optimal flotation results.
Rockwell Automation Benefits in Flotation

Rockwell Automation flotation control has many embedded benefits including:

- Fast response to transient disturbances leading to quicker damping and reduced propagation of upsets
- Adaptive control that accommodates deteriorating valve performance due to wear or silting
- Reduced dependency on specialized PC-based software and specialized engineering labor
- Consistent level control allows for better optimization of other variables such as air and reagent addition
- Logix based control allows for fast, seamless integration to the existing PID base layer without the need for OPC or other third-party connectors
- Operational settings and diagnostics available on the native FactoryTalk® View SCADA eliminating third-party visualization interfaces

A disturbance rejection base that compliments Model Predictive Control (MPC)

For more information, see the Sample Mine Concentration Circuit, publication MIN-QR002.

Stacker Reclaimers

What is a stacker-reclaimer?

Stackers and reclaimers are used in stock yards to stack minerals, ore, and other granular raw materials in piles, and then redistributing them for processing and shipment. Stackers are used to produce these large piles or circular stacks. Reclaimers are used to collect and redistribute the material from the stacks or piles of bulk materials.

Major Challenges

Major challenges that present in the control of stacker reclaimers include the following:

- GPS precision location
- Drive coordination
- Vibration monitoring and detection of harmful vibrations
- Anti-Collision capabilities
- Stockpile shape formation detection and optimization
- System coordination and Stockpile Management

Rockwell Automation Benefits for Stacker-Reclaimers

Rockwell Automation stacker reclaimer solutions include the following benefits:
• Achieve your operational targets with the Integrated Architecture of the connected mine
• Quickly diagnose and fix issues with remote communication from a central location across your entire enterprise
• Anticipate future issues and achieve accountability by using historical data and improved diagnostics
• Improve required safety support by adopting a connected architecture with programmable event-based alarming to support safe automated operations
• Standardize your IACS and benefit from improved energy consumption, monitoring, and maintenance of your machinery
• Visualization data to be fed to the operator, along with real-time video feeds and the ability to communicate via voice are on one network architecture.
• Your executive or office personnel sees the same information that your on-site operations management and equipment operators see.

Popular Configuration Drawing - Stacker-Reclaimer

For more information, see the Mining Stacker-Reclaimer System Architecture, publication MIN-QR006.

Pumping

What is a pump system?

Pumping applications play an integral role in mining operations. Pumping is often relied upon to be a major source of transporting materials within a mine site. Materials could be the discharge and removal of waste, valuable slurries of material, or simple dewatering of a location. Pumps are often in concentrated areas and can be mechanically grouped to form a pump train or duty standby applications. Other pumps are remote and serve as a booster on a pump station application. Pumping in mines can be both a low and medium voltage application.

Major Challenges

Major challenges in pumping can be seen in the form of pump cavitation and mechanical failure of components. These challenges could be the detection of cracked housings, crack impellers, or failing seals on pumps. Energy costs of pumps often provide a control strategy challenge of having enough of capacity while minimizing operational costs.
Rockwell Automation Benefits for pump systems

Rockwell Automation has extensive experience delivering engineered integrated solutions from a simple sump pump to complicated pump train systems. Solutions that include, pump motor control, condition-monitoring, motor overload protection, standalone, and remote implementations that are a part of the site wide DCS.

- Rapid development and deployment, providing excellent reliability and cost-effective solution.
- Simplified common Industry Pump Controlling on Level, Pressure, and Flow.
- Pump Alternation options on Standard Rotation, Least Starts or Least Runtime.
- Potential Faulty instrument switch detection, using process changes to detect faulty switch operation.
- Ease of system fault finding through unified diagnostics pulling all data into one version of the truth, allowing the executive or office personnel see the same information that on-site operations management and equipment operators see but contextualized for their role.

Popular Configuration Drawing pump systems

For more information, see the Mining Slurry Pumping System Architecture, publication MIN-QR007.
### Hardware / Software Used in Testing

#### Hardware

The following table lists the hardware that was used in the testing.

**Table 5 - Hardware Used in Testing**

<table>
<thead>
<tr>
<th>Role</th>
<th>Product</th>
<th>Part Number</th>
<th>Sw. Ver.</th>
</tr>
</thead>
<tbody>
<tr>
<td>IES11</td>
<td>Stratix® 5400</td>
<td>1783-HMS4EG8CGR</td>
<td>15.2(7)E</td>
</tr>
<tr>
<td>IES12</td>
<td>Stratix 5700</td>
<td>1783-BMS12T4E2GNK</td>
<td>15.2(7)E</td>
</tr>
<tr>
<td>IES13</td>
<td>Stratix 5700</td>
<td>1783-BMS12T4E2GNK</td>
<td>15.2(7)E</td>
</tr>
<tr>
<td>Zone A Rack</td>
<td>ControlLogix® PAC</td>
<td>1756-L85E</td>
<td>32.011</td>
</tr>
<tr>
<td></td>
<td>Communication Module</td>
<td>1756-EN2TR</td>
<td>11.001</td>
</tr>
<tr>
<td></td>
<td>ControlLogix PAC</td>
<td>1756-L75</td>
<td>32.011</td>
</tr>
<tr>
<td></td>
<td>Communication Module</td>
<td>1756-EN2TR</td>
<td>11.001</td>
</tr>
<tr>
<td>Skid A Rack</td>
<td>ControlLogix PAC</td>
<td>1756-L85E</td>
<td>32.011</td>
</tr>
<tr>
<td></td>
<td>Communication Module</td>
<td>1756-EN2TR</td>
<td>11.001</td>
</tr>
<tr>
<td></td>
<td>ControlLogix PAC</td>
<td>1756-L75</td>
<td>32.011</td>
</tr>
<tr>
<td></td>
<td>Communication Module</td>
<td>1756-EN2TR</td>
<td>11.001</td>
</tr>
<tr>
<td>Thin Client A</td>
<td>Integrated display thin client</td>
<td>6200T-15WA</td>
<td>8.1</td>
</tr>
<tr>
<td>D105</td>
<td>PowerFlex® 755 VFD</td>
<td>20G11NDFSPO AA0NNNNN</td>
<td>13.003</td>
</tr>
<tr>
<td>D106</td>
<td>Power Flex 755 VFD</td>
<td>20G11NDFSPO AA0NNNNN</td>
<td>13.002</td>
</tr>
<tr>
<td>D107</td>
<td>Power Flex 755 VFD</td>
<td>20G11NDFSPO AA0NNNNN</td>
<td>14.002</td>
</tr>
<tr>
<td>IES21</td>
<td>Stratix 5400</td>
<td>1783-HMS4EG8CGR</td>
<td>15.2(7)E</td>
</tr>
<tr>
<td>IES22</td>
<td>Stratix 5400</td>
<td>1783-HMS4EG8CGR</td>
<td>15.2(7)E</td>
</tr>
<tr>
<td>IES23</td>
<td>Stratix 5400</td>
<td>1783-HMS4EG8CGR</td>
<td>15.2(7)E</td>
</tr>
<tr>
<td>IES24</td>
<td>Stratix 5400</td>
<td>1783-HMS4EG8CGR</td>
<td>15.2(7)E</td>
</tr>
<tr>
<td>IES25</td>
<td>Stratix 5400</td>
<td>1783-HMS4EG8CGR</td>
<td>15.2(7)E</td>
</tr>
<tr>
<td>Role</td>
<td>Product</td>
<td>Part Number</td>
<td>Sw. Ver.</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------------------</td>
<td>-------------</td>
<td>----------</td>
</tr>
<tr>
<td>Zone B Rack</td>
<td>ControlLogix PAC</td>
<td>1756-L85E</td>
<td>32.011</td>
</tr>
<tr>
<td></td>
<td>Communication Module</td>
<td>1756-EN2TR</td>
<td>11.001</td>
</tr>
<tr>
<td></td>
<td>ControlLogix PAC</td>
<td>1756-L75</td>
<td>32.011</td>
</tr>
<tr>
<td></td>
<td>Communication Module</td>
<td>1756-EN2TR</td>
<td>11.001</td>
</tr>
<tr>
<td>Skid B Rack</td>
<td>ControlLogix PAC</td>
<td>1756-L85E</td>
<td>32.011</td>
</tr>
<tr>
<td></td>
<td>Communication Module</td>
<td>1756-EN2TR</td>
<td>11.001</td>
</tr>
<tr>
<td></td>
<td>ControlLogix PAC</td>
<td>1756-L75</td>
<td>32.011</td>
</tr>
<tr>
<td></td>
<td>Communication Module</td>
<td>1756-EN2TR</td>
<td>11.001</td>
</tr>
<tr>
<td>Thin-Client B</td>
<td>Integrated display thin client</td>
<td>6200T-15WA</td>
<td>8.1</td>
</tr>
<tr>
<td>D201</td>
<td>Endress+Hauser Promass 83</td>
<td>83F25-QXU0-0</td>
<td>01.01.02</td>
</tr>
<tr>
<td>D202-Base</td>
<td>Endress+Hauser Promass 100 base device</td>
<td>8E1808-1NE1/0</td>
<td>02.01.00</td>
</tr>
<tr>
<td>D202-WebServer</td>
<td>Endress+Hauser Promass 100 Web Server</td>
<td>—</td>
<td>02.01.00</td>
</tr>
<tr>
<td>D203</td>
<td>Foundation Fieldbus linking device</td>
<td>1788-EN2FFR</td>
<td>1.001</td>
</tr>
<tr>
<td>D203A</td>
<td>Endress+Hauser Deltabar S</td>
<td>PMD75-SPE7F41DANA</td>
<td>02.00.02</td>
</tr>
<tr>
<td>D203B</td>
<td>Endress+Hauser Level Flex</td>
<td>FMPS3-9EF5/0</td>
<td>01.01.00</td>
</tr>
<tr>
<td>D204</td>
<td>Profinbus PA linking device</td>
<td>1788-EN2PARB</td>
<td>2.006</td>
</tr>
<tr>
<td>D204A</td>
<td>Endress+Hauser Prosonic S</td>
<td>FMU90-R12CA213AA1A</td>
<td>01.00.00</td>
</tr>
<tr>
<td>D205</td>
<td>FLEX 5000™</td>
<td>S094-AEN2TR/ (3)I816, (3)OW8I, (1)IY8, (1)OF8</td>
<td>2.001</td>
</tr>
<tr>
<td>D206</td>
<td>Flex 5000</td>
<td>S094-AEN2TR/ (3)I816, (3)OW8I, (1)IY8, (2)OF8</td>
<td>2.001</td>
</tr>
<tr>
<td>D207</td>
<td>Flex 5000</td>
<td>S094-AEN2TR/ (3)I816, (3)OW8I, (2)IY8, (1)OF8</td>
<td>2.001</td>
</tr>
<tr>
<td>EWS</td>
<td>Thin Client with Logix 5000™</td>
<td>6200T-15WA</td>
<td>8.1</td>
</tr>
<tr>
<td>IES31</td>
<td>Stratix 5700</td>
<td>1783-BM512T4E2CGNK</td>
<td>15.2(7)E</td>
</tr>
<tr>
<td>W42</td>
<td>IR809G-LTE-VZ-K9</td>
<td>IR809G-LTE-VZ-K9</td>
<td>15.9.3M</td>
</tr>
<tr>
<td>W43</td>
<td>IR809G-LTE-VZ-K9</td>
<td>IR809G-LTE-VZ-K9</td>
<td>15.9.3M</td>
</tr>
<tr>
<td>Zone C Rack</td>
<td>ControlLogix PAC</td>
<td>1756-L85E</td>
<td>32.011</td>
</tr>
<tr>
<td></td>
<td>Communication Module</td>
<td>1756-EN2TR</td>
<td>11.001</td>
</tr>
<tr>
<td></td>
<td>ControlLogix PAC</td>
<td>1756-L75</td>
<td>32.011</td>
</tr>
</tbody>
</table>
Software

The following table lists the software that was used in the testing.


Table 6 - Software Used in Testing

<table>
<thead>
<tr>
<th>Role</th>
<th>Product</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Machine Operator Workstation</td>
<td>Operator Workstation</td>
</tr>
<tr>
<td>Virtual Machine IXIA Traffic Generator</td>
<td>IXIA Traffic Generator</td>
</tr>
<tr>
<td>Virtual Machine ThinManager®</td>
<td>ThinManager®</td>
</tr>
<tr>
<td>Virtual Machine ControlToolsA</td>
<td>ControlToolsA</td>
</tr>
<tr>
<td>Virtual Machine ControlToolsB</td>
<td>ControlToolsB</td>
</tr>
<tr>
<td>Virtual Machine AppServ-ASM</td>
<td>AppServ-ASM</td>
</tr>
<tr>
<td>Virtual Machine AppServ-BAT</td>
<td>AppServ-BAT</td>
</tr>
<tr>
<td>Virtual Machine AppServ-EWS</td>
<td>AppServ-EWS</td>
</tr>
<tr>
<td>Virtual Machine AppServ-Hist</td>
<td>AppServ-Hist</td>
</tr>
<tr>
<td>Virtual Machine AppServ-OWS</td>
<td>AppServ-OWS</td>
</tr>
<tr>
<td>Virtual Machine AppServ-PADC</td>
<td>AppServ-PADC</td>
</tr>
</tbody>
</table>
Notes:
Converged Plantwide Ethernet (CPwE) Reference Architectures

The foundation for the reliable and secure Mining Smart Industry Architecture (SIA) is CPwE reference architectures. CPwE is a collection of architected, tested, and validated designs. The content of CPwE, which is relevant to both operational technology (OT) and informational technology (IT) disciplines, consists of documented architectures, best practices, guidance, and configuration settings to help industrial operations and original equipment manufacturers (OEMs) achieve the design and deployment of a scalable, reliable, secure, and future-ready site-wide industrial network infrastructure. CPwE can also help industrial operations and OEMs achieve cost reduction benefits using proven designs that can facilitate quicker deployment while helping to minimize risk in deploying new technology. CPwE is brought to market through an ecosystem consisting of industry thought leaders Rockwell Automation, Cisco Systems, and Panduit.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Converged Plantwide Ethernet Architecture Design and Implementation Guide, publication ENET-TD001</td>
<td>Baseline CPwE design and implementation guide, which is relevant to both OT and IT disciplines, consisting of documented architectures, best practices, guidance, and configuration settings to help industrial operations and OEMs with the design and deployment of a scalable, reliable, secure, and future-ready plant-wide or site-wide industrial network infrastructure.</td>
</tr>
<tr>
<td>Deploying Industrial Firewalls within a Converged Plantwide Ethernet Architecture Design and Implementation Guide, publication ENET-TD002</td>
<td>Outlines several use cases for designing, deploying, and managing Stratix® 5950 industrial firewalls throughout a plant-wide or site-wide IACS network. The industrial firewall is ideal for IACS applications that need trusted zone segmentation.</td>
</tr>
<tr>
<td>Deploying Network Address Translation within a Converged Plantwide Ethernet Architecture Design and Implementation Guide, publication ENET-TD007</td>
<td>Outlines several use cases for deploying network address translation (NAT) technology within Stratix industrial Ethernet switches (IES), to help enable OEMs to clone skids/equipment/machines, while seamlessly integrating into plant-wide or site-wide IACS network architectures.</td>
</tr>
<tr>
<td>Deploying Identity and Mobility Services within a Converged Plantwide Ethernet Architecture Design and Implementation Guide, publication ENET-TD008</td>
<td>Outlines several industrial security and mobility architecture use cases, with Cisco® Identity Services Engine (ISE), for designing and deploying mobile devices, with FactoryTalk® applications, throughout a plant-wide or site-wide IACS network infrastructure.</td>
</tr>
<tr>
<td>Securely Traversing IACS Data Across the Industrial Demilitarized Zone Design and Implementation Guide, publication ENET-TD009</td>
<td>Outlines design considerations to help with the successful design and implementation of an IDMZ to share securely IACS data between plant-wide or site-wide operations and the enterprise business systems.</td>
</tr>
<tr>
<td>Deploying A Resilient Converged Plantwide Ethernet Architecture Design and Implementation Guide, publication ENET-TD010</td>
<td>Outlines several use cases for designing and deploying resilient plant-wide or site-wide architectures for IACS applications, utilizing a robust physical layer and resilient topologies with resiliency protocols.</td>
</tr>
</tbody>
</table>
Appendix B  References

<table>
<thead>
<tr>
<th>Resource</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deploying Industrial Data Center within a Converged Plantwide Ethernet Architecture, publication ENET-TD014</td>
<td>Outlines several use cases for designing and deploying end-to-end connectivity between the Industrial Data Center (IDC) located within Level 3 Site Operations to IACS assets located within various Area Zones of the plant-wide or site-wide IACS architecture.</td>
</tr>
<tr>
<td>Deploying Device Level Ring within a Converged Plantwide Ethernet Architecture Design Guide; publication ENET-TD015</td>
<td>Outlines several use cases for designing and deploying Device Level Ring (DLR) protocol technology with IACS device-level, switch-level, and mixed device/switch-level single and multiple ring topologies across OEM and plant-wide or site-wide IACS applications.</td>
</tr>
<tr>
<td>Deploying Scalable Time Distribution within a Converged Plantwide Ethernet Architecture Design Guide, publication ENET-TD016</td>
<td>Outlines several use cases for designing and deploying Stratix IES to enable CIP Sync™ and IEEE 1588 Precision Time Protocol (PTP) across OEM and plant-wide or site-wide IACS applications.</td>
</tr>
<tr>
<td>Cloud Connectivity to a Converged Plantwide Ethernet Architecture Application Guide, publication ENET-TD017</td>
<td>Outlines several industrial security architecture use cases for designing and deploying restricted end-to-end outbound connectivity with FactoryTalk software from the skid/equipment/machine to the enterprise to the cloud within a CPwE architecture.</td>
</tr>
<tr>
<td>OEM Networking within a Converged Plantwide Ethernet Architecture Design Guide, publication ENET-TD018</td>
<td>Outlines several use cases for designing and deploying lightly managed and managed Stratix IES, including convergence-ready design considerations, across OEM and plant-wide or site-wide IACS applications.</td>
</tr>
<tr>
<td>Deploying Network Security within a Converged Plantwide Ethernet Architecture Design and Implementation Guide, publication ENET-TD019</td>
<td>Outlines several use cases for designing, deploying, and managing network security throughout a plant-wide or site-wide IACS network. FactoryTalk® Network Manager™ software for network visibility and identification. Software-defined security group policy segmentation enabled by Cisco Identity Services Engine (ISE), Stratix industrial Ethernet switches (IES), security group tags (SGT), and Cisco TrustSec. Cisco Stealthwatch for network flow and threat detection.</td>
</tr>
<tr>
<td>Deploying Parallel Redundancy Protocol within a Converged Plantwide Ethernet Architecture White Paper, publication ENET-WP041</td>
<td>Outlines several use cases for designing and deploying Parallel Redundancy Protocol (PRP) technology for redundant network architectures across plant-wide or site-wide IACS applications.</td>
</tr>
</tbody>
</table>

ODVA References

<table>
<thead>
<tr>
<th>Resource</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EtherNet/IP website, <a href="http://www.odva.org/Technology-Standards/EtherNet-IP/Overview">http://www.odva.org/Technology-Standards/EtherNet-IP/Overview</a></td>
<td>ODVA is a global association whose members comprise the world’s leading automation companies. ODVA’s mission is to advance open, interoperable information and communication technologies in industrial automation. ODVA recognizes its media-independent network protocol, the Common Industrial Protocol (CIP), and the network adaptation of CIP - EtherNet/IP.</td>
</tr>
</tbody>
</table>

Rockwell Automation References

<table>
<thead>
<tr>
<th>Resource</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>EtherNet/IP Device Level Ring Application Technique:</td>
<td>Describes DLR network operation, topologies, configuration considerations, and diagnostic methods.</td>
</tr>
<tr>
<td>EtherNet/IP Parallel Redundancy Protocol Application Technique:</td>
<td>Describes PRP network operation, topologies, configuration considerations, and diagnostic methods.</td>
</tr>
<tr>
<td>Ethernet Design Considerations Reference Manual:</td>
<td>Describes basic Ethernet concepts, infrastructure components, and infrastructure features.</td>
</tr>
<tr>
<td>EtherNet/IP IntelliCENTER Reference Manual:</td>
<td>Describes the EtherNet/IP IntelliCENTER® motor control center with a focus on the system architecture and integration into your plant.</td>
</tr>
<tr>
<td>The OEM Guide to Networking:</td>
<td>Key Network Technologies and Considerations when Designing and Deploying Industrial Ethernet Networks</td>
</tr>
<tr>
<td>System Configuration Drawings:</td>
<td>Rockwell Automation landing page for System Configuration Drawings. Provides examples of how to build a scalable integrated architecture for your industrial application.</td>
</tr>
<tr>
<td>Industrial Security:</td>
<td>Rockwell Automation landing page for security solutions from Plant to Enterprise.</td>
</tr>
<tr>
<td>Integrated Architecture® Builder:</td>
<td>Provides EtherNet/IP network performance and Logix controller utilization estimates based on a particular system layout via the advanced EtherNet/IP capacity tool (system sizing tool) embedded in IAB.</td>
</tr>
<tr>
<td>Stratix Managed Switches User Manual:</td>
<td>Describes how to configure, monitor, and troubleshoot Stratix 5400, 5410, 5700, 8000, 8300, and ArmorStratix™ 5700 managed switches.</td>
</tr>
<tr>
<td>Configure System Security Features User Manual:</td>
<td>Describes how to configure and use Rockwell Automation products to improve the security of your industrial automation system.</td>
</tr>
<tr>
<td>Securing your PlantPAx system in The Connected Enterprise:</td>
<td>White paper that demonstrates how Rockwell Automation® PlantPAx®, a modern distributed control system (DCS), addresses cybersecurity based on the IEC 62443-3-3 standard.</td>
</tr>
</tbody>
</table>

**Cisco References**

<table>
<thead>
<tr>
<th>Resource</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catalyst 9000 Family:</td>
<td>Cisco landing page for the Catalyst® 9000 family of aggregation/distribution and core switches for CPwE plant-wide or site-wide IACS architectures.</td>
</tr>
<tr>
<td>Industrial Integrated Router 809:</td>
<td>Cisco landing page for the 800 family of integrated routers (IR) used within the Mining Smart Industry Architecture (SIA) test bed.</td>
</tr>
</tbody>
</table>
## Panduit References

<table>
<thead>
<tr>
<th>Resource</th>
<th>Description</th>
</tr>
</thead>
</table>

## Endress+Hauser References

<table>
<thead>
<tr>
<th>Resource</th>
<th>Description</th>
</tr>
</thead>
</table>
Rockwell Automation Support

Use the following resources to access support information.

| Direct Dial Codes | Find the Direct Dial Code for your product. Use the code to route your call directly to a technical support engineer. | http://www.rockwellautomation.com/global/support/direct-dial.page |

Documentation Feedback

Your comments will help us serve your documentation needs better. If you have any suggestions on how to improve this document, complete the How Are We Doing? form at http://literature.rockwellautomation.com/idc/groups/literature/documents/du/ra-du002_-en-e.pdf.


Allen-Bradley, ArmorStrati, CompactLogix, ControlLogix, DeviceLogix, E300, FactoryTalk, Flex 5000, IEC 61131-3, Integrated Architecture, IntelliCENTER, Logix 5000, Network Manager, PanelView, PlantPAx, PowerFlex, Rockwell Automation, Rockwell Software, Studio 5000 Logix Designer, ThinManager, VantagePoint, and VersaView are trademarks of Rockwell Automation, Inc.

CIP, CIP Security, CIP Sync, and EtherNet/IP are trademarks of ODVA, Inc.

Catalyst, Cisco, and Cisco Systems are trademarks of Cisco Systems, Inc.

Trademarks not belonging to Rockwell Automation are property of their respective companies.

Rockwell Otomasyon Ticaret A.Ş., Kar Plaza İş Merkezi E Blok Kat:6 34752 İçerenköy, İstanbul, Tel: +90 (216) 5698400

www.rockwellautomation.com

Power, Control and Information Solutions Headquarters

Americas: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
Europe/Middle East/Africa: Rockwell Automation NV, Pegasus Park, De Kiezelaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
Asia Pacific: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Publication MIN-AT002A-EN-P - November 2019 Copyright © 2019 Rockwell Automation, Inc. All rights reserved. Printed in the U.S.A.