Implementation of Machine Connectivity in Low-Volume High Variety Manufacturing Line

by

Kanishk Pal

Bachelor of Science in Aerospace Engineering
Illinois Institute of Technology, 2023

Submitted to the Department of Mechanical Engineering
in partial fulfillment of the requirements for the degree of

MASTER OF ENGINEERING IN MANUFACTURING

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

September 2024

Authored By: Kanishk Pal
Department of Mechanical Engineering
August 9, 2024

Certified by Brian W. Anthony
Principal Research Scientist
Thesis Supervisor

Accepted by Nicholas Hadjiconstantinou
Professor of Mechanical Engineering
Graduate Officer

This page is intentionally left blank.

Implementation of Machine Connectivity in Low-Volume High Variety Manufacturing Facility

by

Kanishk Pal

Bachelor of Science in Aerospace Engineering
Illinois Institute of Technology, 2023

Submitted to the Department of Mechanical Engineering on August 9, 2024,
in partial fulfillment of the requirements for the degree of
Master of Engineering in Manufacturing.

Abstract

This thesis provides a comprehensive analysis and implementation plan for enhancing machine connectivity within a manufacturing facility at SLB. The study investigates the existing limitations of the facility's connectivity infrastructure and proposes an advanced connectivity software suite as a solution, presenting a compelling business case for its implementation. The software's scope involved DNC (direct numerical control), allowing for line-by-line feeding of CNC code to machine controllers, as well as machine data collection for real-time shop floor monitoring. The research emphasizes the development and implementation of an advanced network infrastructure designed to improve efficiency, security, and data handling capabilities. There is discussion regarding cybersecurity practices, specifically those related to industrial control systems that leverage CNC machining processes. The software implementation process is detailed, highlighting the necessary steps and information required for successful integration. These include: 1) securing connection to critical CNC machine controllers, 2) acquisition of hardware including local server and network switch, 3) server bring-up through remote imaging and installation of standard monitoring tools and 4) implementation of software on edge devices for CNC file transfer and machining data collection. Additionally, the thesis discusses the limitations encountered during implementation and outlines future steps to address these challenges.

This page is intentionally left blank.

Acknowledgements

I extend my deepest gratitude the following people below for their constant support and mentorship:

To the *Advanced Manufacturing and Design Program* at MIT and SLB for making this collaboration possible.

To the 2024 *cohort* and the everlasting friendships we've forged over the course of the year.

To *Kenan Sehnawi* for welcoming me to his home, and to his family for treating me like one of their own.

To *Brandon Sun* for accompanying me to this journey down South.

To my managers *Alex Soo, Xifan Li* and *Bhavna Singh* for their boundless support

To *Dr. Brian Anthony* for his advice and guidance over the course of the project.

To *my brother* for being my confidant, always by my side.

To *my father* for being infinitely patient and pushing me onward,

and to *my mother* for being a pillar of strength despite this tumultuous year.

This page is intentionally left blank.

Table of Contents

Abstract **3**
Acknowledgements **5**
Table of Contents **7**
List of Tables & Figures **10**
Chapter 1: Introduction **11**
1.1 Company Background 11
1.2 Automated Data Collection - Machine Connectivity 12
1.2.1 Industry 4.0 12
1.3 Motivation 13
1.4 Approach 14
1.5 Division of Work 14
1.6 Thesis Outline 15
Chapter 2: Machine Connectivity **16**
2.1 CNC Machines 16
2.2. SLB Houston Area Machine Connectivity Overview and Applications 17
2.3 Machine Connectivity Benefits 17
2.4. Low Volume High Variety Manufacturing Environment 18
2.5. Completions Houston Product Center (CHPC) Facility Overview 19
2.3.1 Completions System 21
2.3.2 Completions Valves Manufacturing Process Flow 23
2.3.3 Valve Manufacturing - Bottleneck Operation 24
2.3.4 Existing Connectivity Infrastructure 25
2.3.5 Connectivity Limitations 26
2.3.6 DCDO (Door Close Door Open) Work Cell 28
Chapter 3: Connectivity Software Overview **29**
3.1. Software Package Overview (CIMCO Suite of Products) 29
3.1.1 NC-Base 29
3.1.2 PDM 30
3.1.3 MDM 30
3.1.4 DNC-Max 30
3.1.6 Software Environment at CHPC 32
3.2. Alternative Connectivity Solutions 33
3.3. Connectivity Solution Selection for CHPC Facility 35
Chapter 4: Network Infrastructure and Setup **37**
4.1. Existing Network Infrastructure 38
4.1.1. Existing Network Overview 38

4.1.2. CIMCO PDM Implementation..... 39
4.2. Proposed Network Infrastructure.....41
4.2.1 Server.....41
4.2.1.1 Azure Cloud Application Requirements.....42
4.2.1.2 Local (CHPC) Hosted Server.....44
4.2.1.3 Server Implementation Recommendations.....46
4.2.2. CIMCO Server Recommendation.....48
4.2.3. CIMCO Network Infrastructure Recommendation..... 50
4.2.4 Network Diagnostics - Traceroute..... 51
4.2.5 Proposed Network Infrastructure.....53
4.3 Network Security and IT considerations.....55
4.3.1 Overall SLB Network Policies.....55
4.3.2 Security Assessment and Qualification Process (SAQP)..... 56
4.3.2 Industrial Automation & Cyber Security (IACS)..... 58
4.3.2.1 IEC 62443 Compliance.....58
4.3.2.2 Air-gapping.....59
4.3.2.3 Cloud Server Requirements.....59
4.3.2.4 Network Segmentation.....60
4.3.2.5 Industrial DMZ (iDMZ) Concept..... 63
4.3.3. Project Network Security Concerns.....66
4.3.4. Network Security Concern Resolution..... 67
4.3. Connection Hardware..... 69
4.3.1 General Connection Hardware.....69
4.3.2 MOXA Hardware.....69
4.3.2.1 Port Configuration..... 70
4.4.2.2 Firewall..... 72
4.4.2.3 In-Built Security.....73
4.4.2.4 NAT Protocol Issues with IACS..... 74
4.4.3 Network Switch..... 75
Chapter 5: Connectivity Solution Execution.....77
5.1. Machine Information..... 77
5.1.1 Pinging Machines.....79
5.2. Azure Server Bringup Attempt..... 81
5.3. Hardware Quotation.....82
5.2. CHPC Network Segmentation Structure..... 82
5.3. Cloud Server Limitations.....83
5.4. Connection Security Challenges.....84
Chapter 6: Future Work..... 86

6.1. CIMCO Connectivity Project Full-scale Implementation Guidelines..... 86
6.2. CIMCO Licensing..... 87
6.3 Cybersecurity Guidelines..... 88
6.3.1 Purdue Enterprise Reference Architecture..... 88
6.3.2 Network Segmentation Goals at CHPC..... 89
6.3.3 Segmentation and Separation..... 91
6.3.4 Segmentation Criteria:..... 93
6.3.5 Cloud Considerations..... 94
6.5. Azure HCI (Hyperconverged Infrastructure)..... 95
Appendix 1: Value Stream Mapping of Production Part..... 97
Appendix 2: General SAQP Process Flow..... 98
Appendix 3: SAQP process flow for an IaaS cloud-based application..... 99
Appendix 4: CIMCO Pricing Structure..... 100
References..... 103

List of Tables & Figures

Figure 1: SLB Manufacturing Overview..... 12
Figure 2.1: CHPC Manufacturing Process Flow..... 19
Figure 2.2: General Flow Control Valve (FCV) Diagram..... 22
Figure 2.3: Cycle-Time Distribution Across Various Manufacturing Operations for a Single Part Production..... 24
Figure 3.1: CIMCO product suite network architecture diagram..... 32
Figure 3.2: MT-Linki Network Architecture..... 33
Table 4.1: Server System Requirements: Minimum vs. Recommended..... 47
Table 4.2: Client System Requirements: Minimum vs. Recommended..... 48
Table 4.3: Latency Recommendation for Data Transfer..... 48
Figure 4.2: Sample Facility Network and vLAN Architecture..... 50
Figure 4.3: Tracerouting on Windows Command Prompt Example Screenshot..... 51
Figure 4.4: Azure Cloud Application Connectivity Network Infrastructure..... 54
Figure 4.5: PERA Model Framework..... 62
Figure 4.6: iDMZ Concept within PERA Model Framework..... 63
Figure 4.7 : Network Port Configuration for Centralized Management of Production Lines..... 70
Figure 4.8 : Firewall Policy for Securing WAN to LAN Traffic..... 72
Table 5.1: Critical CNC Machines at CHPC with Relevant Information..... 77
Figure 5.1: Network Performance Analysis using Ping Response Times and Packet Loss Evaluation for IP Address..... 79
Table 5.2: Hardware Components Quote List..... 81
Figure 6.1: Key Strategies for Effective Network Segmentation..... 89
Figure 6.2: Network Performance Analysis using Ping Response Times and Packet Loss Evaluation for IP Address..... 91

Chapter 1: Introduction

Machine connectivity plays a vital role in boosting operational efficiency, facilitating real-time data collection, and empowering informed decision-making in today's competitive manufacturing landscape. This thesis focuses on improving machine connectivity at an SLB manufacturing facility by identifying and addressing infrastructure limitations while proposing a sophisticated software solution. The section outlines the company's background, motivations, and strategic approach, and also details the authors' contributions within the broader context of other connectivity projects in collaboration with the MIT Advanced Manufacturing and Design Program and SLB.

1.1 Company Background

Founded in Paris, France, in 1926 as the Electric Prospecting Company, SLB began by specializing in wireline logging, a technique for evaluating rock and soil formations [1]. Over the course of a century, SLB underwent significant expansion through operations and acquisitions, carving out a presence in virtually every sector of the oil and gas industry. This rapid expansion resulted in a diverse evolution of SLB's manufacturing facilities, each charting its own path influenced by the distinct management approaches of the acquired entities. Consequently, SLB's facilities exhibit a broad spectrum of operational methodologies and levels of technological advancement [1][[2].

SLB's integrated manufacturing sites serve three primary functions: well construction, reservoir performance, and production systems [2]. The well construction segment concentrates on drilling, measurement, and equipment. Reservoir performance is dedicated to creating tools for subsurface analysis. Lastly, production systems are geared towards developing valves, completions, and surface processes essential for oil and gas extraction [2]. The figure 1 below shows an overview of the manufacturing facilities and their functions at SLB.

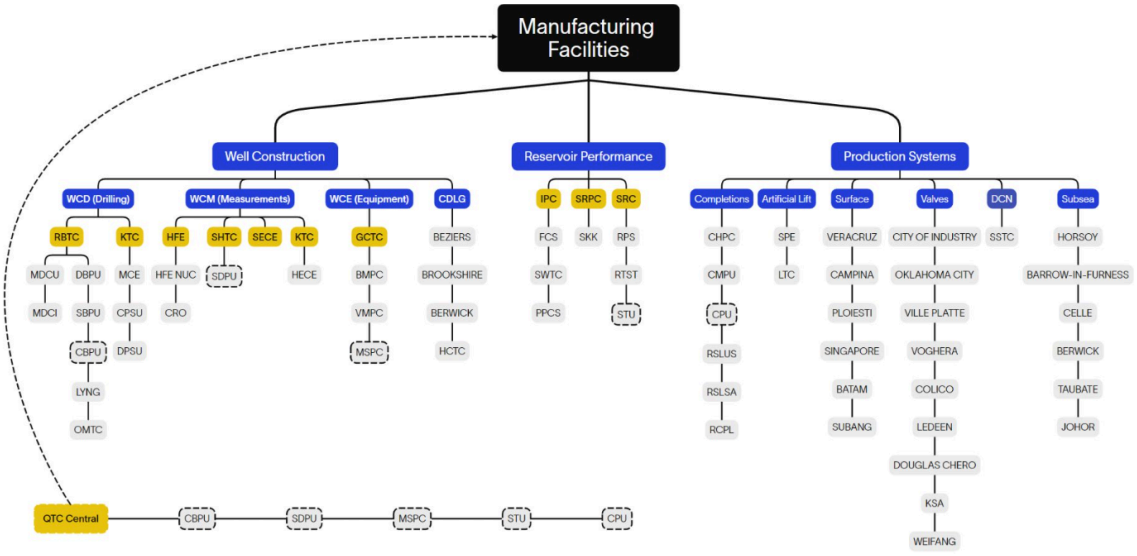


Figure 1: SLB Manufacturing Overview

The diagram displays the different areas of manufacturing within SLB from well construction, reservoir performance and production systems. The diagram breaks down the different functions under each manufacturing areas, as well as the facilities falling under each category [2]

1.2 Automated Data Collection - Machine Connectivity

1.2.1 Industry 4.0

Industry 4.0, also known as the Fourth Industrial Revolution, involves integrating advanced technologies like artificial intelligence (AI), the Internet of Things (IoT), and robotics into manufacturing processes. Smart factories, as cyber-physical systems, use machine-to-machine connectivity, sensors, and automation for real-time monitoring and predictive maintenance [3]. This allows human workers to focus on other tasks while improving overall efficiency. Key components include connectivity, smart machinery, decentralization, big data, and cybersecurity. Additionally, traceability and product identification are enhanced through unique IDs assigned to each component, enabling real-time control throughout the product life cycle [2][3].

1.3 Motivation

SLB's .make program aims at creating cost-basis and performance improvement across manufacturing facilities. Through corporate strategy alignment and strengthening core manufacturing foundation, .make aims to drive a step change in manufacturing performance. The .make program has six critical components:

1. Accelerate and Guide Modernization: This objective focuses on speeding up the company's transition to modern practices and technologies. It involves guiding the organization through the complexities of adopting new systems and processes that align with current industry standards.
2. Evolve Advanced Planning Solutions: The goal here is to refine and enhance the company's planning mechanisms. By evolving these solutions, the company aims to improve its foresight, agility, and ability to respond to market changes effectively.
3. Develop Manufacturing Talent Program: This initiative is about creating a comprehensive talent development program for all manufacturing personnel. It's designed to upskill the workforce, ensuring that employees are well-equipped to handle the latest manufacturing technologies and methodologies.
4. Pivot to Smart Quality Systems: The strategy involves a shift towards intelligent quality control systems that can significantly improve the efficiency and effectiveness of the company's operations. This 'step change' indicates a major improvement over the current processes.
5. Reinvigorate Passion & Pride with Innovation & Technology Programs: Lastly, this objective aims to foster a culture of innovation and pride within the company. By focusing on cutting-edge technology and creative programs, the company hopes to inspire its workforce and reinforce a strong sense of commitment and enthusiasm for their work.
6. Developing supply chain interconnects to create insightful real-time visibility and predictability: This strategic goal aims to enhance the coordination and flow of information across the entire supply chain network. By doing so, the company can achieve more efficient inventory management, reduce lead times, and improve overall supply chain responsiveness to market demands.

1.4 Approach

The motivation for connectivity at low volume high variety manufacturing facilities is discussed, with emphasis on benefits for machine data collection for production parts and remote CNC file transfer to shop-floor machines. A thorough understanding of machine connectivity is gathered through vendor research, correspondence with well-connected SLB facilities and collaboration with global IT, network and security teams. Emphasis is given on the CIMCO suite of connectivity products, namely DNC-Max and MDC-Max for the purpose of executing a trial implementation at an SLB facility in Houston.

The process for implementing machine connectivity at an SLB facility is then extensively explored. Special attention is given to highlighting shortcomings of the current connectivity, network infrastructure and existing vulnerabilities. There is a network infrastructure proposed, which highlights the setup of a new server application to host the connectivity software, the hardware used for the physical connection and security measures taken.

Challenges experienced for connectivity are thoroughly explored, mostly related to the updated cybersecurity requirements for new hardware and software solutions implemented across SLB. This involves the standards that SLB adheres to and the process that will need to be followed for a full-scale implementation of connectivity at the facility. The document therefore also outlines the comprehensive standards that SLB maintains, which serve as a benchmark for the secure implementation of connectivity solutions. It details the procedural steps required for a successful full-scale deployment, emphasizing the need for a methodical approach that aligns with SLB's established security practices.

1.5 Division of Work

This project was undertaken as part of a broader collaboration between SLB and the MIT Advanced Manufacturing and Design Program (AMDP) to exploring and implement machine connectivity at various levels. In conjunction with Mr. Kenan Sehnawi and Mr. Brandon Sun, the author focused specifically on implementing machine connectivity at a manufacturing facility and designing the network architecture to support the software. Sehnawi's thesis provides a comprehensive assessment of machine connectivity across multiple SLB facilities in the Houston area. Meanwhile, Sun's research delves into leveraging machine data collection through connectivity to achieve cycle time savings in a CNC roughing process for a specific production

part. This division of work was strategically planned to demonstrate the value proposition of machine connectivity, encompassing its overall potential, physical implementation, and the tangible benefits realized through enhanced data collection and analysis. Together, these efforts aim to showcase the impact of advanced manufacturing technologies on operational efficiency and productivity, creating a standard for other SLB facilities to follow through their own implementation of connectivity.

1.6 Thesis Outline

This section briefly describes the content of the various sections within this thesis, and provides context to its organization. Chapter 2 focuses on machine connectivity and its benefits to SLB, introduces the manufacturing facility and its operations and provides necessary context into the types of machines used at the facility. There is further detail on the product profile at the facility, as well as the existing connectivity infrastructure and its limitations. Chapter 3 focuses entirely on the connectivity solution software suite to be implemented at the facility, with details on its potential applications. Chapter 4 of the thesis delves into the network infrastructure and setup for the project. It starts by examining the current network setup and policies in place, then moves on to propose enhancements and new implementations to improve the network's efficiency and security. The chapter also addresses various aspects of network diagnostics, data storage, and security measures, ensuring compliance with industry standards. Additionally, it discusses the necessary hardware and software configurations required to connect and manage the machines effectively. The chapter concludes with an analysis of sample data collected from the network, providing insights into its performance and reliability. Chapter 5 focuses on the actual implementation of the solution and specifically into the process followed for connecting and the information required. Chapter 6 explores the limitations of the implementation and highlights future steps to remediate outstanding issues.

Chapter 2: Machine Connectivity

2.1 CNC Machines

CNC (Computer Numerical Control) machines are automated tools used in manufacturing to produce high-precision parts with minimal human intervention [4]. These machines follow programmed instructions to perform complex machining tasks, ensuring consistent and accurate results. The CNC milling process is divided into three main stages: roughing, feature milling, and finishing. Roughing involves removing the bulk of the material quickly to shape the product roughly. Feature milling follows, where higher precision is required to create critical features, using more delicate tools at slower speeds to avoid damage. Finally, the finishing stage refines the product by cleaning up sharp edges and any remaining material, ensuring a smooth and polished final piece. CNC machines are valued for their precision, efficiency, ability to handle complex designs, and consistency, making them indispensable in modern manufacturing [4][5].

SLB, a leading provider of technology and services to the energy industry, relies heavily on CNC machines for manufacturing various components used in their operations. The precision and accuracy offered by CNC machines are crucial for producing parts with tight tolerances, which is essential in the oil and gas industry where even minor deviations can lead to significant operational issues. For example, components like valves, wellhead systems, and drilling tools must meet exact specifications to ensure safety and efficiency.

CNC machines also enhance efficiency in SLB's manufacturing processes. They can operate continuously, 24/7, which significantly increases production rates and reduces downtime. This is particularly important for meeting the high demand for parts and maintaining a steady supply chain. Additionally, CNC machines can handle complex designs and intricate details, which are often required for the sophisticated components used in SLB's advanced technologies.

2.2. SLB Houston Area Machine Connectivity Overview and Applications

Machine connectivity refers to the combination of hardware and software necessary for extracting data from shop floor machines, sensors, and other network-connected devices. It involves equipping machines with adapters, sensors, and software solutions to enable automated data acquisition [8]. Connectivity exists to various extents in SLB facilities across Houston. Some facilities have machine connectivity fully implemented, meaning machines in the facility are connected to a network and machine data is collected and readily accessible remotely. On the other hand, other facilities have dozens of discrete CNC machines with limited connectivity, leading to operational efficiency losses and lowered visibility in their production.

The applications of machine connectivity are vast. Connectivity in the form of a DNC (direct numerical control) software could allow a facility to standardize .nc file management, edit and transfer. Machine data collection from CNC machines could help drive CIP (continuous improvement projects) or when analyzed, provide technical insights on machine health, tool wear, OEE (Overall Equipment Effectiveness). Other connectivity features may include manufacturing document management, which stores files for every production part that is made on the shop-floor.

2.3 Machine Connectivity Benefits

Automated data collection from CNC machines is of particular interest at CHPC, which has over 20 discrete machines used for production parts. Benefits of machine connectivity include:

1. Monitoring of Machine Performance: This involves the real-time tracking of various operational parameters of machines, such as speed, temperature, and output quality. By monitoring these metrics, manufacturers can ensure that machines are operating within their optimal parameters, leading to improved efficiency and product quality. It also helps in identifying potential issues before they lead to downtime [6][8]

2. Aggregation of Data Across Different Machine Types: Machine connectivity allows for the collection and combination of data from diverse types of machinery, regardless of make or model. This aggregated data can provide a comprehensive view of the entire production process, enabling better analysis and insights. It aids in comparing performance across different machines and optimizing the overall workflow [8]
3. Standardization of Machine Communication: This refers to the establishment of common protocols and languages for machine-to-machine communication. Standardization simplifies the integration of new machines into the existing infrastructure and makes it easier to manage and analyze data from various sources. It ensures that all machines 'speak the same language,' which is crucial for efficient data exchange and processing [9]
4. Remote Monitoring of Machine Metrics: With machine connectivity, it's possible to monitor machine metrics from anywhere, not just on the shop floor. This remote monitoring capability is especially beneficial for managers and engineers who need to keep an eye on production without being physically present. It enables quick response to alerts and notifications, leading to faster resolution of issues [8]

2.4. Low Volume High Variety Manufacturing Environment

In the oil extraction process, valves play a critical role in controlling the flow and pressure of oil through the extraction system. The product portfolio for valves boasts tight tolerances, with 0.005" being the standard, ensuring precision and reliability in high-stakes environments. With over 160 unique work centers, CHPC production is equipped to handle a diverse range of valve designs and specifications. Catering to low-volume needs, the manufacturing process is designed for small batch sizes, typically between 1 to 3 per production order, and small sales order quantities ranging from 5 to 10 valves. This approach supports high customization to meet the specific demands of each oil extraction project. Adherence to Quality Control Plan (QCP) requirements guarantees that each valve meets stringent quality standards, while project-specific requirements ensure that the valves are tailored to the unique conditions and challenges of each oil extraction site. This combination of precision, flexibility, and quality control positions these valves as a vital component in the efficient and safe extraction of oil for SLB's customers.

Industry 4.0 tools, especially those focused on machine monitoring, are indispensable in the oil extraction industry, particularly for plants at SLB that prioritize precision and customization. These advanced tools facilitate predictive maintenance, ensuring that machinery operates at peak efficiency and valves meet the exacting 0.005" tolerances required for safe and reliable oil flow control. Real-time data allows for the optimization of the 160 unique work centers, adapting to the small batch production that characterizes SLB's operations. This adaptability is key to meeting the diverse design specifications and quality control plans necessary for each project. By leveraging these smart technologies, SLB can maintain the high standards of quality and customization demanded by their clients, while also enhancing safety and minimizing downtime in the high-stakes environment of oil extraction.

2.5. Completions Houston Product Center (CHPC) Facility Overview

CHPC, or Completions Houston Product Center, is an SLB facility located south-west of Houston, TX. The facility boasts a comprehensive suite of capabilities designed to meet the intricate demands of modern manufacturing. Under Quality Control, the facility offers Optical CMM, Non-Contact CMM Examination, and CNC Machines Inspection, ensuring that products meet the highest standards of precision and quality. The Precision Machining department is equipped with CNC Turning & Mill-Turn, CNC Mill, Semi-Manual Lathe, and Manual Lathe and Mill, allowing for versatile and precise machining operations. Special Processes include RAM & Wire EDM, Hone (Horizontal & Vertical), Gun Drill, and Precision Grinding, providing specialized manufacturing techniques for complex components. The Coating Department handles Zinc Phosphate, Manganese Phosphate, Xylan, Ryton, and Aluminum Oxide Blast, offering a range of protective and functional coatings. Lastly, the Assembly and Test department ensures product integrity with High Pressure Test Bays, Factory Acceptance Tests (FAT), Torque Machine operations, and an in-house developed ESD Laboratory, guaranteeing that each product is tested and validated to perform under the most demanding conditions. Each of these capabilities reflects the facility's commitment to quality, precision, and innovation in manufacturing. The figure 2.1 below shows a process flow diagram of a typical production valve produced at the CHPC facility.

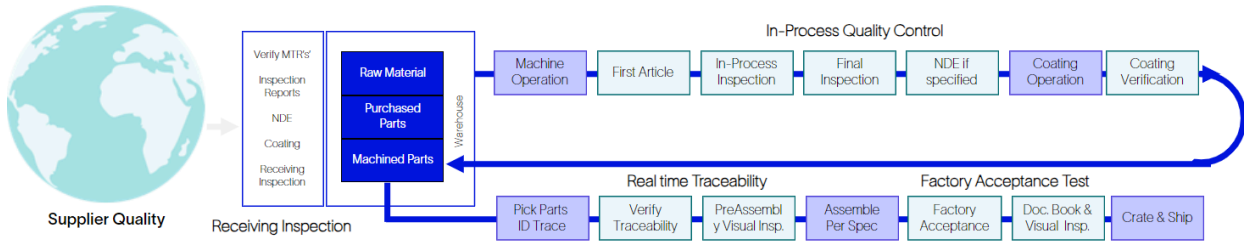


Figure 2.1: CHPC Manufacturing Process Flow

The diagram displays the different areas of manufacturing within SLB from well construction, reservoir performance and production systems. The diagram breaks down the different functions under each manufacturing areas, as well as the facilities falling under each category

The process flow depicted in the Figure 2.1 outlines a comprehensive quality control system for managing raw materials through to the final product shipment. It begins with Supplier Quality, ensuring that the initial materials meet the necessary standards. The raw materials are then categorized into Purchased Parts and Machined Parts, each undergoing a specific set of processes. Heat Treatment is applied where necessary, followed by In-Process Inspection to monitor quality during manufacturing. Afterward, a Final Inspection is conducted to ensure the end product meets the required specifications.

Quality control is further emphasized through Non-Destructive Examination/Testing (NDE/NDT), Coating Operations, and Calibration Verification. These steps are crucial for maintaining the integrity and performance of the products. Alongside these stages, the process flow includes Real-Time Traceability measures such as identifying parts, verifying materials, and tracking personnel and equipment involved. This ensures accountability and traceability throughout the production cycle.

The process concludes with a Factory Acceptance Test, where the final product is rigorously tested and reviewed before being cleared for shipment. This comprehensive approach to quality control and traceability ensures that every product shipped meets the highest standards of quality and reliability.

2.3.1 Completions System

Completions play a crucial role in managing hydrocarbons within the wellbore, with a focus on optimizing reservoir drainage and productivity. The process of completion involves making a well ready for production or injection. It encompasses the design, selection, and installation of tubulars, tools, and equipment located in the wellbore specifically for the purpose of producing or injecting hydrocarbons (oil/gas).

Completions serve various purposes, including:

1. Reservoir monitoring and control, which allow operators to monitor and control reservoir behavior effectively. By selecting the right completion components, operators can optimize production and manage reservoir dynamics
2. Core completions, which involve the critical components necessary for well functionality. These components ensure safe and efficient production or injection
3. Liner Hangers, that are part of the completion assembly and provide support for tubing strings within the wellbore. They play a key role in maintaining well integrity.

The completions products that are developed by SLB in their various completions facilities (including but not limited to CHPC) are:

1. Wellbore/Reservoir Interface:
    a. Open Hole Completions: These occur in wells where the borehole is not cased. Open Hole completions involve directly interacting with the formation.
    b. Cased Hole Completions: In cased hole completions, the wellbore is lined with casing. These completions are common in mature fields or when drilling through unstable formations.
2. Production Method:
    a. Natural Flowing Completions: In natural flowing completions, reservoir pressure drives hydrocarbons to the surface without artificial lift methods.

b. Pumped Production (Artificial Lift) Completions: These involve using artificial lift techniques (such as electric submersible pumps, gas lift, or rod pumps) to enhance production rates.

3. Number of Producing Zones:
    a. Single Zone Completions: These completions target a single reservoir zone. They are simpler but may not fully exploit the reservoir's potential.
    b. Multiple Zone Completions: In wells with multiple productive zones, completions systems allow selective control of each zone. This maximizes overall productivity.

The components that commonly comprise the completions system involve safety valves, tubing, expansion joints, packers and the nipple. The packer is the key equipment in the completion string which provides isolation & downhole anchoring functions. Figure 2.2 shows the components labeled on a generalized completions system

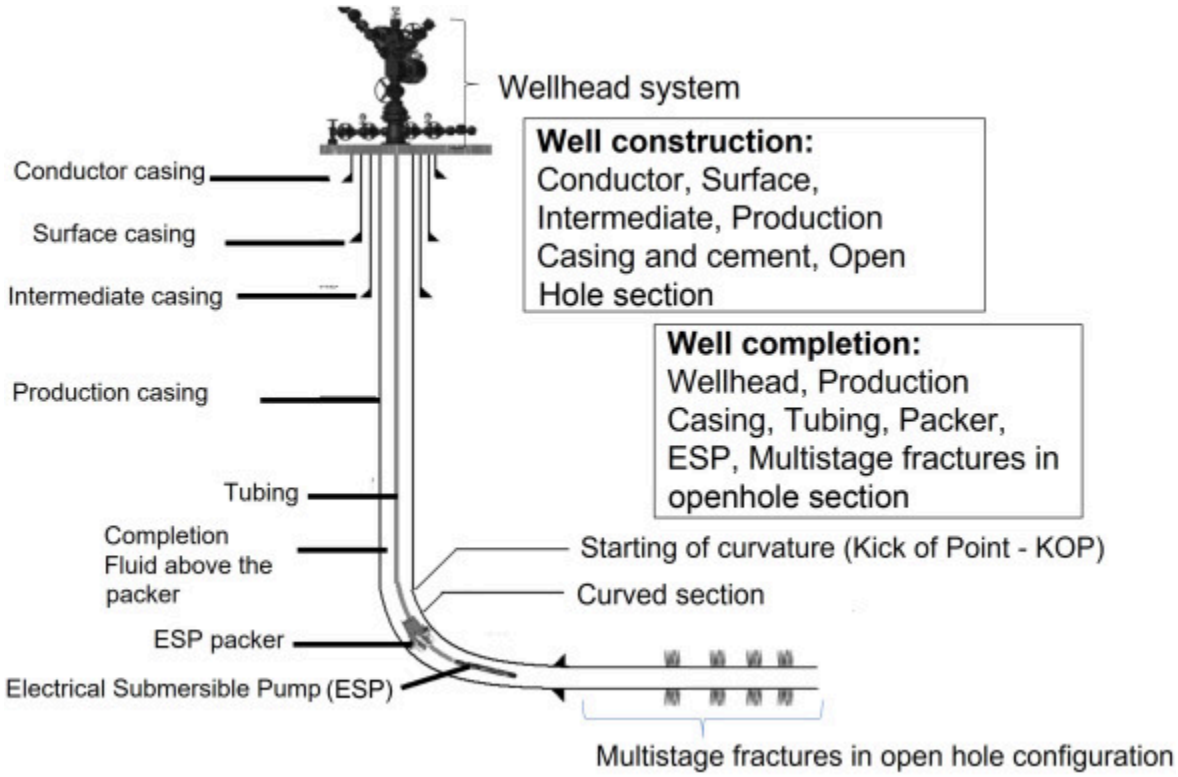


Figure 2.2: General Flow Control Valve (FCV) Diagram

The figure illustrates the complex system for a flow-control valve from the surface to the subterranean layers, highlighting key parts of the valve such as the surface casing, production casing, and tubing. The annulus, marked by low pressure and/or inhibited fluid, is shown to protect the casing strings, ideally maintaining a pressure higher than the formation pressure. Notable features include the packer, landing nipple, and perforated production tube, which are essential for the well's operation in high-pressure and corrosive environments. The perforations allow for the flow of oil into the well [10]

The valves that are manufactured at CHPC are typically placed above the packer. By isolating the valves from reservoir fluids, this positioning prevents leaks or damage due to exposure to corrosive substances or high pressures. It ensures reliable operation and minimizes risks associated with fluid migration.

2.3.2 Completions Valves Manufacturing Process Flow

The Completions Houston Product Center (CHPC) is responsible for manufacturing components for the completion of wells, making them ready for production or injection. A completion system ensures safe, efficient, and economical oil or gas production. CHPC manufactures three types of components:

1. Safety Valves: These fail-safe devices prevent losses by closing the well during emergencies or undesirable events, preventing uncontrolled hydrocarbon releases. Safety valves come in two types: surface-controlled (tubing retrievable, wireline/slickline retrievable) and subsurface-controlled (velocity valve).
2. Flow Control Valves (FCV): These valves manage production or injection flow by selectively controlling multiple zones. They reduce water and gas cut, minimize well interventions, and maximize productivity.
3. Formation Isolation Valves (FIV): FIVs isolate wellbore and reservoir fluids, minimizing formation damage during completion, drilling, and workover operations. These valves are remotely operated ball valves with bi-directional barriers, adhering to standards such as API 19V and ISO 28781.

The purpose of isolation valves includes protecting formations from pressure and fluids, preventing flow from the reservoir before production starts, improving well productivity, minimizing fluid loss to the formation, enabling batch drilling/completion operations, reducing rig time, lowering intervention costs, and allowing fluid exchange to initiate production.

The design overview of Formation Isolation Valves (FIVs) involves monobore completion valves typically placed below the packer. These ball valves seal pressure from both above and below. An N2-charged trip saver system allows the ball to be opened by tubing pressure cycles, and it can also be manually opened/closed using a mechanical shifting tool.

Shifting tool actuation involves collets latching onto the FIV collets, causing the ball to rotate open or closed. Tubing pressure actuation relies on a precharged nitrogen spring that cycles with tubing pressure changes. After a predetermined number of cycles, the FIV opens without intervention, even without running a shifting tool.

2.3.3 Valve Manufacturing - Bottleneck Operation

The value stream map (VSM) of a FCV part is present in Appendix 1. Note that certain confidential information regarding specific values of time have been redacted. This is specifically for a Flow Control valve, the description on the part being. “FLOW CONTROL SUB, EXTENDED BORE”. The lower part of the chart highlights the cycle-time at each step in the production through a bar chart depiction, with the pink representing value added and green being the non-value added time. The various operations used in the manufacturing of the part are listed, with their cycle times represented on the y-axis. These operations include saw, E-70 (CNC), MAHO (CNC), drilling, E-90 (CNC), saw, de-burring, inspection, RAM EDM, honing, Integrex, NDE-11 and further inspection. The “Integrex” data corresponds to the cycle-time for 5-axis machining of the part done on the Mazak Integrex . This is a DCDO (door-close-door-open) CNC machine, and its criticality and use is described in section 2.3.5.

As determined from the Figure 2.3 below, the “Integrex” data shows that this step requires the greatest cycle-time, and is therefore currently the bottleneck operation for this part. Similarly, the 5-axis Integrex machines are frequently the bottleneck operation. Improving cycle-time for these CNC machines can be challenging, especially when there is no information

being collected from the machine such as speed/feed rates, loads and temperatures. Developing an architecture for machine connectivity for 5-axis CNC machines is therefore crucial for championing continuous improvement projects in manufacturing at the CHPC facility.

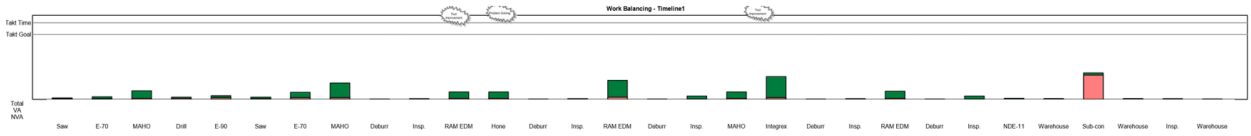


Figure 2.3: Cycle-Time Distribution Across Various Manufacturing Operations for a Single Part Production

The figure presents a comprehensive analysis of the cycle times associated with various manufacturing operations required for the production of a specific part. The y-axis quantifies the cycle times, while the x-axis enumerates the sequential operations, ranging from initial sawing to the final inspection process. Notably, the "Integrex" operation, which involves 5-axis machining on the Mazak Integrex CNC machine, is highlighted as the step with the highest cycle time, indicating its role as the primary bottleneck in the manufacturing sequence. Note that actual times have been redacted

2.3.4 Existing Connectivity Infrastructure

CIMCO PDM (Product Data Management), released pre-2011 was the flagship product released by CIMCO for data management, which organized and managed CAM files and related production documents for the shop-floor. The software provides information management system functionalities, allowing users to gather, structure, and centralize production documents. This includes the ability to transfer essential production documents such as setup sheets, tool lists, pictures, and other information directly to the shop floor.

CIMCO PDM leverages CIMCO NC-Base Database Server and CIMCO PDM Server to manage its communication. To get CIMCO PDM operational, both CIMCO PDM and CIMCO NC-Base Database Server were installed. The NC-Base Database Server is currently run on a local Windows 2008R2 Server, first deployed in 2011. This setup created an efficient and robust environment for managing product data within the CIMCO ecosystem at CHPC.

CNC File transfer is currently completed through the CIMCO server, where .nc files are accessed through the main SLB network. The transfer from the shop-floor edge device and the machine controller is done through USB-drives, from where the program is run.

2.3.5 Connectivity Limitations

The CIMCO PDM system has since been succeeded by CIMCO MDM and CIMCO MDC-Max, which are the manufacturing document management and manufacturing data collection softwares respectively. While PDM offered a foundation for data management, the CIMCO ecosystem has expanded to include .nc file edit and transfer as well as manufacturing information collection and analysis. CIMCO PDM falls short in providing the real-time data insights and other features that CHPC's modern manufacturing operations demand. Therefore, there is motivation behind implementing CIMCO's newer software products to improve the connectivity at the facility.

Additionally, although CIMCO PDM had been implemented, it is currently inoperable at the CHPC facility. The local server US04APP03 currently hosts the information from CIMCO PDM. However, with OS (operating system) support for Windows 7 ending in 2015, the server remains vulnerable to DoS (denial-of-service) attacks. Server patching, which involves applying software updates, to address vulnerabilities and security flaws cannot be completed due to the outdated OS. Furthemore, the server itself is a Windows Server 2008R2 (Standard 64-bit edition), for which support ended in 2013. This has also resulted in SQL services being suspended, prohibiting any management or manipulating of the databases on the server. Without access to the server, the PDM software cannot communicate information. Currently, the following vulnerabilities of high criticality have been identified:

1. Microsoft Windows Security Update Missing Registry Key: This issue pertains to a missing registry key that is required for the verification of a successful installation of a security update, potentially leaving the system vulnerable if the update is not properly recognized [11].
2. Microsoft Windows Search Remote Code Execution (RCE) Vulnerability: This vulnerability in Windows Search could allow an attacker to perform remote code execution, enabling them to take control of the affected system by exploiting a flaw in the search component [12].

3. EOL/Obsolete Software: Microsoft SQL Server 2014 Service Pack: The end-of-life status of Microsoft SQL Server 2014 Service Pack indicates that it no longer receives security updates or technical support, increasing the risk of security vulnerabilities and compliance issues [13].
4. Oracle Java Critical Patch Update Missing: The absence of a critical patch update for Oracle Java can expose systems to severe security risks, as these patches are typically released to fix vulnerabilities that could be exploited by cyber attackers [14]
5. Windows SMB (Server Message Block) Version 1 Obsolete: The obsolescence of Windows SMB Version 1 reflects its vulnerability to security breaches and highlights the necessity for upgrading to more secure versions.

There are limited methods for rectifying the non-compliance issue. Updating the server to a Windows Server 2016R2 or newer would ensure the necessary updates and patches can be completed by the global IT team. Purchasing a new server would require server setup through the ESM (Enterprise Service Management) team, which will install the SLB standard cybersecurity tools for monitoring and access settings.

The .nc file transfer is currently conducted through the outdated CIMCO server, which is accessed through the main SLB server. Integrating machines into the same network as a company's main infrastructure introduces several cybersecurity risks. This practice could leave the network vulnerable to parties who might intentionally impair CNC machine functionality, affecting production. Loose network protocols may allow attackers to exfiltrate sensitive production information or confidential program code from PDM, which itself hosts a repository of manufacturing related documents such as CNC programs, CAD/CAM files, setup sheets, tool lists and images. Unauthorized access to these materials.

Consequently, CHPC currently has minimal connectivity in the facility. There is very little visibility on the NC file transfer, machine or production information. Additionally, the absence of local servers compliant with SLB security protocols has hindered any further development of connectivity solutions.

2.3.6 DCDO (Door Close Door Open) Work Cell

The DCDO Work Cell at CHPC consists of three MAZAK INTEGREX centers, combining the functionalities of a CNC turning center and a machining center. It allows for the completion of various operations such as turning, milling, boring, and drilling in a single setup. This machine ensures high precision and performance, and is particularly suited for large-diameter, shaft-type workpieces, making it ideal for CHPC product lines.

The machining step in the manufacturing process of ___ often becomes a bottleneck, limiting overall production capacity. Introducing these DCDO machines can increase capacity and boost throughput. However, these machines have yet to be fully qualified for use on production parts. Therefore, there is untapped capacity on the shop-floor in the form of idle machines. Qualifying these machines would involve running time-studies on the parts. However, useful information from these machines could be collected to analyze its performance. Information regarding spindle status, speeds/feeds/loads, overrides could help production managers characterize baseline performance, and explore continuous improvement projects.

Chapter 3: Connectivity Software Overview

Machine connectivity software is the technology that enables different machines and systems within a factory to communicate with each other, or to a broader network. This connectivity allows for real-time data exchange, enhancing visibility and control over the entire production process. This section will focus on CIMCO, a machine connectivity software provider with headquarters in Copanhagen, Denmark. With a global network of resellers and consultants, CIMCO has successfully delivered over 100,000 licenses worldwide, demonstrating its extensive reach and influence in the industry [15].

3.1. Software Package Overview (CIMCO Suite of Products)

CIMCO is a leading provider of advanced CNC solutions that facilitate seamless connectivity and management of machine tools on the manufacturing floor. Their suite of products, including NC-Base, PDM, MDM, DNC-Max, and MDC-Max, offers a comprehensive ecosystem for handling CNC program files, production documentation, and real-time machine monitoring [15]. CIMCO's systems enable manufacturers to maintain version control, implement paperless operations, and ensure efficient communication between CNC controllers and databases. With capabilities for secure file transfer, data analysis, and system administration, CIMCO plays a pivotal role in optimizing the productivity and performance of CNC machinery, making it an integral part of modern manufacturing environments where precision and reliability are paramount [15][16]. Their solutions are particularly relevant for industries that rely on CNC machines for their production processes, providing the necessary tools to manage and monitor these complex systems effectively [15].

3.1.1 NC-Base

The NC-Base Database Server operates as a Windows service, managing one or multiple SQL databases. Its core functions include data storage, processing, and retrieval. Additionally, the server offers an extensive range of features for version control, backup, and data import [17].

3.1.2 PDM

CIMCO PDM (Product Data Management) was a flagship product by CIMCO for organizing and managing CAM files and production documents on the shop floor. It served as an information management system, allowing users to centralize and structure essential production documents such as setup sheets, tool lists, and images. By leveraging the CIMCO NC-Base Database Server and CIMCO PDM Server, CIMCO PDM facilitated efficient communication and streamlined data management within the CHPC ecosystem [18].

3.1.3 MDM

CIMCO MDM is the manufacturing document management system that succeeds NC-Base. The software manages, controls and stores production documentation such as CAD, CAM and .nc files. MDM allows users to track changes to documents and programs, implement paperless manufacturing and a consolidated source for all production related files. Automation is built within the software for file handling, allowing users to categorize new additions without individual manual entries [19].

MDM requires CIMCO DNC-Max for operation with FANUC FOCAS or Heidenhain CNC controllers as well as a CIMCO database server (NC-Base). A MSSQL database can be used instead of the CIMCO database which can be configured during the MDM installation, allowing flexibility with data storage. Web clients can also be added, allowing hypertext transfer protocol (http) for handling requests from the database [19].

3.1.4 DNC-Max

CIMCO DNC-Max is a CNC communication software that handles .nc program file transfer, monitoring and system administration [20]. DNC-Max is a client-server solution consisting of the DNC-Max client (or web-client) and DNC-Max server. The DNC-Max server can run as an application or background service, and is responsible for handling all communication [20][21]. This server works on the CIMCO database server, which is the

overarching SQL database on which CIMCO's products run. The DNC-Max client is the PC interface, allowing management of local or remote file transfers, monitoring of machine ports and remote network configuration to multiple servers [21].

DNC-Max allows program transfers directly at the CNC controller level or via a web-client using an edge device. Controllers with ethernet capabilities can browse, select and download programs directly onto the local storage from the server [20]. Version and revision control is another capability of DNC-max, which tracks edits made by operators and programmers, giving a user the ability to track changes and revert to previous versions as necessary [20].

The hardware required for DNC-Max to be fully utilized would involve RS-232 or RJ45 cables allowing devices (controllers or edge devices) to allow file transfer through the database. Legacy controllers may require additional hardware for networking. Some SLB facilities have used Moxa serial-to-Ethernet devices to enable this. Hardware required for connectivity is discussed further in 4.3.2

3.1.5 MDC-Max

MDC-Max is a software solution designed for real-time monitoring of machine tools. MDC-Max allows users to gather and analyze data from machines and operators, providing real-time and historical insights into shop floor productivity, performance, and quality [22]. This data serves various purposes, including real-time monitoring using Andon boards, planning, analysis, and export to other systems like ERP or MES. When events occur (such as a machine starting or stopping), MDC-Max generates messages and stores them in its database. The MDC-Max client utilizes this database to create real-time status screens and historical reports, providing insights into machine activity [22].

The potential applications for data collected and analyzed through MDC-Max may range from OEE (overall equipment effectiveness) calculations or timers (tracking cycle-time, setup-time, down-time and idle-time) to maintenance tracking and scrap rates. Several data visualization options such as time-series charts and tables are available for users to further process [22].

The DNC-Max server still functions as the centralized data collection source with MDC-Max acting as a client. The DNC-Max Server is responsible for processing message data,

calculating timers, and managing states. It must run continuously, as the clients cannot operate independently. When the server detects a string of text or a line change on any of its ports, it converts these events into MDC messages [22][23].

3.1.6 Software Environment at CHPC

DNC-Max software is installed as a server on a virtual machine within the company environment. Companies typically install one DNC-Max server per site to minimize latency in information transfer. This approach eliminates the need for multiple servers and ensures efficient communication. The DNC-Max server supports several simultaneous ports for different communication protocols, including Ethernet and RS-232. This versatility allows compatibility with various CNC controllers and PLCs. This server connects to machine controllers and clients, such as the DNC-Max client, MDC-Max, and web clients. These connections enable data display and interaction. The file management system client (either NC-Base or MDM) links to the CIMCO Database Server. Users can interact with the file directory through this connection. An overview of this architecture is presented in the Figure 3.1 below.

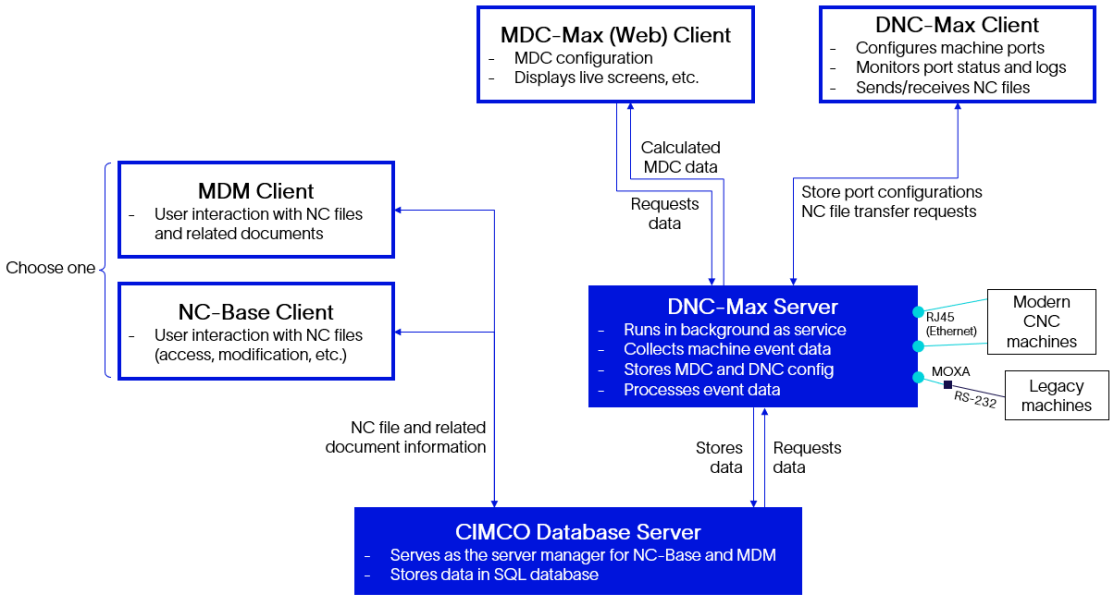


Figure 3.1: CIMCO product suite network architecture diagram

This diagram outlines the relationships between the various servers and clients offered in the CIMCO product suite. The CIMCO Database Server serves as the foundation for the entire ecosystem and is required.

3.2. Alternative Connectivity Solutions

Before diving into the implementation of machine connectivity, it's essential to explore various software solutions that have been successfully adopted by facilities, particularly within SLB. While CIMCO has been a popular choice, it's important to note that other SLB sites have effectively utilized different software to achieve similar goals. This section focuses on FANUC MT-Linki, a powerful connectivity solution that has proven to be highly effective in various shop floor environments.

FANUC, a well-established name in industrial automation, offers MT-Linki, a robust software designed to facilitate connectivity across a wide range of machines and devices. MT-Linki allows for real-time data collection, monitoring, and analysis, enabling operators to optimize machine performance and enhance overall productivity. Its versatility makes it an excellent fit for shop floors with diverse machine types and complex automation needs, ensuring that facilities can maintain high levels of efficiency and reliability [24].

FANUC's MT-Linki is an advanced operational management software tailored for factory environments, offering comprehensive machine connectivity through several protocols such as Ethernet [25]. Designed primarily for use with FANUC CNC controllers and robots, MT-Linki excels in gathering, managing, and visualizing machine data. However, its versatility extends beyond FANUC equipment, as it can also interface with third-party machines using widely adopted protocols like OPC-UA and MTConnect [25]. This flexibility makes it an ideal solution for facilities with a mix of machinery from different manufacturers. Figure 3.2 shows two different methods of connection for different scales of systems.

One of the key strengths of MT-Linki is its scalable architecture, allowing it to grow with a shop floor's evolving needs. Data collection is handled by a specialized collector PC software,

while storage and management occur on a server PC. This server also hosts a web interface accessible from any network-connected device, such as PCs or tablets, making it easy to monitor and manage production from virtually anywhere within the facility.

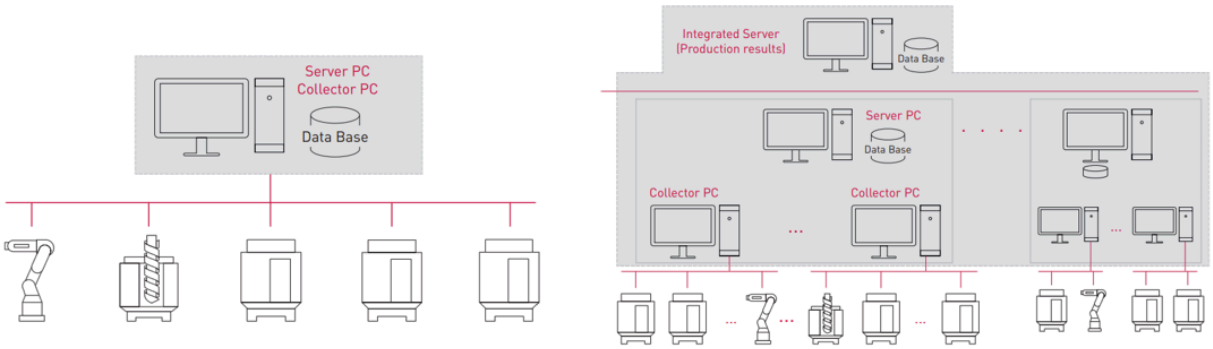


Figure 3.2: MT-Linki Network Architecture

The diagram on the left illustrates the network architecture for smaller systems with a limited number of devices. In contrast, the diagram on the right depicts the architecture for larger systems with over 100 devices. These larger systems necessitate multiple server and collector PCs that integrate with the MT-Linki Integration Server.. [25]

MT-Linki's capabilities include real-time monitoring of machine status, alarm management, signal tracking (e.g., feed rates, spindle loads), and historical data analysis [24]. Additionally, it supports NC file transfer between CNC machines and the server, though it does not support line-by-line DNC control, which may necessitate an additional solution depending on your setup. For larger systems with over 100 devices, FANUC offers an MT-Linki Integration Server that aggregates data from multiple sites, providing a robust solution for enterprise-level monitoring and management [24][25]. Overall, MT-Linki is a powerful tool for any facility looking to enhance its operational efficiency through detailed machine monitoring and data-driven decision-making

3.3. Connectivity Solution Selection for CHPC Facility

When deciding between CIMCO and FANUC's MT-Linki for machine connectivity in a facility, the choice hinges on the specific needs of the shop floor, the type of equipment in use, and the desired features for operational management.

CIMCO is typically chosen for its strong capabilities in CNC file management, DNC (Direct Numerical Control), and comprehensive editing tools. It's particularly favored in facilities where managing large numbers of CNC programs and ensuring precise control over them is critical. CIMCO excels in environments that require extensive file editing, version control, and the ability to send NC programs directly to machines line-by-line, which is essential for real-time, on-the-fly adjustments during machining operations. Additionally, CIMCO offers powerful tools for monitoring and analyzing machine performance, which can be integrated with broader manufacturing execution systems (MES) for end-to-end production management.

CHPC's production capabilities are extensive, with over 160 unique work centers dedicated to manufacturing a diverse range of valve designs and specifications. The facility is optimized for low-volume, high-customization production, with batch sizes typically ranging from 1 to 3 units per order and sales order quantities between 5 to 10 valves. In such settings, although production volumes may be low, each component often requires several different .nc files. This is because the same production part may go through different machining steps at several work centers before completion. CIMCO's ability to manage this complexity, along with its powerful editing and control features, makes it an indispensable tool for maintaining efficiency and precision in such varied manufacturing environments.

MT-Linki, on the other hand, is more suited to facilities where seamless integration with FANUC equipment is a priority, particularly where real-time data collection and monitoring across multiple machines and devices are essential. MT-Linki's strength lies in its ability to easily interface with FANUC CNCs, robots, and other devices, providing a unified platform for operational data management [24]. Although it allows connection to other controllers like Mazak through MTConnect, it recently had challenges connecting with Heidenhain controllers, with no current resolution at a particular facility in Houston. Its scalability and ease of use make it ideal for environments that are heavily automated and require consistent monitoring and visualization of machine performance across a diverse set of equipment. While MT-Linki also supports

third-party equipment, its primary advantage is in FANUC-centric setups, where it can leverage native protocols like FOCAS and Robot Interface for deeper integration.

To this end, CIMCO was selected as the primary connectivity solution for CHPC, and is therefore the focus of this thesis as well.

Chapter 4: Network Infrastructure and Setup

This chapter presents a comprehensive exploration of the existing network infrastructure, dissecting the existing setup and proposing improvements to accommodate the demands of the new CIMCO software implementation and adherence to latest SLB cybersecurity guidelines. After an analysis of the current network environment, focusing on the CHPC Network Policies and the CIMCO PDM Implementation, the proposed network will then be explored.

The discourse progresses to the proposed network infrastructure, where the proposed server (local and cloud application) are both explored. This includes the Azure Cloud Application Requirements and the Server Implementation methods. Recommendations for the CIMCO Server and network infrastructure are presented as guidelines for further implementation of the software.

Attention is given to essential network diagnostics to be conducted, “Traceroute”, to ensure file transfer occurs in compliance with recommendations. There is an emphasis on the cybersecurity requirements at SLB, highlighting the challenging policies that the implementation must be compliant toward. Specifically, the section explores the Security Assessment and Qualification Process (SAQP) and adherence to Industrial Automation & Cyber Security (IACS) protocols, including IEC 62443 Compliance, air-gapping, and additional requirements for cloud-based applications, alongside their potential vulnerabilities. Although IACS represents a new perspective on cybersecurity regulation at SLB, there is currently no documentation detailing its effects on machine connectivity. Consequently, this section also serves as a practical guide for new facilities aiming to implement CIMCO. It provides insights into navigating the complexities of IACS compliance, ensuring secure and efficient machine connectivity, and addressing potential vulnerabilities in cloud-based applications. This guidance is crucial for maintaining robust cybersecurity standards while integrating new technologies.

Network Segmentation is introduced, as well as its applications toward previously explored network security concerns. Some solutions and remediations are discussed, as well as potential exemptions to be requested for trial deployment of the licenses. The chapter culminates with a detailed look at Connection Hardware, featuring General Connection Hardware and

MOXA Hardware, along with their configurations and security mechanisms, providing a thorough understanding of both the tangible and intangible aspects of the network.

4.1. Existing Network Infrastructure

4.1.1. Existing Network Overview

The motivation behind this network setup is to create a highly secure and organized manufacturing environment. Figure 4.1 below shows the network architecture currently at CHPC. Note that other VLAN segments have not been added to the diagram such as wireless (Remote access user) or IoT devices. Furthemore, the Palo Alto firewall that protects SiNet from external access has also been pictured. By segregating devices into different VLANs, the network ensures that critical systems, such as the local server (CIMCO Hosted) on VLAN 10 and the CIMCO Client on VLAN 20, are isolated from the manufacturing floor's CNC machines on VLAN 92. This enhances security by limiting the broadcast domains and reducing potential attack surfaces but also optimizes performance by managing traffic flow. The CIMCO Kiosk on VLAN 49, with limited access, serves as an interface for users to interact with the system without compromising the integrity of the network, and also serves as the edge device that is placed close to the CNC machine itself.

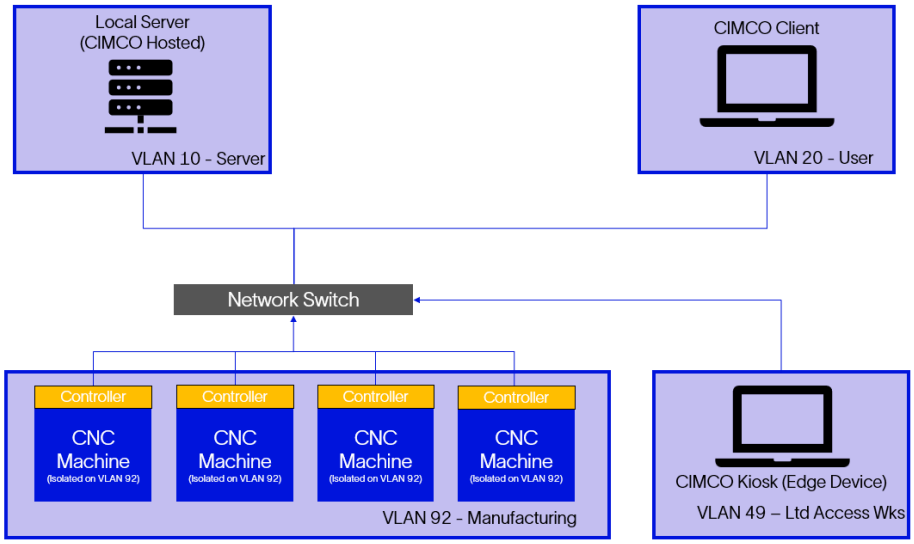


Figure 4.1: CHPC Facility Network Infrastructure and vLAN Segmentation

This diagram illustrates an integrated network architecture designed for the CHPC manufacturing environment. It showcases the distribution of devices across various VLANs. The local server (CIMCO Hosted) on VLAN 10 serves as server-related operations, while the CIMCO Client on VLAN 20 facilitates user interactions. The manufacturing floor is equipped with multiple CNC machines (Controllers) on VLAN 92, ensuring isolated manufacturing processes. An edge device, the CIMCO Kiosk on VLAN 49, provides limited access workstations, enabling secure and restricted user access. The central network switch forms the core of this setup, linking all devices and VLANs to maintain a cohesive and efficient network structure.

4.1.2. CIMCO PDM Implementation

CIMCO PDM established a foundation for data management, centralizing CAM files and production documents for efficient shop-floor operations. Its integration with CIMCO NC-Base Database Server on a local Windows 2008R2 Server allowed CHPC to organize its manufacturing documents effectively. The Windows 2008R2 acted as the CIMCO server, which stored the readily accessible production documents.

The network infrastructure that supported the machine connectivity involved the main SLB network (SiNet), as network segmentation had not been implemented. Consequently, the CNC machines and the shop-floor edge devices are not currently on separate LANs or vLANs which presents a vulnerability.

The facility currently has Palo Alto (PA-450) boxes serving as a firewall which is a range of ML-Powered Next-Generation Firewalls (NGFW) designed for distributed enterprise [26]. This hardware prevents malicious activity concealed in encrypted traffic, identifies and categorizes all applications on all ports at all times with full Layer 7 inspection, and delivers packet processing with a Single-Pass Architecture [26]. This firewall, however, is mostly irrelevant to the proposed connectivity solutions as it prevents unauthorized access to traffic external to the network, rather than between the CNC machines and the cloud application.

The CNC machines themselves are not fully connected. Although some machine controllers do have an IP address and have been previously connected, no transfer of data or files occurs through this connection. File transfer occurs over the existing CIMCO server, where .nc files are accessed through the edge devices and transferred manually to the CNC controllers to run the program.

4.2. Proposed Network Infrastructure

This section delves into the intricacies of the proposed network infrastructure, offering a thorough analysis and recommendations for a robust server setup. It begins with an exploration of server requirements, emphasizing the need for compatibility with Azure Cloud applications or local servers. The discourse then transitions to the practical aspects of server implementation, ensuring that there are adequate measures taken for correct server setup. Recommendations from CIMCO are highlighted, providing expert insights into both server choices and the overall network infrastructure. Additionally, the section includes a critical examination of network diagnostics through traceroute analysis, which is essential for maintaining network health. A detailed network diagram is also presented, offering a visual representation of the proposed setup. Finally, the section addresses server data storage solutions, ensuring that data management is efficient and secure. Readers can expect a comprehensive guide that not only suggests optimal configurations but also equips them with the knowledge to understand and evaluate the proposed network infrastructure.

4.2.1 Server

The necessity for obtaining a new server at the CHPC facility is paramount due to the current server, US04APP03, reaching its end-of-life. The outdated operating systems, such as Windows 7 and Windows Server 2008R2, no longer receive support or updates, leaving the server highly vulnerable to security threats. To mitigate these risks and ensure the continuity of critical operations, it is essential to migrate to a new, more secure, and efficient server solution, such as an Azure cloud server application or the Dell PowerEdge R440, which meets SLB's stringent security and performance standards.

SLB mandates that only necessary and approved servers and services operate on-site. The IT Manager is the key authority, responsible for approving servers, services, and their configurations before deployment. CHPC's onsite IT contact, Mr. James Frier will be responsible for the sever management if a local server is procured. This is discussed further in section 4.2.1.2.

A change management system must be in place, and the IT Manager must define a business owner, a technical application responsible, and a system administrator for each server. This will be related to CHPC's business ownership, and specific details will be provided by Ms. Bhavna Singh, the manufacturing manager leading this connectivity effort.

New server installations and services must adhere to SLB best practices and be executed by qualified personnel. Testing should occur in a non-production environment. Maintenance procedures require IT Manager approval and prior notification to users. HP OpenView is used for proactive administration and monitoring of servers and services, with upgrades and patches applied as necessary. A formal work instruction for monitoring and logging aligns with SLB best practices. Any security incidents on servers must be reported through the QUEST tool.

4.2.1.1 Azure Cloud Application Requirements

The cloud connectivity architecture in Microsoft Azure must meet several requirements. Spoke VNETs connect IaaS resources to the network, with each VNET belonging to a Resource Group managed by either the application owner or the Cloud Operations team. A dedicated subscription under the Cybersecurity Management Group handles connectivity and security resources related to SINet. There is a separate service account that owns this subscription, through which communication will be done. Two separate IaaS environments exist in different Azure regions (West Europe and Central US), each with its assigned internal CIDR block. CIDR is Classless Inter-Domain Routing, which is a method used for allocating IP addresses in IP routing.

Central VNETs have subnets for various security zones and connect to a SLBtransit point via ExpressRoute Private Peering. A Virtual Network (VNET) is a logically isolated network in Azure. It allows resources to securely connect with each other, the Internet and on-premises networks. Data traffic should enter Azure from the closest cloud location, regardless of the application's region. Spoke VNETs may belong to the same subscription or the application's subscription.

SLB's Azure IaaS environment connects to SINet through four ExpressRoute Private Peerings, with two at each transit point. SINet, or, SLB Information Network, the name given to the SLB Intranet, a vast collection of computers and networks used for communicating and

exchanging information in SLB. ExpressRoute Private Peerings represent a trusted extension of the core network into Microsoft Azure. With private peering, one can establish bi-directional connectivity between the core network and Azure virtual networks (VNets). This allows direct communication with virtual machines and cloud services using their private IP addresses.

The provisioning process involves setting up Azure subscriptions, configuring the connectivity solution, and physically connecting the machines. Subsequently, the ExpressRoute circuit is established, allowing the selection of a service provider, peering location, bandwidth, and billing model. The service provider then provisions the connectivity using the service key and VPN IDs. Finally, the ExpressRoute circuit facilitates connections between virtual networks via Azure private peering, as well as providing access to Azure services with public IPs and Microsoft cloud services (such as Office 365).

4.2.1.2 Local (CHPC) Hosted Server

As explored in section 2.3.5, the CIMCO PDM system at the CHPC facility is currently non-functional. The local server, US04APP03, which contains the CIMCO PDM data, is at risk due to outdated operating systems. Windows 7 support ended in 2015, and Windows Server 2008R2 support ended in 2013, making the server susceptible to DoS attacks. The inability to apply updates has led to suspended SQL services, preventing database management. As a result, the PDM software is unable to operate properly, and several high-criticality vulnerabilities have been identified. Therefore, there was a discussion held with the server applications team to determine the possibility of conducting a server migration by obtaining a new local server at CHPC.

The server that would potentially replace the existing server would be the Dell Poweredge R440, which will be requested by Mr. Tee Khee-Joo, the server application manager for the CHPC facility. The PowerEdge R440 is a 1U, 2-socket server that supports a variety of internal and external storage controllers. It can accommodate a significant amount of memory with 16 DDR4 DIMM slots and has a maximum storage capacity of 76.8TB with NVMe SSDs or 64TB with SAS/SATA HDDs. For management and security, the PowerEdge R440 includes iDRAC9, iDRAC Direct, and iDRAC REST API with Redfish, along with a suite of OpenManage tools for server administration. Security features include TPM 1.2/2.0, cryptographically signed firmware, and a Silicon Root of Trust. The server offers a range of I/O and port options, supports various operating systems, and is OEM-ready, allowing for customization from bezel to BIOS (Basic Input/Output System). The PowerEdge R440 is designed to be a versatile and powerful server solution for a wide range of applications. This server is an SLB standard device, and therefore has already passed the necessary security compliances required.

Server setup once the purchase order (PO) is submitted and the server is received is for the EMC (Enterprise Management Center) team in Jakarta, Indonesia to remotely configure the device for deployment. This involves a standard server imaging, which is essentially installing the necessary monitoring, remote access controllers and performing a BiOS scan. Furthermore, the cybersecurity team will install other monitoring tools such as the Carbon Black Cloud Sensor, Universal Discovery Agent for updates and the SLB standard System Health Tool.

Once the server is onsite at CHPC, Mr. James Frier, who is the IT onsite support analyst will work to setup the server. This will begin by unboxing and inspecting the server for any physical damage. Following this, the Dell PowerEdge R440 server will be mounted into the designated server rack, and connect it to the power supply and network infrastructure. After powering on the server, Mr. Frier will access the BIOS/UEFI settings to configure basic system settings such as date, time, and boot order, and apply any available firmware updates to ensure the server is running the latest stable versions.

Next, the remote access tools like iDRAC9 need to be enabled to allow the EMC team in Jakarta to perform remote configurations. Mr Frier will also configure network settings, including IP addresses, subnet masks, gateways, and DNS servers, to integrate the server into the network properly. Finally, Mr. Frier will conduct connectivity tests to verify network communication, perform functionality tests to ensure all installed software and tools are working correctly, and carry out security checks to confirm the server's security measures are in place and effective.

4.2.1.3 Server Implementation Recommendations

To enhance the security and isolation of CNC communication systems, it is advisable to configure the server hosting CIMCO DNC-Max software to operate across two distinct networks. This configuration is particularly crucial for organizations with stringent network access policies, such as SLB, which prohibit direct connectivity of CNC controls to the main corporate network.

To implement this, the server should be equipped with dual network interfaces, each connected to a separate network: one dedicated to the shop floor CNC controls and the other to the corporate network. This dual-network approach allows seamless data transfer and communication between the isolated CNC environment and the corporate infrastructure while maintaining robust security barriers, thereby protecting sensitive manufacturing operations from potential cyber threats. The dual network architecture may be implemented through the application of separate vLANs. VLANs enable the segmentation of a larger physical network into smaller, isolated subnetworks. This segmentation allows each network interface on the server to connect to a distinct VLAN, effectively separating the shop floor CNC controls from the corporate network. Firewalls can be implemented between each of the separate vLANs, allowing greater segmentation and control over the access and traffic through each network. Monitoring traffic can also become a useful tool to blacklist suspicious signals.

The DNC-Max server is configured to operate on two distinct networks, with both interfaces active simultaneously but isolated to prevent any traffic from passing between them. This configuration allows the server to be managed and backed up consistently with other network assets while maintaining strict isolation for the CNC controls connected to it. The communications components of the DNC-Max server are exclusively accessed from the private CNC network, ensuring that CNC controls remain isolated from other devices and computers on the main network. Conversely, the client portion of the DNC-Max server is accessible from the corporate network, enabling programmers to store and transmit files to the DNC-Max server without compromising the isolation of the CNC network. This dual-network strategy ensures that only mission-critical components of the CIMCO software are accessible where necessary, while the CNC network remains secure, capable of only sending and receiving data from the DNC-Max server.

Sample implementation of the server could involve:

1. Select an appropriate IP address subnet for your private CNC LAN, ensuring that the selected subnet doesn't overlap with any existing subnets in the network. The following are other considerations
    a. Subnet Size: Determine the number of devices (CNC controls, servers, workstations, etc.) that will be part of the private CNC LAN. This will help choose an IP address range with sufficient addresses [27]
    b. Subnet Mask: Decide on the subnet mask based on the required number of hosts per subnet.
2. Adding a second network interface card (NIC) to the server hosting DNC-Max is essential for dual-network operation.
    a. Connect one NIC to the corporate network (for management and file transfers) and the other NIC to the private CNC LAN.
    b. Configure the IP addresses for both NICs:
        i. Corporate NIC: Obtain an IP address from the corporate network (e.g., DHCP or static assignment).
        ii. CNC NIC: Assign a static IP address from the chosen private CNC LAN subnet.
3. File management considerations such as,
    a. Defining a consistent file storage structure for CNC programs, tool libraries, and other relevant files.
    b. Set up shared directories accessible from both the CNC network and the corporate network.
    c. Implement access controls to restrict file modifications and ensure data integrity.
4. DNC-Max installation considerations
    a. Configure DNC-Max to use the CNC NIC (private LAN) for communication with CNC controls [27]
5. Firewall considerations

Some international facilities have implemented MOXA NPORT5110 hardware, which allows connecting machines directly to the SLB network without compromising or creating vulnerabilities in the data-stream. Furthermore, MOXA devices support various industrial protocols and interfaces, enabling seamless integration and data exchange between CNC machines and other systems. For CHPC, and the scope of this connectivity implementation, there exist no firewall between the machines and the main network, and therefore, MOXA hardware will not be required. However, following the demonstration for .nc file transfer and machine data collection via CIMCO the addition of MOXA or other hardware for firewall protection can be considered. The MOXA hardware is further discussed in section 4.3.2.

4.2.2. CIMCO Server Recommendation

CIMCO has devised their own recommendation for the hardware specifications. These specifications are designed to ensure that the server can handle the required tasks efficiently. The minimum requirements are suitable for basic server operations, while the recommended specifications aim to provide a buffer for more intensive processes and future-proofing. The figure also takes into account the need for future database growth, which is a critical aspect of server management. The server requirements are displayed in Table 4.1.

Table 4.1: Server System Requirements: Minimum vs. Recommended

The table provided compares the minimum and recommended server technical system requirements for CPU, memory, HDD, OS and other software

	Minimum	Recommended
CPU	Intel Core i5 or AMD FX @ 2.8 GHz	Intel Core i7 or AMD A-Series @ 3.5 GHz Intel Xeon E or AMD Epyc @ 3.5 GHz
	* 4 logical processors	* 8-32 logical processors
Memory	4 GB RAM	16 GB RAM
Hard Drive	HDD 512 GB (7200 rpm) in RAID1	SSD 512 GB in RAID1
	2 GB of disk space for the installation of the full suite. Allocate enough space for database growth.	
Operating System	Windows® Server 2012	Windows® Server 2012 R2 or newer
	(Only 64-bit version is supported)	
Additional Software	Microsoft® Visual C++ 2015-2019 Redistributable Microsoft® .NET Framework 4.5 *(All required redistributables are included within the installer)*	

Table 4.2: Client System Requirements: Minimum vs. Recommended

The table provided compares the minimum and recommended client device requirements for CPU, memory, HDD, OS and other software

	Minimum	Recommended
CPU	Intel Core 2 Duo or AMD Athlon @ 1.6 GHz	Intel Core i3 or AMD Phenom II @ 2.5 GHz
Memory	2 GB RAM	4 GB RAM
Hard Drive	At least 2 GB of disk space.	
Operating System	Windows® 8.1 or newer *(Only 64-bit version is supported)*	
Additional Software	Microsoft® Visual C++ 2015-2019 Redistributable Microsoft® .NET Framework 4.5 *(All required redistributables are included within the installer)*	

The client device requirements from CIMCO are not particularly stringent, as seen in Table 4.2. These specifications suggest that the client devices are expected to handle basic to moderate computing tasks. The CPUs are chosen to provide sufficient processing power for typical office applications and document handling. The memory requirements are modest but adequate for the expected workload. The hard drive space is minimal, since these devices are not intended for heavy storage duties but rather for accessing and working with CNC files and other documents like work instructions. Latency recommendations are also provided in Table 4.3.

Table 4.3: Latency Recommendation for Data Transfer

This table highlights the importance of having low-latency networks to ensure efficient operation, especially for systems involving Direct Numerical Control (DNC), which require even lower latency compared to Machine Data Collection (MDC) systems.

MDC Only	Network with a latency below 50ms
MDC and DNC	Network with a latency below 15ms
For DNC communication, a network with latency above 15ms can result in very slow program transfers and communication problems.	

4.2.3. CIMCO Network Infrastructure Recommendation

CIMCO has developed their own network infrastructure recommendations related to DNC-Max deployment, security best-practices and server location. The guidelines emphasize the importance of controlling access to the DNC-Max server through segregating the networks using LAN (local access networks).

Web and PC clients need to connect to the DNC-Max server. Machines and connected machine hardware should also establish connections with the DNC-Max server. The DNC-Max server acts as the central communication application, facilitating communication (whether serial or Ethernet) with the machine, database, and clients.

For optimal network performance, it's advisable to place all CNC machines, their MDC, and DNC hardware, along with touch screens, on a separate network. This separation helps reduce network noise caused by other communication traffic. The server hosting DNC-Max serves as the bridge between the machine network and the company's internal network.

CIMCO recommends deploying a local server to run the DNC-Max software. A local server minimizes network latency and mitigates remote connection issues that might otherwise arise. While it's technically possible to connect machines to a remote DNC-Max server, this approach is not recommended. CIMCO's experience indicates that performance is consistently better when running DNC-Max on a local server. Using a central server, whether by CIMCO or any other provider, tends to result in reduced system performance and user responsiveness [28].

As seen below, Figure 4.2 illustrates the network architecture of "Site A," which is divided into two main sections: VLAN 1 / LAN 1 and VLAN 2 / LAN 2. On the left, VLAN 1 / LAN 1 includes a server connected to three client PCs (Client PC 1, Client PC 2, Client PC 3) via the LIVE protocol. Each client has access to reports and live screens. The server also connects to a database (DB) server that hosts databases for "Site A" or a remote site. On the right, VLAN 2 / LAN 2 shows three machine workspaces, each containing a machine and an operator panel PC. These workspaces are labeled as Machine workspace 1, Machine workspace 2, and Machine workspace 3. This diagram effectively visualizes how data flows within the network, highlighting the separation of VLANs to manage data and resources efficiently within

the same physical location. It also emphasizes redundancy in database hosting, suggesting a focus on data availability and disaster recovery planning.

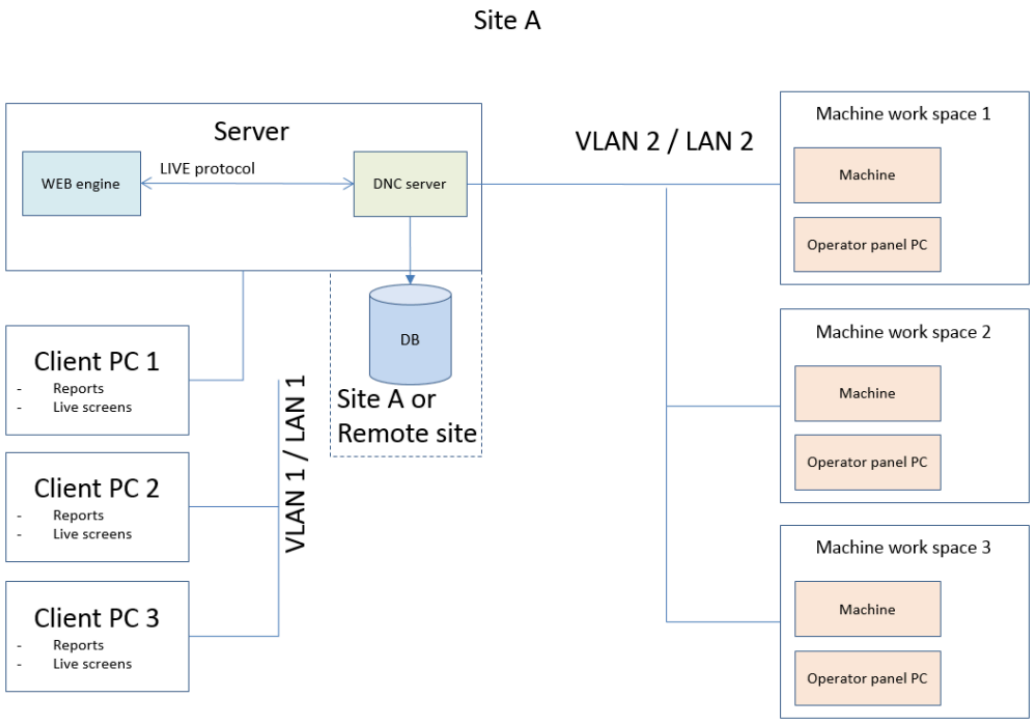


Figure 4.2: Sample Facility Network and vLAN Architecture

VLAN 1/LAN 1 is the company's internal network. VLAN 2/LAN 2 is the machine's dedicated network. The Database server can be located locally (recommended) or located at a remote facility. The machine network can be a software separated VLAN or a physically separated LAN

4.2.4 Network Diagnostics - Traceroute

Traceroute is a valuable network diagnostic tool used to trace the path that data packets take from a local client to a server. This can help identify issues when experiencing connectivity issues, and can pinpoint where the problem occurs. It also reveals delays, packet loss, or misconfigured routers along the route [29]. However, its use-case here would be primarily for measuring the time it takes for packets to travel between each hop, as it helps assess network performance and latency. Figure 4.3 displays a sample traceroute

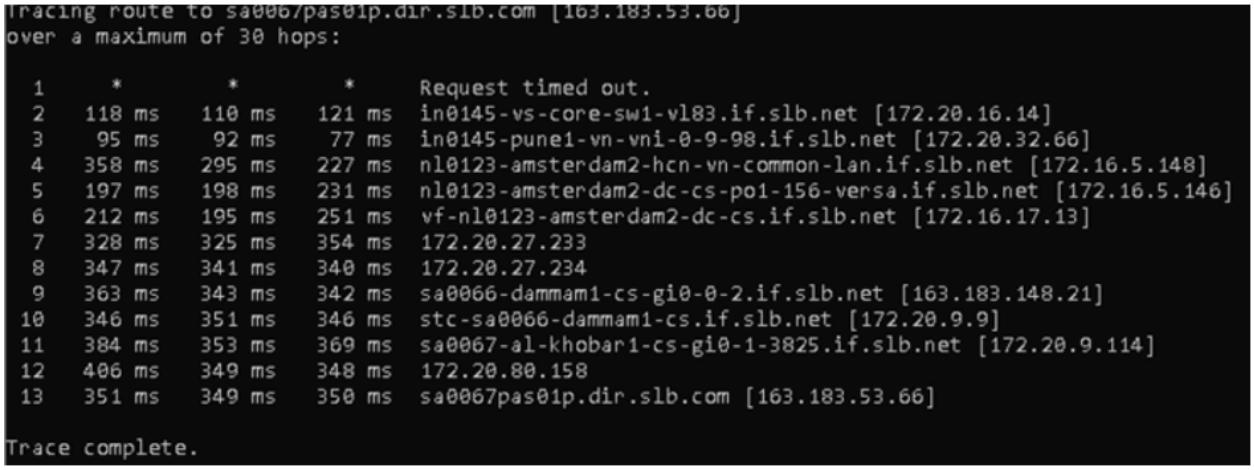


Figure 4.3: Tracerouting on Windows Command Prompt Example Screenshot

The image is showing how Trace-rout traces the path that a packet takes from a computer to an endpoint destination, which in this case is sso-aaa01.kir.ops.sirsi.net. The output lists each "hop" along the route to the destination, with three time measurements in milliseconds representing the latency for each hop.

SLB has recommendations for time to first byte, payload for each transaction (per click) and round trips which cumulatively help determine the server latency. Round Trips can be described as a number of objects/Http requests and communications between two systems between the user machine and a web server. Each round trip needs to traverse the Wide Area Network which introduces unavoidable network latency. As round trips increase, so will the impact of network latency which can introduce significant delay for the end user. Network latency is mostly made up of the geographic distance between the client and the server.

Payload is defined as the amount of data sent to complete the transaction can increase the time taken for a workflow to complete, especially where locations have lower available bandwidth. In addition, for scripts that are cached, cutting down their byte size speeds up the time the browser takes to parse and execute code needed to render the page. With regards to payload, we look at data flowing in both directions between client and server.

User experience hinges on the speed at which files are transferred from the server. Slower load times often prompt users to seek faster alternatives. In the RBTC facility, despite the implementation of a DNC solution, operators still opt for flash drives when making .nc file edits due to server latency.

4.2.5 Proposed Network Infrastructure

The figure provided in section 4.1.1 presents a viable connection option if the incumbent server is replaced with the recommendation provided in section 4.2.1. The network diagram is therefore identical to the existing connection method, but the server does not inherently present vulnerable to breaches in security. Each component within the network diagram is segmented and air-gapped, and therefore is compliant with IACS.

At the core of the setup are workstations or the client devices, which are utilized by operators or engineers to draft designs and dispatch .nc programs to the CNC machines. These instructions are channeled through the local server that hosts DNC Max, which disseminates data and commands to the CNC machines, ensuring they execute the desired operations.

Central to the network's communication is a switch, which interlinks all servers and workstations, facilitating seamless interaction among them. The network could also include MOXA hardware, which serve as access gateways, converting the CNC machines' serial communications into network-compatible signals.

In the instance of a cloud-based Azure server, the IACS requirements are more stringent. As explained further in section 4.3.2.4, cloud applications like Azure exist on the highest priority (enterprise level) network segment. Therefore, traffic originating from outside the IACS network, cannot communicate directly with the lower levels. This necessitates the need for a proxy server/jump host, which exists on the iDMZ (industrial demilitarized zone) allowing an additional layer of security. This is discussed in full detail in section 5.4. The concept of iDMZ is discussed in detail in section 4.3.2.5. The Figure 4.4. below demonstrates how the network architecture would be setup in the case of a cloud application being used.

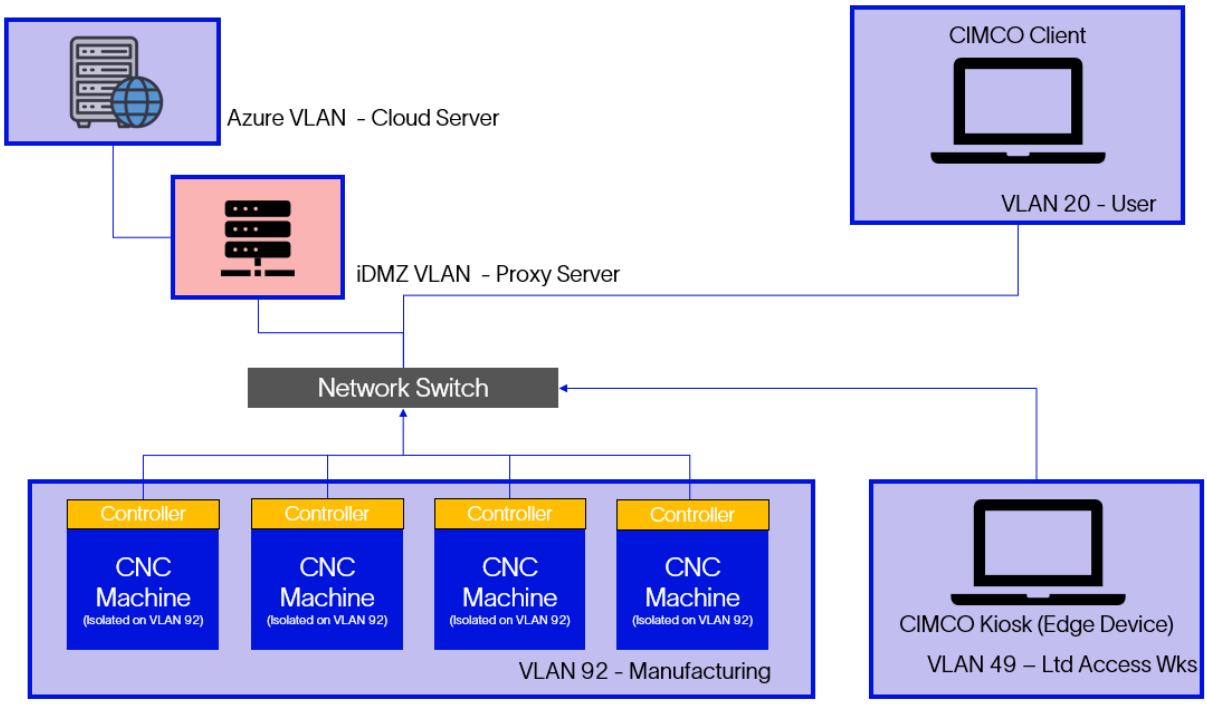


Figure 4.4: Azure Cloud Application Connectivity Network Infrastructure

The diagram depicts a network infrastructure setup where an Azure VLAN Cloud Server connects to a CIMCO Client via a DMZ VLAN Proxy Server. A central Network Switch links various components, including three controllers, each connected to a CNC Machine on VLAN 92. Additionally, a CIMCO Kiosk (Edge Device) is connected on VLAN 9 for limited access workstations.

4.3 Network Security and IT considerations

This section explores SLB's framework for cybersecurity standards and protocols. While the connectivity solution deployed in CHPC will comply with the essential steps outlined below, the application's experimental status and the accelerated timeline for establishing connectivity have warranted a partial exemption from the full certification process. Manufacturing engineer Mr. Chris Hernandez, in collaboration with Mr. James Frier from the local IT department, will be assisting with fulfilling the remaining requirements to achieve complete certification post-trial.

4.3.1 Overall SLB Network Policies

SLB has established a comprehensive set of guidelines to ensure secure and efficient network connectivity for its employees and contractors. These policies are designed to govern the use of the company's site LAN, remote access protocols, and the proper configuration of client computers, ensuring that all connections are secure, authorized, and compliant with the company's high standards for IT infrastructure. The policies most relevant to CHPC are listed below:

1. General Network Use: Access to SLB's site LAN and its services is restricted to employees and approved contractors. Unauthorized computers are not permitted direct LAN connections. The IT Support team manages the site LAN, while the OFS IT WAN Team oversees external connections and SINet connectivity.

2. Client Computer Connections: The preferred method for connecting client computers to the site LAN is through DHCP, which is the standard setup for all SLB desktops and laptops. Computers must be properly named for easy identification by administrators. Direct connections or SecureConnect to the site LAN must not link to other networks. Manual configurations and network addresses require system administrator approval and DNS verification.

3. Remote Network Access: SLB employees can access SINet remotely using approved services such as SecureConnect, SecureGateway, or Pulse Secure. Other methods require explicit approval from the IT Manager and SISC. Non-standard computers using SecureConnect must comply with SLB Best Practices and avoid banned services or applications.

4. Computer Configuration and Software Licensing: Desktops and laptops must adhere to SLB's system configuration guidelines. New PCs should follow the SLB standard, and special-purpose computers need local IT configuration and IT Manager approval before LAN connection. Only licensed software is permitted on SINet machines, with SCCM (System Center Configuration Manager) used for installation on standard computers.

4.3.2 Security Assessment and Qualification Process (SAQP)

The Security Assessment and Qualification Process (SAQP) is an integral part of SLB's Software Lifecycle Management Process. Its primary purpose is to enhance security by safeguarding all applications within the SLB portfolio. SAQP addresses threats related to confidentiality, integrity, and availability, ensuring robust protection for data and systems. Additionally, it plays a vital role in securing the SLB network (SINet) and ensuring compliance with corporate standards and procedures. Implementation of a cloud application hosting new CIMCO licenses would likely require approval through SAQP, which will conduct various security tests to ensure compliance.

SAQP encompasses six application types: Web Applications (on-premises), Mobile Applications, Cloud Applications (IaaS, PaaS, SaaS), Thick Client Applications (both on-premises and cloud-based), OT/IIoT Applications, and O365 Applications. The server that will be hosted at CHPC for the CIMCO DNC-Max and MDC softwares would be a cloud-based server. Cloud based applications relevant to SLB include IaaS, Infrastructure as a Service is a cloud computing service model where computing resources—such as virtual machines, storage, and networking—are provided by a cloud services provider. Appendix 2 provides a process

flow-chart that is followed when determining how to begin SAQP process. The steps for completing the SAQP process are listed below

1. SAQP Request Submission: The application team submits a request for a Cloud application SAQP on the DPM Portal, specifying whether it's IaaS or PaaS.
    a. The team provisions SAQP activities in the product development plan, considering complexity and re-tests
2. Artifact Submission: Involves documents related to a project or application such as block diagrams, account management (users), URLs and logins, cloud critical controls
3. Request Review: Involves resourcing and prioritization assessment, where the applications security team with review the submission and set priority based on criticality
4. Test Planning and Self-tests: Involves scheduling the tests of HTTP Headers test to test URLs (including APIs), SSL certification test and website reputation test
5. Security Test and Review: Involves architecture security review (interfaces and protocols), cloud critical controls review to check for non-compliances, interfaces security to ensure proper communication to other applications (traffic encryption) and risk analysis. Further 3rd party testing can also be considered to check for outstanding vulnerabilities, as well as manual penetration testing
6. Issues Mediation: In case of outstanding issues, the application security team will work and develop plans to address them.

The flowchart in Appendix 2 presents the SAQP process flow for an IaaS cloud-based application sequentially, also providing alternative paths for unfulfilled checks. In rare circumstances, the SAQP can be outsourced and passed with an exemption.

4.3.2 Industrial Automation & Cyber Security (IACS)

IACS is the combination of control components working together to achieve industrial objectives. IACS encompasses various control systems and their associated instrumentation. These systems are essential for field operations and manufacturing, but increased connectivity and digital adoption also introduce risks to critical assets and systems. Within the SLB environment, it's common to encounter machines that integrate multiple Industrial Automation and Control Systems (IACS) components—such as Human-Machine Interface (HMI), Programmable Logic Controller (PLC), sensors, and actuators—into a single unit. These integrated systems enhance efficiency, ease of operation, and cost-effectiveness. Although IACS is currently developmental, adherence with IACS would ensure compliance with the latest SLB connectivity and cybersecurity guidelines. This project aims to be compliant with the current recommendations made by the IACS engineers in SLB, which highlighted mainly the importance of air gapping between nodes in the network. This is also explored further in section 4.3.2.4 with the discussion of the Purdue Enterprise Reference Architecture.

4.3.2.1 IEC 62443 Compliance

IACS mainly complies with IEC 62443, which is an international series of standards specifically designed to address cybersecurity for operational technology (OT) in automation and control systems [30]. It covers both technical and process-related aspects of IACS cybersecurity, considering different roles within the field, such as operators responsible for managing and operating IACS, service providers involved in integration and maintenance, and component manufacturers. The standard provides guidelines for securing critical assets, implementing network segmentation, and prioritizing security measures to ensure comprehensive protection within an operational framework.

4.3.2.2 Air-gapping

Air gapping within IACS is a critical security measure that involves creating a physical separation between sensitive computer systems and other networks, including the internet. This isolation is crucial in environments like SLB, where the integration of IACS hardware components. Such segregation ensures that these vital systems are safeguarded from cyber threats and unauthorized access, preserving the integrity of industrial operations. However, implementing air gapping presents challenges, particularly in system maintenance and updates, which may require physical intervention. To mitigate these issues, organizations often establish separate LANs for different types of devices, enforcing strict access controls and maintaining secure physical perimeters around air-gapped systems. While air gapping significantly bolsters security, it must be part of a broader security strategy that includes network segmentation and prioritization of critical assets to ensure comprehensive protection of IACS within SLB's operational framework.

The relevance of IACS for servers stems from the network security guidelines. Ensuring the security and efficiency of SLB systems is crucial. OS Update, hardware and software patching, IACS maintenance windows, network segmentation and prioritizing critical assets and internet-exposed Systems are all measures that can be followed when implementing the new server.

4.3.2.3 Cloud Server Requirements

For communication between SLB applications hosted in the cloud, several key requirements apply. First, encryption is essential to secure the communication channels. Documented communication protocols should be in place. Strong authentication mechanisms are necessary for verifying the identity of the communicating parties. Lastly, vendors must provide public IP addresses for outbound communication or use private links (e.g., VPN, Azure/AWS)

Communication with the cloud is restricted to authorized components of OT systems using iDMZ brokered communications. Jump stations on the cloud are prohibited. Trusted clouds, where SLB maintains full control over application configuration and user access, are allowed. External cloud service providers must

conform to security standards (e.g., ISO 27017). OT data stored in the cloud must be encrypted at rest and in transit, accessible only to authorized users. Monitoring of user and system activities within the cloud is essential.

4.3.2.4 Network Segmentation

In the SLB IACS environment, network segmentation is crucial for protecting IACS systems based on their criticality and function. The segmentation aligns with the Purdue Enterprise Reference Architecture (PERA) and IEC 62443. It involves layers such as Internet DMZ, Corporate Network, Industrial DMZ (IDMZ), L3 (Manufacturing Operations and Control), L2 (Supervisory Control), L1 (Basic Control), and L0 (Process) [31]. Additionally, IACS network layers are further divided into segments based on criteria like business criticality, segregation of duties, geographical location, technical administration, and business purpose. Each zone should implement at least one segment (e.g., private VLANs), with traffic control facilitated through firewalls.

The Purdue Enterprise Reference Architecture (PERA) model is a widely adopted framework for segmenting industrial networks, particularly in the context of Operational Technology (OT) and Information Technology (IT) integration [31][32]. Figure 4.5 has By dividing the network into distinct zones and levels, the PERA model enhances security by isolating critical assets and reducing the attack surface. This segmentation allows for better monitoring and control, ensuring that any potential threats are contained within specific zones, thereby preventing lateral movement across the network. Additionally, it facilitates the safe collection and analysis of data from OT environments without exposing sensitive systems to accidental or malicious interference.

The diagram illustrates a comprehensive industrial network architecture for a SCADA system, segmented into multiple levels to ensure secure communication and effective management. At the base, Level 0 includes field devices and I/O modules, which are fundamental for data acquisition and control. Moving up, Level 1 houses PLCs (Programmable Logic Controllers) within VLAN H, crucial for executing control processes. Level 2 connects control devices to the enterprise network through a control

DMZ, incorporating essential servers like OPC, database, and CMC servers. Level 3 is more complex, featuring various VLANs dedicated to services such as file services, remote access, MES operations, and network services & remote desktop protocols. These VLANs are connected to enterprise-level networks, with firewalls ensuring robust security. At the top, the Enterprise Zone links to external networks, including the Internet and office networks, highlighting the need for stringent cybersecurity measures. This structured approach underscores the importance of segregating operational technology (OT) from information technology (IT) environments to enhance overall network security and efficiency.

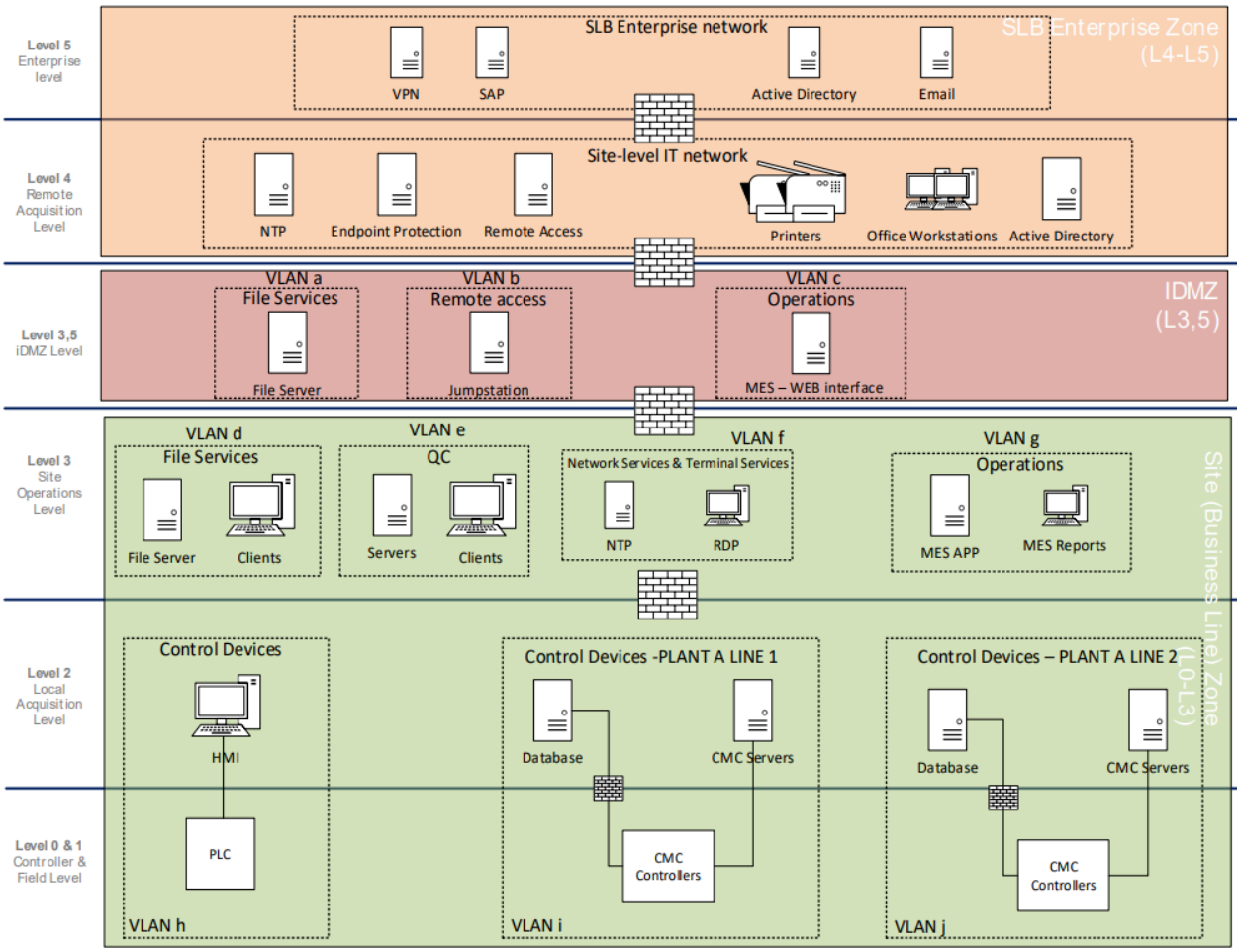


Figure 4.5: PERA Model Framework

This diagram shows the hierarchical structure of a SCADA system network, segmented into levels for secure communication and management. Level 0 includes field devices and I/O modules. Level 1 has PLCs within VLAN H. Level 2 connects control devices to the enterprise network through a control DMZ, including servers like OPC and database servers. Level 3 features VLANs for services such as file services and remote access, with connections secured by firewalls. The Enterprise Zone links to external networks, emphasizing cybersecurity measures. This structure highlights the importance of segregating OT from IT environments to enhance security and efficiency.

The Purdue Enterprise Reference Architecture (PERA) model, widely adopted for segmenting industrial networks, plays a crucial role in enhancing security by isolating critical assets and reducing the attack surface. In accordance with IEC 62443 standards, which emphasize securing IACS through network segmentation, traffic originating from outside the IACS network, including the Internet and internal IT networks, must not directly communicate with lower levels of the Purdue model without passing through a jump host. This policy aligns with the PERA model's approach to network segmentation, ensuring that critical assets remain protected.

4.3.2.5 Industrial DMZ (iDMZ) Concept

The Industrial DMZ (Demilitarized Zone) is a critical security layer designed to enhance the protection of industrial networks. Its primary role is to provide additional security controls, such as Intrusion Prevention Systems (IPS) and Antivirus (AV) solutions, and to terminate untrusted IT services when necessary [34][35]. Within the SLB corporate network, traffic can be categorized into three types: trusted system-to-system traffic, untrusted user-to-system traffic, and untrusted system-to-system traffic. Figure 4.6 provides an example of traffic that goes through different levels of PERA, as well as the iDMZ.

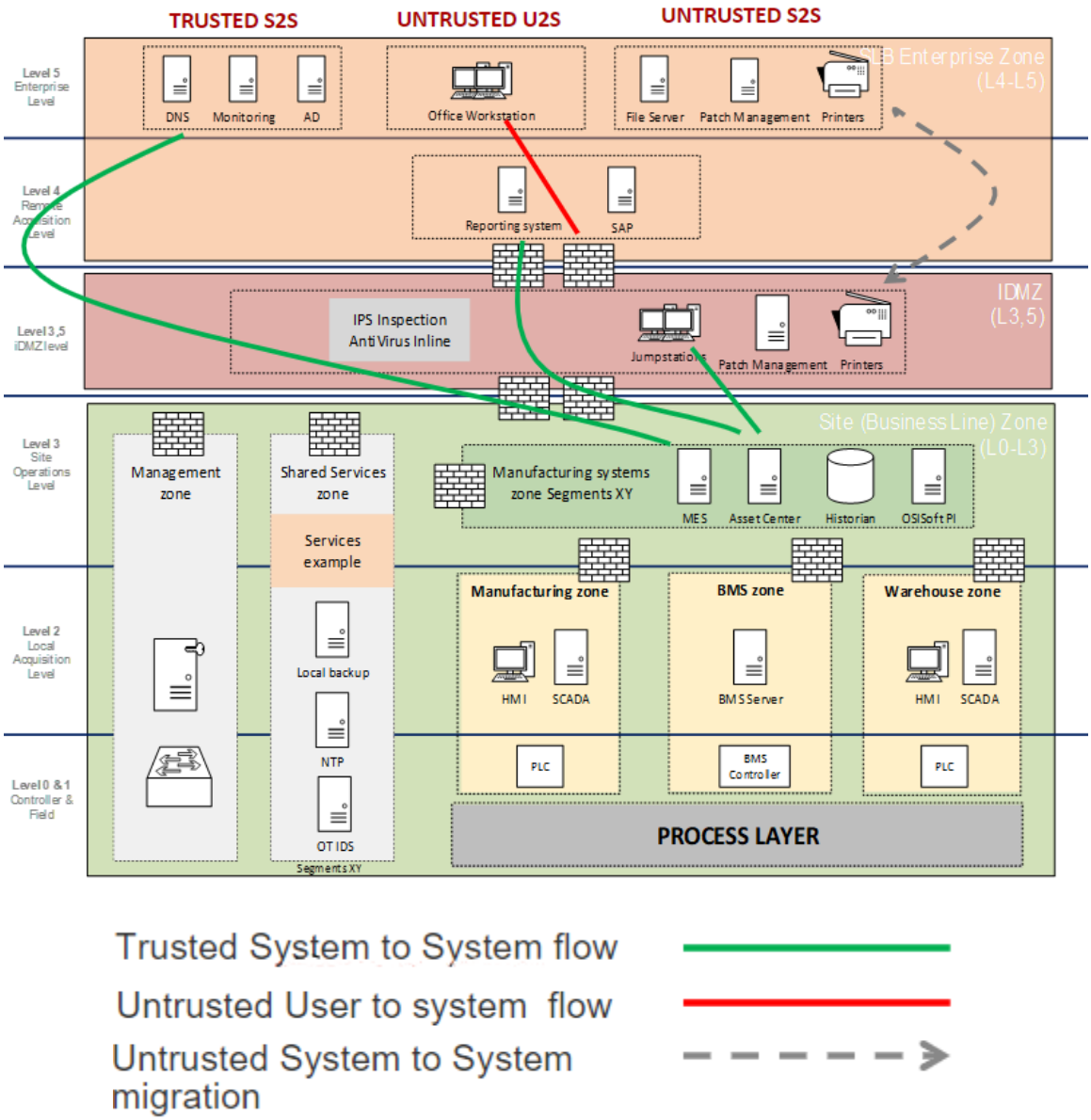


Figure 4.6: iDMZ Concept within PERA Model Framework

The figure above shows an example implementation of the PERA model framework, highlighting various traffic flows. Trusted system-to-system traffic flows through the OT DMZ, where it is inspected by security controls like IPS and AV. Untrusted user-to-system traffic is terminated at Jump stations within the DMZ to prevent unauthorized access. Additionally, untrusted system-to-system traffic is either migrated or duplicated in the OT DMZ to ensure security.

Trusted system-to-system traffic involves systems deployed in the Corporate Network (CN) that are configured and managed according to security best practices [35]. This traffic passes through the Operational Technology (OT) DMZ, where it undergoes inspection. Untrusted user-to-system traffic, on the other hand, must be terminated on Jump stations located within the DMZ to ensure security. Additionally, systems residing in levels L4-L5 that are not trusted should either be migrated or duplicated in the OT DMZ to maintain a secure environment. This layered approach helps safeguard the network by isolating and inspecting different types of traffic based on their trust levels.

SLB implements the Industrial DMZ to address several critical security and operational needs. Firstly, the Industrial DMZ helps mitigate the risk of cyber attacks that could disrupt industrial operations. By segmenting the network and applying stringent security controls, SLB can prevent unauthorized access and protect sensitive data. This is particularly important in the context of increasing cyber threats targeting industrial control systems and operational technology. The Industrial DMZ facilitates secure data exchange between the corporate IT environment and the industrial OT environment. This separation ensures that any potential vulnerabilities in the IT network do not directly impact the OT systems, which are often more critical and sensitive2. The DMZ acts as a buffer zone, allowing controlled and monitored interactions between these two environments.

Moreover, regulatory compliance is a significant driver for implementing an Industrial DMZ. Standards such as NIST 800-82 and ISA/IEC 62443 recommend network segmentation and the use of DMZs to enhance cybersecurity in industrial settings. By adhering to these standards, SLB not only improves its security posture but also ensures compliance with industry regulations.

4.3.3. Project Network Security Concerns

In the context of the DNC-Max server, which initiates connections to machines, this policy would be violated unless the server is placed in a local DMZ at the site. A viable solution involves using a jump host or proxy server (see section 5.4 for additional detail). This intermediary facilitates secure communication between the cloud or datacenter and the local DMZ, ensuring compliance with security policies. The jump host acts as a controlled gateway, allowing only authorized traffic to pass through, thereby maintaining the integrity of the segmented network. A cloud server application, one which is proposed for implementing machine connectivity, could also violate security policies outlined by IEC 62443 and the PERA model if it directly communicates with lower levels of the Purdue model without appropriate safeguards. Direct communication from a cloud server to devices or systems at lower levels (e.g., Levels 0-2) bypasses necessary security controls, exposing critical operational technology (OT) assets to potential threats from external networks. The PERA model emphasizes network segmentation to isolate critical assets and reduce the attack surface, and a cloud server application that does not adhere to this principle can create vulnerabilities by allowing unrestricted access across different network zones. `

According to IEC 62443, traffic from outside the IACS network must pass through a jump host or proxy server before reaching lower levels. If a cloud server application does not utilize a jump host, it violates this requirement, potentially exposing the network to unauthorized access and cyber threats. Additionally, cloud server applications often require multiple TCP/UDP ports for various services. If these ports are not carefully managed and restricted, they can create additional entry points for attackers. To comply with these security policies, a cloud server application should be designed to communicate through a jump host or proxy server, ensuring that all traffic is monitored and controlled. Strict adherence to network segmentation and port management practices is essential to protect the integrity of the industrial network. This is discussed in greater detail in Section 5.4.

Therefore, although a cloud application does not necessarily meet immediate disqualification, the IACS team would need to ensure there is complete end-to-end

protection and potential vulnerabilities are addressed before the full-scale implementation of machine connectivity at CHPC. Furthermore, CIMCO is currently exploring the potential of setting up a CIMCO hosted jump-server in the iDMZ. The area manager for CIMCO who had been working with clarification regarding software capabilities and setup process with the project will be the primary contact regarding this communication.

Regarding the numerous TCP/UDP ports listed, including those for SMTP (Simple Mail Transfer Protocol) and various database software, it is common to see a comprehensive list of port requirements. However, in practice, a much smaller subset of these ports will likely be used based on specific hardware and overall network design. Identifying the critical services and applications supported by the network and configuring only the necessary ports can minimize potential vulnerabilities. By focusing on essential ports and services, network configuration can be streamlined, enhancing security and ensuring that only required communication channels are open.

4.3.4. Network Security Concern Resolution

The specific resolutions for the future execution of connectivity is discussed in section 5.2. However, the intermediary solution for this project was requesting special exemption from the IACS team for utilizing the Azure cloud application. Although this exemption process is informal (due to the constrained timeline for the project), further implementations will require QUEST exemption forms to be filled, which is the official internal SLB process for requesting exemptions. A Quest Exemption is a tool within Quest (internal Health Safety and Environment group) that secures formal approval from management when there is a need to deviate from a rule or standard.

There is a chance of a cloud-based application still being IACS compliant. However, there will be a strenuous certification process to confirm its eligibility. This is not to mention the proxy server/jump host requirement outlined in section 4.3.3. A potential network architecture was discussed for the cloud application in section 4.2.5 as well.

The IACS team mentioned when discussing cloud server compliance, there is a requirement for endpoint agents, which typically means that the server must have specific security software installed on all devices that connect to it. These agents are responsible for a range of security tasks, including real-time threat detection and system activity monitoring to identify and respond to potential cyber threats.

Additionally, there has to be an ability for the server to be scanned, which indicates that it should be accessible for security assessments. These assessments check for vulnerabilities and ensure that the server adheres to established security policies. Scans can be conducted in two primary ways: through agents installed directly on the server (agent-based scanning) or remotely without agents (agentless scanning). The former actively monitors the server's environment, while the latter relies on indirect methods like analyzing logs or API connections to evaluate security.

For a cloud server to be deemed compliant, it must fulfill these requirements by having all necessary endpoint agents in place and being configured to permit security scans. This is essential to meet security standards and safeguard the server and its data against potential security breaches.

Additional recommendations regarding implementation of machine connectivity specifically at CHPC can be obtained from IACS network architect Mr. Rick Beaver. Mr. Beaver was working with the project for obtaining a potential exemption of requiring a jump-host. However, following the conclusion of the 180-day licenses, the formal approval process will be completed according to IACS guidelines.

4.3. Connection Hardware

4.3.1 General Connection Hardware

The hardware required for making the connection between the machines is very simple. CNC controllers made after the year 2000 typically have both ethernet IP and serial communication options, which would require a RJ45 and RS232 cable respectively. Shop-floor edge devices can be connected through ethernet cables as well. Cables from the machines and edge computers on can be routed to a network switch, which allows interconnection and communication between the different inputs.

4.3.2 MOXA Hardware

To connect the CNC machines at other facilities, MOXA NAT-102 boxes have been purchased to assist with security. The MOXA NAT-102 is an industrial Network Address Translation (NAT) device designed to simplify IP configuration for machines in existing network infrastructure within factory automation environments. The NAT-102 has two ethernet RJ45 ports, allowing network segmentation as one port can connect to the external network (e.g., the internet or another subnet), while the other connects to your internal machines. This isolation enhances security by preventing direct access to sensitive devices. This provides complete NAT functionality, adapting machines to specific network scenarios without complex configurations. These devices also protect internal networks from unauthorized external access, which is an important consideration for complying with the SLB cybersecurity guidelines. There are concerns from the security team regarding the lack of visibility in monitoring the network with the presence of MOXA (and similar hardware), and how it poses a company-wide issue. MOXA boxes will therefore not be utilized for the trial implementation for CHPC, but will remain a possible solution for segmentation.

4.4.2.1 Network Address Translation

Network Address Translation (NAT) serves as a pivotal security mechanism that modifies IP addresses during the transmission of Ethernet packets. This function is particularly useful when there is a need to conceal internal network addresses from external observers. By translating an internal IP to a designated address or mapping a range of internal IPs to a single external address, NAT enhances the security of industrial networks. One of its key features, the N-1 or Port forwarding NAT, effectively obscures the IP address of essential networks or devices. Additionally, NAT facilitates the management of identical sets of Ethernet devices by assigning them the same private IP, simplifying the replication or expansion of production lines. The operational protocol of NAT involves a systematic check of data packets against predefined policies, translating addresses as soon as a match is found, and sequentially moving through policies until the appropriate one is applied. This ensures that only authorized traffic navigates through the network, bolstering its defense against potential intrusions.

4.3.2.1 Port Configuration

When setting up the MOXA NAT-102 box, port settings need to be configured, which let one manage port access, port transmission speed, flow control, and port type (MDI or MDIX). Figure 4.7 shows an example of how the MOXA hardware can be used for segmenting network but using different port connections.

Configuring and adding ports requires information regarding its status, media type, description, speed, flow control. The NAT-102 can also be used for configuring VLAN functionality for the ports. Configuring VLANs on the device can enhance the network's performance by segmenting the network into distinct logical divisions rather than physical ones. Configuring the VLANs requires information on VLAN ID, management port (1 or 2), mode (access, trunk or hybrid),

Segmentation for the VLAN could be setup as:

1. Departmental Segmentation: Implement distinct VLANs for various departments; one for marketing, another for finance, and a separate one for product development.
2. Hierarchical Segmentation: Establish VLANs based on organizational hierarchy; one for directors, another for managers, and a different one for the general workforce.
3. Functional Segmentation: Create VLANs according to the type of network usage; one for those primarily using email and another dedicated to multimedia tasks.

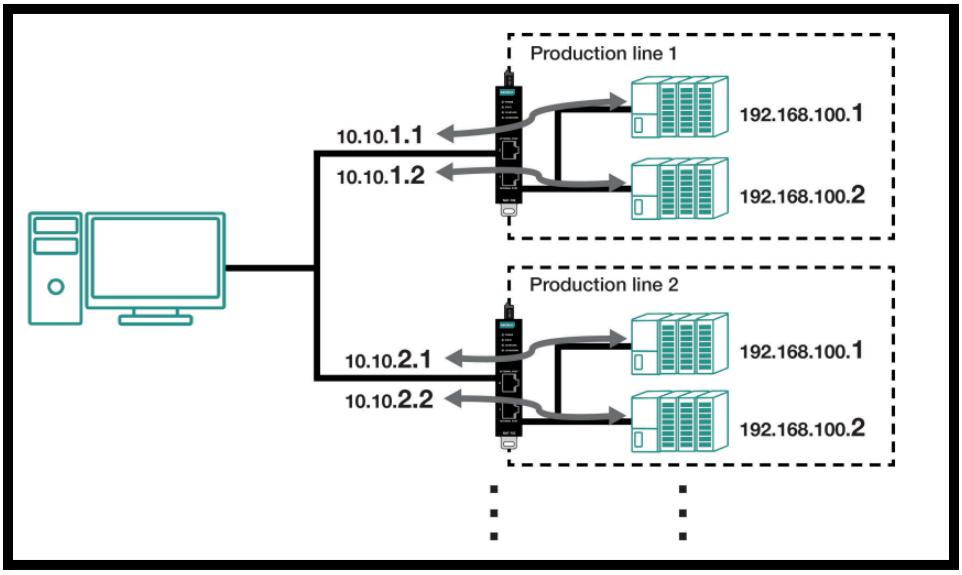


Figure 4.7 : Network Port Configuration for Centralized Management of Production Lines

The diagram illustrates the network setup for managing two separate production lines from a central computer, and having a MOXA device for each production line. Each production line consists of two devices, each with a unique IP address. The central computer is connected to both production lines via the MOXA network, allowing it to communicate with and manage the devices on each line. The use of different IP address ranges for each production line helps in segregating and managing the network traffic efficiently, ensuring that each production line operates independently while being centrally controlled.

4.4.2.2 Firewall

Firewall devices serve as robust security gatekeepers, strategically positioned at the demarcation points where an external network—often considered untrusted or non-secure—interfaces with an internal network, which is deemed trusted and secure. These devices analyze incoming and outgoing network traffic based on an established set of security rules. By doing so, they effectively determine which traffic is safe to allow into the internal network, thereby protecting the organization's digital assets from various cyber threats such as unauthorized access, hacking attempts, and malware distribution.

Firewall policies can be configured separately on the NAT-102, which offer enhanced security and granular control over network traffic. When activated, the Industrial NAT device records real-time event logs for various firewall activities. These logs could be crucial for monitoring and analyzing the security events that transpire within the network. Users have the flexibility to either store these logs on the device itself for easy access or forward them to a Syslog server for centralized management and long-term archival. Enabling the Malformed Packets option on the Industrial NAT device activates a vigilant logging system that tracks and records instances when malformed packets are identified and discarded. This feature is essential for maintaining network integrity, as it allows for the close monitoring of irregular packet structures that could indicate a security threat or network issue. See figure 4.8 for more information regarding firewalls on MOXA.

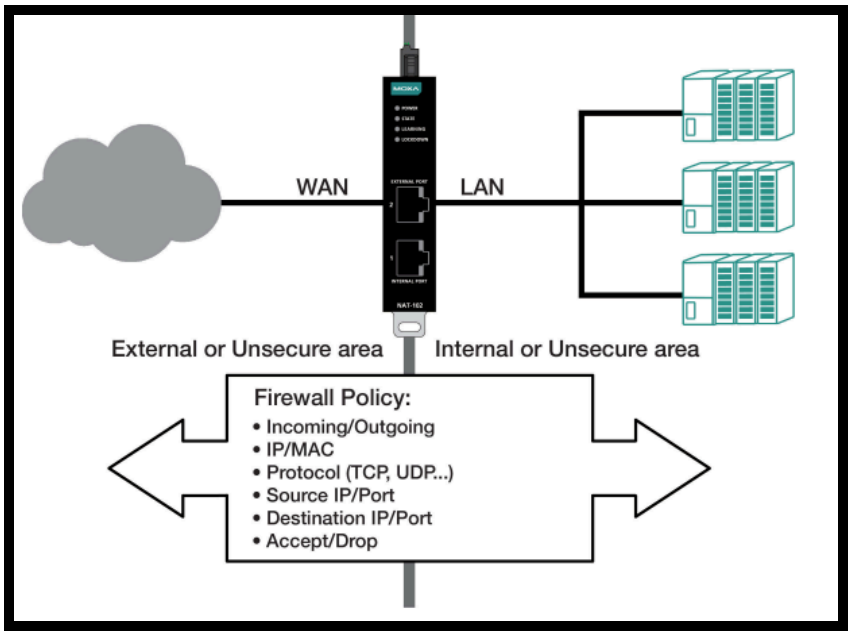


Figure 4.8 : Firewall Policy for Securing WAN to LAN Traffic

The diagram represents a network firewall policy, illustrating how data traffic is managed and secured between a Wide Area Network (WAN) and a Local Area Network (LAN). On the left side, the WAN is depicted as a cloud, symbolizing an external or unsecure area. On the right side, the LAN is shown with three server icons, representing an internal or secure area. In the center, the MOXA, acts as a barrier between the WAN and LAN. This firewall has various ports and indicators, showing its role in controlling the flow of data.

4.4.2.3 In-Built Security

The MOXA NAT-102 device enhances network security through robust certificate management and device lockdown features. Utilizing X.509 SSL certificates, commonly employed for IPsec, OpenVPN, and HTTPS authentication, the device can serve as a Root Certificate Authority (CA), issuing trusted Root Certificates. X.509 is a standard format for public key certificates, which are digital documents that securely associate cryptographic key pairs with identities such as websites, individuals, or organizations. These certificates are used in many Internet protocols, including SSL/TLS, which is the basis for HTTPS. They help establish secure communications by binding an identity to a public key using a digital signature.

Internet Protocol Security (IPsec) is a suite of protocols designed to secure Internet Protocol (IP) communications by authenticating and encrypting each IP packet in

a data stream. It is commonly used to create secure virtual private networks (VPNs) and can protect data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host2.

OpenVPN is an open-source VPN protocol that uses custom security protocols to create secure point-to-point or site-to-site connections in routed or bridged configurations. It is widely used for its flexibility and strong security features, allowing users to establish encrypted tunnels between networks3.

HTTPS (Hypertext Transfer Protocol Secure) is an extension of HTTP that uses encryption to secure communications over a computer network. HTTPS authentication involves the use of SSL/TLS protocols to encrypt data between a web server and a web browser, ensuring that the data transmitted is secure and that the identities of the communicating parties are authenticated4.

Users also have the flexibility to import certificates from external CAs. A Root Certificate Authority (CA) is at the top of the certificate hierarchy and is inherently trusted. When a device like the MOXA NAT-102 issues a Root Certificate, it's declaring that any certificates signed by this root are trustworthy. This enables verification, where devices or services that receive a certificate signed by this trusted Root CA can be authenticated. Others can verify that the certificate is legitimate and hasn't been tampered with. This also secures communications as with a trusted Root Certificate, encrypted connections (like HTTPS) can be established, ensuring that data transferred between devices is secure from eavesdropping or interception.

4.4.2.4 NAT Protocol Issues with IACS

There is an outstanding concern about the MOXA NAT-102 "hiding everything", which refers to its role in network segmentation, particularly within the Purdue Enterprise Reference Architecture (PERA) model. The PERA model is a framework for organizing and securing industrial control systems by segmenting networks into different levels, each with specific functions and security requirements, further explained in section 4.2.7.2.3. When a MOXA NAT-102 device is placed between the IT and OT networks, it effectively isolates the internal OT network from the external IT network. While this

enhances security by preventing direct access to sensitive OT devices, it also creates a "blind spot" for security monitoring. This means that any potential security risks or malicious activities within the OT network may go undetected because the NAT device obscures internal IP addresses and traffic patterns. Consequently, the security team loses the ability to perform passive monitoring and gain visibility into the internal network's activities. This lack of visibility can hinder the detection and response to security incidents, making it challenging to ensure comprehensive network security and compliance with cybersecurity guidelines. Therefore, while the MOXA NAT-102 provides significant security benefits, it also necessitates careful consideration of how to maintain adequate monitoring and visibility within the segmented network.

4.4.3 Network Switch

In a manufacturing shop floor environment, a network switch would serve as a central hub to connect CNC machines for data collection and .nc file transfer. The term "switch" refers to the device's ability to 'switch' traffic between its ports. When a data packet arrives at a port, the switch reads the packet's header to determine its destination and then forwards it to the correct output port. A network switch is a physical device that contains multiple network ports to connect devices within a LAN. The switch has Ethernet ports, typically RJ-45, which are used to connect devices like CNC machines via Ethernet cables. These ports can be of different types, such as:

1. Downlink Ports: Connect end devices like CNC machines to the switch. They can also provide power if the switch supports PoE (Power over Ethernet)
2. Uplink Ports: Connect the switch to other switches or routers to facilitate communication with the broader network or internet

The CISCO C9300-48PE-PoE is currently being used in the CAL and CMPU facilities, and is therefore the network switch of choice for machine connectivity at CHPC. Upstream of the switch, the CIMCO hosting server, whether a local or cloud

based application will be connected or configured onto which CIMCO client devices (PCs, mobile devices, tablets, etc.) can be connected.

Chapter 5: Connectivity Solution Execution

This section focuses on chronologically laying out the steps undertaken in order to begin implementing machine connectivity at the facility. The process begins with gathering comprehensive information about the machines, such as CNC machines and controllers. This involves understanding their network interfaces, communication protocols, and any specific configuration they might require.

Next, it's essential to comprehend the existing network infrastructure, including the segmentation of the network and the setup of Virtual Local Area Networks (VLANs). Network segmentation is crucial for security and performance, as it separates different types of traffic and can restrict access to certain parts of the network. Understanding VLANs is equally important, as they allow for creating multiple virtual networks over a single physical network infrastructure, which can be used to group machines by type, department, or any other classification that suits the facility's operational needs.

Once the preliminary information is gathered and the network is understood, the next step is to begin setting up the servers that will manage the connectivity. This includes configuring the servers with the necessary software, ensuring they have the correct network settings, and testing their ability to communicate with the machines. Throughout this process, tools like ping are used to verify connectivity and network performance, ensuring that each machine is reachable and that the data exchange is within acceptable parameters. This meticulous approach ensures a robust and reliable network setup that facilitates smooth communication between machines, which is vital for efficient and uninterrupted operations.

5.1. Machine Information

Machine information is pivotal in the realm of machine connectivity, particularly when implementing software solutions like CIMCO DNC-Max and MDC-Max. Before establishing connections, it's essential to have a comprehensive understanding of each machine's specifications, such as model number, function, work-cell ID, and manufacturer details. For instance, the table you mentioned includes critical data like the connection method, which could be RS232 or RJ45, indicating the physical interface for data transfer. Additionally, unique identifiers like MAC addresses, and IPv4 and IPv6 addresses, are indispensable for network

communication. These identifiers enable the Azure server to accurately locate and interface with CNC machines, facilitating the exchange of data, including machine status, program files, and operational commands. Moreover, a properly configured IP setup is not just about connectivity; it's the backbone of remote management and monitoring capabilities. It allows for efficient software updates and troubleshooting, ensuring that CNC machines operate smoothly within the networked ecosystem

The Table 5.1 below summarizes the machines that will be connected first for the CIMCO DNC-Max and MDC-Max software. Note that certain sensitive information has been redacted. The table has information regarding the model number, function (5-axis), work-cell (Machine Workcenter ID), machine manufacturer (Mazak), connection method (RS232 AND RJ45), which will be used to physically connect machines for data transfer. The hardware used for the connection is discussed further in Section 4.3. The rest of the columns, MAC address, IPv4 address and IPv6 link local address are unique identifiers for the machines that will be used to set up connections. The IP address allows the Azure server to locate and communicate with the CNC machine over the network, whether it's through a wired Ethernet connection or a wireless network. With the correct IP configuration, the CNC machine can send and receive data to and from the Azure server. This can include machine status updates, program files, and operational commands. This also allows remote management and monitoring CNC machines from the Azure server, allowing for tasks such as updating software and troubleshooting issues.

Table 5.1: Critical CNC Machines at CHPC with Relevant Information

This table contains information of 7 CNC machines and their controllers. There is the satellite center where they are located (CHPC), Equipment Manufacturer, Model Number, Year of Build, Machine Workcenter ID, Function, CNC Controller Model, Connection Methods, MAC address, IPv4 address and IPv6 Link Local Address

Number	Satellite Center	Equipment Manufacturer	Equipment Model Number	Year of Build	Machine Workcenter ID	Function	CNC Manufacturer	CNC Model	Connectivity Method	MAC Address	IPv4 Address	IPv6 Link Local
1	CHPC	Mazak	INTEGREX-500 H II	2010	WA625K_1160_002	Mill-Turn-Bore-Drill	Mazak	Mazatrol Matrix 2	RJ45 & RS232	XX-XX-XX-XX-XX-XX	XX.XXX.XX.XX	XXXX::XXXX:XXXX:XXXX:XXXXXX
2	CHPC	Mazak	INTEGREX-670 H II	2010	WA621K_1160_002	Mill-Turn-Bore-Drill	Mazak	Mazatrol Matrix 2	RJ45 & RS232	XX-XX-XX-XX-XX-XX	XX.XXX.XX.XX	XXXX::XXXX:XXXX:XXXX:XXXXXX
3	CHPC	Mazak	INTEGREX E-420HS2	2009	WA619K_1160_002	Mill-Turn-Bore-Drill	Mazak	Mazatrol Matrix 2	RJ45 & RS232	XX-XX-XX-XX-XX-XX	XX.XXX.XX.XX	XXXX::XXXX:XXXX:XXXX:XXXXXX
4	CHPC	Mazak	INTEGREX E-650H2	2006	WA601B_1160_002	Mill-Turn-Bore-Drill	Mazak	Mazatrol Matrix 1	RJ45 & RS232	XX-XX-XX-XX-XX-XX	XX.XXX.XX.XX	XXXX::XXXX:XXXX:XXXX:XXXXXX
5	CHPC	Mazak	INTEGREX E-650H2	2007	WA602O_1160_002	Mill-Turn-Bore-Drill	Mazak	Mazatrol Matrix 1	RJ45 & RS232	XX-XX-XX-XX-XX-XX	XX.XXX.XX.XX	XXXX::XXXX:XXXX:XXXX:XXXXXX
6	CHPC	Mazak	INTEGREX E-650H2	2008	WA604B_1160_002	Mill-Turn-Bore-Drill	Mazak	Mazatrol Matrix 1	RJ45 & RS232	XX-XX-XX-XX-XX-XX	XX.XXX.XX.XX	XXXX::XXXX:XXXX:XXXX:XXXXXX
7	CHPC	Mazak	INTEGREX E-650H2	2009	WA609O_1160_002	Mill-Turn-Bore-Drill	Mazak	Mazatrol Matrix 1	RJ45 & RS232	XX-XX-XX-XX-XX-XX	XX.XXX.XX.XX	XXXX::XXXX:XXXX:XXXX:XXXXXX

The machine specific information with the MAC address and IP addresses were collected by going to each CNC machine controller. The CNC controllers all use Windows 7, and the information was collected by going into the command prompt to obtain information under the “Ethernet Adapter”. Some CNC machines were not connected to the SLB network, and therefore lacked an IP address. The method for connecting these machines is by physically tethering an ethernet cable from the CNC machine controller to the network switch, and then from the network switch to the local server.

5.1.1 Pinging Machines

After finding the IP addresses for each of the machines, an important check to determine whether the machines are properly connected to the network is through pinging from a local device. The Figure 5.1 image shows the output of a network utility command called ping. The ping command is used to test the reachability of a specific IP address on a network and measure the time it takes for messages to travel to the destination and back. The summary statistics at the bottom of the figure show that all four packets were sent and received without any loss, resulting in a 0% packet loss rate. The round-trip times are summarized as follows: minimum = 1ms, maximum = 76ms, and average = 23ms. These results confirm that the host at the specified IP address is reachable and responds within an acceptable time frame, demonstrating stable network connectivity and performance.

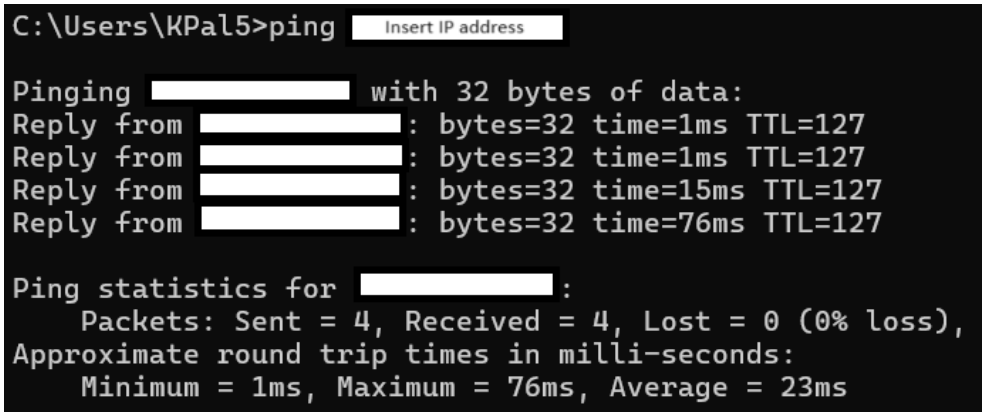


Figure 5.1: Network Performance Analysis using Ping Response Times and Packet Loss Evaluation for IP Address

This figure illustrates the results of a ping command executed to assess the network performance and connectivity to the IP address. The command was run from a command prompt, and the output includes four individual ping attempts. Each attempt successfully received a reply, indicating no packet loss. The response times for the four attempts were 1ms, 1ms, 75ms, and 76ms, with a consistent Time To Live (TTL) value of 127.

Although some machines responded to being pinged, other CNC machines had some difficulty responding. The command prompt at the local device would output a “Request timed out”. When a “Request Timed Out” message appears during a ping test, it indicates that the computer sent ping packets to the destination IP address but did not receive any acknowledgment within the expected time frame. Essentially, the computer was waiting for a response that never arrived. This issue can arise due to several reasons. One common cause is network configuration errors, such as an incorrect IP address or routing issues that prevent packets from reaching their destination. Another frequent cause is firewall blocking, where either the local firewall on the computer or the remote firewall on the destination device is configured to block ping requests or responses. Network congestion can also lead to timeouts, especially if the network is experiencing heavy traffic, causing packets to be delayed or dropped. Additionally, device issues like the destination device being offline or having a malfunctioning network interface can result in no response to the ping requests.

5.2. Azure Server Bringup Attempt

The Azure server first needs to be requested through submission of "Request Cloud Work Area" intake form. This form will ask for information such as cloud service provider (Microsoft Azure, Google Cloud, Amazon AWS, MongoDB Atlas), cost center (where the monthly charge will be assigned), company (workcenter) code, ownership (technical contacts, business and application owners), application end user (client, contractor, employee) and network exposure (SInet, DMZ, iDMZ). This form will then be assessed by the global IT team, after which the purchase will be approved.

During discussion with the IACS team regarding the exemption to be submitted, it was discussed that without having a strategic path forward for implementing the solutions highlighted in section 4.3.3, the exemption request would likely be rejected. There is an ongoing inquiry toward CIMCO on whether they have the capability of setting up a proxy server to exist in the iDMZ, allowing communication between the Azure server on level 5 of PERA down to the CNC machines in levels 1 and 2. The reasoning behind obtaining a proxy server was discussed in section 4.3.3.

5.3. Hardware Quotation

Hardware quotation requests were sent out for critical hardware requirements. The table below shows the status of the quotation, as well as the components which have already been scoped. This is presented in Table 5.2 below.

Table 5.2: Hardware Components Quote List

This table contains information of hardware components that will be required for connectivity implementation at CHPC, alongside information on the specific model, quantity and quote status

Part Name	Category	Brand	Model	QTY	Use For	Status	Notes
Serial Device Server	Hardware	MOXA	Nport 5110A	7	Enable networking for controller	Quoted	Quoted by CIMCO
Connector (Serial Cable)	Hardware	MOXA	CBL-RJ45M9-150	10	Recrimp to RJ45 cables	Quoted	
Rack Server	Hardware	Dell	PowerEdge R750 Server	1	Supports DNC Service, PDM files	Quote Pending	Migration required from old server
SSD (Server Storage)	Hardware	Dell	MD1400	1	Storage for server	Quote Pending	Comes with Dell Server
CIMCO Licenses	Software	CIMCO	DNC-Max, MDC-Max	N/A	DNC, MDC	Quoted	
Network Switch	Hardware	Cisco	N5860	1	Shop-floor machine connection	Quote Pending	

5.2. CHPC Network Segmentation Structure

When setting up the server, it is important to understand what the network segmentation at the facility was like, specifically for the machines related to manufacturing (CNC controllers, edge devices, remote devices and client machines). The network segmentation for CHPC is organized to cater to different functional areas and ensure security and efficiency. The Server VLAN (10) is isolated with its own IP range, ensuring that server traffic is segregated from other types of traffic. User VLANs (20) have a broader range, accommodating a larger number of devices, which is typical for general user access. Limited access workstations are segmented into VLANs 21 and 49, likely to restrict access to sensitive areas or data. Wireless users are assigned to VLAN 25, separating them from wired users for better management and security. The Voice VLAN (50) ensures that voice traffic is prioritized and managed separately from data traffic. Specialized VLANs like 81 for SLB, 90 for printers, 91 for PACS-Security, 92 for manufacturing, and 94 for IoT Sinet indicate a tailored approach to network segmentation, addressing specific needs and enhancing security. Finally, VLAN 400 for L3.5 suggests a higher-level management or specialized network segment. This structured approach helps in maintaining network performance, security, and manageability.

The Manufacturing VLAN (92), supports critical operations within the facility. This VLAN is dedicated to manufacturing processes, which means it was setup to handle data from various industrial devices and systems, such as machinery, sensors, and control systems. By isolating manufacturing traffic, the network ensures that these essential operations are not disrupted by other types of network traffic, enhancing both performance and security. Additionally, this segmentation helps in monitoring and managing the manufacturing environment more effectively, potentially integrating with IoT devices and other advanced technologies to optimize production and maintenance processes. For this implementation of CIMCO, this VLAN will be critical for connecting the CNC machine controllers to the cloud application, as communication of machine data and .nc files will occur over it. Wireless users (or remote clients) will utilize a different VLAN to access the main network, while edge devices are under VLAN 20.

5.3. Cloud Server Limitations

When utilizing Azure cloud server applications for machine connectivity purposes, such as .nc file transfer and machine data collection, several limitations may arise. Firstly, network bandwidth, and a secure connection can significantly impact the transfer speed and fidelity of files; thus the actual network performance will depend on factors such as network congestion and application loads. As seen in an example in another facility in Houston, RBTC, despite there being a DNC software to facilitate .nc file transfer from the server to the CNC machines on the shop floor, minor file edits are still done by transferring the file from the controller to a USB drive and then moved to edge devices. Operators complained that downloading, editing and re-uploading the .nc file to the edge device often took longer than the aforementioned. However, this is also a concern for locally placed servers, as is the case with RBTC.

Secure communication can also be challenging, as there might not be a full-time secure connection between the on-premise network and the cloud-based solution, potentially requiring the use of VPNs or agents, which can introduce complexity and reliability issues. As highlighted in sections 4.3.3 and 4.3.4 SLB has stringent policies for the usage of cloud based applications, simply because of the vulnerabilities they may pose to the SLB network. One of the primary concerns is system misconfigurations, which can occur during setup or operation, leading to

unintentional vulnerabilities. However, in the context of SLB's guidelines, cloud applications simply pose an avoidable risk to the other devices on the network, and are therefore difficult to approve. The following section will go into detail regarding the specific concerns regarding the cloud server application.

5.4. Connection Security Challenges

As mentioned previously, the application for connectivity is currently experimental. However, as the local team at CHPC moves forward with connecting all the CNC machines on the shop floor for full visibility - i.e. full CIMCO connectivity implementation in the facility - there are likely some challenges with the security team.

1. Traffic Control and Segmentation: In line with IEC 62443, traffic from outside the IACS network, including the internet and internal IT networks, is not permitted to reach the lower levels of the Purdue model directly. This is to prevent unauthorized access and potential cyber threats to sensitive operational technology (OT) environments.

2. Jump Hosts and DMZ: To facilitate secure communication, a jump host or a demilitarized zone (DMZ) is used. A jump host acts as a secure and controlled entry point for users before accessing the OT network, while a DMZ serves as a subnetwork that exposes external-facing services to an untrusted network, typically the internet, adding an extra layer of security.

3. DNC-Max Server Connectivity: The DNC-Max server, which initiates connections to machines, must comply with these security policies. If the server is not on-site, it should be placed in a local DMZ, allowing it to communicate with the IACS network securely. Alternatively, a jump host or proxy server can be implemented to enable the server's location in the cloud or a data center, ensuring that all communications are properly secured and monitored.

4. Port Management: Regarding the TCP/UDP port requirements, it's essential to minimize the number of open ports to reduce the attack surface. While the list may include multiple ports for SMTP and database services, in practice, only a subset of these ports that are necessary for the specific hardware and overall design will be utilized. This approach aligns with the principle of 'least privilege', ensuring that only the required ports are active and all others are disabled or blocked.

Chapter 6: Future Work

6.1. CIMCO Connectivity Project Full-scale Implementation Guidelines

The trial implementation for the CIMCO software was highlighted in Section 5, where steps involved gathering detailed information about the machines, such as CNC machines and controllers, including their network interfaces and communication protocols. Furthermore, Understanding the existing network infrastructure, including network segmentation and VLANs, is crucial for security and performance as the server is deployed. After collecting this information, the next step is to set up the servers that will manage connectivity, configure them with the necessary software, and test their communication with the machines using tools like ping. This thorough approach ensures a reliable network setup that supports smooth machine communication and efficient operations. Although the following steps were completed, the implementation of the software was incomplete, due to unforeseen technical challenges the author faced which necessitated further adjustments and testing before full deployment could be achieved.

Therefore, this section will focus on the immediate next steps that the engineer taking over this project can follow to begin the actual implementation. The following steps can be followed to ensure a successful deployment:

1. Ensure successful connection for critical CNC machines: Although all seven critical machines listed in Table 5.1 have IP addresses, only four responded to ping tests. This is likely due to inactivity from PDM, as local IT had disconnected the machines to ensure air gapping. Therefore, it is crucial to verify the connections of the remaining machines and ensure their IP addresses are responsive.
2. Hardware Inquiry and Quotation: While we have received some hardware quotations, there are still outstanding submissions needed. The requirements for servers and storage differ between cloud and local servers. Therefore, it’s crucial to involve the server team and local IT who have detailed information on the necessary specifications, including supported virtual machines, SSD storage, RAM, and 10GbE network interfaces.

3. Server Bring-up: Once the PO is submitted and the server is received, the EMC team in Jakarta will remotely configure it, including server imaging and installing monitoring tools. Upon arrival at CHPC, IT support analyst James Frier will unbox, inspect, and mount the Dell PowerEdge R440 server, connect it to power and network, and configure BIOS/UEFI settings. Enable remote access tools like iDRAC9 for further remote configurations, set up network settings, and perform connectivity, functionality, and security tests to ensure the server is fully operational and secure.
4. CIMCO On-site: CIMCO's technical customer service will arrange for a field representative to visit CHPC. The field rep will be responsible for evaluating the necessary connections to your machinery and addressing any technical issues that may arise. The main objective would be to configure the machine ports onto the software, and ensure both DNC-Max and MDC-Max are operational. Furthermore, training sessions can be hosted for operators and engineers, depending on individual use-cases.
5. Continued Documentation: Although these steps provide general instructions toward implementing connectivity, there will likely be several challenges to overcome. Maintain track of the challenges and remediation is crucial to ensure proper guideline development for other facilities to follow. Confluence wiki pages are standard in SLB for maintaining records of instructions for various projects, and would be a valuable resource

6.2. CIMCO Licensing

CIMCO is set to integrate with manufacturing equipment to manage and track production data. SLB will carry out an initial assessment for high-level planning, followed by a detailed assessment with CIMCO for quoting and installation. If further in-depth assessment is needed, CIMCO may conduct an on-site evaluation at a predetermined price. In cases where machine protocols are unclear, CIMCO will include legacy hardware in their quotation. SLB will receive a firm quote for each project, covering all aspects from planning to support, which will define the Scope of Work (SOW). Any additions to the SOW will incur charges as per the service rates specified. CIMCO will also provide a rough estimate after the initial survey and a firm quote post a detailed survey or site visit. Charges for additional hardware or services outside the initial quote will be billed hourly. Work outside the original scope will only begin after CIMCO receives a purchase order for the extra services. Any changes to the SOW require a change order

and purchase order to proceed. Appendix 4 also consists of information between the SLB and CIMCO agreement for license pricing.

Additional information regarding the pricing and cost structure for the licenses, and additional costs associated with the setup of the software are provided in Appendix 4.

CIMCO's obligations to provide Maintenance and Support Services are contingent upon several customer responsibilities. Customers must grant CIMCO remote access to their personnel, equipment, and testing environments during regular business hours to duplicate and resolve errors. Failure to provide this access will void CIMCO's support target obligations. Customers are also responsible for supervising and managing the use of the Licensed Software, implementing procedures for information protection, and maintaining backup facilities in case of software errors or malfunctions. Additionally, customers must document and promptly report all software errors or malfunctions to CIMCO and follow procedures for error rectification within a reasonable time. Maintaining a current backup copy of all data used by the software and meeting or exceeding minimum hardware, OS, and network specifications are also required. Proper training of users in the software and equipment is essential. If faults cannot be replicated remotely, customers may need to cover the costs for CIMCO staff to attend the site, with preapproval and a purchase order required.

CIMCO may update the Licensed Software periodically and will provide these updates to customers free of charge during the Maintenance Subscription Term. However, hardware is not covered by CIMCO's maintenance agreement, and any warranty issues will be handled by the hardware suppliers.

6.3 Cybersecurity Guidelines

6.3.1 Purdue Enterprise Reference Architecture

The Purdue Enterprise Reference Architecture (PERA), also known as the Purdue Model, is a framework developed in the 1990s for enterprise architecture. It was created by Theodore J. Williams and his colleagues from the Industry-Purdue University Consortium for Computer Integrated Manufacturing [36]. PERA is designed to help organize and guide the architectural development of enterprise systems through multiple layers and stages of the life cycle. It

includes a methodology for master planning and concepts for dividing enterprise systems into physical and logical architectures. The model is particularly noted for its levels of enterprise integration, ranging from the physical process to business logistics systems, providing a structured approach to managing manufacturing operations and their control systems. Additionally, it serves as a baseline for segmenting industrial control system networks from corporate enterprise networks and the internet, ensuring secure and efficient operations.

PERA is highly relevant to SLB, as the new cybersecurity guidelines being developed by IACS leverages the model as guidelines for connectivity at facilities due to its structured approach to network segmentation and its emphasis on security. In the context of IACS, which includes a variety of control systems and associated instrumentation, the PERA model provides a valuable framework for ensuring that these systems are organized and managed securely. The model's layers, which separate physical processes from enterprise-level logistics, align well with the IACS goal of integrating components like HMIs, PLCs, sensors, and actuaries into a cohesive unit. This integration is crucial for maintaining operational efficiency and cost-effectiveness while also adhering to cybersecurity guidelines.

6.3.2 Network Segmentation Goals at CHPC

Network segmentation is a critical security strategy that involves dividing a network into smaller, manageable segments to enhance control and visibility. Although CHPC has network segmentation already implemented in its facility, as discussed in section 5.2, guidelines by IACS suggest a better segmentation methodology to follow.

The primary goals of network segmentation include creating a clear separation between the Corporate Network and Operational Technology (OT) Network, which helps in monitoring and controlling network traffic. This separation is essential to reduce the impact on critical manufacturing systems and to increase the overall security of OT networks. By implementing security through standardization, organizations can modernize outdated network mechanisms, such as end-of-life firewalls and switches, ensuring a robust defense against potential cyber threats. Furthermore, network segmentation supports the operating model by enforcing segregation of duties, limiting system access to authorized personnel within controlled layers and

zones. These measures collectively contribute to a secure network environment that protects sensitive systems and data from unauthorized access and cyberattacks, aligning with the best practices for maintaining a resilient industrial infrastructure.

The figure 6.1 below highlights the different “pillars” of network segmentation proposed for SLB. The pillars include Segmentation, iDMZ (Industrial Demilitarized Zone), Benefits, Zoning, and Conduits. Segmentation involves isolating devices and network traffic for cybersecurity, focusing on access control between IT and OT networks. The iDMZ acts as a buffer zone to secure IT/OT convergence, allowing data flow in one direction. The benefits of these strategies include enhanced design controls, risk management, and ensuring health and safety. Zoning creates granular security policies for system access, while conduits define communication paths between zones with varying trust levels, using firewalls to minimize the impact of malicious traffic. Each pillar is characterized by specific features such as enforced firewalls, unidirectional data flow, and defined data flow paths, all aimed at strengthening network security and resilience.

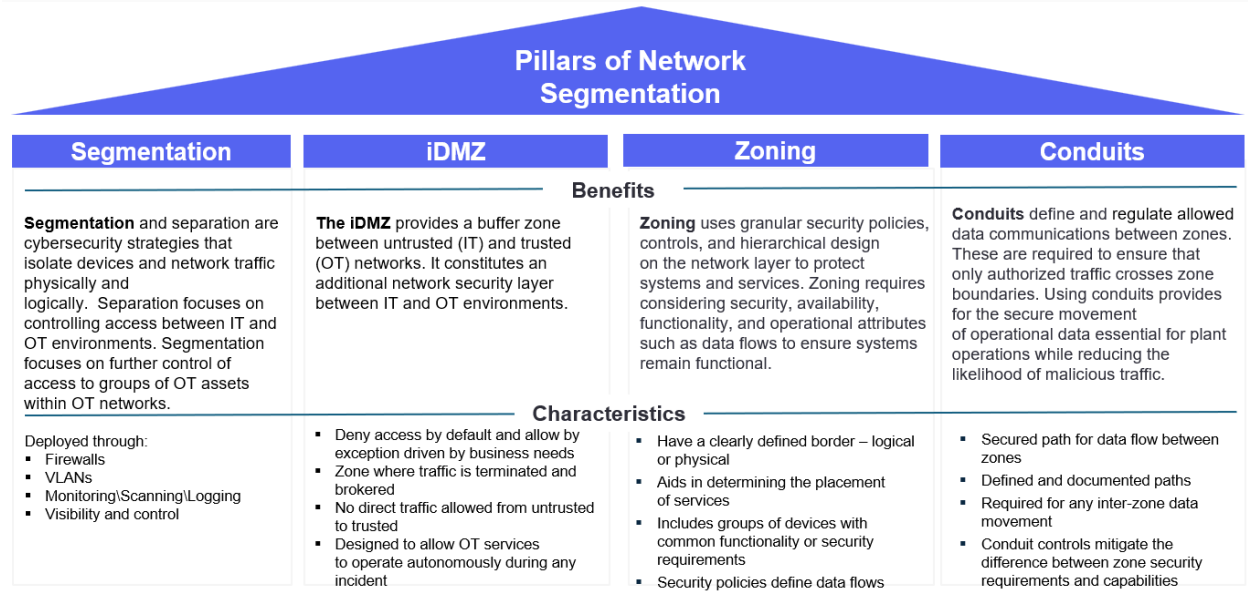


Figure 6.1: Key Strategies for Effective Network Segmentation

The figure outlines the "Pillars of Network Segmentation," which include Segmentation, iDMZ, Zoning, and Conduits. Each pillar represents a different strategy for isolating devices and network traffic to enhance security. Segmentation involves separating IT assets for better control and monitoring. The iDMZ acts as a buffer zone between untrusted and trusted networks, adding an extra layer of security. Zoning uses granular policies to control access based on user roles or device types. Conduits regulate data communications between zones, ensuring secure data transfer through controlled entry points. This structured approach helps organizations implement effective network security measures.

6.3.3 Segmentation and Separation

Network Segmentation and Network Separation are seen as measures that enhance the security of a network. They offer protection for critical Operational Technology (OT) assets by establishing network levels, zones, and segments that reflect the system's criticality and function. The flow of network traffic between these levels is meticulously controlled in adherence to the principle of least privilege access. Within each level, a variety of security controls are diligently implemented.

The process of Network Separation and Segmentation is regarded as a complex, multistep endeavor. It encompasses the identification of assets and network structure, the design of a

reference model, meticulous planning for implementation, and the execution of Network Separation/Segmentation, which includes thorough validation and acceptance phases. Network Separation is the idea of creating layers of network to separate systems based on their criticality to ensure appropriate security levels. Network Segmentation is the idea of implementing cybersecurity strategies that isolate devices and network traffic both physically and logically. The figure 6.2 below show a different PERA model, with an example implementation of facility wide resources.

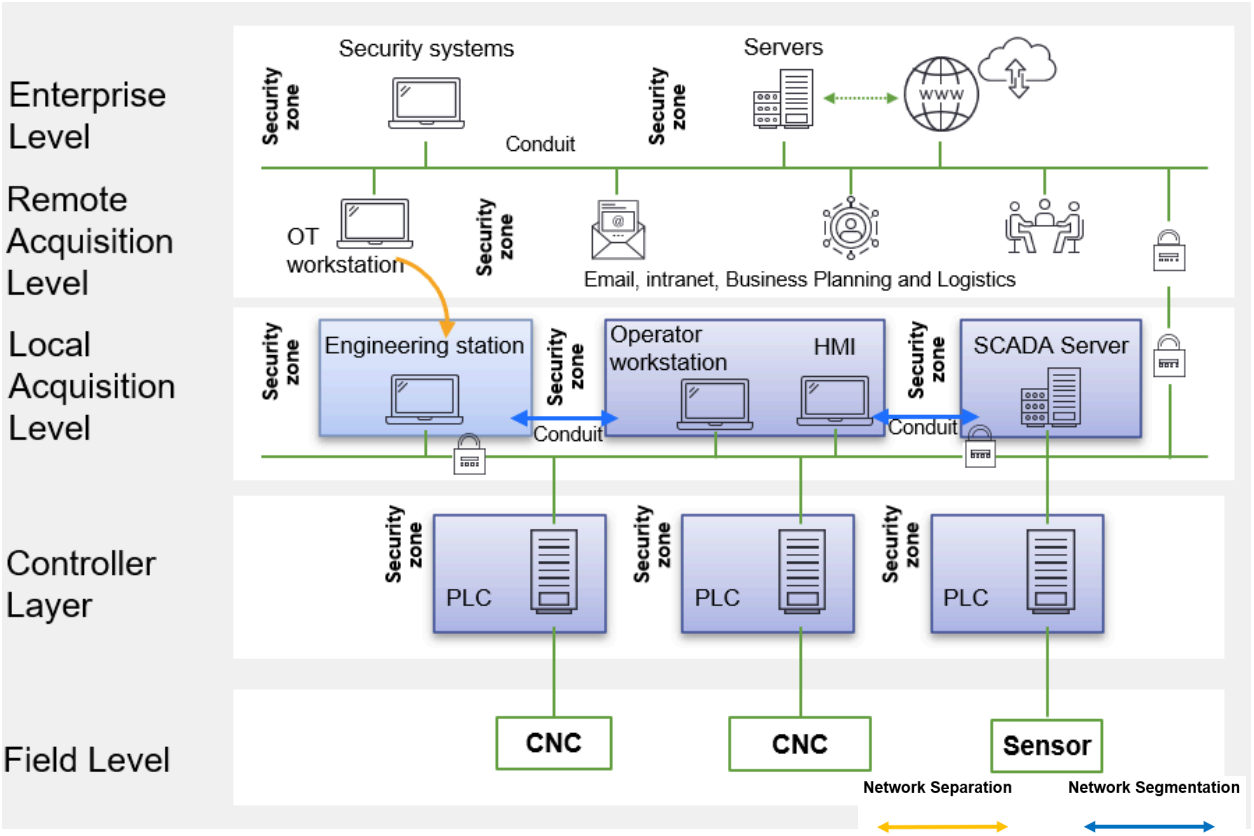


Figure 6.2: PERA Model with Segmentation and Separation

This figure illustrates another version of the PERA model, which shows multi-layered industrial control system architecture, depicting the integration of enterprise, remote, and local acquisition levels with field-level equipment. This diagram has allows depicting different arrows for Network separation (in yellow), and network segmentation (in blue)

6.3.4 Segmentation Criteria:

Security zones enhance network protection by dividing into segments according to criteria like business criticality, common business functions, separation of duties, geographic location, and technical administration. This segmentation ensures that different user groups and technical support teams have appropriate access. Additionally, each zone may contain assets for distinct business functions and can be subdivided based on sub-processes. Every zone requires at least one segment, established through VLAN configurations. Advanced technologies like EVPN, VXLAN, and NvGRE are considered for deployment. Inter-segment traffic is regulated by firewalls, ensuring secure, controlled access within the network.

6.3.5 Cloud Considerations

Implementing strict cloud communication protocols where only authorized OT system components initiate contact through iDMZ-mediated exchanges is a robust security measure. It prevents unauthorized access and ensures that sensitive operations technology data remains within a controlled environment. The prohibition of jump stations in the cloud further eliminates potential vulnerabilities. Trusting connections only to clouds where SLB exercises full configuration control over applications and user access fortifies security. Requiring external cloud service providers to demonstrate compliance with standards like ISO 27017 assures adherence to best practices in data protection. Encrypting OT data at rest and in transit, coupled with exclusive access for authorized users and comprehensive monitoring of all activities, creates a formidable defense against data breaches and cyber threats, thereby maintaining the integrity and confidentiality of critical OT data.

Mandating encryption for all communications between SLB's cloud-hosted applications is a prudent security practice that safeguards data integrity and confidentiality. Documenting communication protocols ensures transparency and adherence to security standards. Authentication is a critical gateway, and enforcing robust mechanisms such as open standards used for securely transmitting information between parties as a JSON object. Requiring vendors to disclose public IP addresses used for outbound communications establishes accountability and traceability, while the option to use VPNs or private links like Azure/AWS for inter-provider exchanges offers secure, dedicated pathways for data transfer. Limiting service exposure to specific IPs and providing comprehensive audit logs for integration not only enhances security but also enables effective monitoring and auditing, aligning with best practices for cloud security management.

6.5. Azure HCI (Hyperconverged Infrastructure)

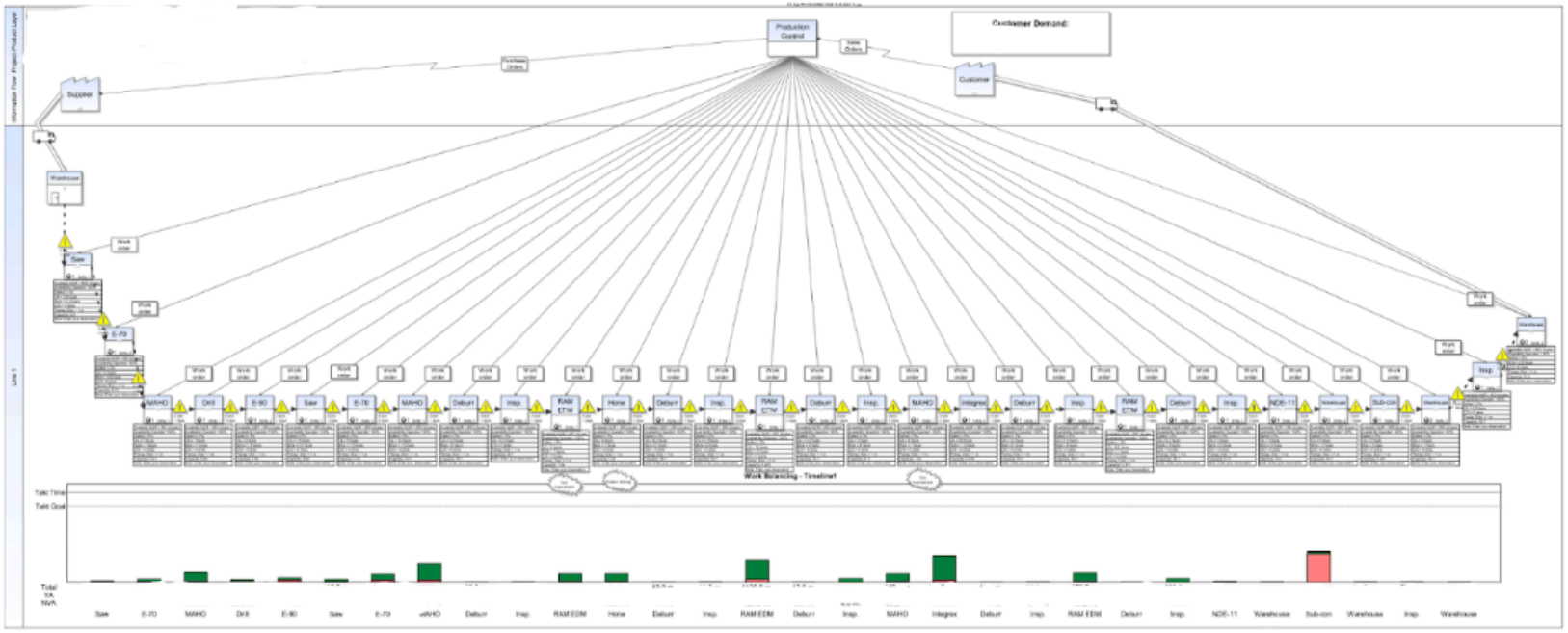
Although the cloud application through Azure has inherent challenges highlighted by IACS guidelines at SLB (as discussed in section 4.2.2.3) , there was discussion regarding other potential cloud-based server solutions that may be compliant. The following section discusses Azure HCI, which although pending approval, can be evaluated upon request by the IACS team if CHPC decides to continue exploring cloud-based server solutions for their machine connectivity.

Azure Stack HCI (Hyperconverged Infrastructure) is a hybrid solution that combines on-premises infrastructure with Azure cloud services, enabling organizations to run virtualized workloads on Windows and Linux VMs or containerized applications. It provides a unified system for storage, networking, and compute resources, and connects to Azure for cloud-based services, monitoring, and management, offering a consistent and integrated management experience. Azure Stack HCI can help conform with Industrial Automation and Control Systems (IACS) by enhancing security, reliability, and compliance. It includes built-in security features such as encryption, secure boot, and compliance with industry standards, and integrates with Azure Security Center for continuous monitoring and threat detection. By keeping critical data on-premises while leveraging Azure's cloud capabilities, Azure Stack HCI helps meet data sovereignty and regulatory requirements, which is crucial for industries with strict compliance needs. The integration with Azure allows for centralized management of both on-premises and cloud resources, simplifying the management of IACS environments and ensuring consistent policies and configurations. Additionally, Azure Stack HCI supports scalable and flexible deployment options, allowing organizations to adapt to changing workloads and requirements, which is essential for maintaining operational efficiency in industrial environments. It also provides robust disaster recovery and backup solutions, ensuring business continuity and data protection, which is vital for maintaining the integrity and availability of IACS. By leveraging Azure Stack HCI, organizations can enhance the security, compliance, and efficiency of their industrial automation and control systems, aligning with best practices and regulatory standards.

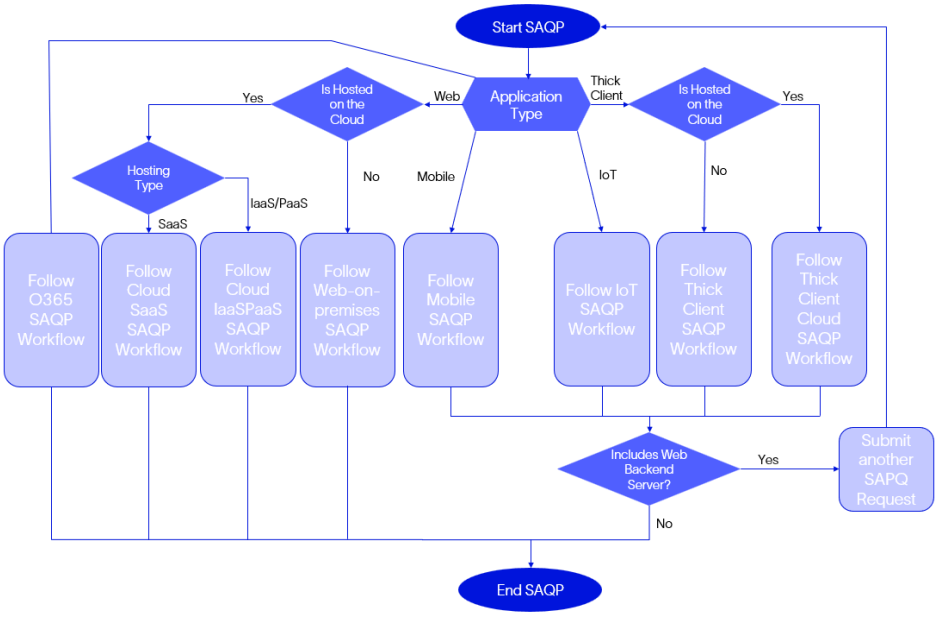
Azure Stack HCI also offers several advantages over traditional Azure cloud applications, particularly for organizations with specific on-premises needs. Firstly, Azure Stack HCI provides industry-leading virtualization performance and value by combining compute, storage, and networking into a single, easy-to-manage platform1. This integration reduces complexity and

enhances efficiency, freeing up IT resources to focus on strategic initiatives. Additionally, Azure Stack HCI allows for flexible deployment options and unrestricted access to Hyper-V features, making it ideal for scenarios requiring minimal server footprint and low latency, such as remote offices and branches. It also supports hybrid scenarios by connecting to Azure for cloud-based services like backup and monitoring, ensuring a consistent and integrated management experience. Moreover, Azure Stack HCI helps meet data sovereignty and regulatory requirements by keeping critical data on-premises while leveraging Azure's cloud capabilities. This is crucial for industries with strict compliance needs. The solution also provides robust disaster recovery and backup options, ensuring business continuity and data protection.

Appendix 1: Value Stream Mapping of Production Part

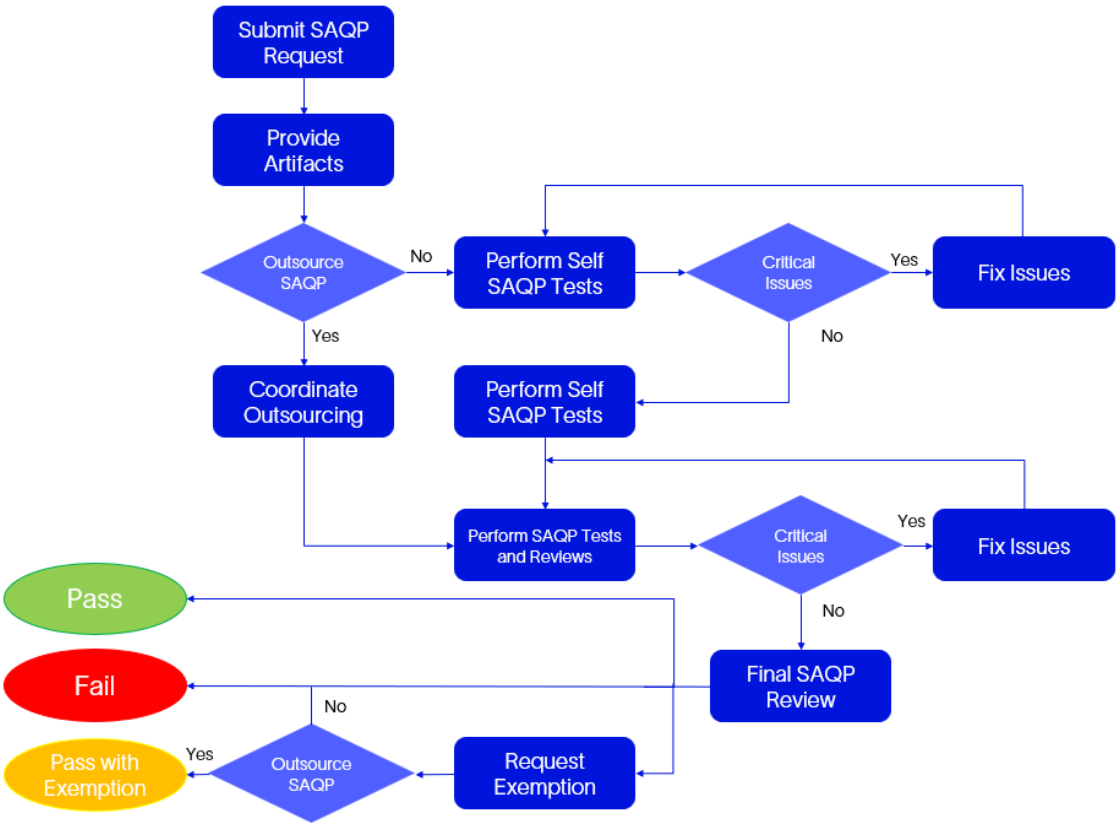


Appendix 2: General SAQP Process Flow



The process flow shows the different applications that require SAQP approval including: O365, Cloud Saas, Iaas, Paas, web, mobile, IoT, and Thick Client and Backend Server Requirement

Appendix 3: SAQP process flow for an IaaS cloud-based application



The process flow shows specifically the steps in the SAQP for cloud-based applications approval. The process involves providing information (Artifacts), performing self-tests, SAQP tests, amending issues and going through final approval before passing, failing or passing with exemption in rare cases

Appendix 4: CIMCO Pricing Structure

CIMCO Edit, DNC-Max, NC-Base, MDM License pricing:

Description	License cost	Maintenance (per year)
CIMCO Software Manager	$0	$0

- CIMCO's NLS Software. One CIMCO Software Manager NLS should be present per network.

MDC-Max/DNC-Max server license	$0	$ 0

- CIMCO DNC-Max, NC-Base, MDC-Max and MDM Servers
- The $850 license cost is waived for new Schlumberger installations

DNC Port (only) License	$200	$ 36

- One license needed per machine tool for DNC communication

DNC/ MDC Port/Client License Bundle	$600	$108

- Includes DNC-Max Port License, MDC-Max port License, and one floating client license
- List price is $950 per machine

DNC or MDC Client floating licenses	$300	$ 54

- List price is $350/client
- web or installed clients
- One license needed per concurrent user

CIMCO BKTrans	$200	$ 36

- Used to enable communication with Windows-based networkable machines with disabled protocols, such as SMB1

CIMCO Edit License	$400	$ 72
CIMCO Edit with NC-Base Licenses	$640	$115
CIMCO MDM Client with CIMCO Edit License	$1200	$216

- List price is $1500/client

CIMCO MDM Web client	$440	$ 79

- CIMCO Edit is not included with web client licenses
- List price is $550/client

If licenses for software not listed above are required, the licenses will be quoted at CIMCO's current list price. All license keys will be created for the quantity of licenses ordered.

Additional Hardware Costs

Hardware pricing fluctuates and will be quoted with current pricing at the time of quotation. Hardware that may be used for DNC communication is as follows:

Description	**Current cost**
Moxa Nport 5110A with RJ45 to DB9/25 adapters	$250

- Connects to ethernet
- One serial port device server
- A device with two serial ports is available if needed.

Moxa Nport 2150A with RJ45 to DB9/25 adapter	$450

- For wireless connection
- One serial port wireless device server
- A device with two serial ports is available if needed.

OT Max secure Box for DNC/MDC $990

- Supports secure encrypted communication for machines with blocked protocols such as FTP and SMB1.

CIMCO provides firm quotations for service time based on machine information and project scope. They ensure that charges do not exceed the quoted amount unless additional services are requested. Typical installation times vary depending on customer requirements and equipment, with rough estimates provided for various tasks such as server setup, NC-Base configuration, MDM configuration, and DNC installation per machine. Service rates include $200 per hour for on-site service with an 8-hour minimum, plus expenses, and $100 per hour for travel time. After-hours service is available at a higher rate if requested and agreed upon in advance. Remote service and development are also offered at $200 per hour with a 1-hour minimum. CIMCO emphasizes the importance of proper preparation to reduce on-site installation time and requires a pre-installation meeting to ensure all action items are completed before their arrival.

Expenses for travel, including hotel, flight, and rental car, are billed at cost, with estimates provided in quotations. CIMCO's standard maintenance and support agreement includes an annual fee of 18% of the software purchase cost, covering software maintenance and global project coordination. This agreement is optional but recommended, providing access to the latest software versions and bug fixes. Post-implementation support is available during regular business hours, with designated technical liaisons able to request support via phone, email, or web. The support agreement covers global site support, ongoing maintenance, application testing, and user support, but additional functionality or changes to the core configuration may incur additional charges.

References

[1] Bloomberg, “Schlumberger,” Schlumberger. Accessed: Jun. 03, 2024. [Online]. Available: https://www.bloomberg.com/profile/company/SLB:US

[2] “SLB.” Accessed: Jun. 12, 2024. [Online]. Available: https://www.slb.com/

[3] R. L. Wichmann, “THE DIRECTION OF INDUSTRY: A LITERATURE REVIEW ON INDUSTRY 4.0,” INTERNATIONAL CONFERENCE ON ENGINEERING DESIGN, Aug. 2019.

[4] D. A. Espejo-Peña, “Computational Numerical Control (CNC) Machines: A Systematic Review From 2015 To 2022,” 21st LACCEI International Multi-Conference for Engineering, Education, and Technology & 4th CLADI-CONFEDI:, no. 2414–6390, Jul. 2023.

[5] B. Hess, “What Is CNC Machining? An Overview of the CNC Machining Process,” Astro machine works. [Online]. Available: https://astromachineworks.com/what-is-cnc-machining/#:~:text=Computer%20Numerical%20Control%20(CNC)%20machining,to%20mills%20and%20CNC%20routers

[6] “Industrial Connectivity for Machine Builders.” Accessed: Jun. 19, 2024. [Online]. Available: https://www.ptc.com/en/technologies/iiot/industrial-connectivity/machine-builders

[7] A. Peherstorfer, “Machine Connectivity – Requirements & Added Value.” [Online]. Available: https://www.industrieinformatik.com/en/newsbeitrag/maschinenanbindung-voraussetzungen-2/

[8] Jaiswal Shivam Rajendrakumar and –Dr Manav Thakur, “Wireless Communication for Machine-to-Machine (M2M) Connectivity in the Internet of Things (IoT),” *NeuroQuantology*, vol. 20, no. 17, pp. 2273-, 2022, doi: 10.48047/Nq.2022.20.17.Nq880292.

[9] M. Dąbrowska, “M2M services layer standardisation 2024 update,” IoTNow.

[10] M. R. Islam and M. E. Hossain, *Drilling Engineering: Towards Achieving Total Sustainability*, 1st ed. San Diego: Elsevier Science & Technology, 2020. doi: 10.1016/C2019-0-00943-0.

[11] “Windows security updates and antivirus software,” Microsoft. Accessed: Jul. 15, 2024. [Online]. Available: https://support.microsoft.com/en-us/topic/important-windows-security-updates-and-antivirus-software-4fbe7b34-b27d-f2c4-ee90-492ef383fb9c

[12] “Windows Search Remote Code Execution Vulnerability,” Microsoft. Accessed: Jul. 15, 2024. [Online]. Available: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36884#:~:text=This%20metric%20reflects%20the%20context,to%20exploit%20the%20vulnerable%20component

[13] “Microsoft Windows Server Lifecycle,” Servers Plus. Accessed: Jul. 16, 2024. [Online]. Available: https://www.serversplus.com/windows-server-lifecycle-dates

[14] “Oracle Critical Patch Update Advisory - July 2024,” Oracle. [Online]. Available: https://www.oracle.com/security-alerts/cpujul2024.html

[15] “CIMCO,” CIMCO. Accessed: Jun. 12, 2024. [Online]. Available: https://www.cimco.com/

[16] “CIMCO Software,” CIMCO.

[17] “CIMCO NC-Base.” Accessed: Jun. 13, 2024. [Online]. Available: https://www.cimco.com/

[18] “CIMCO DNC-Max v7 User Guide,” CIMCO. [Online]. Available: https://www.cimco.com/documentation/documents/cimco_dnc-max/user_guides/en/cimco-dnc-max-7-user-guide-en.pdf

[19] “CIMCO MDM,” CIMCO. [Online]. Available: https://www.cimco.com/software/cimco-mdm/

[20] “CIMCO DNC-Max,” CIMCO.

[21] “CIMCO DNC-Max v7 User Guide,” CIMCO. [Online]. Available: https://www.cimco.com/documentation/documents/cimco_dnc-max/user_guides/en/cimco-dnc-max-7-user-guide-en.pdf

[22] “CIMCO MDC-Max Collects and Analyzes Shop Floor Productivity,” CIMCO.

[23] “CIMCO MDC-Max,” CIMCO. [Online]. Available: https://www.cimco.com/software/cimco-mdc-max/

[24] “FANUC MT-LINKi Machine Tool Monitoring Software,” FANUC. [Online]. Available: https://www.fanucamerica.com/products/cnc/cnc-software/machine-tool-data-collection-software/cnc-machine-monitoring-software-mtlink-i

[25] “FANUC MT-Linki,” FANUC. [Online]. Available: https://www.fanuc.co.jp/en/product/catalog/pdf/cnc/MT-LINKi(E)-01a.pdf

[26] “PA-400 Series,” PaloAlto. [Online]. Available: https://www.paloaltonetworks.com/resources/datasheets/pa-400-series

[27] “How to Isolate your CNC Network by Dual Homing DNC Max,” Managed Solutions. [Online]. Available: https://managedsolutions.com/2014/04/isolate-your-cnc-network-dual-homing-dnc-max/

[28] “CIMCO DNC-Max v7 User Guide2,” CIMCO. [Online]. Available: https://www.cimco.com/documentation/documents/cimco_dnc-max/user_guides/en/cimco-dnc-max-7-user-guide-en.pdf

[29] “What is Traceroute: What Does It Do & How Does It Work?,” Fortinet. [Online]. Available: https://www.fortinet.com/resources/cyberglossary/traceroutes#:~:text=Running%20traceroute%20is%20helpful%20for,to%20locate%20points%20of%20failure

[30] “The Essential Guide to the IEC 62443 industrial cybersecurity standards,” Industrial Cyber. [Online]. Available: https://industrialcyber.co/features/the-essential-guide-to-the-iec-62443-industrial-cybersecurity-standards/

[31] “Purdue Model for ICS Security,” Check point. [Online]. Available: https://www.checkpoint.com/cyber-hub/network-security/what-is-industrial-control-systems-ics-security/purdue-model-for-ics-security/

[32] D. Garton, “PURDUE MODEL FRAMEWORK FOR INDUSTRIAL CONTROL SYSTEMS & CYBERSECURITY SEGMENTATION,” Technology Advancement and Deployment Task Group, Dec. 2019.

[33] “What is an IDMZ?,” Automation Blog. [Online]. Available: https://pages.rexelusa.com/blog/automation/idmz

[34] “An intro to the IDMZ, the demilitarized zone for ICSes,” TechTarget. [Online]. Available: https://www.techtarget.com/searchsecurity/feature/An-intro-to-the-IDMZ-the-demilitarized-zone-for-ICSes

[35] T. J. Williams, “Interface design for the Purdue enterprise reference architecture (PERA) and methodology in e-Work,” Production Planning and Control, doi: 10.1080/09537280310001647841.

This page is intentionally left blank.

This page is intentionally left blank.

This page is intentionally left blank.