DRAFT NISTIR 8183A
Volume 3

Cybersecurity Framework Manufacturing Profile Low Security Level Example Implementations Guide:

Volume 3 – Discrete-based Manufacturing System Use Case

Keith Stouffer
Timothy Zimmerman
CheeYee Tang
Jeffrey Cichonski
Neeraj Shah
Wesley Downard

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8183A-3-draft

National Institute of Standards and Technology
U.S. Department of Commerce

DRAFT NISTIR 8183A
Volume 3

Cybersecurity Framework Manufacturing Profile Low Security Level Example Implementations Guide:

Volume 3 – Discrete-based Manufacturing System Use Case

Keith Stouffer
Timothy Zimmerman
CheeYee Tang
Intelligent Systems Division
Engineering Laboratory

Neeraj Shah
Strativia, LLC
Largo, Maryland

Jeffrey Cichonski
Applied Cybersecurity Division
Information Technology Laboratory

Wesley Downard
G2, Inc.
Annapolis Junction, Maryland

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8183A-3-draft

May 2019

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

National Institute of Standards and Technology Internal Report 8183A, Volume 3
333 pages (May 2019)

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8183A-3-draft

Public comment period: *May 28, 2019* through *July 8, 2019*

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000
Email: CSF_Manufacturing_Profile_Implementation@nist.gov

Abstract

This guide provides example proof-of-concept solutions demonstrating how open-source and commercial off-the-shelf (COTS) products that are currently available today can be implemented in discrete-based manufacturing environments to satisfy the requirements in the Cybersecurity Framework (CSF) Manufacturing Profile [4] Low Security Level. The example proof-of-concept solutions include measured network, device, and operational performance impacts observed during the implementation. Depending on factors like size, sophistication, risk tolerance, and threat landscape, manufacturers should make their own determinations about the breadth of the proof-of-concept solutions they may voluntarily implement. The CSF Manufacturing Profile can be used as a roadmap for managing cybersecurity risk for manufacturers and is aligned with manufacturing sector goals and industry best practices. The Manufacturing Profile provides a voluntary, risk-based approach for managing cybersecurity activities and cyber risk to manufacturing systems. The Manufacturing Profile is meant to compliment but not replace current cybersecurity standards and industry guidelines that the manufacturer is embracing.

Keywords

Computer security; Cybersecurity Framework (CSF); distributed control systems (DCS); industrial control systems (ICS); information security; manufacturing; network security; programmable logic controllers (PLC); risk management; security controls; supervisory control and data acquisition (SCADA) systems.

Supplemental Content

Additional volumes of this publication include:

Draft NISTIR 8183A Volume 1, *Cybersecurity Framework Manufacturing Profile Low Security Level Example Implementations Guide: Volume 1 – General Implementation Guidance.* https://doi.org/10.6028/NIST.IR.8183A-1-draft

Draft NISTIR 8183A Volume 2, *Cybersecurity Framework Manufacturing Profile Low Security Level Example Implementations Guide: Volume 2 – Process-based Manufacturing System Use Case.* https://doi.org/10.6028/NIST.IR.8183A-2-draft

Acknowledgments

The authors gratefully acknowledge and appreciate the significant contributions from individuals and organizations in the public and private sectors, whose thoughtful and constructive comments improved the overall quality, thoroughness, and usefulness of this publication. A special acknowledgement to the members of the ISA99, Industrial Automation and Control Systems Security Committee and the Department of Homeland Security Industrial Control System Joint Working Group (ICSJWG) for their exceptional contributions to this publication.

Note to Reviewers

This guide does not describe the solution, but a possible solution. This is a draft guide. We seek feedback on its contents and welcome your input. Comments, suggestions, and success stories will improve subsequent versions of this guide. Please contribute your thoughts to CSF_Manufacturing_Profile_Implementation@nist.gov.

Call for Patent Claims

This public review includes a call for information on essential patent claims (claims whose use would be required for compliance with the guidance or requirements in this Information Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication or by reference to another publication. This call also includes disclosure, where known, of the existence of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or

b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:

> i) under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or
>
> ii) without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its behalf) will include in any documents transferring ownership of patents subject to the assurance, provisions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.

Such statements should be addressed to: CSF_Manufacturing_Profile_Implementation@nist.gov

Table of Contents

Executive Summary

This guide provides example proof-of-concept solutions demonstrating how open-source and commercial off-the-shelf (COTS) products that are currently available today can be implemented in discrete-based manufacturing environments to satisfy the requirements in the Cybersecurity Framework (CSF) Manufacturing Profile [4] Low Security Level. The example proof-of-concept solutions include measured network, device, and operational performance impacts observed during the implementation. Depending on factors like size, sophistication, risk tolerance, and threat landscape, manufacturers should make their own determinations about the breadth of the proof-of-concept solutions they may voluntarily implement.

The CSF Manufacturing Profile can be used as a roadmap for managing cybersecurity risk for manufacturers and is aligned with manufacturing sector goals and industry best practices. The Manufacturing Profile provides a voluntary, risk-based approach for managing cybersecurity activities and cyber risk to manufacturing systems. The Manufacturing Profile is meant to compliment but not replace current cybersecurity standards and industry guidelines that the manufacturer is embracing.

The CSF Manufacturing Profile focuses on desired cybersecurity outcomes and can be used as a roadmap to identify opportunities for improving the current cybersecurity posture of the manufacturing system. The Manufacturing Profile provides a prioritization of security activities to meet specific business/mission goals. Relevant and actionable security practices that can be implemented to support key business/mission goals are then identified.

While the proof-of-concept solutions in this guide used a suite of commercial products, this guide does not endorse these particular products, nor does it guarantee compliance with any regulatory initiatives. Your organization's information security experts should identify the products that will best integrate with your existing tools and manufacturing system infrastructure. Your organization may voluntarily adopt these solutions or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a solution. This guide does not describe regulations or mandatory practices, nor does it carry any statutory authority.

1. Introduction

The Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," [1] directed the development of the voluntary Cybersecurity Framework that provides a prioritized, flexible, repeatable, performance-based, and cost-effective approach to manage cybersecurity risk [1] for those processes, information, and systems directly involved in the delivery of critical infrastructure services.

The Cybersecurity Framework is a voluntary risk-based assemblage of industry standards and best practices designed to help organizations manage cybersecurity risks [2]. The Framework, created through collaboration between government and the private sector, uses a common language to address and manage cybersecurity risk in a cost-effective way based on business needs without imposing additional regulatory requirements.

To address the needs of manufactures, a Manufacturing Profile [4] of the Cybersecurity Framework was developed, through collaboration between government and the private sector, to be an actionable approach for implementing cybersecurity controls into a manufacturing system and its environment. The Profile defines specific cybersecurity activities and outcomes for the protection of the manufacturing system, its components, facility, and environment. Through use of the Profile, the manufacturer can align cybersecurity activities with business requirements, risk tolerances, and resources. The Profile provides a manufacturing sector-specific approach to cybersecurity from standards, guidelines, and industry best practices.

1.1 Purpose and Scope

Many small and medium sized manufacturers have expressed that they are challenged in implementing a standards-based cybersecurity program. This guide provides example proof-of-concept solutions demonstrating how open-source and commercial off-the-shelf (COTS) products that are available today can be implemented in manufacturing environments to satisfy the requirements in the Cybersecurity Framework (CSF) Manufacturing Profile Low Security Level. Example proof-of-concept solutions with measured network, device, and operational performance impacts for a process-based manufacturing environment (Volume 2) and a discrete-based manufacturing environment (Volume 3) are included in the guide. Depending on factors like size, sophistication, risk tolerance, and threat landscape, manufacturers should make their own determinations about the breadth of the proof-of-concept solutions they may voluntarily implement. The CSF Manufacturing Profile can be used as a roadmap for managing cybersecurity risk for manufacturers and is aligned with manufacturing sector goals and industry best practices. The Manufacturing Profile provides a voluntary, risk-based approach for managing cybersecurity activities and cyber risk to manufacturing systems. The Manufacturing Profile is meant to enhance but not replace current cybersecurity standards and industry guidelines that the manufacturer is embracing.

While the proof-of-concept solutions in this guide used a suite of commercial products, this guide does not endorse these particular products, nor does it guarantee compliance with any regulatory initiatives. Each organization's information security experts should identify the products that will best integrate with their existing tools and manufacturing system

infrastructure. Organizations may voluntarily adopt these solutions or one that adheres to these guidelines in whole, or can use this guide as a starting point for tailoring and implementing parts of a solution. This guide does not describe regulations or mandatory practices, nor does it carry any statutory authority.

This project is guided by the following assumptions: The solutions were developed in a lab environment. The environment is based on a typical small manufacturer. The environment does not reflect the complexity of a production environment. An organization can access the skills and resources required to implement a manufacturing cybersecurity solution.

1.2 Audience

This document covers details specific to manufacturing systems. Readers of this document should be acquainted with operational technology, general computer security concepts, and communication protocols such as those used in networking. The intended audience is varied and includes the following:

- Control engineers, integrators, and architects who design or implement secure manufacturing systems.
- System administrators, engineers, and other information technology (IT) professionals who administer, patch, or secure manufacturing systems.
- Managers who are responsible for manufacturing systems.
- Senior management who are trying to understand implications and consequences as they justify and implement a manufacturing systems cybersecurity program to help mitigate impacts to business functionality.
- Researchers, academic institutions and analysts who are trying to understand the unique security needs of manufacturing systems.

1.3 Document Structure

Volume 3 is divided into the following major sections:

- Section 2 provides an overview of the discrete-based manufacturing system use case.
- Section 3 provides the detailed policy and procedure documents developed for the discrete-based manufacturing system use case.
- Section 4 provides the detailed technical capability implementations and associated performance measurements for the discrete-based manufacturing system use case.
- Appendix A provides a list of acronyms and abbreviations used in this document.
- Appendix B provides a glossary of terms used in this document.
- Appendix C provides a list of references used in the development of this document.

2. Discrete-based Manufacturing System Low Security Level Use Case

2.1 Introduction

This use case is a proof-of-concept solution demonstrating how open-source and commercial off-the-shelf (COTS) products that are currently available today can be implemented in a manufacturing environment to satisfy the requirements in the CSF Manufacturing Profile Low Security Level. Depending on factors like size, sophistication, risk tolerance, and threat landscape, manufacturers should make their own determinations about the breadth of proof-of-concept solution they may voluntarily implement.

2.2 Discrete-based Low Security Level Use Case

The fictional company, Alpha Manufacturing (i.e., Alpha), is a small manufacturer that produces common metal components for the automotive industry. These parts are typically subcontracted to Alpha by larger manufacturers. The finished parts are then integrated into larger subassemblies that perform non-safety related functions within a vehicle.

To meet increasing production demand, an automated workcell was contracted and purchased from a manufacturing systems integrator. The first workcell was purchased to evaluate and validate its operation, with the intent of purchasing more workcells to further increase production. Two of the machining stations integrated into the workcell were existing at the Alpha facility, while the other two stations were purchased by the integrator. The workcell operates independently of all other shop operations, and is tended to by a single operator, who: loads raw material, unloads finished parts, responds to alarm conditions, and validates the quality of finished parts.

2.2.1 Facilities

Alpha operates a single small leased building less than 15,000 ft^2 (1394 m^2) in size.

2.2.2 Employees

Alpha has ten full-time employees, of which, six are machine operators. Alpha has no full-time control system engineers or IT personnel. Employees have no formal cybersecurity training.

Organizational Role	Count
President	1
HR Manager	1
Bookkeeper	1

Foreman/Supervisor	1
Machine Operators	6
Total	**10**

330

331 ### 2.2.3 External Personnel

332 Some facility operations are outsourced to external entities.

Role
Information Technology (IT) Services
Operational Technology (OT) Services
Machine Tool Support, Service, and Repair
Janitorial Services

333

334 ### 2.2.4 Supply Chain

335 Raw material suppliers are utilized on-demand. No formal relationships or direct-order
336 networking/online/cloud connections with any suppliers currently exist. Alpha is considered a
337 "tier two" supplier. Alpha sends completed parts to a tier one manufacturer. At the tier one
338 manufacturer's facility, Alpha's parts are integrated into subassemblies that are subsequently
339 installed into a vehicle by the original equipment manufacturer (OEM).

340 ### 2.2.5 Supporting Services

341 The only supporting service required by Alpha is electricity to power IT systems, manufacturing
342 machines, and lights.

343 ### 2.2.6 Legal and Regulatory Requirements

344 Alpha does not have knowledge of any legal or regulatory requirements in regards to its
345 cybersecurity. However, as a tier two supplier, it is contractually obligated to follow all
346 standards, procedures, and guidance provided by the tier one manufacturer(s) and the OEM (e.g.,

ISO/TS 16949, ISO 9000). Alpha does not produce any components that fall within the regulatory jurisdiction of 49 CFR Part 571: Federal Motor Vehicle Safety Standards. [5].

2.2.7 Critical Infrastructure

The DHS Critical Manufacturing sector considers vehicle manufacturing (and its supply chain) a core industry to be protected. However, Alpha is a tier two manufacturer that produces parts that are not critical to vehicle safety and can easily be produced by other tier two job shops if Alpha cannot meet its production demand. It is likely that the tier one manufacturer has already implemented supply chain redundancy to enable continuity of production.

Alpha will not be able to produce if the primary metals critical manufacturing sector cannot provide Alpha with the required raw materials. However, this sector is outside of the scope of Alpha's implementation of the Manufacturing Profile.

2.2.8 Manufacturing Process

Parts are created in a sequential manufacturing process with four CNC machines within a workcell. The CNC machines are tended to by two industrial robotic arms, which transfer parts to each station until all of the machining processes are completed. Raw materials are loaded into a queue by an operator. A supervisory PLC monitors the dynamic status of each machining station and contains logic to disseminate jobs to the robots. Each robot executes its jobs using preprogrammed scripts and waypoints. Finished parts are placed onto a conveyor by a robot, subsequently dropping into either a finished parts bin, or a rejected parts bin. The bins are emptied by operators once they are full.

The manufacturing process is as follows:

2.2.9 Systems

Most of the business functions are supported by general enterprise IT, and share information with the OT (e.g., CNC machines). Typical IT software usage includes email and web browsing. Any IT work is contracted out to local companies.

2.2.10 Critical Systems

The following systems are critical for proper operation of the workcell:

- Engineering workstation
- Supervisory PLC
- HMI
- Machining stations
- Robot arms

- Robot controllers
- Robot driver
- Networking equipment

2.2.11 Data

Data transferred over, or stored within, Alpha's network includes:

- PLC code
- Robot code
- MODBUS TCP registers
- Computer-aided Manufacturing (CAM) files (e.g., G code)
- Workcell operating manuals and documentation
- Electrical diagrams
- Network diagrams
- Computer-aided drafting (CAD) files
- Part inspection measurements
- Historical production data

NOTE: All data listed above are proprietary, trade secrets, and/or confidential.

2.2.12 Network

The manufacturing system network is connected to the corporate network through a dedicated top-level router/firewall, and is organized into subnetworks and a DMZ. The network is managed by the external IT contractor. The workcell has a dedicated router/firewall utilizing network address translation (NAT) to help segment and isolate the workcell from the rest of the network. The workcell itself is split into two subnets: the Supervisory LAN, and the Control LAN.

Most of the network traffic utilizes Ethernet and TCP/IP protocols, while the dedicated field-bus level communications for the robots utilize the EtherCAT protocol.

2.2.13 Mission Objectives

The Manufacturing Profile describes five business/mission objectives common to the manufacturing sector. The following sections describe what Alpha must protect, in regards to their manufacturing process and assets, in order to meet each of the missions:

1. **Maintain Personnel Safety**
   - Safety PLC - The workcell has a safety-rated PLC to terminate operations when an emergency condition is detected. Industry standard emergency stop buttons and light curtains are used to protect operators from entering the work area while the workcell is active.

2. **Maintain Environmental Safety**
   - None - The workcell, and its underlying manufacturing process, do not use any raw ingredients or produce any by-products that can compromise the environmental safety mission.

3. **Maintain Quality of Product**
   - Machining Stations 1, 2, 3 - All manufacturing functions are performed by sequential CNC machining stations (1, 2, and 3). Each station uses preprogrammed operations (e.g., G code) to complete its required manufacturing process tasks. This code, and all station functions, have direct control over the output product quality.
   - Inspection Station 4 - If product quality has been impacted outside of product quality specifications, the inspection station will reject the part. Modification of the specifications within the inspection station can allow out-of-spec parts to pass inspection.
   - Robots - Tending of parts between the machines is handled by the two workcell robots. This process requires accurate and repeatable placement of parts within the machining station fixtures, which is performed through robot calibration and preprogrammed waypoint coordinates. Parts that are not properly placed within fixtures, or collide with the fixtures, may not meet product quality specifications.
   - Supervisory PLC - The supervisory PLC tracks each part as it goes through the manufacturing process and commands the robots to transport each part between machines in a sequential manner. If a robot executes a job out-of-order, a part may bypass one of the machining stations, impacting product quality.
   - HMI - Through the HMI, operators can manipulate workcell operation parameters, machining station programs, and inspection station acceptance parameters. Modification of any of these parameters outside of expected bounds can impact product quality.
   - Engineering Workstations - Privileged control and administrative functions of workcell components is granted to engineers via the Engineering Workstation.

4. **Maintain Production Goals**
   - Machining Stations - The amount of time each machining station takes to perform its manufacturing functions, and the frequency of alarm conditions, can impact production goals.
   - Robots - The amount of time the robots require to transport the parts between machining stations can impact the production goals.
   - Supervisory PLC - The amount of time it takes the PLC to disseminate jobs to the robots, or communicate with the machining stations, can impact production goals.
   - HMI - Operators have direct control over the amount of parts produced in a batch via the HMI.
   - Engineering Workstations - Numerous privileged functions available through the engineering workstation can impact production goals.
   - Operator Workstations - Operators obtain production planning goals (e.g., product type and quantity), machining station data files (e.g., G code) from network shares and email systems. Inability to access these systems can impact production goals.

- Networking equipment - All coordination between workcell components occurs through the installed network equipment. If this equipment degrades or ceases to function, production goals will be impacted.

5. **Protect Trade Secrets**
   - Machining Stations - The operations performed by each machining station are a protected trade secret of the company.
   - Network - The machining station data files (e.g., G code) are typically stored on network shares, and must be protected.

3. Policy and Procedure Implementations

This section includes example policy and procedure documents and statements that were developed for the fictional company Alpha. An overview of these documents is discussed in Section 5 of Volume 1. Each organization's information security experts should identify the policy and procedure documents and statements that will best integrate with their existing cybersecurity program and manufacturing system infrastructure.

3.1 Security Program Document Example

Security Program

for

Alpha

Document Owner:	Supervisor, Alpha

Version

Version	Date	Description	Author
1.0	02-22-2018	Initial Draft	Supervisor
2.0	04-21-2018	Major changes to the initial draft	Supervisor

Approval

(By signing below, all Approvers agree to all terms and conditions outlined in this document.)

Approvers	Role	Signed	Approval Date
	President		4-22-2018

3.1.1 Purpose

The Information Security Program establishes guidelines and principles for initiating, implementing, maintaining, and improving cybersecurity management for Alpha.

This program is designed to:

- Ensure the security and confidentiality of employees and business information;

- Protect against any anticipated threats or hazards to the security or integrity of such information; and
- Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to Alpha, its partners, customers, or any member.

In addition, the Supervisor (Foreman) oversees the development, implementation, and maintenance of the information security program

3.1.2 Who Should use this Document?

This document is intended to be used by the President, HR Manager, Shop Supervisor and any other members as deemed appropriate by the Supervisor. It supports an agencies responsibility for implementing an INFOSEC program.

3.1.3 Commitment from Management

Alpha's leadership team is committed to the development of this Information Security Program. It fully supports and owns the ultimate responsibility of this Security program. This commitment involves allocating necessary funding to information security work and responding without delay to new situations. The leadership team will participate in any information security related event as organized.

3.1.4 Organization Overview

Role in the Industrial sector

Alpha produces common metal components for the automotive industry. These parts are subcontracted to Alpha by larger manufacturers. The finished parts are then integrated into larger subassemblies that perform non-safety related functions within a vehicle

Raw material suppliers are utilized on-demand, and supplier selection is determined in-stock availability. No formal relationships or direct-order networking/online/cloud connections with any suppliers currently exist. Alpha is considered a "tier two" supplier. Alpha sends completed parts to a tier one manufacturer for integration into subassemblies that are subsequently installed into a vehicle by the original equipment manufacturer (OEM).

Alpha will not be able to produce if the primary metals critical manufacturing sector cannot provide Alpha with the required raw materials. However, this sector is outside of the scope of Alpha's implementation of the Manufacturing Profile.

Mission Objectives:

The Manufacturing Profile describes five business/mission objectives (in order of priority) common to the manufacturing sector. The following sections describe what Alpha must protect, in regard to the manufacturing process and assets, in order to meet each of the missions.

1. Maintain Personnel Safety

- Safety PLC - The workcell has a safety-rated PLC to terminate operations when an emergency condition is detected. Industry standard emergency stop buttons and light curtains are used to protect operators from entering the work area while the workcell is active. Each station has the ability to send emergency stop commands to the safety PLC.

2. Maintain Environmental Safety

- None - The workcell, and its underlying manufacturing process, do not consume any raw ingredients or produce any by-products that can compromise the environmental safety mission.

3. Maintain Quality of Product

- Machining Stations 1, 2, 3 - All manufacturing functions are performed by sequential CNC machining stations (1, 2, and 3). Each station uses preprogrammed operations (e.g., G code) to complete its required manufacturing process tasks. This code, and all station functions, have direct control over the output product quality.
- Inspection Station 4 - If product quality has been impacted (i.e., the product dimensions do not meet the defined specifications), the inspection station will reject the part. Misconfiguration or modification of specifications loaded into the inspection station could allow out-of-spec parts to erroneously pass inspection.
- Robots - Tending of parts between the machines is handled by the two workcell robots. This process requires accurate and repeatable placement of parts within the machining station fixtures, which is performed through proper robot calibration and the programming of waypoint coordinates. Parts that are not properly placed within fixtures, or collide with the fixtures, may not meet product quality specifications.
- Supervisory PLC - The supervisory PLC tracks each part as it goes through the manufacturing process and commands the robots to transport each part between machines in a sequential manner. If a robot executes a job out-of-order, a part may bypass one of the machining stations, impacting product quality, or damaging one of the downstream stations.
- HMI - Operators can manipulate workcell parameters, machining station programs, and inspection station acceptance parameters through the HMI. Modification of any of these parameters outside of expected bounds can impact product quality.
- Engineering Workstations - Privileged control and administrative functions are granted to authorized personnel via the Engineering Workstation.

4. Maintain Production Goals

- Machining Stations - The amount of time each machining station takes to perform its manufacturing functions, the frequency of alarm conditions, tooling wear/failure, and machine component failure can impact production goals.

- Robots - The amount of time the robots require to transport the parts between machining stations, robot faults, and robot wear/failure can impact the production goals.
- Supervisory PLC - The amount of time it takes the PLC to disseminate jobs to the robots or communicate with the machining stations, and PLC faults can impact production goals.
- HMI - Misconfiguration of the production settings on the HMI can impact production goals.
- Engineering Workstations - Numerous privileged functions available through the engineering workstation can impact production goals.
- Networking equipment - All coordination between workcell components occurs through its network equipment. If this equipment experiences degraded performance or ceases to function, production goals can be impacted.

5. Protect Trade Secrets

- Machining Stations - The individual operations performed by each machining station, and all supporting information the describes these operations, are protected trade secrets of the company.
- Network - The machining station data files (e.g., G code) are typically stored on network shares, and must be protected

Role in the Supply chain:

Raw material suppliers are utilized on-demand, and supplier selection is determined in-stock availability. No formal relationships or direct-order networking/online/cloud connections with any suppliers currently exist. Alpha is considered a "tier two" supplier. Alpha sends completed parts to a tier one manufacturer for integration into subassemblies that are subsequently installed into a vehicle by the original equipment manufacturer (OEM).

Communication to Organization

All critical and operational aspects of the Manufacturing system, key resources should be documented in network diagrams, manuals or other artifacts. The documentation will be reviewed on a yearly basis by the Supervisor with assistance from the machine operators. This information will be shared with all employees, contractors depending on their role in the Company.

Critical Manufacturing System Components:

The following are a list of critical Manufacturing system components:

- Engineering workstation
- Supervisory PLC
- HMI
- Machining stations
- Robot arms

- Robot controllers
- Robot driver
- Networking equipment

Supporting Services:
The only supporting service required by Alpha is electricity to power IT systems, manufacturing machines, and lights.

3.1.5 Information Security Policy

The purpose of the Information Security Policy, which can be found in Section 3.2, is to provide an overview of the policies, standards, procedures and Technical controls that make up Alpha's Information Security Program. This policy is developed and executed by the Supervisor, and expectations are set for protecting Alpha's IT and OT assets.

3.1.6 Applicable Laws and Regulations

Alpha does not have knowledge of any legal or regulatory requirements in regards to its cybersecurity. However, as a tier two supplier, it is contractually obligated to follow all standards, procedures, and guidance provided by the tier one manufacturer(s) and the OEM (e.g., ISO/TS 16949, ISO 9000). Alpha does not produce any components that fall within the regulatory jurisdiction of 49 CFR Part 571: Federal Motor Vehicle Safety Standards.

3.1.7 Security Organization and Governance

Information security is an inherent part of governance and consists of the leadership, organizational structures and processes that safeguard Alpha's information, its operations, its market position, and its reputation.

The President is responsible for:

- Reviewing and approving the written information security program and supporting policies, at least annually.
- Assigning the shop Supervisor responsibility for organization's policies and procedures for use of Alpha's IT/OT assets, implementation, documentation and for meeting its compliance obligations.
- Overseeing efforts to develop, implement, and maintain an effective information security program including regular review of reports from the Supervisor.

The Supervisor is responsible for:

- Serving as a Security Officer and as a Single point of contact for any physical or cybersecurity related incident.
- Implementing and maintaining Security Policy documents.
- Overall security of all IT/OT assets, operations and remediating risks and vulnerabilities.
- Acting as a liaison between plant operators, vendors and management on matters relating to information security.
- Reporting to the President about the status of the program, any security related risks or incidents via reports.

All employees, contractors and vendors are responsible for ensuring the security, confidentiality, and integrity of information by complying with all corporate policies and procedures.

3.1.8 Privacy of Personal Information

Employees should not assume any degree of privacy to information they create or store on Alpha's systems. Alpha is a private organization and any information stored on its information systems may be subject to disclosure under state law. Alpha will disclose information about individuals only to comply with applicable laws, regulations or valid legal requests.

3.1.9 Operational Security

Risk Management:

The Organization's Risk Management Strategy can be found here in Section 3.4 Risk Management Document. The Supervisor shall conduct yearly risk assessments to identify potential internal and external risks to the security, confidentiality and integrity of Alpha.

Risk assessment involves evaluating risks and their likelihood along with selecting and implementing controls to reduce risks to an acceptable level. Each risk assessment documents major findings and risk mitigation recommendations.

All employees are encouraged to report any potential or existing risks to the Supervisor. Once the Supervisor has identified or acknowledged the risks, the next course of action will be determined (e.g., accept the risk, seek assistance from the IT Team, contact a vendor to remediate the risk). Similarly, a vendor or contractor can also notify the Supervisor if they identify any threats or risks to their equipment. A detailed description of risk notification process can be found in Section 3.4 Risk Management Document.

Physical Security:

The perimeter of the facility is fenced, and the main entrance has gate that is open during business hours and locked after hours. There are two entrances to the main building. One is for Employees only which is normally locked, employees need to swipe their personal badges to enter the building. The other entrance located at the front lobby is open during normal business hours. Guests and visitors are required to sign in with proper identification. Additional details about Physical security requirements are mentioned in the Physical Security Section of the Security Policy document.

Additionally, Personnel security is addressed through pre-employment screenings, adequate position descriptions, terms of employment, and security education and training.

Access Control:

User access to IT and OT systems is based on the principle of least privilege depending on the user's role in the organization. Proper authorization and approval by the Supervisor is required prior to granting access or operating any manufacturing system equipment. Sets of controls are in place to restrict access through authentication methods and other technical means. Passwords are managed through a formal process and secure log-on procedures. Sensitive systems are explicitly identified and audited regularly.

Appropriate authentication controls are used for external connections and remote users. Physical and logical access to critical infrastructure is controlled. Duties are separated to protect systems and data. Access rights are audited at regular intervals

3.1.10 Security Awareness Training

Security awareness information is provided to new employees at the time of hire. Online resources are provided to educate employees on best practices and the importance of reporting security incidents. Additionally, the Supervisor will ensure the employee understands their role and responsibilities in Alpha's information security program.

Any information about potential or existing cyber threats to Alpha's systems may be exchanged routinely between the Supervisor and external vendors. Likewise, any news about email scams, phishing attempts and other malicious actions are posted to inform users of possible threats.

Training for Users and Managers

Employees must perform online computer-based training or classroom-based training per management approval. Below is a list of training options. Trade organization subscriptions to newsletters and magazines will offer more industry specific training classes.

Computer Based Training

- ICS-CERT VLP (Virtual Learning Portal)
  https://ics-cert-training.inl.gov
- DHS Recommended Training
  https://www.dhs.gov/chemical-sector-training
- SCADAhacker
  https://scadahacker.com/training.html
- In Person Training
  Sans Industrial Control Systems Training
  https://ics.sans.org/training/courses

Training for Privileged Users

Privileged Users in the Organizational Use case:

- Foreman/Supervisor
  This user has complete control of the manufacturing process within Alpha.

Responsibilities:

- Any privileged user within manufacturing environment will have two accounts. A primary account used for normal activities, and a privileged "administrator" account for performing privileged functions.
  - Primary accounts are used for normal daily operations.
  - Primary accounts will have same rights as a standard Alpha user account (e.g., email access, Internet access).
  - Privileged accounts will have administrative privileges, and must only be used when performing administrative functions within manufacturing system (e.g., system updates of firmware or software, system reconfigurations, device restarts).
- Privileged users will adhere to securely using Administrative account when performing duties within manufacturing system. If a privilege account becomes compromised this could have a damaging impact on the manufacturing process.

Training**:**

- Training for privileged users will include the training for regular users. Advance training will be provided from industry trade group specializing in automation process, or other specialty training organization focusing on manufacturing security for ICS environments.

  Examples:
  - International Society of Automation (ISA) https://www.isa.org
  - SANS (Information Security Training) https://www.sans.org

Training for Third Party contractors

- There are many different training options available. Training can be completed in person at a training facility, or online in a virtual classroom environment. In person training at a facility will have a cost associated and it not always appropriate depending on the level of training required. Online training can also have a cost depending on the level required, but there are also options that a free and provide a good understanding of the difference between a traditional Information Technology (IT) environment and Operations Technology (OT) environment.
- Payed Training Options.
  - https://www.sans.org/course/ics-scada-cyber-security-essentials (Offers hands on training with experienced instructors).
- Free Online Training Options.
  - https://ics-cert-training.inl.gov/learn (Offers virtual classroom environment at no cost).

3.1.11 Third Party Responsibilities and Requirements

- Third party contactors and vendors are required to be aware of the sensitive information within Alpha facility and the steps to ensure propriety information is kept secret.
- Third party contactors and vendors will be re-evaluated yearly from the date of completion of first security compliance check. During this re-certification all objectives listed in the Security Awareness Training section above will be reviewed again to ensure security compliance with original plan.
- All Remote connections from third party providers will be conducted using a Desktop sharing Program Connection. These remote connections will be monitored and audited.
- All software and hardware tools used within Alpha's network will be approved first before service provider can proceed.
- No data shall leave Alpha's network without written approval from President.
- Network accounts will be limited to only enabled when needed. Accounts used by service for remote access will require approval before being allowed to connect during normal business

hours. Refer to Remote Maintenance Approval process in the Security Policy document for additional details.

3.1.12 Fire and Safety Regulations

- Fire Protection Systems will compile with Local, State, and Federal laws. This is to include Fire Protection Systems specially designed for manufacturing process. Fire Protection System will place emphasis on human safety first and for most, before concern for manufacturing system. Fire Protection Systems will be checked minimum once per year unless shorter intervals are required from superseding regulations.
- Only Industry approved Environmental Controls will be used within manufacturing systems, to included compliance with all Local, State, Federal laws. Environmental Control will be implemented to place human/community safety first before manufacturing systems.
- Fire protection for a manufacturing environment should be designed to safeguard electrical equipment. Fire Protection should be designed and implemented to protect human life first and equipment second. Installed fire protection systems will be certified compliant with existing/new environment by a licensed and accredited vendor. Check industry standards for any required baselines.

3.1.13 Emergency Power

A short-term uninterruptible power supply (UPS) to facilitate both an orderly shutdown and transition of the organization to a long-term alternate power in the event of a major power loss.

3.1.14 Incident Management

Alpha's Incident Response and Recovery Plan describes the detection, analysis, containment, eradication, recovery and review of security incidents. The process for responding to security incident is designated in Incident Response Plan, while the procedures for incident recovery and resilience requirements are defined in the Incident Recovery Plan. Security incidents are managed by the Supervisor who ensures that security incidents are promptly reported, investigated, documented and resolved in a manner that restores operation quickly and, if required, maintains evidence for further disciplinary, legal, or law enforcement actions. The Incident Response Plan and Recovery Plans are reviewed annually and updated as needed.

Lessons learned from cybersecurity events will be used to revise and improve device detection ability while increasing protection for the organization and manufacturing system.

3.1.15 Information Sharing Plan

Information sharing with outside entities like trade organizations and local, state, and federal agencies can help strengthen cybersecurity. Information sharing, especially when receiving information from other outside entities, will improve Alpha's situational awareness, and result in a more secure manufacturing system.

Trade Organizations:

Relationships will be established with trade organizations. These relationships will be used to share information regarding cybersecurity incidents detected within the manufacturing facility. Information shared with trade organizations regarding cybersecurity incidents must have all proprietary information and trade secrets removed. This information will be listed as unclassified. Information regarding a cybersecurity incident containing information relating to proprietary, customer, or trade secret process will require a Non-Disclosure Agreement before data is transmitted; this would be considered classified information requiring approval from executive management before being sent.

Local Government:

Relationships with any local government organization whose purpose is to share cybersecurity incident data should be established.

State Government:

Relationships with any state government organization whose purpose is to share cybersecurity incident data should be established. Trade organizations should be able to provide contact information for state government incident sharing organizations, if they exist.

Federal Government:

Relationships with federal government agencies whose purpose is to share cybersecurity incident data should be established. Some federal government agencies are listed below.

DHS (CISA) Agency for reporting incidents of Phishing, Malware, Vulnerabilities.
https://www.us-cert.gov/report
DHS (NCCIC) Agency for reporting cybersecurity incidents relating to Industrial Control Systems.
https://ics-cert.us-cert.gov/Report-Incident

3.1.16 Periodic Reevaluation of the Program

The Security Program document will be continuously updated to reflect changes made to manufacturing system and to improve cybersecurity. Lessons learned will be incorporated to help improve this document in the event a cybersecurity incident occurs.

The Supervisor shall reevaluate and update the Program from time to time as deemed appropriate. The Supervisor shall base such reevaluation and modification on the following:

- The results of the risk assessment and monitoring efforts;
- Any material changes to the Alpha's operations, business or infrastructure components.
- Any cybersecurity incident.

840 • Any other circumstances that the Supervisor knows or is informed of by the President.

841 ### 3.1.17 References

842 1. Implementing Effective Information Security Program by SANS Resources
843 https://www.sans.org/reading-room/whitepapers/hsoffice/designing-implementing-
844 effective-information-security-program-protecting-data-assets-of-1398

845 2. InfoSec Program Plan by University of Tennessee Knoxville https://oit.utk.edu/wp-
846 content/uploads/2015-11-11-utk-sec-prog-plan.pdf

847 3. GCADA Sample Information Security Procedure
848 http://www.gcada.org/pdf/Sample%20Information%20Security%20Procedure%20(safeg
849 uard%20policy).pdf

850 4. IT Security Program by Old Dominion University
851 https://www.odu.edu/content/dam/odu/offices/occs/docs/odu-it-security-program.pdf

852

853

3.2 Security Policy Document Example

Security Policy

for

Alpha

Document Owner:	Supervisor, Alpha

Version

Version	Date	Description	Author
1.0	02-22-2018	Initial Draft	Supervisor
2.0	04-21-2018	Major changes to the initial draft	Supervisor

Approval

(By signing below, all Approvers agree to all terms and conditions outlined in this document.)

Approvers	Role	Signed	Approval Date
	President		4-22-2018

3.2.1 Purpose

This Security Policy document defines the security requirements for the proper and secure use of IT and OT services in the organization. The goal of the policies defined within is to protect the organization and its users to the maximum extent possible against cybersecurity threats that could jeopardize their integrity, privacy, reputation, and business outcomes.

3.2.2 Scope

Any employee, contractor, or individual with access to the organization's systems or data.

3.2.3 Policy Maintenance

The Security Policy needs to be approved by the Supervisor in consultation with the President before it can be made official to all employees of Alpha. Any updates to this document will need to be preapproved by the Supervisor.

880 This policy document will be reviewed by the Supervisor on an annual basis. The Supervisor will
881 notify all employees for any updates made to the policy.

882 ### 3.2.4 Role-based Security Responsibilities

883 Security responsibilities vary depending on an individual's role in the company. Each is defined
884 below.

Organizational Role	Security Role	Security Responsibilities
President		• Serve as Point of Escalation for any incidents. • Responsible for data breaches. • Comply with Alpha's security policy
HR Manager		• Report any security risks to the Supervisor • Comply with Alpha's security policy
Bookkeeper		• Report any security risks to the Supervisor • Comply with Alpha's security policy
Foreman/ Supervisor	CISO/Security Officer	• Responsible for overall security of all IT/OT assets. • Responsible for remediating detected events or vulnerabilities. • Implement and maintain Security Policy documents. • Serve as a SPOC for any security related incident and keeping upper management in the loop.
Operators		• Help with the security requirements for their specific area. • Often assume responsibility for intrusion detection. • Report any security risks or events detected to the Supervisor. • Comply with Alpha's security policy • Assist in remediating vulnerabilities if asked by Foreman.

885

886

887 **External Personnel**

Role	Security Responsibilities
IT / OT Contractor	• Implement/Setup Tools and Technologies as requested by the Foreman. • Report any security risks to the Supervisor • Assist in remediating vulnerabilities if required. • Comply with Alpha's security policy
Machine Vendor	• Assist in remediating vulnerabilities, upgrading software or hardware as required. • Comply with Alpha's security policy if called in.
Visitor	• Comply with Alpha's security policy if called in.

888

889 ### 3.2.5 Employee requirements

890 1. Employees must complete security awareness training and agree to uphold the acceptable
891 use policy.
892 2. Employees must immediately notify the Supervisor if an un-escorted or unauthorized
893 individual is found in the facility.
894 3. Employees must always use a secure password on all systems as per the password policy.
895 These credentials must be unique and must not be used on other external systems or
896 services.
897 4. Terminated employees must return all company records, in any format.
898 5. Employees must verify with the Supervisor that authorizations have been granted before
899 allowing external personnel to connect to the IT or OT network.
900 6. Employees must report any physical security incidents to the Supervisor.
901 7. Employees must understand and diligently follow the physical security requirements stated
902 in the next section.

903
904 ### 3.2.6 Physical Security

905 1. Employees must always use and display physical identification (ID) provided by the
906 company.
907 2. IDs must be designed to enable the immediate visual distinction between employees,
908 external personnel, and visitors.
909 3. Sharing of IDs for any reason is strictly prohibited.
910 4. Employees must only access areas they are assigned.
911 5. A sign-in sheet will be maintained to record all Visitor visits. These log records will be
912 reviewed periodically by a designated Alpha employee.

6. Any visitors, contractors and/or maintenance personnel must always be escorted by an employee.
7. Unauthorized removal of any documentation, equipment, or media from is restricted, unless authorized. Authorization can be obtained from the Supervisor.
8. All activities of visitors, contractors, and maintenance personnel will be subject to monitoring while onsite. An employee from the IT team will be assigned to monitor all computer activities if the visitor, contractor, or maintenance personnel is connected to any company network.
9. A supervisor will conduct monthly security status monitoring of the company to check for any physical security incidents.

3.2.7 Information Technology (IT) Assets

1. IT assets must only be used for the business activities they are assigned and authorized to perform.
2. Every employee is responsible for the preservation and proper use of the IT assets they have been assigned.
3. IT assets must not be left unduly exposed.
4. Desktops and laptops must be locked if left unattended. This policy should be automatically enforced whenever possible.
5. IT assets must not be accessed by non-authorized individuals. Authorization can be obtained from Supervisor.
6. Configuration changes are to be conducted through the change control process, identifying risks and noteworthy implementation changes to security management.
7. All assets must be protected by authentication technologies (e.g., passwords).
8. Passwords must follow the password policy.
9. The Supervisor must be notified immediately after an asset is discovered to be lost or stolen.
10. Use of personal devices to access IT resources is prohibited.
11. Storage of sensitive information on portable media is prohibited, unless authorized by the Supervisor.
12. Any sensitive information stored on IT assets, or being transported on a portable device, must be protected in such a way to deny unauthorized access, and must be encrypted in line with industry best practices and any applicable laws or regulations.

3.2.8 Operational Technology (OT) Assets

1. OT assets must not be used for operations they are not assigned or authorized to perform.
2. The Supervisor and Operators are responsible for the preservation and correct use of the ICS assets they have been assigned.
3. Physical access to OT assets is forbidden for non-authorized personnel. Granting access to the assets involved in the provision of a service must be authorized by Security Officer.
4. All personnel interacting directly with OT assets must have proper training.
5. The Supervisor is responsible for all OT devices. Supervisor is solely responsible for maintenance/configuration of the device they are assigned. No other personnel are authorized to modify OT asset configurations, including any modification to interfacing hardware or software.
6. Usage of security tools on the OT network must be approved by the Security Officer, and all affected Operator must be notified.
7. Concept of least privilege must be followed when authorizing access to OT assets.
8. OT assets, such as PLCs, safety systems, etc., should have their keys in the "Run" position at all times unless being actively programmed.
9. Accessing IT devices or internet use from the OT network, or OT assets, unless authorized, is prohibited.
10. Use of personal devices to access OT resources is prohibited.

Description	
Beckhoff Automation PLC	Dell Servers (Linux)
Red Lion HMI	Machining Stations
Wago Remote I/O	Siemens RUGGEDCOM Network Switches
KUKA Industrial Robots	

OT Assets Inventory

3.2.9 Lifecycle Accountability of assets

1. Any IT or OT asset that needs to be decommissioned must be sanitized of all data, as per the manufacturer guidelines.
2. In case of an employee termination, an IT asset such as desktop PC or laptop must be reimaged prior to assigning it to a different employee.

3.2.10 System Maintenance

1. Any maintenance tasks involving external resources such as Vendors, Contractors or other non-employees must be pre- approved by the Supervisor. This can be coordinated by filling out the Maintenance Order approval form.
2. It is the responsibility of Vendors, Contractors and/or Maintenance personnel with access to resources that due care is ensured to properly secure their own resources.
3. It is Alpha's responsibility that due care is ensured when using vendor devices on networks.
4. All remote maintenance activities provided by a vendor will be controlled and monitored to ensure no harmful or malicious activities occur. Detailed logging of the activity will be performed by an Alpha employee using in-house tools.
5. All systems and/or technical controls must be verified upon the completion of maintenance for any cybersecurity related impact.
6. All maintenance work details will be logged in a Maintenance Tracker Excel sheet. The Supervisor will update all details of the work performed in the sheet.

3.2.11 Data

1. Access to sensitive data must be authorized by Supervisor.
2. Data should not be shared informally. When access to sensitive information is required, personnel can request it from their supervisors and should take all necessary steps to prevent unauthorized access.
3. You must immediately notify the Supervisor in the event a device containing sensitive data is lost (e.g. mobiles, laptops, USB devices).
4. It is recommended personnel use encrypted portable media or secure protocols while transferring data across systems. Supervisor can provide you with systems or devices that fit this purpose. You must not use other mechanisms to handle sensitive data.
5. If you have been permitted to work remotely, extra precautions must be taken to ensure sensitive data is appropriately protected.
6. Physical copies of data should be stored in a secure location where unauthorized personnel cannot access it.
7. Personnel should ensure physical copies of sensitive data are not left unattended on a printer.
8. Physical copies of sensitive data should be shredded or disposed in a secure manner.

Description	Digital Files	Physical Copies	Databases
PLC programs	✓	✓	
Robot programs	✓	✓	
CAM/G code	✓	✓	
Operating manuals and documentation	✓	✓	
Electrical diagrams	✓	✓	
Network diagrams	✓	✓	
CAD Files	✓	✓	
Inspection measurement files	✓		
Historical production data	✓		✓

Data types considered sensitive, proprietary, or containing trade secrets.

3.2.12 Credentials Management

The purpose of this policy is to establish a standard for the creation of strong passwords, protection of those passwords, frequency of change and employee expectations.

All staff, vendors, contractors or other stakeholders who use Alpha's IT and OT systems should be given authenticated access to those systems by assigning individual credentials [username and password]. All access and restrictions to those access will be controlled by these credentials.

The creation and removal of IT system accounts is managed via Microsoft Active Directory. In addition, The Supervisor will determine and authorize user access to IT or OT systems.

Alpha reserves the right to suspend without notice access to any system or service.

3.2.13 Password Policy for Active Directory Accounts

1. All employee and system passwords must be at least 10 characters long and contain a combination of upper-case and lower-case letters, numbers, and special characters.

2. Passwords must be changed every 90 days and cannot match a password used within the past 12 months.
3. Passwords must not be a dictionary name or proper name.
4. Passwords must not be inserted into email messages or other forms of electronic communication.
5. Employees must choose unique passwords for all company accounts and may not use a password that they are already using for a personal account.
6. Whenever possible, use of multi-factor authentication is recommended.
7. Default passwords, such as those preconfigured in newly-procured assets, must be changed before the asset is installed or connected to any organizational network.
8. Sharing of passwords is forbidden.
9. Passwords must not be revealed or exposed to public sight.
10. Personnel must refrain from writing passwords down.
11. Personnel must not use the "remember password" feature prevalent on many applications.

3.2.14 Privileged Accounts

The following standards will be used for determining Privileged access to systems.

Privileged Users

- **Foreman/Supervisor**
  - This user has complete control of the manufacturing process within Alpha.

Responsibilities

- Any privileged user within manufacturing environment will have two accounts. A primary account used for normal activities, and a privileged "administrator" account for performing privileged functions.
  - Primary accounts are used for normal daily operations.
  - Primary accounts will have same rights as a standard Alpha user account (e.g., email access, Internet access).
  - Privileged accounts will have administrative privileges, and must only be used when performing administrative functions within manufacturing system (e.g., system updates of firmware or software, system reconfigurations, device restarts).
- Privileged users will adhere to securely using Administrative account when performing duties within manufacturing system. If a privilege account becomes compromised this could have a damaging impact on the manufacturing process.

3.2.15 Antivirus

1. Antivirus will be installed on all devices that are able to support this protections, and be configured to limit resources consumed as not to impact production within OT environment.

2. All devices within OT environment will be configured to receive daily update to include virus signatures.
3. Installed antivirus will be configured to receive push updates from central management server, or others antivirus clients if supported.

3.2.16 Internet

1. Internet access is provided for business purposes.
2. Limited personal navigation is permitted from IT networks if no perceptible consumption of organizational system resources is observed, and the productivity of the work is not affected.
3. Only authorized Internet access from the OT network is permitted. Authorized access can be obtained from Supervisor
4. Inbound and outbound traffic must be regulated using firewalls in the perimeter.
5. All Internal and External communications must be monitored and logged by in-house network security tools. Logs must be reviewed regularly by the plant operators and reported to the Supervisor.
6. When accessing the Internet, users must behave in a way compatible with the prestige of the organization.

3.2.17 Continuous Monitoring

1. Alpha will implement a Security Continuous Monitoring program. This will include performing comprehensive network monitoring using Commercial or Open source tools to detect attacks, attack indicators and unauthorized network connections.
2. The Manufacturing system will be monitored for any cybersecurity attack indicators or IOC's.
3. All External boundary network communications will be monitored.
4. All cybersecurity incidents must be logged in the Incident Response Management tool for documentation purposes.
5. All Local, State, and Federal detection activities applying to organization or manufacturing system will be followed in accordance within the law. Detection activities are to include any industry regulations, standards, policies, and other applicable requirements.
6. Monitoring activity levels will be increased during periods of increased risk and/or any other factors as necessitated by the Alpha Management.
7. All cybersecurity events detected will be communicated to the below list of defined personnel identified by the Supervisor.

Event Severity	List of Personnel
Low (All Events)	All Machine Operators
Medium	Machine Operators, Supervisor

High (Requiring Urgent Attention)	Machine Operators, Supervisor

8. Details of cybersecurity events will be shared with agencies such as ICS-CERT (https://ics-cert.us-cert.gov/). to help secure the organization, including helping secure the industry. Cyber + Infrastructure (CISA) is an agency of Department of Homeland Security which provides reporting capabilities for manufactures related to cybersecurity events.

3.2.18 External Service Provider Communications:

1. All communications from External Service Providers to Alpha's systems will be monitored to ensure work provided by service provider is done correctly, including following all cybersecurity best practices and complying with Alpha's security policies. Monitoring will include designated employee to oversee all activities performed.
2. Any Indicator of Compromise (IOC's) detected while monitoring external service provider communications will be reported and escalated via appropriate communication channels. The Supervisor will reach out to the External service provider upon verifying the threat to discuss and seek an immediate remediation path accordingly.

3.2.19 User Access Agreement

Each employee provided with access to any Alpha resources, including Email and HR system, will be required to review and accept the terms of the User Access Agreement.

As an employee of Alpha

1. You may use Alpha's IT, OT systems and networks to which you have been granted access for work related purposes only. Accounts and access are granted based on each individual's roles and responsibilities.
2. You should not expect any privacy on Alpha's premises or when using Alpha's property or networks either when onsite or accessing remotely
3. You will act responsibly to maintain the security and integrity of the information systems that you use, to minimize the chance of any problems or security breaches for Alpha.
4. You agree to co-operate with any audit by Alpha or our Contractors of your access to the System.
5. You understand your responsibility for respecting other employee's privacy and protecting the confidentiality of information to which you have access, and will comply with all privacy laws, codes and guidelines including,
6. Internet access must not be used for activities that are not authorized under existing laws, regulations, or organization policies.
7. Any company laptops assigned to you should only be used for the purpose of conducting Alpha's business. You are expected to take due care while using laptops.

8. All laptops must be returned at the end of employment.
9. You understand that Transmission or intentional receipt of any inappropriate material or material in violation of law or district policy is prohibited. This includes but is not limited to: copyrighted material; threatening or obscene material: material protected by trade secrets; the design or detailed information pertaining to explosive devices: criminal activities or terrorist acts; gambling; illegal solicitation; racism; inappropriate language.
10. You shall be subject to disciplinary action up to and including termination for violating this agreement or misusing the internet.

3.2.20 Remote Access

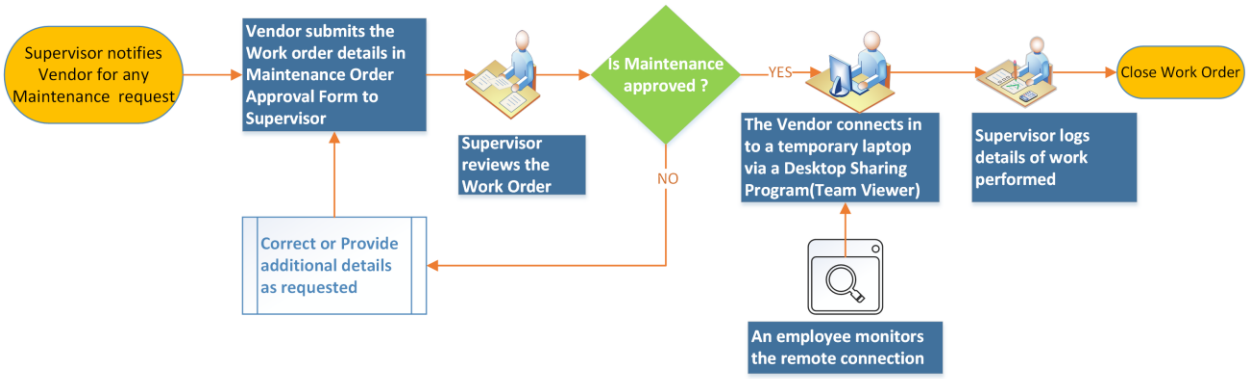
This policy applies to the users and devices that need access the organization's internal resources from remote locations. The following rules are applicable for a one-time request

1. Remote access for personnel requires pre-approval by the Security Officer (Supervisor). Please refer to the approval process for Maintenance to have the Maintenance Order Approval form approved by the Supervisor
2. The Supervisor will determine list of authorized users for remote access.
3. Remote access to sensitive or confidential information is not permitted on an unencrypted connection. Exception to this rule may only be authorized in cases where strictly required.
4. For temporary remote access tasks, an approved desktop sharing program such as TeamViewer will be used. A temporary laptop (workstation) will be arranged with TeamViewer client installed on it. The laptop may have dual network connections, one for internet access and other from the manufacturing network to access the necessary systems. The remote connection will be disconnected upon completion of work.
5. All remote connection activities will be monitored by an employee of Alpha. Monitoring will start and continue until remote session is no longer required, or work has been completed. Appointed individual will indicate when remote session is active and ensure manufacturing system environment has been returned to same state before remote connection was established
6. Installation and use of remote access software (desktop sharing software) etc. on authorized devices must be approved by the Security officer.
7. Any device used for remote access work must have Anti-virus installed along with up to date antivirus signatures.

3.2.21 Usage Restrictions

1. To avoid confusing official company business with personal communications, employees, contractors, and temporary staff with remote access privileges must never use non-company e-mail accounts (e.g. Hotmail, Yahoo, etc.) to conduct business.
2. No employee is to use Internet access through company networks via remote connection for illegal transactions, harassment, competitor interests, or obscene behavior, in accordance with other existing employee policies.
3. Where supported by features of the system, session timeouts are implemented after a period of no longer than 30 minutes of inactivity. Where not supported by features of the system, mitigating controls are implemented.

1181
1182 ### 3.2.22 Remote Maintenance Approval Process



1183 REMOTE MAINTENANCE APPROVAL PROCESS & WORKFLOW

1184

3.2.23 Maintenance Approval Form

Maintenance Order Approval Form	
Vendor Name	
Vendor Address	
Vendor Phone number	
Does the Vendor provide support to Alpha currently?	☐ YES ☐ NO
Does the Vendor system intended to be used have an Anti-virus installed?	☐ YES ☐ NO
What items will be supported and/or worked upon during this session?	☐ PC / Laptops ☐ Servers ☐ Control System Devices ☐ Any other IT/OT Device ☐ Software Details:
Will any software or program need to be installed on Alpha's systems?	☐ YES ☐ NO Details (if YES):
Does this software require licensing to be purchased?	☐ YES ☐ NO
Details of the task to be performed	
Is this a recurring activity	☐ YES ☐ NO
Vendor Signature	
Work Approved *(To be filled by Alpha's Supervisor)*	☐ YES ☐ NO
Supervisor Signature	

3.2.24 Communicate Information to Organization

All critical and operational aspects of the Manufacturing system, key resources should be documented in network diagrams, manuals or other artifacts. The documentation will be reviewed on a yearly basis by the Supervisor.

This information will be shared with all employees, contractors depending on their role in the Company.

3.2.25 Definitions and Acronyms

Asset	A device owned by the organization
AV	Anti-virus
AV scanning	The act of scanning a device for viruses
Change control process	A systematic approach to managing all changes made to a product or system. The purpose is to ensure that no unnecessary changes are made, that all changes are documented, that services are not unnecessarily disrupted and that resources are used efficiently.
Device	Electronic hardware (e.g., machine, computer, laptop, phone, networking equipment)
Employee	An individual directly employed by the organization
External personnel	An individual who is not an employee (e.g., contractor, visitor)
Human machine interface (HMI)	Asset used by personnel to interface and interact with OT (e.g., machines)
ID	Physical identification (e.g., badge)
Industrial control system (ICS)	Typically, the hardware and software used to control processes, or operate machines and manufacturing processes
Information technology (IT)	Hardware devices such as computers, laptops, network switches, firewalls etc.
Least privilege	A user is only authorized to perform the functions necessary to perform their job
Operating system	Software that operates a device (e.g., Windows, Linux); typically, the interface used by the user
Operational technology (OT)	ICS and other devices (typically internetworked) used by the manufacturing process
Personal device	A device owned by an individual; not owned or controlled by the organization

Personnel	All employees and external personnel, excluding visitors
Portable media	USB flash drive, compact disc (CD), external hard drive, laptop
Remote access technologies	Software used to connect a device to the IT or OT network via the Internet, usually performed by personnel located off-site
Sensitive data	Data containing proprietary information or trade secrets pertaining to the operations of the organization; data that could cause damage to the organization if obtained by an attacker
Split tunneling	Split tunneling allows a mobile user access public network (e.g. Internet) and local LAN/WAN Corporate network at the same using same or different network connections
User	Individual using a device
Virus signature	Data used by antivirus software to identify viruses
VPN	Virtual private networking; see 'remote access technologies'.
Vulnerability scanning	Software used to detect common or known vulnerabilities on a device

3.2.26 References

1. Security Policies by SANS Resources https://www.sans.org/security-resources/policies
2. Template for Security Policy by Project Management Docs http://www.projectmanagementdocs.com/template/Security-Policy.doc

5. Data Security Policy by Sophos labs https://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-example-data-security-policies-na.pdf?la=en

3.3 Standard Operating Procedures Document Example

Standard Operating Procedures

for

Alpha

Document Owner:	Supervisor, Alpha

Version

Version	Date	Description	Author
1.0	02-22-2018	Initial Draft	Supervisor
2.0	04-21-2018	Major changes to the initial draft	Supervisor

Approval

(By signing below, all Approvers agree to all terms and conditions outlined in this document.)

Approvers	Role	Signed	Approval Date
	President		4-22-2018

3.3.1 Introduction

This document defines the procedural steps management and employees will follow ensuring consistence daily actives along with response to events occur within the manufacturing system for Alpha. Within this document contains content which should be referred to often ensuring all employees/individuals performing work within manufacturing system are not inadvertently compromising cybersecurity posture by not following Standard Operation Procedures (SOPs).

3.3.2 Purpose

To provide a consistent repeatable process that can be followed to perform tasks within manufacturing system.

3.3.3 Scope

Management, employees, contractors, or individuals requiring access to manufacturing system for changes should be familiar with the contents included within this document.

IDENTIFY

3.3.4 Asset Inventory

Identifying assets within manufacturing system for Alpha is a vital first step in protecting organization from malicious activates that could result in disruption to production. Alpha uses multiple tools for asset inventory, some manual processes and other automated. Knowing the environment and what devices are installed allows the ability to detect devices not approved to be on the network which could be an indication of malicious activity. Keeping devices updated with the latest software patches ensure to mitigate potential weakness within manufacturing system. All patches will be carefully examined to determine if there is any performance impact effecting production within manufacturing system.

Manual

Devices not having ability to be automatically scanned will be added to excel spreadsheet and updated quarterly. Devices included in manual process would be PLC and machine stations, including any additional devices that are not able to be scanned automatically with a tool. All inventory will be conducted during manufacturing system planned down time and inventory will include hardware and software.

Automated

Devices with the ability to be scanned will be added to Alpha's asset inventory tool and scanned quarterly. Scanning quarterly will ensure manufacturing process is not affected. All scanning should be performed when manufacturing system has been placed into a non-production mode (system down time). Alpha has chosen an asset inventory tool that has multiple version from open source to enterprise edition. Alpha has selected Enterprise edition since this version provides the ability to schedule scans, baseline systems for monitoring changes. For additional information and references see.

Alpha inventory management tools will be configured for group access to ensure only individuals requiring access are allowed. This ensure that people within the organization only needing read accesses are not granted a higher level, which could lead to inadvertent changes to scanning tools configuration. See reference for how groups are created.

Scans of manufacturing system will be conducted quarterly ensuring not to effect manufacturing process. Scans will audit software including license information, version, and configuration. Devices within the manufacturing systems will have software inventory audited and reviewed quarterly. Changes occurring to devices' software before the next update will trigger a required

inventory to remain compliant. See reference for additional details for performing scanning within manufacturing system.

Alpha will apply updates to asset inventory software as they become available. Updates are required to keep systems patched and free from known vulnerabilities while adding additional features. See reference for additional information.

3.3.5 Network Baseline

Network baseline is important as it provides the ability to detect malicious active occurring on manufacturing system network. Alpha will periodically perform baseline scans to identify any unusual traffic, which could be indication of malicious activity. All traffic observed during scanning should be reconciled to help create a securer network. See reference for network baseline performed.

3.3.6 External Connections

Using company provided network diagram tools all network connection for external communication will be mapped. Mapping will include all relevant information for connection service provided. Example of information required would be assigned IP address for device providing service, support phone number, customer number, person of contact, and support level agreement and hours. External providers will include cloud services. Network diagram will be updated quarterly.

3.3.7 Baseline Configurations

Baseline configurations was captured using two methods since some ICS devices don't allow automated tool scanning; for these devices' spreadsheet tracking is the preferred method. Devices lacking SSH, SNMP, WMI ability will require manual entry in spreadsheet.

Steps used to perform automated scanning for Alpha.

Baseline configurations Alpha implemented within Manufacturing systems helps to ensure inadvertent changes are detected before systems' integrity has been compromised.

Open-AudIT [1] has been chosen for Alpha due to scalable configuration depending on required needs. Instruction are listed for performing scanning. Once scanning has been performed changes with ICS devices are detectable by running reporting identifying new software changes.

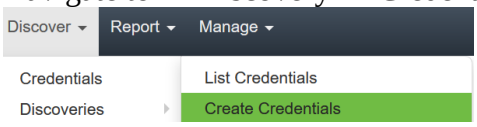
Manufacturing systems was scanned to get initial baseline. Steps performed are listed below. Once scan/s have been completed information was exported to CSV file for storage. See end of instructions for exported configuration.

[1] Open-Audit: https://www.open-audit.org

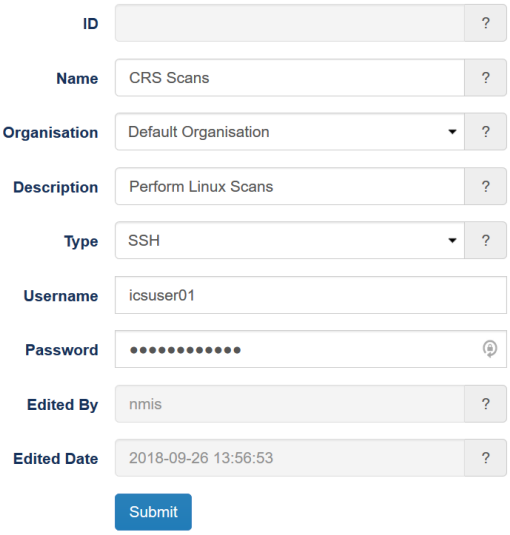
Open-AudIT Configuration steps within Collaborative Robotics System once system has been installed

Initial Configuration:

- Login via web portal
- Navigate to → Discovery → Credentials → Create Credentials

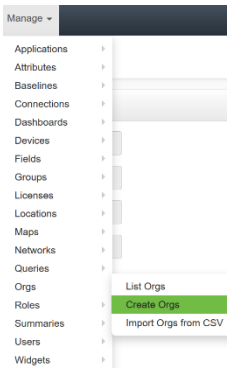


- Credentials can be assigned to any organization that has already been created. If you want credentials to only apply to specific organizational group, then select that from the appropriate drop-down during credential creation and select the desired group these credentials will apply to.
- Alpha's environment consists of mainly Linux based machine, so **SSH** will be discussed for connection type.
- Now create a credential and select **SSH** for the type. Once completed click **Submit** button.

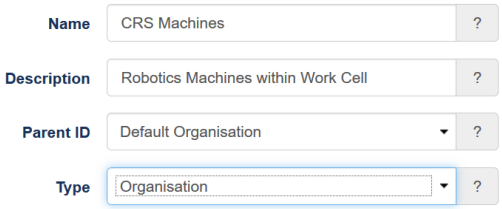


Organization Groups Creation:

- Click on Manage → Orgs → Create Orgs



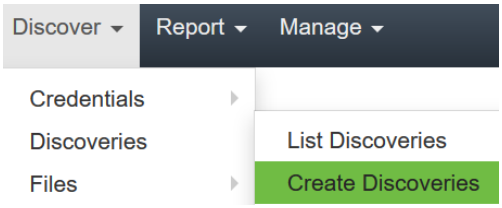
- Now enter **Name: Description:** and click submit at the bottom of the page to save.



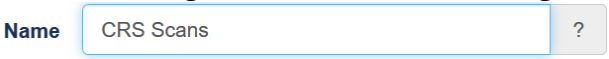
- If you have multiple machines / equipment in different locations you can make Organizational groups based on the business units, or related task.

Configure Discovery Scan:

- Now click on Discover → Discoveries → Create Discoveries



- Enter a meaningful name for discover being created



- Next, enter the subnet that'll be used for performing this scan. This scan is using 192.168.0.0/23

Search online for additional subnetting information / calculators if you'd like to learn more.

- **Network address:** should already be defaulted to Open-AudIT installed location, if this is not true, click the drop-down arrow and select your installed location.

- Now, click on the advanced button to see more options. 

- Once **Advanced** has been expanded you'll have additional options to select if desired. These options are **Org, Type, Devices Assigned to Org,** and **Devices Assigned to**

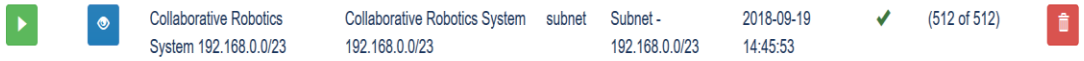
Location. These options aren't required but allow you to start placing found devices into different Organizational groups.

- Once all are selected click on **Submit** button to continue.

Discoveries:

- Once the steps above have been completed clicking on **Submit** button you'll be taken to a new webpage that'll allow you to run discovery process created in the previous step.

- To start discovering devices click on **green** arrow button. If you need to verify details for this scan click on the button that looks like an **eye**: finally, if you need to delete this scan click on the **trash** can icon to the right. See screen shot for details.



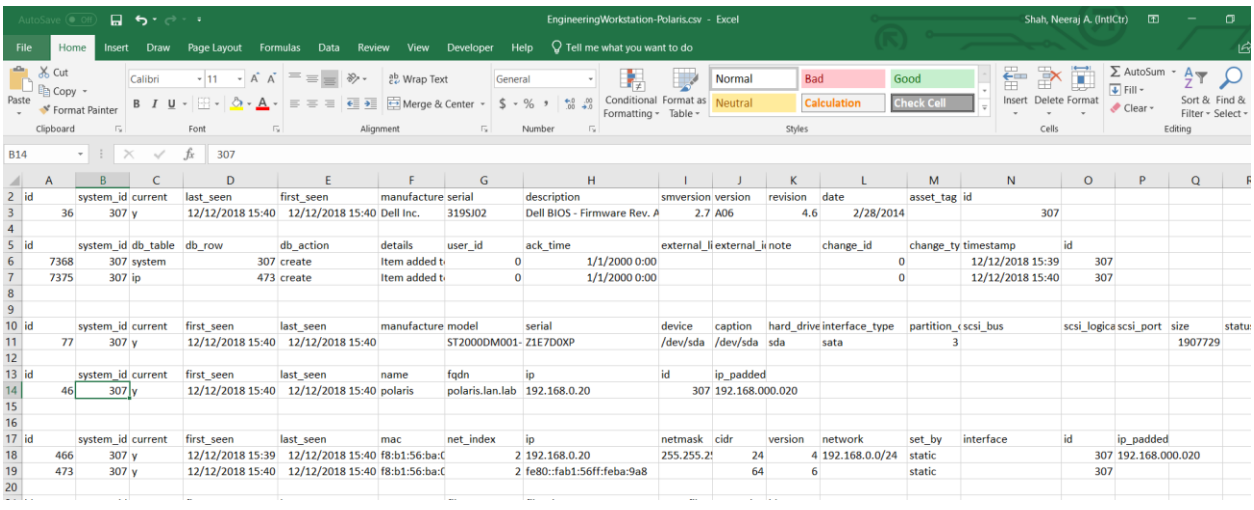
- Once discovery has started you'll be taken to a new page allowing you to view status or cancel if needed.

Newly found devices are added to **My Devices** which is found on the home screen.

Collaborative Robotics System 

Detailed baseline reports generated out of Open-AudIT can be obtained from [CRS Baseline Reports]

Shown below is a sample export of the baseline data from one of the devices using Open Audit in the Robotics system.



id	system_id	current	first_seen	last_seen	mac	manufacturer	model	description	alias	ip_enabled	net_index	dhcp_enabled	dhcp_server	dhcp_lease	dhcp_lease
302	307	y	12/12/2018 15:40	12/12/2018 15:40	f8:b1:56:ba:(	Intel Corporation	82579LM Gigabit Network (	82579LM Gigabit Net		TRUE	2	FALSE			
303	307	y	12/12/2018 15:40	12/12/2018 15:40	68:05:ca:1c:2	Intel Corporation	C600/X79 series chipset PC	C600/X79 series chips		FALSE	4	FALSE			
304	307	y	12/12/2018 15:40	12/12/2018 15:40	68:05:ca:2e:2	Intel Corporation	Ivytown PCI Express Root P	Ivytown PCI Express F		FALSE	3	FALSE			

id	system_id	current	first_seen	last_seen	name	size	initial_size	max_size	id
21	307	y	12/12/2018 15:40	12/12/2018 15:40	/dev/sda5	0	8331260	8331260	307

id	system_id	current	first_seen	last_seen	serial	name	description	device	hard_drive	partition_(	mount_type	mount_point	size	free	used
137	307	y	12/12/2018 15:40	12/12/2018 15:40	8e974296-0369-487c-8f59-6db7b6	144483		/dev/sda1	sda	sda	partition	/	1899591	1735038	39624
138	307	y	12/12/2018 15:40	12/12/2018 15:40				/dev/sda2	sda	sda	partition		0	0	0
139	307	y	12/12/2018 15:40	12/12/2018 15:40	9c155e7d-fcf8-4911-bc63-7c28963	fb5b6		/dev/sda5	sda	sda	partition	[SWAP]	8136	8135	0

id	system_id	current	first_seen	last_seen	physical_cou	core_count	logical_count	description	speed	manufactu	architecture	socket	id
46	307	y	12/12/2018 15:40	12/12/2018 15:40	2	8	8	Intel Xeon	1200	Intel		Socket LGA201	307

id	system_id	current	first_seen	last_seen	destination	mask	metric	next_hop	protocol	type	id	destination_pac	next_hop_padded
297	307	y	12/12/2018 15:40	12/12/2018 15:40	0.0.0.0	0.0.0.0	0	192.168.0.2		UG	307	000.000.000.00	192.168.000.002
298	307	y	12/12/2018 15:40	12/12/2018 15:40	169.254.0.0	255.255.0.0	1000	0.0.0.0		U	307	169.254.000.00	000.000.000.000
299	307	y	12/12/2018 15:40	12/12/2018 15:40	192.168.0.0	255.255.255.0	1	0.0.0.0		U	307	192.168.000.00	000.000.000.000

List of services running:

id	system_id	current	first_seen	last_seen	name	description	executable	user	start_mod	state	id
6208	307	y	12/12/2018 15:40	12/12/2018 15:40	acpid	acpid start/running, process 1552 (using upstart)			Auto	Running	307
6209	307	y	12/12/2018 15:40	12/12/2018 15:40	alsa-restore	alsa-restore stop/waiting (using upstart)			Manual	Stopped	307
6210	307	y	12/12/2018 15:40	12/12/2018 15:40	alsa-store	alsa-store stop/waiting (using upstart)			Manual	Stopped	307
6211	307	y	12/12/2018 15:40	12/12/2018 15:40	anacron	anacron stop/waiting (using upstart)			Manual	Stopped	307
6212	307	y	12/12/2018 15:40	12/12/2018 15:40	apport	apport start/running (using upstart)			Auto	Running	307
6213	307	y	12/12/2018 15:40	12/12/2018 15:40	atd	atd start/running, process 1553 (using upstart)			Auto	Running	307
6214	307	y	12/12/2018 15:40	12/12/2018 15:40	avahi-daem	avahi-daemon start/running, process 1245 (using upstart)			Auto	Running	307
6215	307	y	12/12/2018 15:40	12/12/2018 15:40	binfmt-supp	binfmt-support stop/waiting (using upstart)			Manual	Stopped	307
6216	307	y	12/12/2018 15:40	12/12/2018 15:40	bluetooth	bluetooth start/running, process 1226 (using upstart)			Auto	Running	307
6217	307	y	12/12/2018 15:40	12/12/2018 15:40	centrifydc	centrifydc start/running, process 1650 (using upstart)			Auto	Running	307
6218	307	y	12/12/2018 15:40	12/12/2018 15:40	console-set	console-setup stop/waiting (using upstart)			Manual	Stopped	307
6219	307	y	12/12/2018 15:40	12/12/2018 15:40	console	console stop/waiting (using upstart)			Manual	Stopped	307
6220	307	y	12/12/2018 15:40	12/12/2018 15:40	container-d	container-detect stop/waiting (using upstart)			Manual	Stopped	307
6221	307	y	12/12/2018 15:40	12/12/2018 15:40	control-alt-d	control-alt-delete stop/waiting (using upstart)			Manual	Stopped	307
6222	307	y	12/12/2018 15:40	12/12/2018 15:40	cron	cron start/running, process 1551 (using upstart)			Auto	Running	307
6223	307	y	12/12/2018 15:40	12/12/2018 15:40	cups	cups start/running, process 1247 (using upstart)			Auto	Running	307
6224	307	y	12/12/2018 15:40	12/12/2018 15:40	dbus	dbus start/running, process 1213 (using upstart)			Auto	Running	307
6225	307	y	12/12/2018 15:40	12/12/2018 15:40	dmesg	dmesg stop/waiting (using upstart)			Manual	Stopped	307
6226	307	y	12/12/2018 15:40	12/12/2018 15:40	failsafe	failsafe stop/waiting (using upstart)			Manual	Stopped	307
6227	307	y	12/12/2018 15:40	12/12/2018 15:40	failsafe-x	failsafe-x stop/waiting (using upstart)			Manual	Stopped	307
6228	307	y	12/12/2018 15:40	12/12/2018 15:40	flush-early-j	flush-early-job-log stop/waiting (using upstart)			Manual	Stopped	307
6229	307	y	12/12/2018 15:40	12/12/2018 15:40	friendly-rec	friendly-recovery stop/waiting (using upstart)			Manual	Stopped	307
6230	307	y	12/12/2018 15:40	12/12/2018 15:40	gssd	gssd stop/waiting (using upstart)			Manual	Stopped	307
6231	307	y	12/12/2018 15:40	12/12/2018 15:40	hostname	hostname stop/waiting (using upstart)			Manual	Stopped	307
6232	307	y	12/12/2018 15:40	12/12/2018 15:40	hwclock-sav	hwclock-save stop/waiting (using upstart)			Manual	Stopped	307
6233	307	y	12/12/2018 15:40	12/12/2018 15:40	hwclock	hwclock stop/waiting (using upstart)			Manual	Stopped	307
6234	307	y	12/12/2018 15:40	12/12/2018 15:40	hybrid-gfx	hybrid-gfx stop/waiting (using upstart)			Manual	Stopped	307
6235	307	y	12/12/2018 15:40	12/12/2018 15:40	idmapd	idmapd start/running, process 1198 (using upstart)			Auto	Running	307

List of patches/packages installed:

id	system_id	current	first_seen	last_seen	name	version	description	location	uninstall	install_da	installed_by	installed_on	pub
54348	307	y	12/12/2018 15:40	12/12/2018 15:40	Ubuntu 12.04.5 LTS	12.04	Operating System					1/1/2000 0:00	
54349	307	y	12/12/2018 15:40	12/12/2018 15:40	accountsservice	0.6.15-2ubuntu9.7						1/1/2000 0:00	
54350	307	y	12/12/2018 15:40	12/12/2018 15:40	acl	2.2.51-5ubuntu1						1/1/2000 0:00	
54351	307	y	12/12/2018 15:40	12/12/2018 15:40	acpi-support	0.140.2						1/1/2000 0:00	
54352	307	y	12/12/2018 15:40	12/12/2018 15:40	acpid	1:2.0.10-1ubuntu3						1/1/2000 0:00	
54353	307	y	12/12/2018 15:40	12/12/2018 15:40	activity-log-manager-con	0.9.4-0ubuntu3.2						1/1/2000 0:00	
54354	307	y	12/12/2018 15:40	12/12/2018 15:40	activity-log-manager-con	0.9.4-0ubuntu3.2						1/1/2000 0:00	
54355	307	y	12/12/2018 15:40	12/12/2018 15:40	adduser	3.113ubuntu2						1/1/2000 0:00	
54356	307	y	12/12/2018 15:40	12/12/2018 15:40	adium-theme-ubuntu	0.3.2-0ubuntu1						1/1/2000 0:00	
54357	307	y	12/12/2018 15:40	12/12/2018 15:40	alsa-base	1.0.25+dfsg-0ubuntu1.1						1/1/2000 0:00	
54358	307	y	12/12/2018 15:40	12/12/2018 15:40	alsa-utils	1.0.25-1ubuntu5.2						1/1/2000 0:00	
54359	307	y	12/12/2018 15:40	12/12/2018 15:40	anacron	2.3-14ubuntu1						1/1/2000 0:00	
54360	307	y	12/12/2018 15:40	12/12/2018 15:40	apg	2.2.3.dfsg.1-2						1/1/2000 0:00	
54361	307	y	12/12/2018 15:40	12/12/2018 15:40	app-install-data	0.12.04.4						1/1/2000 0:00	
54362	307	y	12/12/2018 15:40	12/12/2018 15:40	app-install-data-partner	12.12.04.1						1/1/2000 0:00	
54363	307	y	12/12/2018 15:40	12/12/2018 15:40	apparmor	2.7.102-0ubuntu3.11						1/1/2000 0:00	
54364	307	y	12/12/2018 15:40	12/12/2018 15:40	appmenu-gtk	0.3.92-0ubuntu1.1						1/1/2000 0:00	
54365	307	y	12/12/2018 15:40	12/12/2018 15:40	appmenu-gtk3	0.3.92-0ubuntu1.1						1/1/2000 0:00	
54366	307	y	12/12/2018 15:40	12/12/2018 15:40	appmenu-qt	0.2.6-0ubuntu1						1/1/2000 0:00	
54367	307	y	12/12/2018 15:40	12/12/2018 15:40	apport	2.0.1-0ubuntu17.15						1/1/2000 0:00	
54368	307	y	12/12/2018 15:40	12/12/2018 15:40	apport-gtk	2.0.1-0ubuntu17.15						1/1/2000 0:00	
54369	307	y	12/12/2018 15:40	12/12/2018 15:40	apport-symptoms	0.16.1						1/1/2000 0:00	
54370	307	y	12/12/2018 15:40	12/12/2018 15:40	apt	0.8.16~exp12ubuntu10.27						1/1/2000 0:00	
54371	307	y	12/12/2018 15:40	12/12/2018 15:40	apt-transport-https	0.8.16~exp12ubuntu10.27						1/1/2000 0:00	
54372	307	y	12/12/2018 15:40	12/12/2018 15:40	apt-utils	0.8.16~exp12ubuntu10.27						1/1/2000 0:00	
54373	307	y	12/12/2018 15:40	12/12/2018 15:40	apt-xapian-index	0.44ubuntu5.1						1/1/2000 0:00	
54374	307	y	12/12/2018 15:40	12/12/2018 15:40	aptdaemon	0.43+bzr805-0ubuntu10						1/1/2000 0:00	
54375	307	y	12/12/2018 15:40	12/12/2018 15:40	aptdaemon-data	0.43+bzr805-0ubuntu10						1/1/2000 0:00	
54376	307	y	12/12/2018 15:40	12/12/2018 15:40	apturl	0.5.1ubuntu3						1/1/2000 0:00	
54377	307	y	12/12/2018 15:40	12/12/2018 15:40	apturl-common	0.5.1ubuntu3						1/1/2000 0:00	

3.3.8 Update Baseline after Modifications

Manufacturing baseline will be reviewed quarterly and updated with any changes that have occurred since last review. During period between baseline updates any new equipment added, or configuration changes implemented will initiate a new baseline scan to be performed. GRASSMARLIN[2] and Wireshark[3] are the tools used for updating baseline after modification have occurred. Examples of changes within the manufacturing system would be updating software, license, system patches, firmware updates, new devices like PLCs' or HMIs' and other ICS components required for operations.

3.3.9 Network Operations Baseline

Network baseline will be created within manufacturing system to identify all crucial components required for production to operate. Tools used for this process are as listed, GRASSMARLIN and Wireshark. Each tool listed provides slightly different capabilities and detail. GRASSMARLIN generates a diagram for easy visualization, compare to Wireshark which provides data without diagrams. These tools provide the required network operations baseline required for manufacturing process.

3.3.10 Priorities for Manufacturing Missions

The priorities for manufacturing missions have been identified in the "Organization Overview" Section of the Security Program document.

3.3.11 Critical Manufacturing system components and functions

The critical manufacturing system components and functions have been identified in the Organization Overview Section of the Security Program document.

PROTECT

3.3.12 Security

Security within the organization including the manufacturing system will be followed at all time to reduce risk of cybersecurity incidents. Sections below contain multiple references to procedures used at Alpha for security manufacturing system.

[2] GRASSMARLIN: https://github.com/nsacyber/GRASSMARLIN

[3] WireShark: https://github.com/nsacyber/GRASSMARLIN

3.3.13 Training

Training is a vital role for keeping the company safe for Cybersecurity threats. All employees, contractors and vendors should have completed required training before being allowed to work within manufacturing system. Awareness and Training for Third Party Contractors and Vendors should be reviewed and signed before being allowed to access manufacturing systems.

3.3.14 Port Security

Port security allows the ability to configure network ports to be associated with individual device's Media Access Control (MAC) addresses. Enabling port security ensures only designated devices are allowed access, any device not already in the approved list will be denied access. Port Security along provides additional protection, when used with defense-in-depth strategies. See reference for steps required for setup within Alpha.

3.3.15 Network Segmentation

Alpha's manufacturing network has been segmented to improve speed and security within the environment. Network segmentation provides ability to control traffic from each network, ensuring only allowed communication can pass between each network. See reference for steps used for Alpha.

Task: Implement network segmentation.

- The Work Cell consists of the following network hardware.

Type	Description
RuggedCom RX Firewall	Boundary protection firewall, router
Siemens i800 Switch	Layer-2 Switch for the Control Network
Netgear GS724T Switch	Layer-2 Switch for the Supervisory Network

- Network segmentation was implemented using the RuggedCom firewall. The firewall has the following interfaces defined. There were two subnets created as listed in the below table.

Interface	IP address of Interface	Subnet	Description
Ge-2-1	192.168.1.2	192.168.1.0/24	Control LAN Network
Ge-2-2	N/A	N/A	Mirror Port
Ge-3-1	192.168.0.2	192.168.0.0/24	Supervisory LAN Network
Ge-3-2	10.100.0.20	N/A	Uplink to Cybersecurity LAN

- The Siemens i800 switch is connected to the Ge-2-1 interface of the RX1510 and used for the Control LAN network. Devices connected to this i800 switch such as the 4 Machining stations, Robot Driver server were assigned an IP address from the Control LAN subnet (192.168.1.0/24).

- The Netgear switch is connected to the Ge-3-1 interface of RX1510 and used for the Supervisory LAN network. Devices connected to this switch such as the PLC, HMI, Engineering workstation were accordingly assigned an IP address from this Supervisory LAN subnet (192.168.0.0/24)

Task: Identify and control connections.

	From	To	Direction	Controlled using
Connection	Cybersecurity LAN	Supervisory LAN	Bi-directional	NAT Configuration on the Boundary Firewall (RuggedCom)
Connection	Cybersecurity LAN	Plant LAN	Bi-directional	NAT Configuration on the Boundary Firewall (RuggedCom)
Connection	Supervisory LAN	Plant LAN	Bi-directional	ACL rules on the Boundary Firewall (RuggedCom)
Connection	Supervisory and Plant LAN	Internet	One way	Boundary Firewall (Cisco ASA) in the Cybersecurity LAN

3.3.16 Monitor Boundary Connections

Network traffic will be monitored for external and internal communications using a firewall, or other type of device that allows for the ability to control connection traffic. Required network traffic leaving the manufacturing system will be allowed, all other traffic will be explicitly dropped. Traffic to manufacturing system will be limited to only those machines required for monitoring from corporate network to manufacturing system and machines won't be allowed internet access. Device monitoring external/ internal connection/communications will forward all logging to internal Syslog server for archival purposes.

- External Boundary communications are monitored using Cisco ASA Firewall in the Cybersecurity LAN network.
- Internal Boundary communications are monitored using RuggedCom RX series Firewall in the Work Cell.

Tool: Boundary Protection Device

1432 The table below lists the boundary protection devices implemented

Type	Description
RuggedCom RX Firewall	Firewall/Router for Work Cell
Cisco ASA Firewall	Firewall/Router in the Cybersecurity LAN

1433

1434 **Boundary protection device configuration.**

1435 Refer to section 4.16 Network Boundary Protection

1436 ### 3.3.17 Actions with/without Authentication

1437 Shown below are a list of actions that can be performed with or without Authentication

Authentication Required to Physically/Logically Interact with Device?								
	Engineering Workstation	**Supervisory PLC**	**HMI**	**Machining Stations**	**Robot Arms**	**Robot Controllers**	**Robot Driver**	**Process Historian**
Physical Interaction (All Users*)	Y	N	N	N	N	N/A	N/A	Y
Logical/Network Interaction (All Users*)	Y	Y	Y	Y	Y	Y	Y	Y

1438
1439

HMI User Actions Requiring Authentication							
	View Workcell Settings	**Modify Workcell Settings**	**View Station Settings**	**Modify Station Settings**	**Reboot Station**	**Silence/Clear Alarms**	**Access HMI HTTP Server**
All Users*	N	N	N	N	N	N	Y

1440

1441

Engineering Workstation User Actions Requiring Authentication							
	Login to Workstation	**View/Modify PLC Logic**	**View/Modify HMI Logic**	**View/Modify Robot Logic**	**View/Modify Station Logic**	**Access Engineering Files**	**All Other Actions**
All Users*	Y	Y	Y	Y	Y	Y	Y

1442

Historian User Actions Requiring Authentication				
	View Historical Data	**Modify Historical Data**	**Modify Configuration**	**Login to Server Desktop/CLI**
All Users*	Y	Y	Y	Y

1443

1444

Robot Actions Requiring Authentication				
	Power On/Off	**Start/Stop Driver**	**Start/Stop Controllers**	**View/Modify Logic**
All Users*	N	Y	Y	Y

1445

1446

Machining Station Actions Requiring Authentication				
	Power On/Off/Reboot	**Reset**	**View/Modify Configuration**	**View/Modify Logic**
All Users*	N	N	N	Y

1447

1448

PLC Actions Requiring Authentication

	Power On/Off	Reboot	Process Interaction (Run/Stop/Reset)	Modify Logic	Change Mode (Run/Config)
All Users*	N	N	N	Y	Y

* Authentication for *all users* does not imply authorization has been granted to any specific user or role.

3.3.18 Network Connections

All network connection with manufacturing system will be documented to include port numbers and cables will be labeled indicating their designated purpose.

Using company provided network diagram tools, all network connection for internal communication will be mapped. Mapping will include all relevant information for connection. Example of information required would be assigned IP address for device providing service and person of contact. Network diagram will be updated quarterly.

All connection will be reviewed and authorized before being placed into production.

3.3.19 Remote Maintenance

Remote maintenance activities will be coordinated and approved before vendor access is allowed. All remote maintenance activities provided by a vendor will be controlled and monitored to ensure no harmful or malicious activities occur. Any vendors or contractors connecting to Alpha for remote maintenance will require approval before connecting. Requests will be documented to ensure proper audit trail for activity conducted within manufacturing system. See reference for detailed plan.

3.3.20 System Maintenance

Please see System Maintenance Section within Security Policy document.

3.3.21 Change Control

Changes to manufacturing system will be submitted to a change control process ensuring that all applicable parties are aware and agree on actions being performed. Management will have final approval since production could be affected by down time.

Changes within the manufacturing systems will be scheduled during non-production hours as not to affect processing within manufacturing system. Changes will be reviewed and authorized before being implemented. Potential system performance issues from the potential change must be determined before the change is made. Once changes have been completed a review will be conducted ensuring same security level continues to be maintained after changes have been implemented.

Responsible parties will evaluate security impact on change controls being performed within the manufacturing system environment. Change control reviewers will have final say for changes being implemented along with changes having an impact on security

An Excel sheet will be used to document all change control items.

Below is a list of items that need to be configuration controlled.

Device Name	Item Type	Details
POLARIS (Engineering Workstation), MINTAKA (Robot Driver), vController1, vController2 (Robot Controllers)	Software	BIOS/Firmware patches, ROSS code, OS Firewall rules (iptables) and any OS parameter changes
	Hardware	Storage and Memory upgrade
PLC	Software	Firmware upgrade
HMI	Software	Firmware upgrade
RuggedCom Boundary Router	Software	Firmware upgrade, Firewall rules and any other configuration change
Layer-2 Switches	Software	Firmware upgrade and any type of configuration change

3.3.22 Backup Procedures

Servers, Workstations:

Refer Section 4.6 Veeam Backup and Replication

Network Devices – Switches:

1. Login to the Web UI of the device from the Engineer Workstation

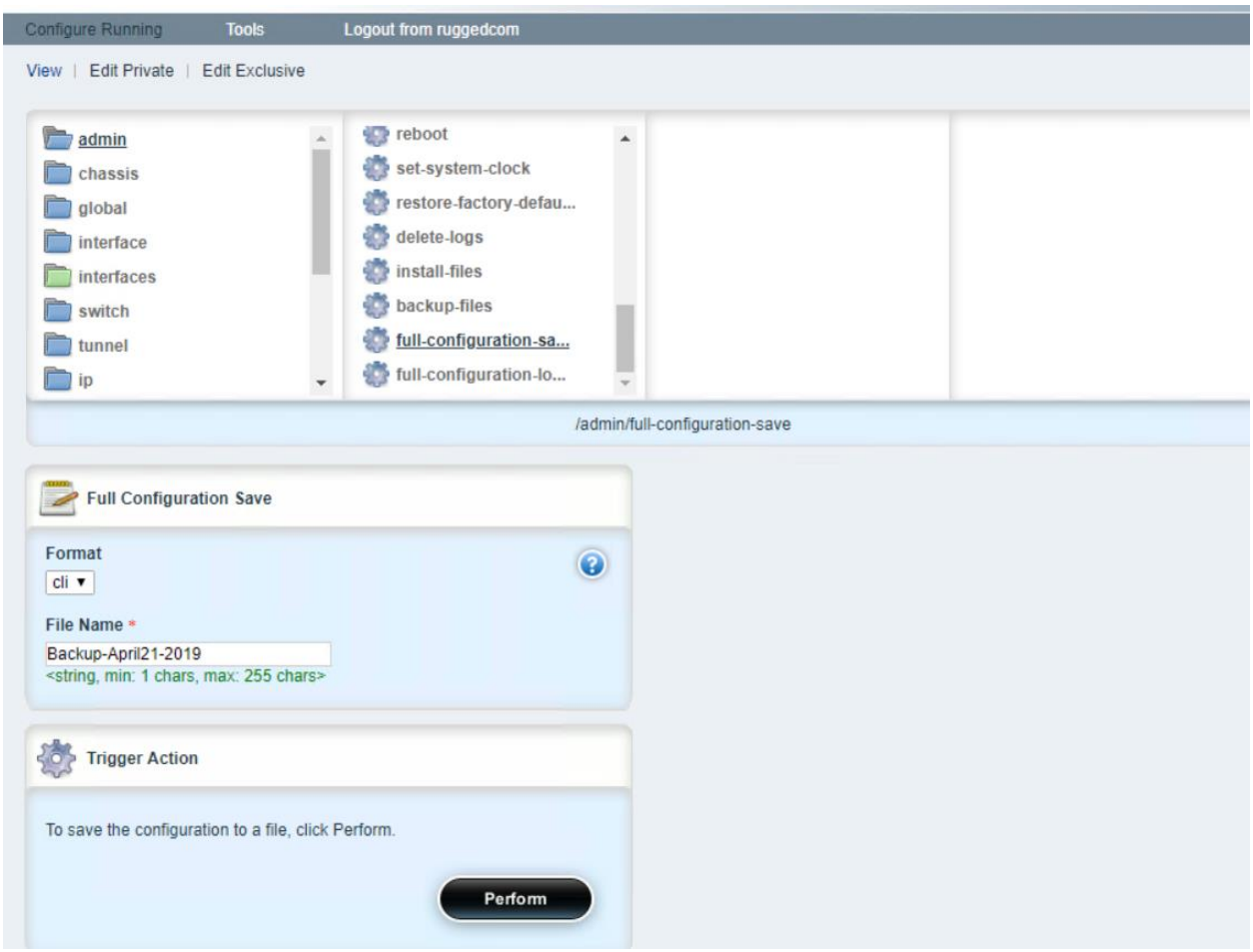
2. In the Web UI, browse to the Backup option, select the type of backup and click Download

3.Ensure to manually save the configuration backup at a central secure location

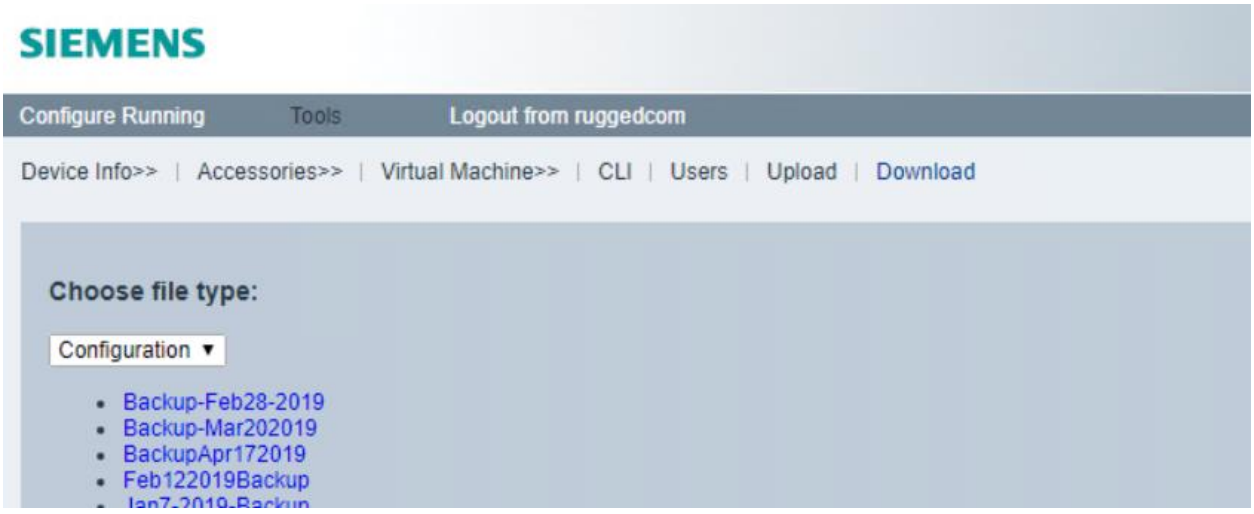
Network Devices – RuggedCom Router:

1. Login to the Web UI of the device from the Engineer Workstation

2.Click **Admin** >> **Full-Configuration-Save** >> Format- **Cli >>** Enter a File Name >> Perform



3.Click on **Tools** >> **Download** >> Choose File Type – **Configuration** >> Click on the **file** to download



ICS Devices:

Follow the Manufacturer's product manual to perform a backup

Ensure to manually save the configuration backup at a central secure location

3.3.23 Media Sanitization for Devices

Assets / Device type	Method used	Details
Hard Drives on servers, workstations	**CLEAR**	Tool: DBAN [4], Category: Software, Type: Open-Source Instructions: (1) Download and create a bootable media of DBAN (2) Boot the server using the bootable media (3) Follow the on-screen instructions to run the multiple passes of data wipe. (4) Once complete, verify if wipe was successful by booting the server without the DBAN media
Beckhoff PLC	**CLEAR**	The Beckhoff CX PLC contains an embedded Windows CE loaded on a Micro SD card. As per the manufacturer, to reset the CX back to factory settings, the best option would be to reimage it. (1) Obtain a copy of the base image of the Windows CE prior to reimaging. (2) Remove the MicroSD and load it in a card reader. Clear the data on the SD card using the procedure recommended in Section 2 above for SD cards. (3) Load the base image on the SD card and plug it in back.
Red Lion HMI	**CLEAR**	As per the manufacturer's official documentation[5] (1) When making selections in the system menu, you must touch and hold your selection until it turns green. (2) When system menu is display, touch and hold **Database Utilities**. Then in the next window, touch and hold **Clear Database**, then select yes. Then hit back, then hit **continue**. You will get a page invalid database, which

[4] https://dban.org/

[5] http://www.redlion.net/sites/default/files/1299/6670/Crimson%203.0%20-%20System%20Menu%20Tech%20Note.pdf

		means the database has been cleared off the unit.
RuggedCom L3 switches (Router)	**CLEAR and PURGE**	The below instructions are found in Siemens RuggedCom Manual (ROX II v2.10 User Guide[6]) Clear: (1) Login to Web Admin console (2) Navigate to **admin** and click **restore-factory-defaults** in the menu (3) Select **"Delete Logs, Delete both partitions, Delete saved configurations**" and click on **Perform.** Purge: (1) Obtain a copy of the RUGGEDCOM ROX II firmware currently installed on the device. For more information, contact Siemens Customer Support. (2) Log in to maintenance mode. For more information, refer to the RUGGEDCOM ROX II v2.10 CLI User Guide. (3) Delete the current boot password/passphrase by typing: rox-delete-bootpwd --force (4) Type **exit** and press **Enter**. (5) Log in to RUGGEDCOM ROX II. (6) Flash the RUGGEDCOM ROX II firmware obtained in Step 1 to the inactive partition and reboot the device (7) Repeat Step 5 and Step 6 to flash the RUGGEDCOM ROX II firmware obtained in Step 1 to the other partition and reboot the device. (8) Shut down the device.
RuggedCom L2 switch	**CLEAR**	The below instructions are found in Siemens RuggedCom Manual (ROX v4.83 i8xx User Guide[7]) Clear: (1) Login to Web Admin console of the switch. (2) Navigate to **Diagnostics » Load Factory Defaults**. The Load Factory Defaults form appears. (3) Select **Default Choice = None** from the dropdown. Hit **Apply**.

[6] https://www.plcsystems.ru/catalog/ruggedcom/doc/ROXII_RX1500_User-Guide_WebUI_EN.pdf

[7] https://support.industry.siemens.com/cs/attachments/109737193/ROS_v4.3_i80x_User-Guide_EN.pdf?download=true

Netgear L2 Switch	**CLEAR**	The below instructions are found in Netgear GS724T Manual[8] Clear: (1) Login to Web Admin console of the switch. (2) Click on **Maintenance** Tab (3) Click on **Factory Default** and hit **Apply**.
Wago Modular IO Device	**CLEAR**	

1509

1510 ### 3.3.24 Priority Analysis

1511 Manufacturing system will be evaluated quarterly to identify devices importance. Devices
1512 importance will be used to provide a criticality report containing the minimum pieces of
1513 equipment required to continue production.

1514

[8] http://www.downloads.netgear.com/files/GDC/GS716TV2/GS716T_GS724T-SWA-October2012.pdf?_ga=2.154219964.507023277.1517932216-1121248166.1517932216

3.3.25 Vendor Requirements

Service Level Agreements (SLA) will be outlined and discussed, along with the need for required notification when an employee transfers departments', leaves the company, or is terminated that had direct network connectivity into Alpha network. An example SLA developed for Alpha is below.

Service Level Agreement (SLA)

for *Vendor*

by

Alpha

Effective Date: 02-22-2019

Document Owner:	

Version

Version	Date	Description	Author
1.0	02-22-2019	Service Level Agreement	

Approval

(By signing below, all Approvers agree to all terms and conditions outlined in this Agreement.)

Approvers	Role	Signed	Approval Date
Alpha	Customer		2-22-2019
Vendor	Service Provider		2-22-2019

Agreement Overview

This Agreement represents a Service Level Agreement ("SLA" or "Agreement") between Alpha and Vendor (Service Provider) for the provisioning of IT/OT services required to support and sustain the Product or Service.

This Agreement remains valid until superseded by a revised agreement mutually endorsed by the stakeholders.

This Agreement outlines the parameters of all IT/OT services covered as they are mutually understood by the primary stakeholders. This Agreement does not supersede current processes and procedures unless explicitly stated herein.

Goals and Objectives

The **purpose** of this Agreement is to ensure that the proper elements and commitments are in place to provide consistent IT/OT service support and delivery to Alpha by the Service Provider(s).

The **goal** of this Agreement is to obtain mutual understanding for IT/OT services provision between the Service Provider and Alpha.

The **objectives** of this Agreement are to:

- Provide clear reference to service ownership, accountability, roles and/or responsibilities.
- Present a clear, concise and measurable description of service provision to the customer.
- Match perceptions of expected service provision with actual service support and delivery.

Stakeholders

The following Service Provider and Alpha will be used as the basis of the Agreement and represent the **primary stakeholders** associated with this SLA:

IT Service Provider: Service Provider
IT/OT Customer: Alpha

Periodic Review

This Agreement is valid from the **Effective Date** outlined herein and is valid until further notice. This Agreement should be reviewed at a minimum once per fiscal year; however, in lieu of a review during any period specified, the current Agreement will remain in effect.

The **Business Relationship Manager** ("Document Owner") is responsible for facilitating regular reviews of this document. Contents of this document may be amended as required, provided mutual agreement is obtained from the primary stakeholders and communicated to all affected parties. The Document Owner will incorporate all subsequent revisions and obtain mutual agreements / approvals as required.

Business Relationship Manager: Alpha (President)
Review Period: Yearly (12 months)
Previous Review Date: 02-22-2019
Next Review Date: 02-22-2020

Service Agreement

The following detailed service parameters are the responsibility of the Service Provider in the ongoing support of this Agreement.

Service Scope

The following Services are covered by this Agreement:

- Apply system updates to manufacturing environment per vendor's recommendation
- Apply system updates to IT equipment when patches are released per vendor.
- Backup configure information for all IT/OT equipment within Alpha
- Ensure cybersecurity tools are operating correctly within the environment
- Provide liaison service between OT vendor and Alpha
- Product recommendation for new equipment being purchased and installed with Alpha's manufacturing environment
- Manned telephone support
- Monitored email support
- Remote assistance using Remote Desktop and a Virtual Private Network where available
- Planned or Emergency Onsite assistance (extra costs apply)
- Monthly system health check

Customer Requirements

Alpha's responsibilities and/or requirements in support of this Agreement include:

- Payment for all support costs at the agreed interval.
- Reasonable availability of customer representative(s) when resolving a service related incident or request.

Service Provider Requirements

Service Provider responsibilities and/or requirements in support of this Agreement include:

- Meeting response times associated with service related incidents.
- Appropriate notification to Customer for all scheduled maintenance.

Service Assumptions

Assumptions related to in-scope services and/or components include:

Changes to services will be communicated and documented to all stakeholders.

Service Management

Effective support of in-scope services is a result of maintaining consistent service levels. The following sections provide relevant details on service availability, monitoring of in-scope services and related components.

Service Availability

Coverage parameters specific to the service(s) covered in this Agreement are as follows:

- Telephone support: 8:00 A.M. to 5:00 P.M. Monday – Friday
    - Calls received out of office hours will be forwarded to a mobile phone and best efforts will be made to answer / action the call, however there will be a backup answer phone service
- Email support: Monitored 8:00 A.M. to 5:00 P.M. Monday – Friday
    - Emails received outside of office hours will be collected, however no action can be guaranteed until the next working day
- Onsite assistance guaranteed within 72 hours during the business week

Service Requests

In support of services outlined in this Agreement, the Service Provider will respond to service related incidents and/or requests submitted by Alpha within the following time frames:

- 0-8 hours (during business hours) for issues classified as **High** priority.
- Within 48 hours for issues classified as **Medium** priority.
- Within 5 working days for issues classified as **Low** priority.

Remote assistance will be provided in-line with the above timescales dependent on the priority of the support request.

Personal Changes:

When an individual user with remote access leaves service provider, is transferred, or is terminated the service provider will notify Alpha. If user had access to Alpha's network, that access will be disabled, or deleted as soon as possible. System account passwords the service provider had will need to be changed to ensure user access into the network has been completely removed.

DETECT

3.3.26 Event Logging

Devices within manufacturing system shall be configured to send log data to central repository (Syslog Server) when supported. Logs sent from devices allow additional forensics analysis, which will be useful after a cybersecurity event. Alpha logs all devices event alerts to central log server for review and archive purpose. Recorded events help identify any malicious activity within the manufacturing systems. Logs will be checked periodically looking for abnormal alerts being generated from manufacturing system. See reference for additional information.

3.3.27 Event Impacts

Logged events will be examined to determine the impact if any against the manufacturing system. Events impacting manufacturing system will be reviewed to determine correlation with risk assessment outcomes. Once correlation has been completed action will be taken if required to increase cybersecurity posture to lessen future threats.

3.3.28 Monitor

All personnel within the manufacturing system will be required to sign-in upon entering ICS environment with date and time of entry, including when leaving work space. Any person found in violation of mandatory sign-in/sign-out sheet will be escorted out of the manufacturing environment. Individuals will be challenged to ensure they are employees or are being escorted around the environment.

All network switches will be configured for port security, so unauthorized devices won't be able to access manufacturing network without prior approval.

Weekly wireless scans will be completed using a laptop within manufacturing system. Rouge or unknown wireless devices will be brought to management's attention for additional review.

Periodic hardware and software scans with be performed on devices within manufacturing system to detect any unauthorized hardware or software changes.

Switch logs within manufacturing system will be checked regularly to ensure no rogue devices have attempted to connect. Output from switch logs will be compared against hardware inventory performed in.

Manufacturing system environment will be monitored for unauthorized personnel, connections, devices, access points, and software using multiple tools. Each tool provides a specify purpose and is designed to record and archive data. Syslog monitoring will be configured to captures all system generated logs and stored for archival/forensics purposes. Inventory management is used to detect rogue devices, include unauthorized software installations via scheduled scans within the manufacturing system.

3.3.29 Forensics

Syslog server will be used for collection of system logs. Logs can analysis to understand the attack target along with determining the method that was used during the attack against devices within manufacturing system.

3.3.30 Ensure resources are maintained

Systems performance and resources can have a drastic effect on manufacturing process. Individual in charge of manufacturing systems will be responsible for performing daily checks on all systems within the manufacturing system environment (OT). Checks will include, but not limited to physical observation of all operational components ensuring any warning lights or other area of concern are investigated further. System logs of all manufacturing devices will be checked at the beginning and end of every shift looking for any deviation from the normal baseline performance.

3.3.31 Detect non-essential capabilities

System scanning/auditing tool will be used to identify non-essential software applications installed on devices within manufacturing system. Software not required for operations will be removed and baseline configuration updated to reflect new configuration state.

RESPOND

3.3.32 Fire Protection Systems

Fire protection for a manufacturing environment should be designed to safeguard electrical equipment. Manufacturing systems requiring protection can be PLCs', HMIs', Robots, Machining equipment, computers and other required devices. Fire Protection should be designed and implemented to protect human life first and equipment second. Installed fire protection systems will be certified compliant with existing/new environment by a licensed and accredited vendor. Check industry standards for any required baselines.

3.3.33 Emergency and Safety Systems

Emergency and Safety Systems will compile with Local, State, and Federal laws. This is to include safety regulations for workers' safety from Occupational Safety and Health

Administration (OSHA). Industry regulation for safety will be followed per guidance from regulating industry.

Fire Protection Systems will compile with Local, State, and Federal laws. This is to include Fire Protection Systems specially designed for manufacturing process. Fire Protection System will place emphasis on human safety first and for most, before concern for manufacturing system. Fire Protection Systems will be checked minimum once per year unless shorter intervals are required from superseding regulations.

Only Industry approved Environmental Controls will be used within manufacturing systems, to included compliance with all Local, State, Federal laws. Environmental Control will be implemented to place human/community safety first before manufacturing systems.

3.3.34 Detected Events

Detected cybersecurity event notification will be investigated to determine root cause and appropriate remediation steps will be taken to clear events returning the organization / manufacturing system to known good operating state.

3.3.35 Vulnerability Management Process

Vulnerability management is an essential component of any information security program and the process of vulnerability assessment is vital to effective vulnerability management

Vulnerability Scanning and Management Tool

Tenable- Nessus will be used to perform vulnerability scans. The Results report generated by Nessus at the completion of the scan, is then fed into NamicSoft which is a vulnerability management, parsing and reporting tool.

NamicSoft can create customized reports and logically group results for a consistent workflow within the organization. The reports are reviewed by the foreman and then shared with the machine operators.

Vulnerability Scan Targets

All devices connected to both Control and Supervisory network segments are scanned. There is a policy and scan configured for scanning all network segments of Alpha.

A new scan can be established, or an existing one changed, by submitting a request to the Foreman.

Vulnerability Scan Frequency/Schedule

Scans are performed by engaging the IT Contractor on an on-demand, per-request basis as needed. The Supervisor shall make provisions for an assessment once per month. Running

vulnerability scans using automated tools once per month will ensure continuous monitoring of the Manufacturing system is in place.

- All IT/OT device scans should be scheduled between the 1st and the 15th of each month. This accommodates critical patches released by vendors such as Microsoft.
- All device scans should be performed during hours appropriate to the business needs of the organization and to minimize disruption to normal operations
- Any new device discovered needs to be classified under its appropriate group.

General Rules

- The Supervisor or machine operators will not make any temporary changes to information systems, for the sole purpose of "passing" an assessment. Vulnerabilities on information systems shall be mitigated and eliminated through proper analyses and repair methodologies.
- No devices connected to the network shall be specifically configured to block vulnerability scans from authorized scanning engines.
- Use caution when running vulnerability scans against OT Networks such as the Supervisory LAN and Control LAN Network. Scans should be scheduled off hours and during periods of maintenance.
- It is recommended to run authenticated scans from the vulnerability scanner.

Vulnerability Reporting

Upon completion of a vulnerability scan, the data is fed into NamicSoft out of which report is generated. A report will always be generated as proof that an assessment occurred.

All IT/OT devices are organized into appropriate groups in NamicSoft as per the system they reside in. A device may belong to one or more systems. Reporting is done system wide so that the devices and vulnerabilities can more easily be distributed to the Supervisor and machine operators. Below is a table of type of reports that will be sent out.

Status Reports	Frequency	Purpose
Host table with affected vulnerabilities	Monthly	Information is presented for each host.
Vulnerability Assessment Report	Monthly	Information is presented for both scanned networks.
Host specific report	Ad-hoc	Information is presented for requested host.
Mitigated vulnerabilities report	Post remediation	Upon re-scanning a host to check if vulnerabilities have been mitigated or not

Remediation Management and Priorities

All vulnerabilities discovered must be analyzed by the Supervisor and Control Engineers with assistance from IT/OT Contractor if needed to decide on the next course of action.

All vulnerabilities discovered should be remediated.

The below chart should be used for remediation timelines.

Severity	Description	Remediation time
Critical	Nessus uses Common Vulnerability Scoring System (CVSS) for rating vulnerabilities. A Critical vulnerability has a CVSS base score of 9.0 or 10.	15 days of discovery
High	High-severity vulnerabilities have a CVSS score between 7.0 and 8.9.	30 days of discovery
Medium	Medium-severity vulnerabilities have a CVSS score of 4.0 to 6.9 and can be mitigated within an extended time frame.	45 days of discovery
Low	Low-severity vulnerabilities are defined with a CVSS score of 1.0 to 3.9. Not all low vulnerabilities can be mitigated easily due to applications and normal operating system operations. These should be documented	180 days of discovery
Info	Info level do not present security risk and are listed for informational purposes only. It is optional to remediate them.	Not required to remediate

Exceptions Management

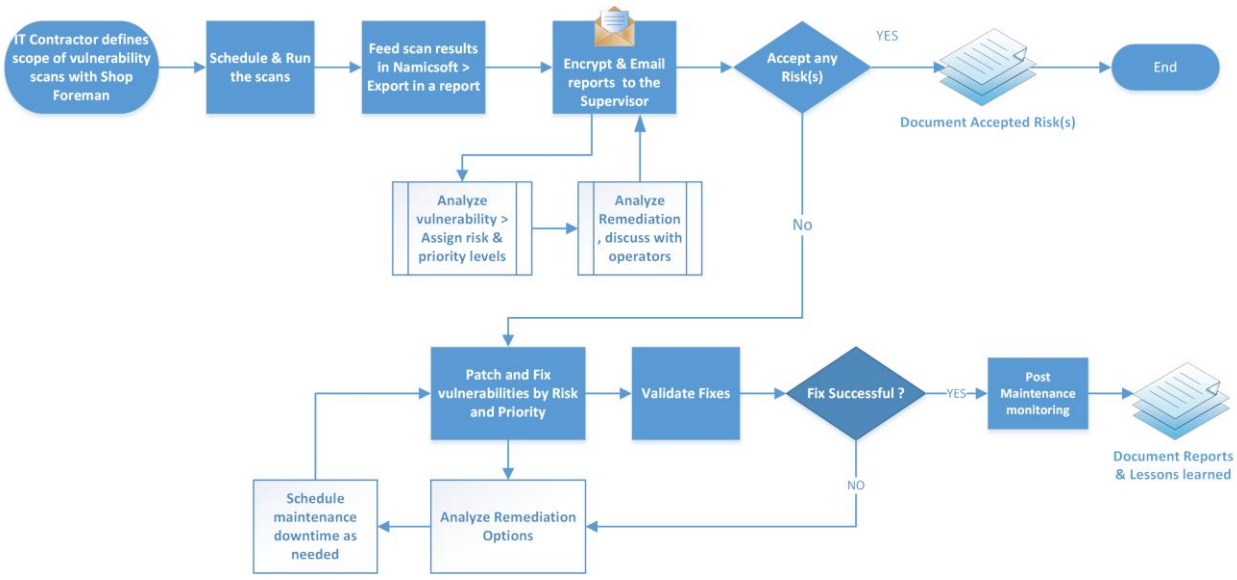
Any exceptions to this policy, such as exemption from the vulnerability assessment process must be internally discussed and approved by the Foreman.

Vulnerabilities may exist in operating systems, applications, web applications or OT devices. While every effort must be made to correct issues, some vulnerabilities cannot be remediated. Vendors may have appliances that are not patched, services may be exposed for proper application operations, and systems may still be commissioned that are considered end-of-life by the developer and manufacturer. In these cases, additional protections may be required to mitigate the vulnerability. Exceptions may also be made so that the vulnerabilities are not identified as items of risk to the system and organization.

False Positives identification may be documented through emails or the NamicSoft tool with the security staff. Acceptable Risk exceptions must be requested through the IT Team with an explanation containing:

- Mitigating controls – what changes, tools, or procedures have been implemented to minimize the risk.
- Risk acceptance explanation – details as to why this risk is not relevant to the company and systems.
- Risk analysis – if the vulnerability is indeed compromised, what risk and systems will be affected.

Process Overview



Alpha Manufacturing Vulnerability Management Process

RECOVER

3.3.36 Recovery Plan

Purpose and Objective:
Alpha developed this incident recovery plan (IRP) to be used in the event of a significant disruption to the features listed in the table below. The goal of this plan is to outline the key recovery steps to be performed during and after a disruption working to return to normal operations as quickly as possible.

Scope:

The scope of this IRP document addresses technical recovery only in the event of a significant disruption. The intent of the IRP is to be used in conjunction with the business continuity plan (BCP) Alpha developed. The IRP is a subset of the overall recovery process contained in the BCP. Plans for the recovery of people, infrastructure, and internal and external dependencies not directly relevant to the technical recovery outlined herein are included in the Business Continuity Plan and/or the Corporate Incident Response and Incident Management plans that Alpha has in place.

The specific objectives of this incident recovery plan are to:

- Establish a core group of leaders to assess the technical ramifications of a situation;
- Set technical priorities for the recovery team during the recovery period;
- Minimize the impact of the disruption to the impacted features and business groups;
- Stage restoration of operations back to full processing capabilities;
- Enable rollback operations once disruption has been resolved and determined appropriate by recovery team.

Within the recovery procedures there are significant dependencies between and supporting technical groups within and outside Alpha. This plan is designed to identify the steps that are expected to take to coordinate with other groups / vendors to enable their own recovery. This plan is not intended to outline all the steps or recovery procedures that other departments need to take in the event of a disruption, or in the recovery from a disruption.

Incident Recovery Strategies:

The overall IR strategy of Alpha is summarized in Section 3.6 Incident Recovery Plan.

3.4 Risk Management Document Example

Risk Management Procedures

for

Alpha

Document Owner:	Supervisor, Alpha

Version

Version	Date	Description	Author
1.0	02-22-2018	Initial Draft	Supervisor
2.0	04-21-2018	Major changes to the initial draft	Supervisor

Approval

(By signing below, all Approvers agree to all terms and conditions outlined in this document.)

Approvers	Role	Signed	Approval Date
	President		4-22-2018

A risk is an event or condition that, if it occurs, could have a positive or negative effect on a project's objectives. Risk Management is the process of identifying, assessing, responding to, monitoring, and reporting risks. This Risk Management Plan defines how risks associated with Alpha will be identified, analyzed, and managed. This document can be used by the Management to foresee risks, estimate impacts, and define responses to issues.

3.4.1 Scope

Any employee, contractor, or individual with access to the organization's systems or data.

3.4.2 Risk Management Process

Process

The overall process involves Identifying, Analysis, Categorizing, Reporting and Remediating. Risks will be identified as early as possible in the project to minimize their impact. The steps for accomplishing this are outlined in the following sections.

Risk Identification

Risk identification will involve the shop Supervisor, Machine operators, evaluation of environmental factors, organizational culture and the project management plan including the project scope. There are many different types of threats that can affect IT and OT infrastructure. These can include:

- Technical threats — disruption caused by technological advances or failures
- Structural threats — anything related to the building that houses your IT/OT infrastructure that could cause it to be harmed
- Financial threats — If the business loses funding or experiences another significant financial change
- Human threats — human error or loss of important individual
- Natural threats — weather and natural disasters such as earthquakes, tornadoes, and floods

A Risk Management Log will be generated and updated as needed, a sample of which is shown in the latter half of this document.

Software tools such as CSET[9] will be used to perform RISK Assessments. The reports generated will be discussed with the President.

Additionally, the plant operators and Supervisor will subscribe to NVD, USCERT, ICS-CERT and ISACS alert feeds to keep up with the latest vulnerabilities.

This is an iterative process. As the program progresses, more information will be gained about the program and the risk statement will be adjusted to reflect the current understanding. New risks will be identified as the project progresses through the life cycle.

Risk Analysis

All risks identified either manually or via CSET will be assessed to identify impact on operations. Qualification will be used to determine which risks are the top risks and which ones can be ignored.

[9] CSET: https://ics-cert.us-cert.gov/Assessments

Qualitative Risk Analysis

The probability and impact of occurrence for each identified risk will be assessed by the shop supervisor with input from the machine operators using the following approach:

Probability

- High – Greater than <70%> probability of occurrence in a year
- Medium – Between <30%> and <70%> probability of occurrence in a year
- Low – Below <30%> probability of occurrence in a year

Impact

- High – Risk that has the potential to greatly impact project cost, project schedule or performance
- Medium – Risk that has the potential to slightly impact project cost, project schedule or performance
- Low – Risk that has relatively minor impact on cost, schedule or performance

Quantitative Risk Analysis

This involves assigning a numeric value to the risk calculated as the product of probability of occurrence and impact score. Analysis of risk events that have been prioritized using the qualitative risk analysis process and their effect on project activities will be estimated, a numerical rating applied to each risk based on this analysis, and then documented in the risk management log.

3.4.3 Risk Monitor and Control

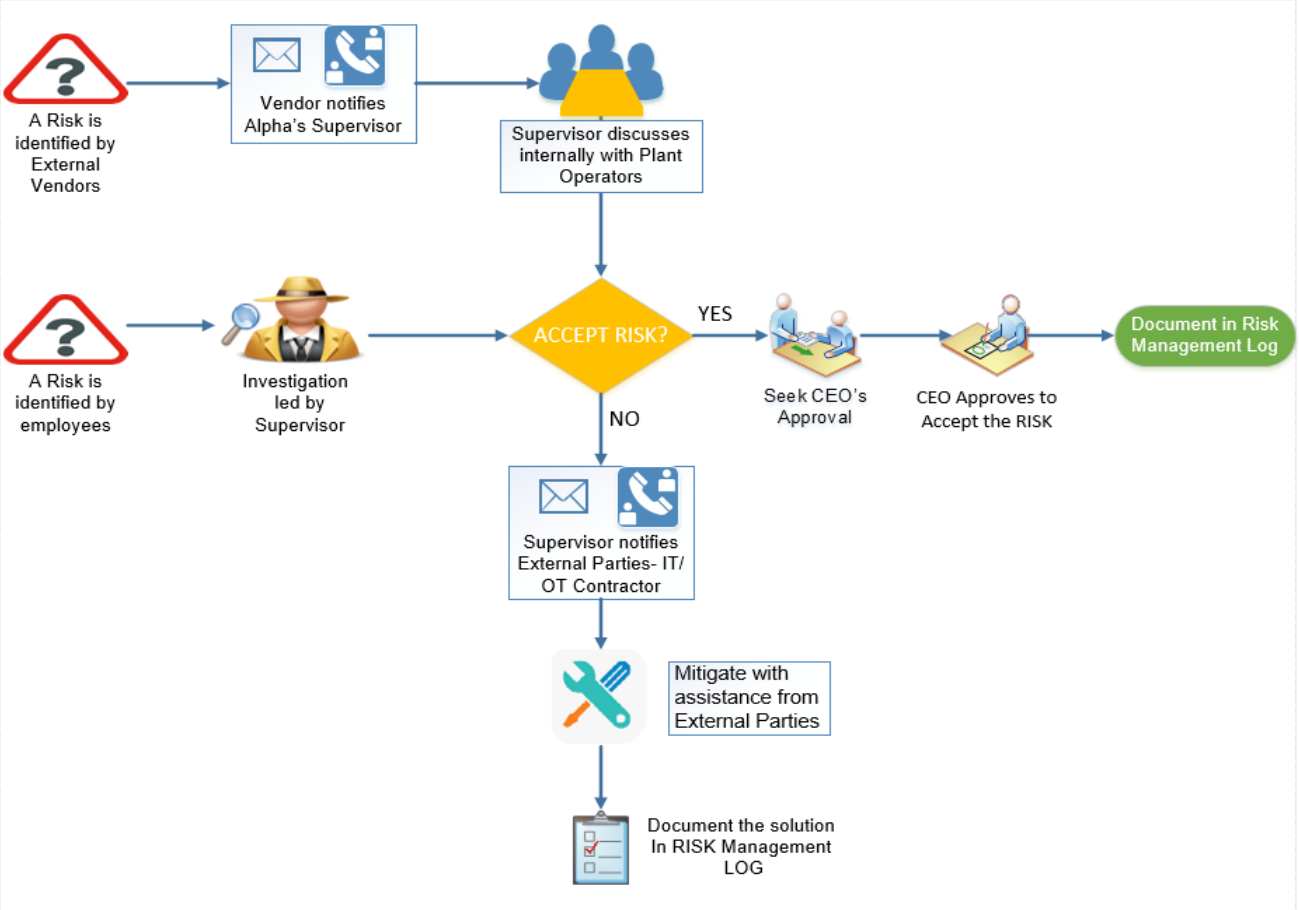
The Supervisor and IT/OT contractors will conduct yearly risk assessments which includes CSET assessments, vulnerability scans of the manufacturing system taking into account vulnerabilities and potential impact to the manufacturing operations. An identified risk can be bought to Supervisor's attention either by Alpha's employees or by external contractors.

The IT Contractor will scan the IT and OT assets when called upon; with Nessus to monitor for any software-based risks. Nessus results will be fed into NamicSoft. Reports will be generated out of this tool and shared with the Supervisor. Any other type of risks like hardware based, physical, environmental will be identified and documented manually.

All software-based vulnerabilities discovered using Nessus should be mitigated as per the Vulnerability Management Plan.

If a software vulnerability has been remediated; a Nessus scan be re-run to see whether the situation has changed in a way that affects the manufacturing operations. For any corrective action has been taken, the risk management log will be updated.

3.4.4 Risk Notification Process



3.4.5 Risk Response / Remediation Strategy

For each major risk, one of the following approaches will be selected to address it:

- **Avoid** – eliminate the threat by eliminating the cause
- **Mitigate** – Identify ways to reduce the probability or the impact of the risk
- **Accept** – Nothing will be done
- **Transfer** – Make another party responsible for the risk (buy insurance, outsourcing, etc.)

For each risk that will be mitigated, the Supervisor and operators will identify ways to prevent the risk from re-occurring or reduce its impact or probability of occurring. This may include

- Prototyping.
- Adding tasks to the project schedule
- Determining and allocating resources.

For each risk that needs to be "Accepted", a document containing the list of accepted risks will be maintained by the Supervisor.

The Supervisor will reach out to an IT/OT Contractor for any risks and request remediation assistance.

3.4.6 Risk Appetite

Risk appetite - is the broad-based amount of risk an organization is willing to accept in pursuit of its mission/vision. [4]

Risk Appetite scale [5]:

- High - the manufacturing system accepts disciplined risk taking because the organization has determined the potential benefits outweigh the potential risk.
- Moderate - the manufacturing system accepts some risk taking, assuming the organization has reviewed the potential benefits and potential risks.
- Low - the manufacturing system accepts minimal risk taking.
- None - the manufacturing system accepts no risk taking because the risk is intolerable.

3.4.7 Risk Tolerance

Risk tolerance - is the acceptable level of variance in performance relative to the achievement of objectives. In setting risk tolerance levels, management considers the relative importance of the related objectives and aligns risk tolerance with risk appetite. [4]

Risk tolerance scale [6]:

- Low - the level of risk will not considerably impact the ability of the manufacturing system to meet its mission objectives.
- Moderate - the level of risk may impact the ability of the manufacturing system to meet its mission objectives.
- High - the level of risk will significantly impact the ability of the manufacturing system to meet its mission objectives.

3.4.8 Risk Categories

Risk Categories are used to classify a risk. This table represents a sample of potential categories that may be applied to each risk.

- Safety - the risk that human and/or environmental safety are compromised by an incident in the manufacturing system.
- Production - the risk that product quality and/or production goals are compromised by an incident in the manufacturing system.
- Trade Secrets - the risk that intellectual property and sensitive business data are compromised by an incident in the manufacturing system.

Risk Category	Risk Tolerance	Risk Appetite	Mission Objectives
Safety	Moderate	Moderate	Maintain human safety
			Maintain environmental safety
Production	Moderate	High	Maintain quality of product
			Maintain production goals
Trade Secrets	Moderate	Moderate	Maintain trade secrets

3.4.9 Risk Reporting

This table describes the frequency and format of how the Supervisor will document, analyze, communicate, and escalate outcomes of the risk management processes.

Reporting Method	Description	Frequency
Risk Management log	A document to report the results of risk identification, analysis, and response planning	Twice a year
CSET Report	A document describing Risk assessment results	Twice a year
NamicSoft report	A document containing results of Nessus vulnerability scans.	Manual/Post vulnerability assessment

The Supervisor will share the results of risk assessments (either the Risk Management Log or CSET Report) with the appropriate stakeholders of Alpha and the President.

3.4.10 Sample Risk Management Log

A Risk Log will be maintained by the Supervisor and Book keeper. These will be reviewed in the project team meetings. This log captures the results of a qualitative and quantitative risk analysis and the results of planning for response.

Risk	**Category (Technical, Management, Contractual, External)**	**Probability (High /** Likely to occur =3, Medium / May or May not occur =2, Low / Unlikely =1)	**Impact (**High = 3, Medium = 2 , Low =1)	**Score (Product of Probability x Impact 1-3 Green 4-6 Yellow 7-9 - Red)**	**Risk Mitigation Strategy** (e.g. Avoid, Transfer, Mitigate or Accept the risk)	**Actions required**	**Status (Open, closed, In Progress)**	**Due Date**

3.4.11 Periodic Review

This document will be reviewed and updated annually by the Supervisor in consultation with the machine operators.

Annual reviews will be conducted determining component value within the manufacturing process being performed. Values will be used to determine required devices for continued manufacturing process and the effects if a cyber incident occurs against a device.

3.4.12 Asset Criticality Matrix

After a list of Alpha's assets or systems of value requiring protection have been identified by the Hardware Inventory process, they will be assigned a value. Asset Value is the degree of impact that would be caused by the unavailability, malfunctioning or destruction of the asset.

2004 Alpha will use the following scale to calculate Asset value.

ASSET VALUE	
Critical	10
High	7-9
Medium	3-6
Low	1-3

2005

2006 **Critica**l – Loss or damage of this asset would have grave / serious impact to the Operations of
2007 the Manufacturing system directly impacting production. This can result in total loss of primary
2008 services, core processes or functions. These assets are single point of failure.

2009 **High** - Loss or damage of this asset would have serious impact to the Operations of the
2010 Manufacturing system directly impacting production. This can result in major loss of primary
2011 services, core processes or functions. These assets can also be single point of failure.

2012 **Medium** - Loss or damage of this asset would have moderate impact to the Operations of the
2013 Manufacturing system or Production. This can result in some loss of primary services, core
2014 processes or functions.

2015 **Low** - Loss or damage of this asset would have minor to no impact on the Operations of the
2016 Manufacturing system or Production. This can result in little or no loss of primary services, core
2017 processes or functions.

2018

A list of assets belonging to Alpha with assigned value is presented below.

Asset	Value	Numeric Value
IT / Communication Systems	High	8
OT / Field Devices – PLC, HMI	Critical	10
OT / Machining Stations	High	8
OT / Robots	High	9
Electrical Systems	Critical	10
Utility Systems	Medium	6
Site	Medium	6

3.4.13 Definitions and Acronyms

IT	Information Technology which includes devices such as servers, laptops, workstations, switches and routers.
OT	Operational Technology which includes Industrial control system devices that are used by the manufacturing process.
Vulnerability	A weakness or a flaw in the system which an attacker can exploit to gain access.

3.4.14 References

1. Risk Management plan – Maryland Department of Information Technology
doit.maryland.gov/SDLC/Documents/Project%20Risk%20Managment%20Plan.doc

2. Sample Risk Management plan – State of North Dakota
https://www.nd.gov/itd/sites/itd/files/legacy/services/pm/risk-management-plan-sample.pdf

3. Office of Management and Budget, "Management's Responsibility for Enterprise Risk Management and Internal Control", *Office of Management and Budget,* OMB Circular No. A-123, 2016. [Online]. Available: https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-17.pdf.

4. United States Agency for International Development, "U.S. Agency for International Development Risk Appetite Statement", *United States Agency for International Development*, 2018. [Online]. Available: https://www.usaid.gov/sites/default/files/documents/1868/USAID_Risk-Appetite-Statement_Jun2018.pdf.

5. Office of the Comptroller of the Currency, "Enterprise Risk Appetite Statement", *Office of the Comptroller of the Currency*, 2016. [Online]. Available: https://www.occ.treas.gov/publications/publications-by-type/other-publications-reports/risk-appetite-statement.pdf.

3.5 Incident Response Plan Document Example

Incident Response Plan

for

Alpha

Document Owner:	Supervisor, Alpha

Version

Version	Date	Description	Author
1.0	02-22-2018	Initial Draft	Supervisor
2.0	04-21-2018	Major changes to the initial draft	Supervisor

Approval

(By signing below, all Approvers agree to all terms and conditions outlined in this document.)

Approvers	Role	Signed	Approval Date
	President		4-22-2018

3.5.1 Statement of Management commitment

Alpha's leadership team is committed to information security and appropriate incident response to accidental or deliberate incident within the company. Alpha has established the Incident Response Program to establish an actionable information security incident handling capability that includes preparation, detection, analysis, containment, recovery, and reporting for information security incidents. Alpha's President oversees the Incident Response Program as a whole, supports and funds maintenance of the program and ensures that resources are appropriately maintained for preparedness.

3.5.2 Purpose

An incident can be defined as any event that, if unaddressed, may lead to a business interruption or loss. This document describes the plan for responding to information security incidents at Alpha Inc. It defines the roles and responsibilities of participants, characterization of incidents, relationships to other policies and procedures, and reporting requirements. The purpose of this

plan is to detect and react to security incidents, determine their scope and risk, respond appropriately to the incident, communicate the results and risk to all stakeholders, and reduce the likelihood of the incident from reoccurring.

This Plan is to be executed during or after a cybersecurity incident.

3.5.3 Scope

This plan applies to all the employees of Alpha.

3.5.4 Roles and Responsibilities

The Alpha Incident Response Team is comprised of:

ROLE	RESPONSIBILITIES	CONTACT DETAILS
Supervisor	• Supervise other employees and working of the organization. • Serves as a primary point of contact for any type of incident • Making sure that all employees understand how to identify and report a suspected or actual security incident • Leading the investigation for any type of incident, initiating the Security Incident Response Plan, filling out the Incident Report Form and reporting status to the President as needed. • Documenting details of all incidents.	Name: Phone: Email:
Machine Operators	• Reporting a suspected or actual security incident to the Supervisor. • Reporting any other operational issues or concerns to the Supervisor • Complying with the security policies and procedures of Alpha	Names: Phone: Email:
IT / OT Contractors	• Manages access to systems and applications for internal staff. • Complying with the security policies and procedures of Alpha • Assist in investigation, troubleshooting and resolving any IT/OT related incident summoned for. • Advising the Supervisor for any recommendations to procedures, policies and best practices.	Name: Phone: Email:

3.5.5 Categories of Incidents

Alpha defines the following categories/types of incident for internal classification. These have been mentioned in the Incident Reporting Form as well.

- Intrusion
- Denial of Service
- Loss of Power
- Virus / Malware
- Social Engineering (Phishing, Phone, Email, etc.)
- Data Breach
- Hardware Stolen
- User account compromise
- System Misuse
- Technical Vulnerability

3.5.6 Severity Classification

The Severity of an incident is determined based on the impact to the company and the urgency of restoration.

SEVERITY	DEFINITION
High	• All users of the company are affected • Work stoppage situation • The incident involves sensitive data breach. • The incident threatens Alpha's operational goals • There is no viable workaround
Medium	• There is a viable workaround • Moderate to Low impact to the Operations. • Service interruption potentially affects specific users and does not involve sensitive or personal data breach.
Low	• No impact to operations. • Service interruption potentially affects only one person and does not involve sensitive or personal data breach.

3.5.7 Restoration Priorities

RESTORATION PRIORITIES	DEFINITION
High	• Service Restoration must be completed immediately, or significant loss of revenue, reputation, or productivity will occur.
Medium	• Service Restoration must be completed within two business days or there is a potential for significant loss of revenue, reputation or productivity.
Low	• Service Restoration can be delayed up to three or more business days without loss of revenue, reputation or productivity.

3.5.8 Incident Alert Thresholds

Manufacturing system alert thresholds will be configured as such to limit the number of false positives generated while working to capture valid data which could be an indication of cybersecurity incident. False-positives are classified as events indicating a problem, but further examination are not actual issues. Important, false-positives should always be treated as normal alerts requiring attention until determined otherwise.

3.5.9 Incident Response Policy

1. An incident upon detection or being reported needs to be thoroughly investigated as per the process defined under "Detection and Analysis" step of the IR process in the next section. The investigation may be performed by the Supervisor or by convening an IR Team.
2. The incident needs to be classified as per the categories defined previously.
3. Upon Investigation, the impact to the Manufacturing system must be determined. The IR Team may co-relate detected event information with Risk assessment outcomes to achieve perspective on the incident impact across the Organization. The incident will accordingly be assigned a Severity level and reported to the President. The Incident Report Template form should be used for this purpose.

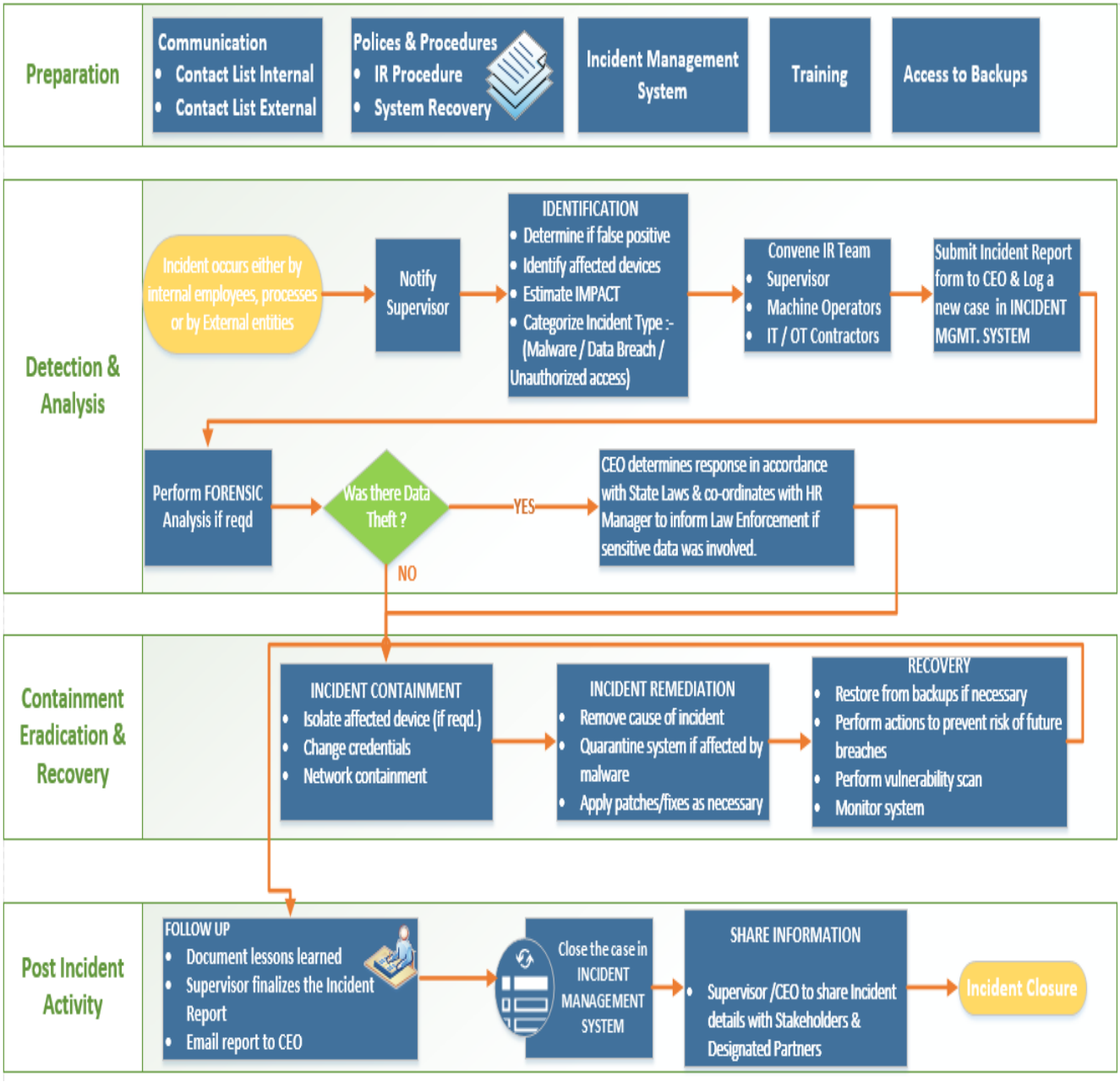
4. During the "Detection and Analysis" step, detailed troubleshooting or forensic analysis should be performed to determine the root cause. This may be done using in place log management tools or commercial products such as Wireshark.
5. Upon investigation, the incident must be mitigated as per the "Containment, Eradication and Recovery" step of the IR Process.
6. The Supervisor upon consultation with the President. The Incident Report Template form should be used for this purpose.
7. will communicate, co-ordinate and share incident response plan with Alpha's stakeholders.
8. The President will share information about any cybersecurity incidents and its mitigation with its designated sharing partners.
9. The overall Incident Response program and plan will be revised or improved upon after every incident. Procedures must be updated regularly to address evolving threats such as APTs, Organizational changes, Manufacturing changes and/or after any problems discovered during implementation, execution or testing
10. User awareness Training and Testing procedures will be updates after every incident.
11. The Supervisor will communicate any changes or updates made to this policy.

3.5.10 Incident Plan Response Steps / Workflow

The NIST Computer Security Incident Handling [1] Guide divides the incident response lifecycle into the following four steps:

1. Preparation
2. Detection and Analysis
3. Containment, Eradication and Recovery
4. Post-incident Activity

Alpha's IR process contains the following activities corresponding to each of the above steps:



3.5.11 Guidelines for Information Sharing

Interactions with Law Enforcement

- All communications with external law enforcement authorities should be made after consulting with the President.
- The Supervisor will co-ordinate with the President to determine and share the minimum necessary information as required for incident response.

Communications Plan

- The President will share information about any cybersecurity incidents and its mitigation with its designated sharing partners. Refer to the Next section for additional details
- All public communications about an incident or incident response to external parties outside of Alpha are made in consultation with the President.
- The minimum information necessary to share for a particular incident is determined by the Supervisor in consultation with President or administrative authorities such as the bookkeeper.

3.5.12 Guidelines for Reporting to Stakeholders

Overview:

- The Supervisor will compile all the details of incident(s) occurred in consultation with the IT/OT consultant.
- The Supervisor will share the details in the IR Report Template form with President. This will be used to determine level of severity, allowing the company to plan according.
- The Company's leadership team consisting of President and HR Manager will make sure all facts have been gathered relating to the security incident before addressing any concerned with outside parties.
- The Company's response needs to be consistent ensuring message being delivered will not need to be retracted or changed due to lack of clarity.

Who will be responding:

- Depending on the severity of the security incident this role can be filled by President, or the Supervisor
- If the severity of a security incident requires additional resources, they should be contacted and brought in to help gather forensic information along with responding to inquiries.
    - Examples:
        - Legal Counsel
        - Forensic Investigator
        - IT consultant (Work in conjunction with IT Manager)
        - Security Consultant (Work in conjunction with IT Manager and Supervisors)
        - Law Enforcement (Depends on severity)

Notification:

- A Legal counsel will be contacted to oversee notification planning since the potential for legal actions against Alpha arising from security incident in question.
- If required, an outside Public Relations firm may be required depending on the severity level of the incident to help with crafting a response.

- The President will both approve all communication being sent out regarding a security incident.

Communications:

- The President will contact primary partners/vendors via phone call to inform them of the security incident. This should be done once all information has been gathered and a corporate response has been prepared.
- No voicemails will be left concerning the security incident in question. If recipient is unavailable schedule a follow up call.
- The Supervisor is the **only** Alpha employee authorized to call partners/vendors not already contacted by the President.
- Responses to partners/vendors should be scripted to ensure the delivered message is consistent, while ensuring only information regarding security incident are discussed.
- Email communication will be completed as a follow-up to a phone.
- Any email communications being sent will have additional proof reading completed by the President.
- Depending on the impact of security incident a Public Relation firm may be required to help with a response when providing communications via electronic or verbal.
- Media communication can **ONLY** be approved by President.

Restoring Trust:

- Alpha's President or Supervisor with the advice consultants and Forensic experts will notify partners/vendors and customers with the steps being taken to restore and strength system security.
- The Supervisor will discuss with employees what caused security incident and what is being done to avoid a similar issue in the future.
- Once the security incident has been resolved and all fact are known Alpha leadership team will provide a full report which will be made publicly available containing facts relating to the security incident, along with the steps being taking to safe guard IT/OT infrastructure ensuring this and future events don't happen again.

3.5.13 Incident Report Form Template

Incident Reporting Template Form			
Contact information			
Date Reported :		Time Reported:	
Name:	Title:	Dept:	
Office Phone:			
Details			
Date of Incident :		Time of Incident:	
Type of Incident - Check all that apply			
☐ Intrusion	☐ Social Engineering (Phishing, Phone,Email etc)	☐ Technical Vulnerability	
☐ Denial of Service	☐ Data breach	☐ System misuse	
☐ Loss of power	☐ Hardware stolen	☐ Others, pls specify	
☐ Virus / Malware	☐ User account compromise		
Incident Description			
Provide a brief description:			
Impact / Potential impact - Check all of the following that apply to this incident.			
☐ Loss / Compromise of Data	☐ Financial Loss		
☐ Damage to systems	☐ Other Organizations affected		
☐ Damage to public	☐ Damage to Integrity or Delivery of Goods, Services		
☐ System downtime	☐ Unknown at this time		
Provide a brief description:			
Affected System(s) information			
Host	IP	Application (if any)	O.S
Sensitivity of Data compromised (incase of Data loss)			
☐ Public (Information is already approved for release & unauthorized disclosure will not cause problems for the Company).			
☐ Internal Use (Information is intended for internal use within the Company or with other affiliated orgnaziations, business partners. Unauthorized disclosure may be against laws, regulations and may harm the Company or its business partners or its customers. For example: Email contacts, emails etc).			
☐ Confidential (Related to Privacy Violation. Information is private & sensitive in nature. It must be restricted to those with legitimate business need for access. Unauthorized disclosure is against laws, regulations and will harm the Company or its business partners or it Customers. For example: Trade secrets, Software code, Citizen's data etc).			
Details of the Data loss			
Provide a description of what was compromised:			
Follow up action taken so far			
☐ Law enforcement notified	☐ System disconnected from Network.		
☐ Restored backups	☐ Log files examined		
☐ AV Virus definition updated	☐ Any other action taken, pls specify		
☐ System reimaged or quarantined	☐ No action taken		
Supervisor's Name:	Supervisor's Signature:	Date:	

3.5.14 Definitions and Acronyms

President	Head of the organization. Serves as an escalation point.
HR Manager	An employee who deals with recruitment efforts and overall administration.
Incident	An event that is not part of normal operations that disrupts operational processes.
Supervisor	An employee who supervises other employees and working of the organization.
Vulnerability	A weakness or flaw in the system which an attacker can exploit to gain access to.
Vulnerability Scan	The act of scanning a device or network for vulnerabilities
Machine Operator	An employee who operates the manufacturing equipment and reports to Supervisor.
IT/OT Contractor	Non-employee(s) who are summoned on a need be basis for technical support or maintenance tasks related to IT and OT equipment.
Stakeholders	Business Owners, System Owners, Integrators, Vendors, Human Resources Offices, Physical and Personnel Security Offices, Legal Departments, Operations Personnel.

3.5.15 References

1. NIST Publication for handing Computer Security Incident
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

3.6 Incident Recovery Plan Document Example

Incident Recovery Plan

for

Alpha

Document Owner:	Supervisor, Alpha

Version

Version	Date	Description	Author
1.0	02-22-2018	Initial Draft	Supervisor
2.0	04-21-2018	Major changes to the initial draft	Supervisor

Approval

(By signing below, all Approvers agree to all terms and conditions outlined in this document.)

Approvers	Role	Signed	Approval Date
	President		4-22-2018

3.6.1 Scope

The scope and purpose of this document is to inventory all of infrastructure and capture information relevant to the Alpha's ability to recover its IT/OT environment from a cybersecurity incident. It, in turn also aims to provide an effective and efficient recovery effort.

3.6.2 Objectives

This plan has been developed to accomplish the following objectives:

1. Limit the magnitude of any loss by minimizing the duration of a critical application service interruption.
2. Assess damage, repair the damage, and activate the repaired computer center.
3. Manage the recovery operation in an organized and effective manner.
4. Prepare technology personnel to respond effectively in an incident recovery situation.

Incident Response:

This IR Plan is to be executed during or after a cybersecurity incident.

The person discovering the incident must notify the Supervisor, who collectively assume responsibility for deciding which - if any - aspects of the IR plan should be implemented, and for establishing communication with employees, management, partners and customers

3.6.3 RPO and RTO Targets

Alpha defines the following SLA's or Restoration times for operations recovery

Type of Incident	RTO [2]	RPO [2]	Restoration Priority
Environmental Disasters such as Fire, Flood.	72 hours	24 hours	High
Recovery from Virus/Malware attack	24 hours	24 hours	High
Recovery from user account compromise	24 hours	24 hours	Medium
Recovery from Data Breach	48 hours	24 hours	High
Hardware failure, System Parts Replacement	48 hours	24 hours	High

3.6.4 Incident Recovery Team

Alpha's Incident Recovery (IR) Team will consists of the following individuals.

ROLE	RESPONSIBILITIES
Supervisor	• Lead and oversee the entire DR process • Contact any Contractors/Vendors for assistance as needed. • Making sure that all employees understand their roles and responsibilities. • Update this document as per the Maintenance policy • Notify the President for any escalation issues.
President	• Assist the DR Lead (Supervisor) in their role as required.

	• Make any Business decisions that are out of scope for the Supervisor. • Serve as point of escalation for any issues.
Machine Operators	• Install, implement or assist in implementing any tools, hardware software and systems as required • Escalate any issues related to recovery to the Supervisor. • Complying with this plan.
	• Assist in Recovery, Troubleshooting and resolving any IT/OT related incident summoned for • Advising the Supervisor for any recommendations to procedures, policies and best practices. • Complying with this plan

Contact Information

3.6.5 Contact Information

Name	Title	Contact Type	Contact Information
Employee A	ABC	Work	555-555-5555 ext 2
		Mobile	
		Alternate	
		Email	
Employee B	ABC	Work	555-555-5555 ext 3
		Mobile	
		Alternate	
		Email	
Employee C	ABC	Work	555-555-5555 ext 4
		Mobile	
		Alternate	
		Email	

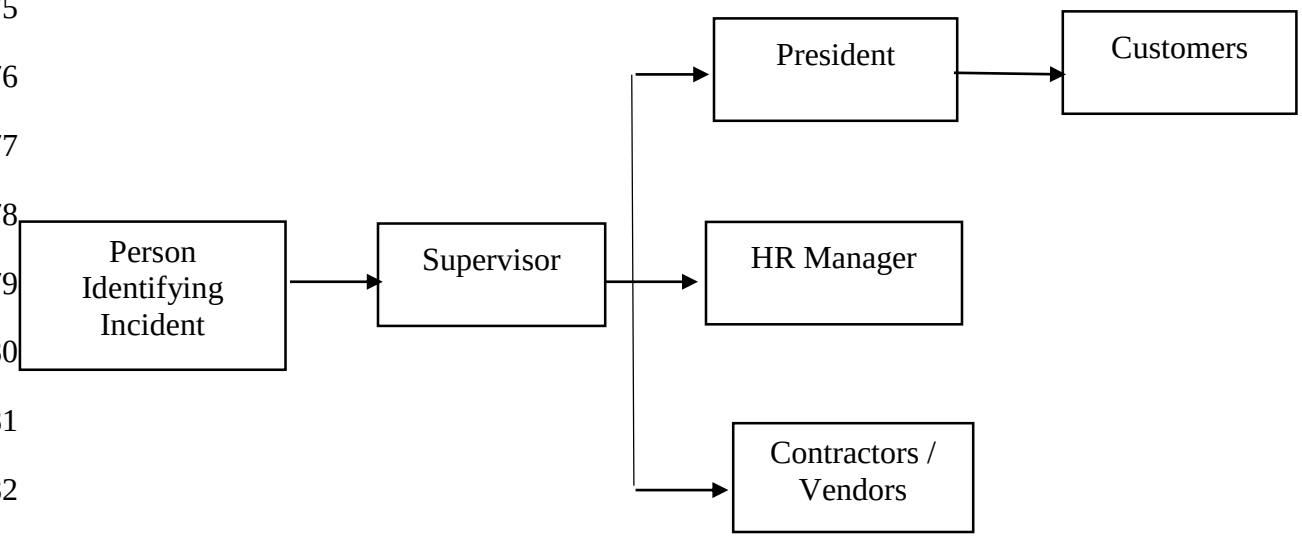
2271 **External Contacts**

Name	Title	Contact Type	Contact Information
Power Company		Work	
Account #		Mobile	
		Alternate	
		Email	
IT Contractor		Work	
Account #		Mobile	
		Alternate	
		Email	
OT Contractor		Work	
Account #		Mobile	
		Alternate	
		Email	
Network Provider		Work	
Account #		Mobile	
		Alternate	
		Email	
Telecom Carrier		Work	
Account #		Mobile	
		Alternate	
		Email	
Insurance Provider		Work	
Account #		Mobile	
		Alternate	
		Email	
Hardware Provider		Work	
Account #		Mobile	
		Email	

2272

2273

3.6.6 Notification Calling Tree



3.6.7 Communications

Notification

- The Supervisor in consultation Machine Operators will periodically update the President on the progress of Recovery Activities.
- A Legal Counsel may be hired to oversee notification planning since the potential for legal actions against Alpha arising from security incident in question.
- If required, an outside Public Relations firm may be required depending on the severity level of the incident to help with crafting a response.
- The President's approval is required for work with any outside agency.

Communications

- The President will contact primary partners/customers via phone call to inform them about Recovery activities. This should be done once all information has been gathered and a corporate response has been prepared.
- The Supervisor is the **ONLY** Alpha employee authorized to call partners/vendors not already contacted by the President.
- Responses to partners/vendors should be scripted to ensure the delivered message is consistent, while ensuring only information regarding security incident are discussed.
- Email communication will be completed as a follow-up to a phone.
- Any email communications being sent will have additional proof reading completed by the President.
- Depending on the impact of security incident a Public Relation firm may be required to help with a response when providing communications via electronic or verbal.

- Media communication can **ONLY** be approved by the President.

Restoring Trust

- Alpha's President or Supervisor with the advice consultants and Forensic experts will notify partners/vendors and customers with the steps being taken to restore and strength system security.
- The Supervisor will discuss with employees what caused security incident and what is being done to avoid a similar issue in the future.
- Once the security incident has been resolved and all fact are known, Alpha's leadership team will provide a full report which will be made publicly available containing facts relating to the security incident, along with the steps being taking to safe guard IT/OT infrastructure ensuring this and future events don't happen again.

3.6.8 Plan Testing and Maintenance

Maintenance

- The Incident Response Plan will be revised and updated after every recovery executed following a cybersecurity incident, Organizational changes, Manufacturing changes and/or after any problems discovered during implementation, execution or testing.
- The Supervisor will be responsible for updating the document in consultation with Machine Operators and other personnel as required.
- During Maintenance periods, any changes to the IR Team must be accounted for.

Testing

- Walkthroughs- IR Team members will verbally go through the specific steps as documented in the plan to confirm effectiveness, identify gaps or other weaknesses. The team should be familiar with procedures, equipment and operations.

- Simulations- An incident is simulated so that normal operations will not be interrupted. Hardware, software, personnel, communications, procedures, supplies and forms, documentation and utilities should be thoroughly tested in a simulation test.
- Full-Interruption Testing- IR Team members will perform a full-interruption test to activate a total IRP scenario. Caution must be exercised as this type of test disrupts normal operations.

3.6.9 Hardware Information

SYSTEM TYPE	HARDWARE INFORMATION	
IT Servers	**Hostname: POLARIS** System Model: Dell T5610 IP Address: 192.168.0.20 Location: Cabinet 101 Network: Control LAN Type: Physical Other: Eng. Workstation, Ubuntu Linux 12.04	**Hostname: MINTAKA** System Model: Dell R420 IP Address: 192.168.1.105 Location: Cabinet 101 Network: Control LAN Type: Physical Other: Robot Driver, Ubuntu Linux 14.04
	Hostname: VController1 System Model: Hyper-V VM IP Address: 192.168.1.103 Location: Robotics-VH Hyper-V Type: Virtual Network: Control LAN Other: Robot Controller, Ubuntu Linux 14.04	**Hostname: VController2** System Model: Hyper-V VM IP Address: 192.168.1.104 Location: Robotics-VH Hyper-V Host Type: Virtual Network: Control LAN Other: Robot Controller, Ubuntu Linux 14.04
	Hostname: Robotics-VH System Mode: Dell PE R420 Location: Cabinet 101 Type: Physical Other: Windows Server 2012 R2, Hyper-V Server	
Network Devices	**Model: RuggedCom RX1510** Management IP: 10.100.2. Location: Cabinet 101 Other: Boundary Router	**Model: Netgear GS724T** Management IP: 192.168.0.239 Location: Cabinet 101 Network: Supervisory Bus LAN Switch
	Model: Siemens i800 Management IP: 192.168.0.1 Location: Cabinet 101 Network: Control LAN Switch	
OT Devices	**Model: Beckhoff CX9020** IP Address: 192.168.0.20 Location: Cabinet 101 Function: PLC	**Model: Red Lion G310** IP Address: 192.168.0.98 Location: Cabinet 101 Function: HMI

	Model: Beagelbone Black IP Address: 192.168.1.101 - 104 Location: Work Cell Function: Machining Stations Quantity: 4	**Model: Robots** Manufacturer: KUKA Location: Work Cell Function: Robots Quantity: 2

3.6.10 Backup Strategy

SYSTEM TYPE	BACKUP STRATEGY
IT Servers	**POLARIS**: System Image - Thrice Weekly using Veeam, Directory Level Backup Monthly once **MINTAKA:** System Image - Daily using Veeam **vController1**: Full VM image Weekly once **vController2**: Full VM image Weekly once
Application Code	Code is checked into a secure central network share. Server hosting the network share is backed up using Veeam
Network Devices **Boundary Router**	**Frequency:** Quarterly: Manual using Manufacturer instructions. All configuration backup data will be saved to a secured central network share. **RuggedCom RX1510:** 1. Login to the RX1510 Web UI >> Click on **Admin** >> Click on **Full configuration backup** 2. Enter a backup name, select backup format as **cli** from the Drop-down menu > On the **Trigger Action** form, click **Perform**. 3. The backup file will then be created and saved locally at /admin/backup-files 4. [Optional]The above file can further be downloaded via SFTP or copied over to a USB

	Drive. Click on **Admin** > Click **Backup-Files** in the menu 5. In the Backup Files form, select "**Config**" under **File Type** drop-down, enter a backup file name > Under **URL** enter the path of USB Drive or SFTP server's network path > Click **Perform**. 6. Save the backup file to the central network share/repository. For more details, refer to RX1510 manual available on Siemens website upon registration.
OT Devices	**Frequency:** Quarterly: Manual as per Manufacturer procedures. Ensure backups are saved to a secure central network share. **PLC:** 1.Power off the embedded PC. Remove the microSD card as per the steps mentioned in the manual [3] 2.Copy the data from the microSD card to a central secure location. **HMI**: 1.Setup a link between the HMI and PC(Workstation) using the RS-232 port or USB port. 2.Download the database via the LINK Menu in the HMI. Use either the Link-Send of Link-Update commands. Link-Send will copy over the entire database while Link-Update is for incremental backups. Detailed instructions can be found in the Crimson 3.1 Manual [4]

3.6.11 Recovery Procedures

- The Incident Recovery plan will be executed following a cybersecurity incident.
- Any exceptions or issues during the Recovery process must be communicated to the Supervisor and/or President.
- Depending on the incident, and on the number and nature of the IT services affected, one or more of the following IR procedures may be activated by the IR team:

Type of Incident	Plan of Action
Environment Disaster – Fire, Flooding	1. Identify root cause, co-ordinate initial response 2. Remove damaged systems from the work cell. 3. Evaluate damage 4. Review Insurance policies and reach out to Insurance companies. 5. Procure new hardware systems as required. Reach out to a Data recovery company for data recovery from damaged hard drives.
Virus / Malware – IT / OT Systems	1. Disconnect the affected systems from the network. 2. Reach out to the IT/OT Contractor for assistance. 3. Perform a full manual Anti-virus scan on the system 4. If the Anti-virus software cannot detect or quarantine the infection, you may need to reinstall or restore the entire Operating System. Use Veeam to restore a full image backup, if the system in question is an IT system. 5. Upon reinstalling the operating system, install all the appropriate patches to fix known vulnerabilities.

	6. Depending on the nature of the virus attack, change your original passwords as these could have been compromised during the infection.
Data Theft	1. Fulfill all legal obligations. Supervisor to inform law enforcement and other customer protection agencies notifying them of breach. 2. Immediately change system credentials, account passwords to public websites (if personal data is involved) 3.Monitor in-house security controls or tools for any signs of new activity. 4. Identify and erase any new files or programs that may have been installed as part of this attack. Use system baselines for reference. 5. Engage a Contractor or other professional to conduct security audit.
Data Loss - IT Systems	1. Browse through the list of directory level backups captured by Veeam for that host to select the backup to restore data from. 2. Initiate a restore of the file or directory from the affected system using Veeam. If the system in question is a virtual machine, restore the most recent full VM image as it is using Veeam. 3. Verify the file, folders and their permissions upon completion of the restore.
Hardware failure – IT Systems	1. Follow up with the vendor for getting the hardware replaced. 2. Install and setup the new hardware as per the original baseline configuration.

	3. Refer to File system table below to configure any File system dependencies such as NFS mount points. 4. Initiate a Restore operation from the most recent backup using Veeam. The restore procedure varies depending on if the system is physical or virtual. For more details, refer to the Veeam Backup guide. 5. Upon completion of restore, verify connectivity and operations.
Hardware failure –Network Devices	1. Order a replacement from a vendor. 2. Setup and configure the new device as per its original counterpart. For more details, refer to the asset inventory database and/or any supporting documentation to reference the original baseline config such as Firewall rules, ACLS, VLAN, etc. 3. Restore system configuration using Manufacturer instructions from the secure central repository. 4. Verify connectivity between devices. Run operations to confirm.
Hardware failure / Configuration Restore-OT Systems	1. Order a replacement from a vendor. 2. Setup the new device by assigning it the original static IP address and restore the configuration on it as per manufacturers manual. Following are high level instructions for a config restore <u>PLC:</u> 1.Power off the device. Pull out the microSD card from the PLC and load a previously saved image on it using a card reader. Saved images can be copied over from the central

	secure location or a new base image can also be obtained from the manufacturer. 2.Insert the microSD card back into the PLC and power on the device. 3. Test Connectivity and operations. <u>HMI:</u> 1. Copy a working image to a USB stick and plugin the USB in the HMI. 2. Access the "**System menu**" of the HMI. For more details, please refer to manufacturer's manual. 3.Click on "**Database Image Menu**" >> **Load Image from Memory Card** >> **Yes** <u>Machining stations:</u> 1.Power off the device. Pull out the microSD card from the beagle bone device and load a previously saved image on it using a card reader. 2.Insert the microSD card back into the beagle bone and power on the device. 3. Test Connectivity and operations. <u>Robots</u>: 1. Order a replacement from the vendor. 2. Install and connect new device in place of the original. 3. Verify operations

2349 **File System Layouts**

System	Local Hard Drive	File System layout	Network Storage (NFS, SMB)	Dependencies/ Notes
POLARIS	2TB	Output of "df -kh"	N/A	NFS Server
MINTAKA	500GB	Output of "df -kh"	N/A	
vController1	50GB	Output of "df -kh"	**polaris**:/opt/catkin_ws/src/youbot	NFS client. POLARIS should be UP before power ON
vController2	50GB	Output of "df -kh"	**polaris**:/opt/catkin_ws/src/youbot	NFS client. POLARIS should be UP before power ON

2350

2351 **Restoration Priorities**

2352 Should an incident occur and Alpha need to exercise this plan, this section will be referred to
2353 reference restoration priorities in bringing systems online.

2354 IT Systems

Priority	IT System	Description
High	LAN-AD	Active Directory / DNS Server
High	Veeam	Veeam Backups Server
High	MINTAKA	Robot Driver
High	vController1, 2	Robot Controllers
High	POLARIS	Engineering Workstation

High	Robotics-PI	Local Historian Database
Medium	PI-DMZ	DMZ-Historian
Medium	SymantecMgr	Symantec Antivirus Manager SEPM
Low	GTB Inspector	DLP
Low	Graylog	Syslog server
Low	Hive	Incident Response Server

Networking Equipment

Priority	Device Info	Description
High	Boundary Router	Allen Bradley Router 8300
High	Supervisory LAN Switch	Net gear GS724T
High	Control LAN Switch	Siemens i800 Switch

OT Systems

Priority	OT System	Description
High	PLC	Beckhoff PLC
High	HMI	Red lion HMI

3.6.12 Definitions and Acronyms

SLA	Service Level Agreement
Recovery Time Objective (RTO)	RTO defines the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported mission/business processes, and the Maximum Tolerable Downtime. [2]
Recovery Point Objective (RPO)	The RPO represents the point in time, prior to a disruption or system outage, to which mission/business process data can be recovered (given the most recent backup copy of the data) after an outage. [2]

3.6.13 References

1. SANS Guide for DR: https://www.sans.org/reading-room/whitepapers/recovery/disaster-recovery-plan-strategies-processes-564
2. NIST SP 800-34 Contingency planning guide for Federal Systems https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-34r1.pdf
3. Allen Bradley ControlLogix 5571 Manual https://literature.rockwellautomation.com/idc/groups/literature/documents/um/1756-um001_-en-p.pdf

4. Technical Solution Implementations

4.1 Introduction

This section includes proof-of-concept technical solution implementations developed for the fictional company Alpha. An overview of these technical solutions is discussed in Section 6 of Volume 1 and potential technical solutions are discussed in Section 7 of Volume 1. Each organization's information security experts should identify the technical solutions that will best integrate with their existing cybersecurity program and manufacturing system infrastructure.

All of the technical solutions were installed and configured within the Collaborative Robotics System (CRS) [6]. The manufacturing process was operated after each technical solution was implemented, producing 35 parts for each "experiment". Technical solutions that had multiple modes of operation were tested for each mode that aligned with the requirements of the low security level and the applicability of the mode to the use case [7].

Three types of performance measurements were performed during the implementation: baseline measurements of the initial workcell performance, impact of individual technologies or configurations, and impact of the completed security level implementation. The process of sequentially implementing and measuring enabled the detection of performance-impacting interactions between the technical solutions.

- **Security level baseline** - Before any changes were made to the workcell, baseline measurements were captured. Since all experiments are meant to be comparative, a baseline reference of system performance must be obtained to determine if the manufacturing process or its sub-systems have been impacted after a technical solution is installed or reconfigured.
- **Technology/configuration implementation impact** - These measurements were performed after each technical solution was installed and configured to meet the security level requirements. Some technical solutions provided multiple modes of operation that met the security level requirements and had the potential to affect the manufacturing process differently. Measurements were performed for each unique configuration to compare its impact to the previous configurations.
- **Security level implementation impact** - These measurements were performed after all technical solutions have been installed and configured. These measurements are used to determine the total impact to the manufacturing process and compared with other security level implementation impact measurements to determine the relative performance impact between the security levels. The final technology implementation impact (if it not a multi-mode measurement) can also be used as the security level implementation impact.

Before the security level baseline measurements were performed, the workcell manufacturing process was characterized by producing 1000 parts over ten experiments of 100 parts each, and the results analyzed. This characterization procedure (further described in [7]) validated that the process was in-control, stable, and random.

The primary key performance indicator (KPI) used to determine if the manufacturing process experienced a performance impact was "part production time" (KPI 2.1 in [6]), which measures the amount of time required for a part to travel through the manufacturing process. Numerous other performance measurements were captured on many of the CRS systems, and were subsequently used to produce the plots shown in the following sections, and to assist in determining the root cause of any realized performance impacts.

4.1.1 Implementation Note – Due Diligence Implementing Technical Solutions

It is important to note that the procedures used during this implementation (i.e., install a tool, then measure the impact) should not be used in a production system. Care must be taken before using any technical solutions, especially those that actively scan the manufacturing system ICS network and its devices; manufacturers should first conduct an assessment of how these tools work and what impact they might have on the connected control equipment [3]. Technology evaluations may include testing in similar, non-production control system environments to ensure that the tools do not adversely impact the production systems. Impact could be due to the nature of the information or the volume of network traffic. While this impact may be acceptable in IT systems, it may not be acceptable in a manufacturing system. In general, any operation that actively scans the manufacturing network should be scheduled to occur only during planned downtimes. [3]

4.1.2 Implementation Note - Sensor Error and Adaptation of KPI

After the Low baseline implementation was completed, an analysis of the KPI was performed. During this analysis, a small but consistent increase in the Station 4 allocation ratio was observed after each chronological experiment. The source of the increase was found to be occurring during the Station 4 "FINISHED" state, which is when the machining station has completed its manufacturing procedure and is waiting for the robot to remove the part. A plot showing the amount of time each station was in the "FINISHED" state across all experiments (compared to the baseline experiment CL001.1) was created (see Figure 4-1), which exhibited a high correlation to the part production time KPI measurements (see Figure 4-2).

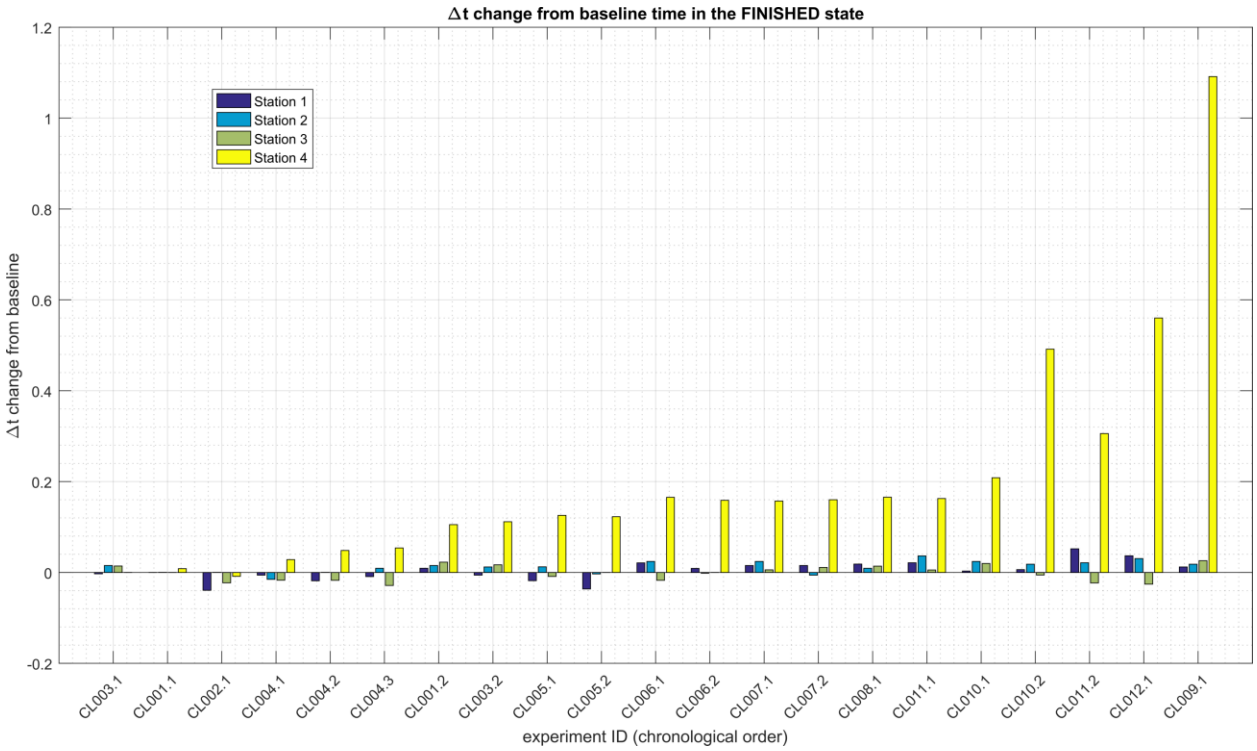


Figure 4-1 - Bar plot showing the increasing Station 4 "FINISHED" state deviation from the baseline. The data from Station 1, 2, and 3 are also shown. The plotted values are the mean for all 35 parts in the experiment. The largest discrete deviation measured was around 1.55 sec.

After further analytical review of the testbed measurements, the problem was isolated to a retroreflective proximity sensor located in the workcell on Station 4. The sensor specification defined a 20 mm sensing distance, but testing revealed the sensor intermittently reporting part presence after the part was removed upwards of 100 mm from the sensor. This effect was exacerbated by the motion of the robot, which keeps the part within the sensor field of view while removing the part from the station. Testing of the sensor response time revealed intermittent times upwards of 1.5 sec. when a part was removed from the station (the sensor specification reported a maximum switching frequency of 250 Hz, equivalent to a 0.004 sec. response time). The response time when a part was placed into the station was not affected.

The faulty sensor data was reviewed to determine if it could be eliminated from the KPI measurements. Since the only measurements affected were when parts were *removed* from Station 4, an analysis was performed to determine the feasibility of changing the KPI definition to be measured using the *arrival* of a part at Station 4, instead of the *departure* of a part. This method proved to be feasible. All mentions of this KPI throughout the remainder of this document should be considered defined in this manner. A comparison of the "part production time" KPI for the original and modified definition is shown below in Figures Figure 4-2 and Figure 4-3.

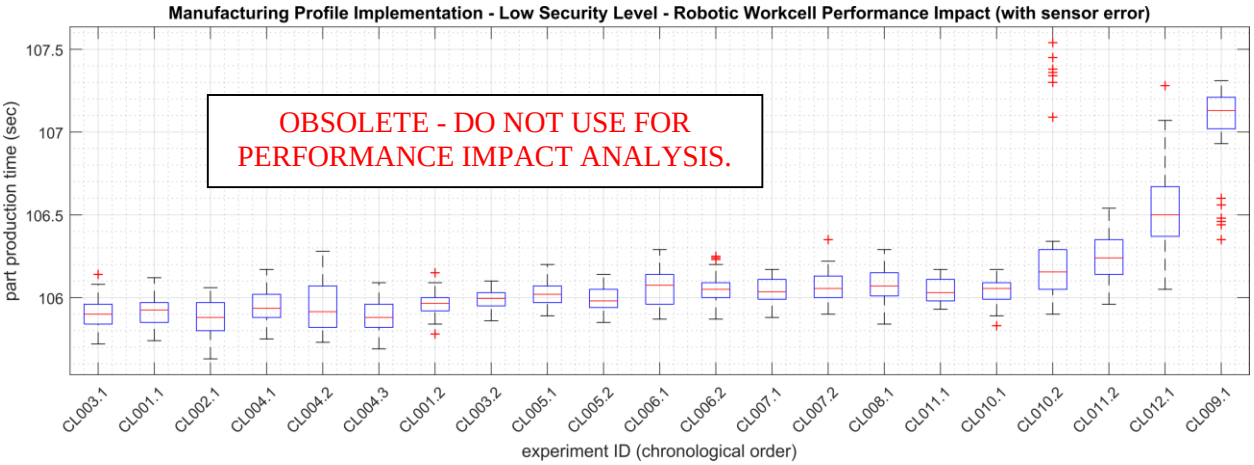


Figure 4-2 - Performance impact to the manufacturing process KPI "part production time" using the original definition, where the time is measured from the arrival of the part at Station 1 to the departure of the part from Station 4. Note the large increase and outliers for the last four experiments (CL010.2, CL011.2, CL012.1, and CL009.1).

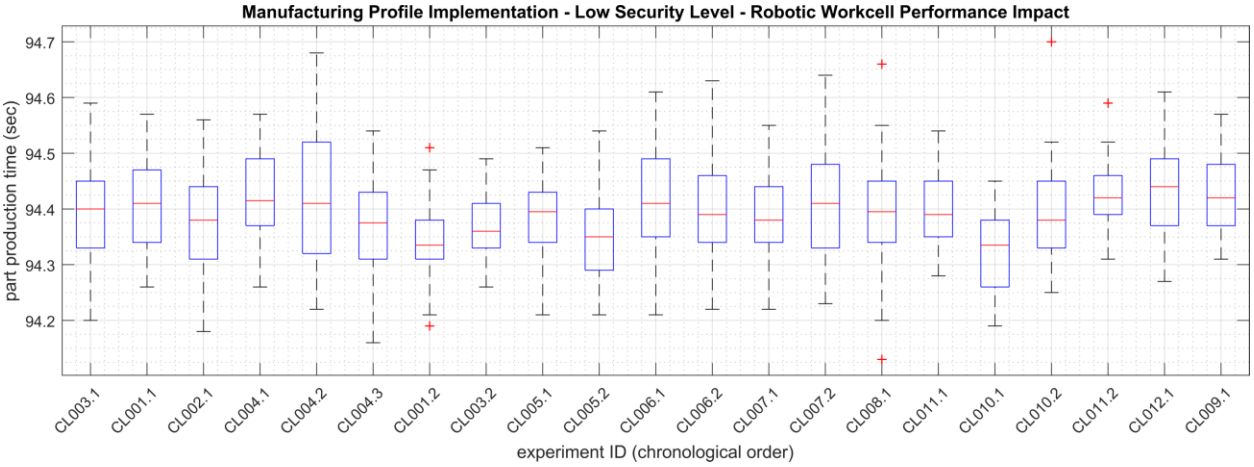


Figure 4-3 - Performance impact to the manufacturing process KPI "part production time" using the updated definition, where the time is measured from the arrival of the part at Station 1 to the arrival of the part at Station 4. Note the improvement in stability compared to the original definition shown in Figure 4-2.

4.1.3 Implementation Note - Availability of Measurement Data

All the raw and processed measurement data captured from each experiment is freely available online as compressed ZIP files. Links to all of the data files are provided below, and directly referenced at the end of each implementation below.

- CL001.1-Baseline.zip
- CL001.2-BaselineUpdate.zip
- CL002.1-ActiveDir.zip
- CL003.1-Syslog.zip
- CL003.2-Syslog.zip
- CL004.1-HostBackups.zip

- CL004.2-FullImageBackup.zip **
- CL004.3-DirectoryBackup.zip **
- CL005.1-AntivirusRealTimeScan.zip
- CL005.2-AntivirusFullScan.zip
- CL006.1-NessusNetworkScan.zip
- CL006.2-NessusAuthenticatedScan.zip
- CL007.1-OpenAudITNetworkScan.zip
- CL007.2-OpenAudITAuthenticatedNetworkScan.zip
- CL008.1-LeastPrivilege.zip
- CL009.1-BoundaryFirewall.zip
- CL010.1-NetworkPhysicalConnections.zip
- CL010.2-NetworkMACFiltering.zip
- CL011.1-PatchesNetworkHardware.zip
- CL011.2-PatchesServersICSDevices.zip
- CL012.1-CiscoASA5506.zip

** - The network capture files provided for CL004.2 and CL004.3 (capture.pcap) have been modified to exclude all Veeam traffic recorded during the experiment, as the traffic contains sensitive testbed data in clear-text. To obtain access to these files, please contact the authors directly.

4.2 Open-AudIT

4.2.1 Technical Solution Overview

Open-AudIT is an asset inventory tool providing scanning of hardware and software within the manufacturing environment. Open-AudIT scans are highly customizable to each environment, depending on the level required.

Open-AudIT cost depends on the level of functionality desired for your environment. Editions offered by Open-AudIT vary from entry level community edition which is free, all the way up to enterprise edition. Enterprise was chosen since it contains the ability to setup schedule scanning, dashboards, and baselining of equipment.

Open-AudIT is a downloadable OVA which is easy to install. OVA install allows installation in a Hyper-Visor environment allowing for installation within an existing virtual environment without requiring purchasing additional hardware. Configure for initial discovery scans are straight forward and easy to configure and perform.

4.2.2 Technical Capabilities Provided by Solution

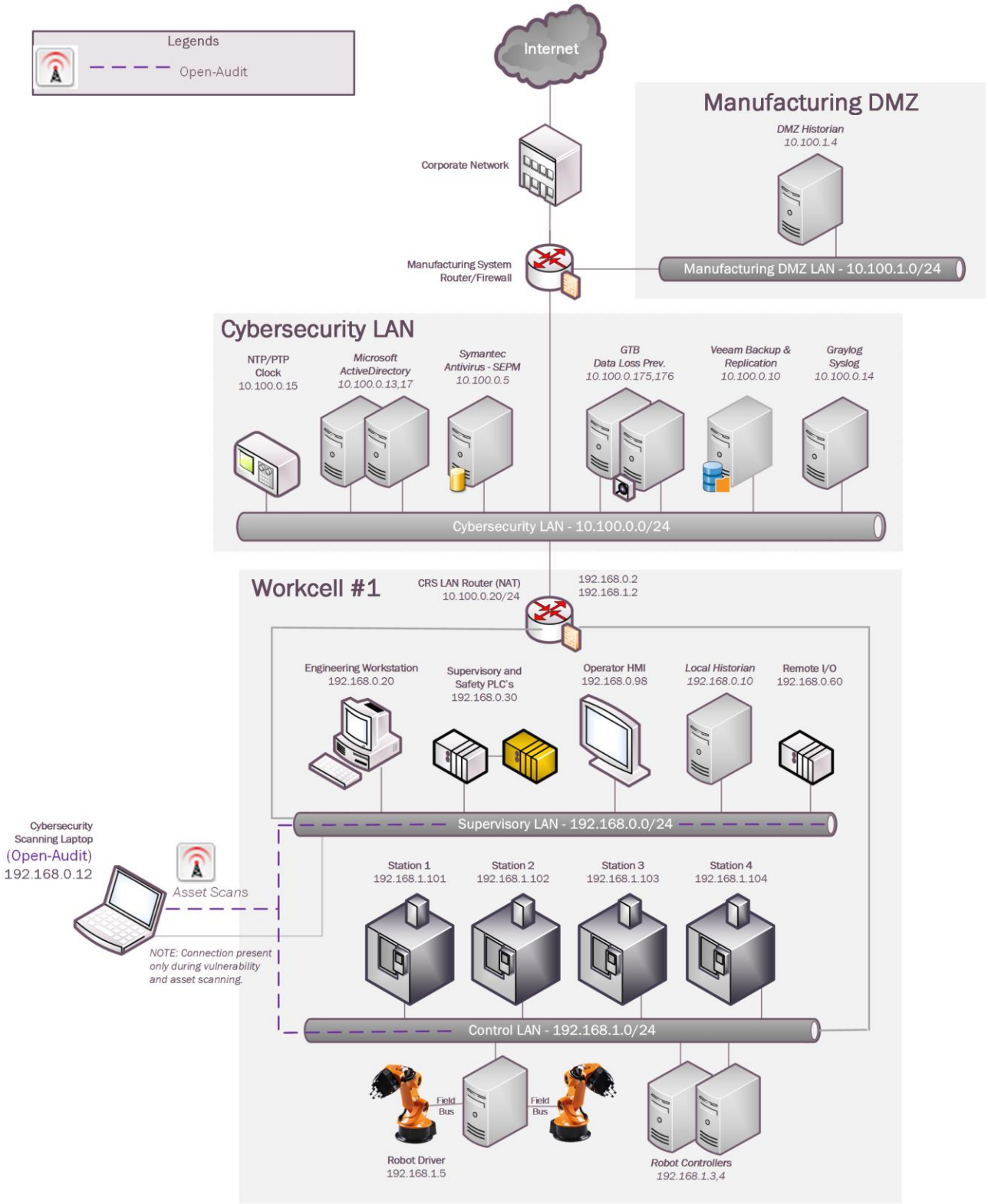
Open-AudIT provides components of the following Technical Capabilities described in Section 6 of Volume 1:

- Hardware Inventory
- Software Inventory
- System Development Lifecycle Management
- Configuration Management
- Baseline Establishment (Enterprise Edition)
- Change Control

4.2.3 Subcategories Addressed by Implementing Solution

ID.AM-1, ID.AM-2, ID.AM-3, ID.AM-4, PR.DS-3, PR.IP-1, PR.IP-2, PR.IP-3, PR.IP-4, PR.IP-6, PR.MA-1, DE.AE-1, DE.CM-7

4.2.4 Architecture Map of Where Solution was Implemented



4.2.5 Installation Instructions and Configurations

Open-AudIT Setup Steps

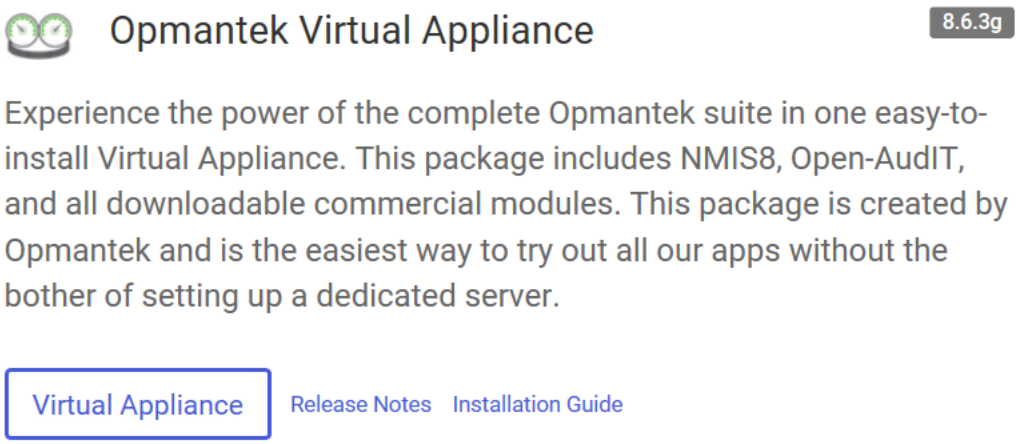
Prerequisites:

- Identify if physical hardware or virtual machine will be used
- Requirements from Opmantek who developed **"Open-AudIT"** indicate the specification required are low. Please see this link for exact details provided by the vendor link.

Instruction:

Download:

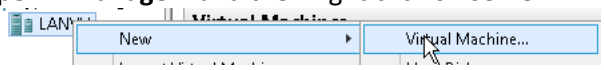
1. Download and save **Opmantek Virtual Appliance** from Opmantek website.[10]



2. Once download has completed **".ova"** file will need to be extracted to view the contents and move to the next step **(any tool supporting extracting .ova and .gz can be used)**.
3. Open the folder where the files were extracted too. There should be a total of four files.
4. Next, extract the two files with extension **(.vmdk.gz)** since this file is still compressed. Once completed two files with the same extension **(.vmdk)** should now exist.
5. Now two files just extracted need to be convert to **"VHDX"** format so we can run these disk in a Hyper-V environment. See this link for instruction and additional information useful for converting virtual drive format.
6. Once both drives have been converted to **"VHDX"** format proceed to next section.

Virtual Machine Setup:

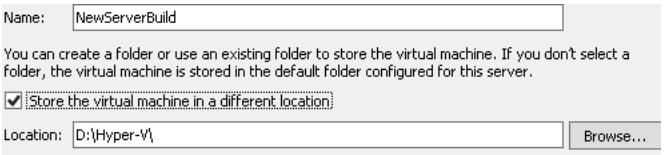
1. On the virtual server host open **"Hyper-V Manager"** and then right click on server name selecting New → Virtual Machine



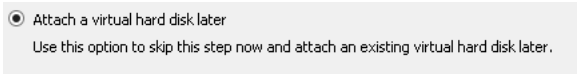
2. Now type in the name you going to give this server.

[10] Opmantek Intelligent Network Management Software https://opmantek.com/

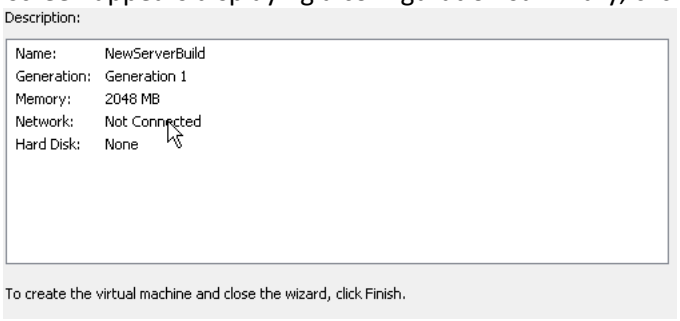
3. Place a check in the box **"Store the virtual machine in a different location"** click next.



4. The step above will place the configuration and hard drive files for the newly create Virtual Machine in D:\Hyper-V\NewServerBuild **(See Screenshot)**
5. Leave **Generation 1** selected and click Next. This machine doesn't require additional features provided from **Generation 2**.
6. Now assign how much memory your new machine will be given for use. For our environment we are using **"2048"** Click next to continue.
7. Select the network this virtual machine will be using and click Next.
8. Now select **"Attach a virtual disk later"** and click next.

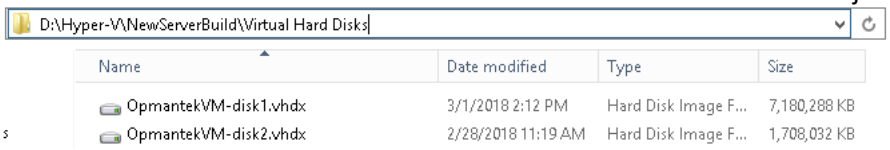


9. Now a screen appears displaying a configuration summary, click Finish to complete.

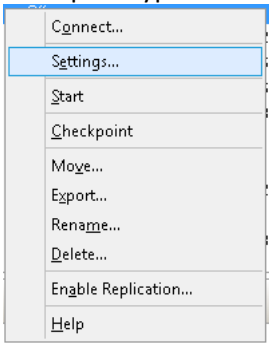


10. Next, open Windows Explorer and navigate to the location of your newly created virtual machine and create a new folder labeled **"Virtual Hard Disk"**

11. Now moves the hard drive files converted earlier to this new folder location just created.

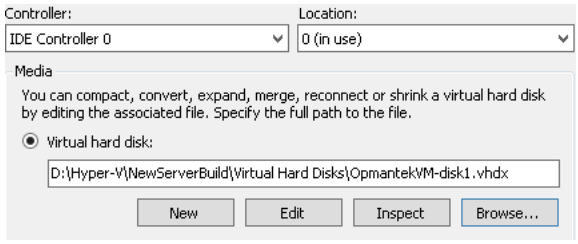


12. Open Hyper-V Manager and right click on Virtual Machine just created and select **"Setting…"**

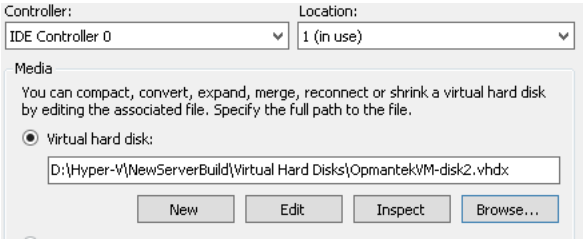


13. Memory should be configured for **"2048"**

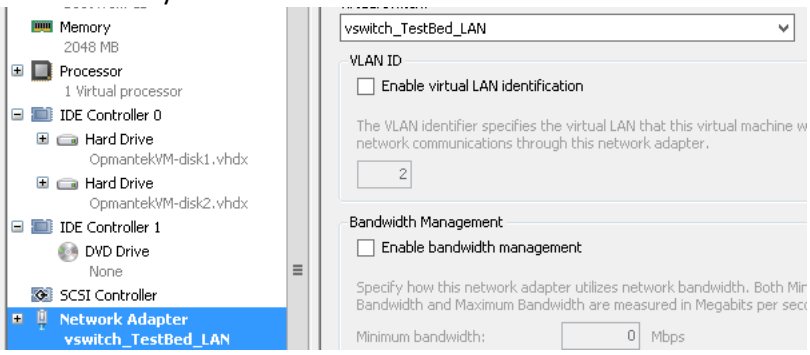
14. Virtual Processor **"2"**
15. Click on **"IDE Controller 0"** then click on "**Add"** button to attach a virtual hard.
16. Click browse button and select the first virtual drive that was moved earlier, click apply.



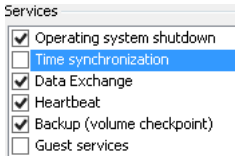
17. Now click on **"IDE Controller 0"** again and click "**Add"** button to attach a virtual hard.
18. Click browse button and select the second virtual drive that was moved earlier, click apply.



19. Now, select Network adapter and click the drop down and select **"vswitch_TestBed_Lan"** or what you have labeled your network.



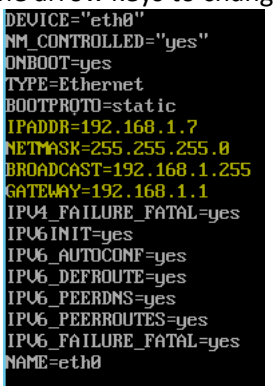
20. Click on Name and make sure to add some descriptive information that will allow other to easily see this information without having to login into machine.
21. Select Integration Service and remove check from **"Time Synchronization"** Time will be sync using internal NTP server via DNS pointer. Click **"Apply"** and then **"OK"**.



Configure Virtual Machine Networking:

1. Open Hyper-V Manager and then right click on newly created machine and select start.
2. Double click on machine being configured to open a Console window.
3. Now type in **"root"** and then hit enter. Now type in Password provided from documentation. Once logged in make sure to change password from default. Additional information for default login credentials can be found here.

4. Now type this command without the quotes to copy a static configuration for networking. **"cp ifcfg-eth0.static /etc/sysconfig/network-scripts/ifcfg-eth0"** if prompted to overwrite file type **"Yes"**
5. Now type this command without the quotes **"sudo nano /etc/sysconfig/network-scripts/ifcfg-eth0"**
6. Now use the arrow keys to change the highlighted fields to your desired network configuration.



7. Once all fields have been updated use **Ctrl + O "^O"** to write the file and then **Ctrl + X "^X"** to exit.

8. Now type **"service network restart"** This restarts networking services with the newly configured settings.

Complete Additional Setup via Web Browser:

1. Now with any web browser navigate to **"IP Configured Earlier"** example would be **"10.100.0.177"**
2. If prompted to proceed to untrusted site, select **"Yes"**. This error is produced since SSL has not been configured and Open-AudIT redirects HTTP sessions over to HTTPS.

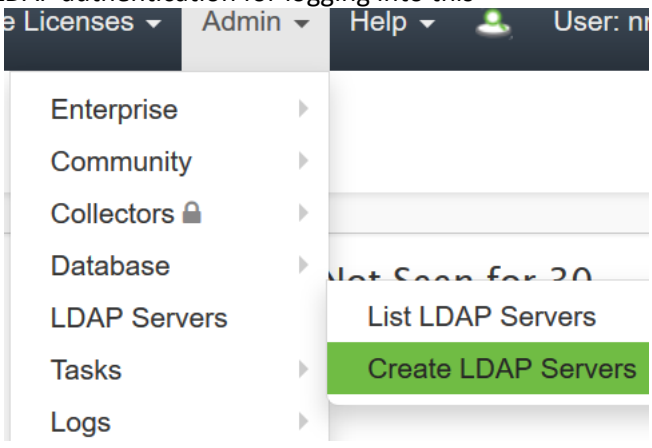
3. Once this page opens you'll see lots of different options this tool provides. We're using "**Open-AudIT Enterprise"** This version allows for up to 20 nodes to be audited / monitored for free.

Opmantek Documentation and Community

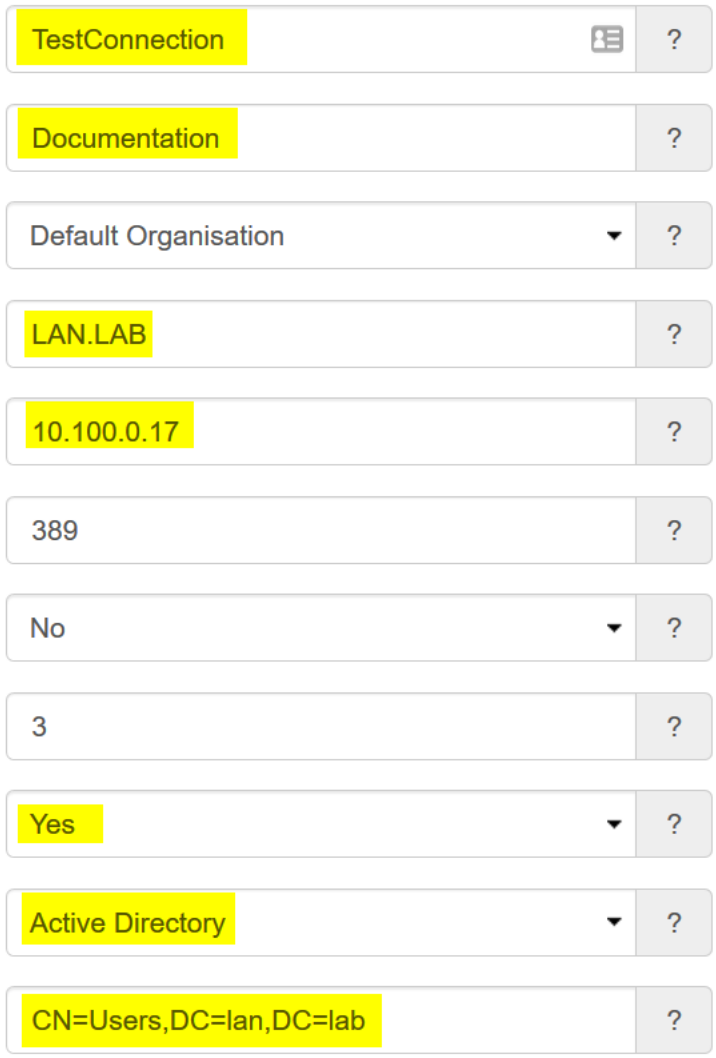
NMIS8 Dashboard
opCharts - interactive Charts and Dashboards
opEvents - Event Management
opFlow - NetFlow Analysis
opConfig - Configuration and Compliance Management
opReports 3.0 - Network Reporting
Open-AudIT Enterprise

Open-AudIT V2 Dashboard
Open-AudIT Documentation and Community

4. You'll now be prompted for login with username and password. This default information is provided above **"username / password"**.
5. Once logged in we need to make some required changes to allow this produce to function in our environment.
6. Click on **"Admin → LDAP Server → Create LDAP Servers"** This will allow integration with Active Directory using LDAP authentication for logging into this application.



7. Required setting for LDAP server connection. Screen shot provide for reference.



   a. Name – **TestConnection**
   b. Description -- **Documentation**
   c. Domain – **LAN.LAB**
   d. Host – **10.100.0.17**
   e. Use LDAP Roles -- **Yes** (Additional configuration is required in AD Groups. See section below in this document for additional steps.
   f. Base DN – **"cn=user,dc=lan,DC=lab"**

8. Click **"Submit"** once all information has been entered.

Active Directory Groups for LDAP Integration:

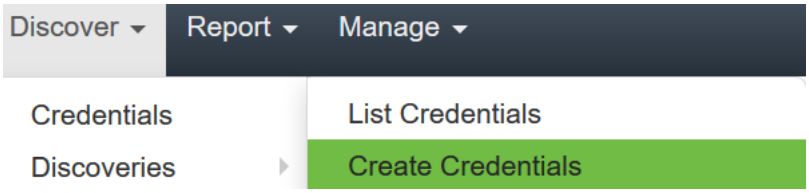
1. Groups listed below are required for integration to work with Open-AudIT and Active Directory.
   a. **Admin "open-audit_roles_admin"**
   b. **org_admin "open-audit_roles_org_admin"**
   c. **reporter "open-audit_roles_reporter"**
   d. **user "open-audit_roles_user"**

e. **Default Organization "open-audit_orgs_default_organisation"**

2. Create each group listed within quotes in your Active Directory. Each group should be created with Group Scope (**Global**) Group Type (**Security**)
3. Once each group has been created and the appropriate users add you can now login with your Active Directory credentials.

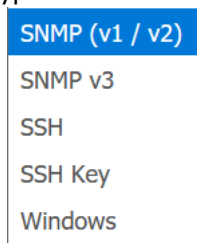
Discover Credentials and Discover Scans

1. From the home screen click on Discover button → Credentials →Create



Credentials.

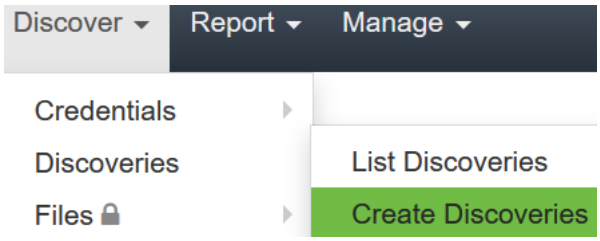
2. Now enter in the requested information.
   a. Name – Name of the Credentials being used. Example (**SSH**)
   b. Organization – Default Organization is selected. Pickup another if your configuring more the one organization.
   c. Description – Description of item being added.
   d. Type – Select which type of credentials will be used**. (SNMP (v1 / v2), SNMP v3, SSH,**



SSH Key, or Windows)
   e. Credentials – enter the appropriate credentials for the select type from above.
   f. Click submit to save this entry.

Discovered Scan:

1. Click Discover button → Discoveries →Create



Discoveries.

2. Name – The name for this scan which should be unique.
3. Subnet – The network discovery will be performed on.
4. Click submit to save and return to main discovery screen.
5. Main discovery screen allows you to start a scan at any time. Scans can also be configured to run on a schedule interval.

Useful information and links:

1. Default password were not changed, so remember to change all default password before this is put into production. **(THIS IS VERY IMPORTANT)**
2. Software Vendor webpage. → https://opmantek.com
3. Community forums. → https://community.opmantek.com

4. Software is Open Source. Your able to use Professional Edition for up to 20 machines after that there is a cost which is relatively inexpensive.
5. Comparison below.

Both the community and enterprise products share a common code base, however, Open-AudIT Enterprise includes additional modules that improve discovery, simplify administration and increase reporting ability. Use the comparison chart below to decide which version best suits your organization's requirements.

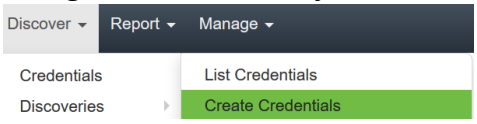
	Community	Professional	Enterprise
Network Discovery	Yes	Yes	Yes
Device and Software Auditing (including Device Port and Storage Appliances)	Yes	Yes	Yes
Configuration Changes Detection and Reporting	Yes	Yes	Yes
Hardware Warranty Status	Yes	Yes	Yes
Inventory Management	Yes	Yes	Yes
Custom Fields	Yes	Yes	Yes
Interactive Dashboard		Yes	Yes
Geographical Maps		Yes	Yes
Devices Export		Yes	Yes
Scheduling – discovery and reporting		Yes	Yes
Enhanced Reports including Tine based, Historical and Multi Reporting		Yes	Yes
High Scale			Yes
High Availability			Yes
File Auditing			Yes
Baselines			Yes
Configurable Role Based Access Control including Active Directory and LDAP			Yes
Integration with agents and CMDB			Yes
Commercial Support		Yes	Yes

6. Ability to perform baseline scan on devices is provided by Enterprise edition. This could be very useful for determining changes over time.

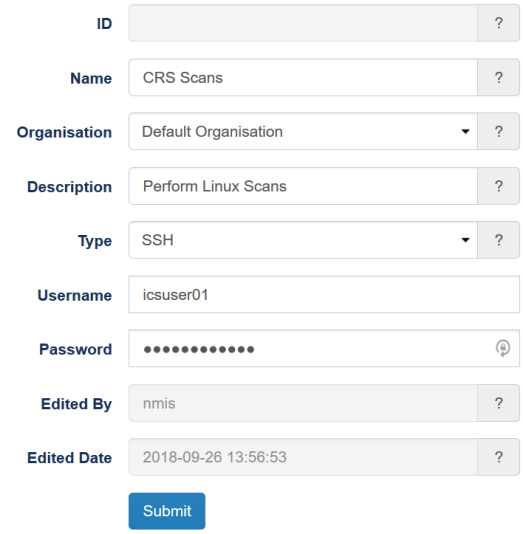
Open-AudIT Configuration steps within CRS once system has been installed

Initial Configuration:

- Login via web portal
- Navigate to → Discovery → Credentials → Create Credentials

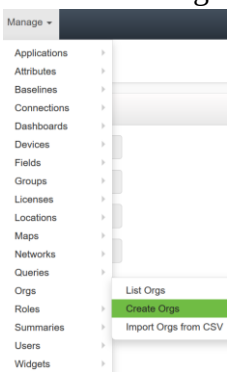


- Credentials can be assigned to any organization that has already been created. If you want credentials to only apply to specific organizational group, then select that from the appropriate drop-down during credential creation and select the desired group these credentials will apply to.
- The environment consists of mainly Linux machines, so SSH will be used for connection type.
- Now create a credential and select **SSH** for the type. Once completed click

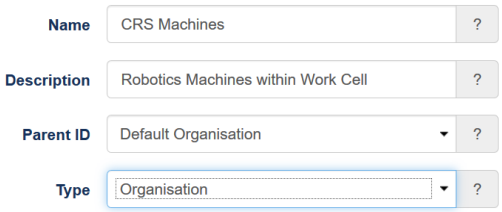


Organization Groups Creation:

- Click on Manage → Orgs → Create Orgs



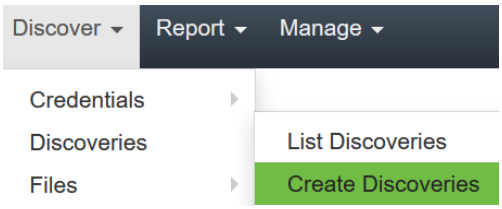
- Now enter **Name**: **Description**: and click submit at the bottom of the page to save.



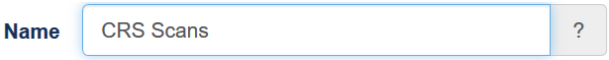
- If you have multiple machines / equipment in different locations you can make Organizational groups based on business units, or related task.

Configure Discovery Scan:

- Now click on Discover → Discoveries → Create Discoveries



- Enter a meaningful name for discover being created



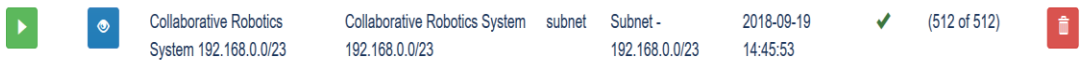
- Next, enter the subnet that'll be used for performing this scan. This scan is using 192.168.0.0/23

Search online for additional subnetting information / calculators if you'd like to learn more.
- **Network address:** should already be defaulted to Open-AudIT installed location, if this is not true, click the drop-down arrow and select your installed location.
- Now, click on the advanced button to see more options. 

- Once **Advanced** has been expaned you'll have additional options to select if desired. These options are **Org, Type, Devices Assigned to Org,** and **Devices Assigned to Location**. These options aren't required, but allow you to place found devices into different Organzations groups.
- Once all selection have been made click on **Submit** button to continue.

Discoveries:

- Once the steps above have been completed clicking on **Submit** button you'll be taken to a new webpage that'll allow you to run discovery process created in the previous step.
- To start discovering devices click on **green** arrow button. If you need to verify details for this scan click on the button that looks like an **eye**: finally, if you need to delete this scan click on the **trash** can icon to the right. See screen shot for details.



- Once discovery has started you'll be taken to a new page allowing you to view status or cancel if needed.
- Newly found devices are added to **My Devices** which is found on the home screen.

Lesson Learned:

Ensure default passwords are changed

Use Secure LDAP (LDAPS) If unable to use LDAPS make sure account being used for syncing groups has least privilege rights. (Not an Administrator and not a Domain Administrator)

When configuring SNMP make sure to use SNMP V3 if possible.

4.2.6 Highlighted Performance Impacts

Two performance measurement experiments were performed for the Open-AudIT tool while the manufacturing system was operational:

1. CL007.1 - A discovery scan was performed.
2. CL007.2 - A discovery scan with credentials was performed.

4.2.6.1 Experiment CL007.1

An Open-AudIT "discovery" scan without credentials (i.e., network scan) was performed on three IP address ranges in the CRS network:

- 192.168.1.101 to 192.168.1.104 (CRS Control LAN),
- 192.168.1.1 to 192.168.1.5 (CRS Control LAN), and
- 192.168.0.1 to 192.168.0.239 (CRS Supervisory LAN).

The Open-AudIT logs reported scanning was active for each IP address range for 1 second, 1 second, and 7 minutes, respectively. Notes taken by the researchers while the experiment was underway reported that the tool was active from 308 seconds to around 700 seconds (experiment time). The network traffic captures show that the tool was actively communicating on the CRS network from 300 seconds to 358 seconds (experiment time), with a peak network throughput of around 150 kbps (see Figure 4-4).

No components of the CRS showed any measurable performance impact from the discovery scans beyond the anticipated increase in network traffic.

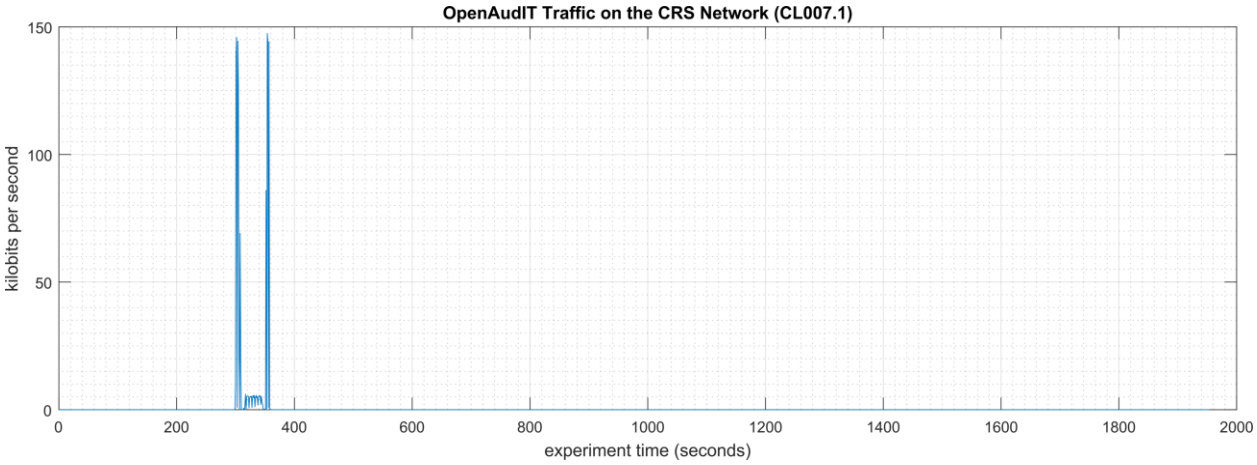


Figure 4-4 - Time series plot showing the rate of network traffic (in kilobits per second) transmitted and received by the Open-AudIT tool during the experiment time period, with the most prominent activity between 300 to 358 seconds.

No performance impact to the manufacturing process was measured during the experiment.

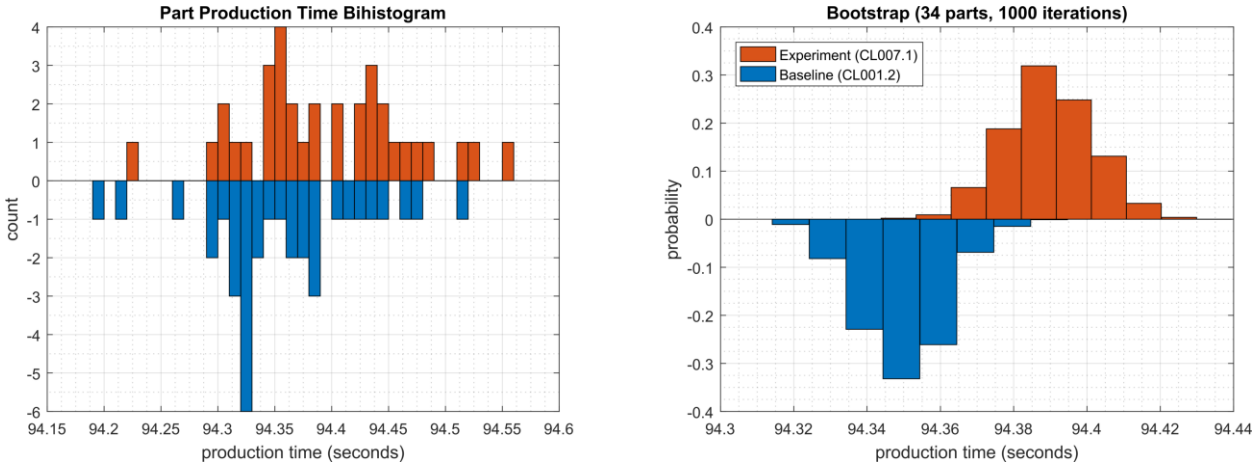


Figure 4-5 - Bihistograms showing the part production time (left) and estimated mean production time using the bootstrap method (right) using the measurements from baseline CL001.2 and experiment CL007.1.

4.2.6.2 Experiment CL007.2

An Open-AudIT "discovery" scan with credentials (i.e., authenticated scan) was performed on three IP address ranges in the CRS network:

- 192.168.1.101 to 192.168.1.104 (CRS Control LAN),
- 192.168.1.1 to 192.168.1.5 (CRS Control LAN), and
- 192.168.0.1 to 192.168.0.239 (CRS Supervisory LAN).

Credentials were provided to Open-AudIT, which gave the tool access to the following CRS hosts: the engineering workstation (POLARIS), the robot driver (MINTAKA), the robot controllers (vController1, vController2), and the machining stations. The Open-AudIT logs

reported scanning was active for each IP address range for 5 minutes 17 seconds, 6 minutes 18 seconds, and 7 minutes 24 seconds, respectively. Notes taken by the researchers while the experiment was underway reported that the tool was actively scanning from 293 seconds to around 750 seconds (experiment time). The network traffic captures show that the tool was actively communicating on the CRS network from 290 seconds to 681 seconds (experiment time), with a peak network throughput of around 300 kbps (see Figure 4-6).

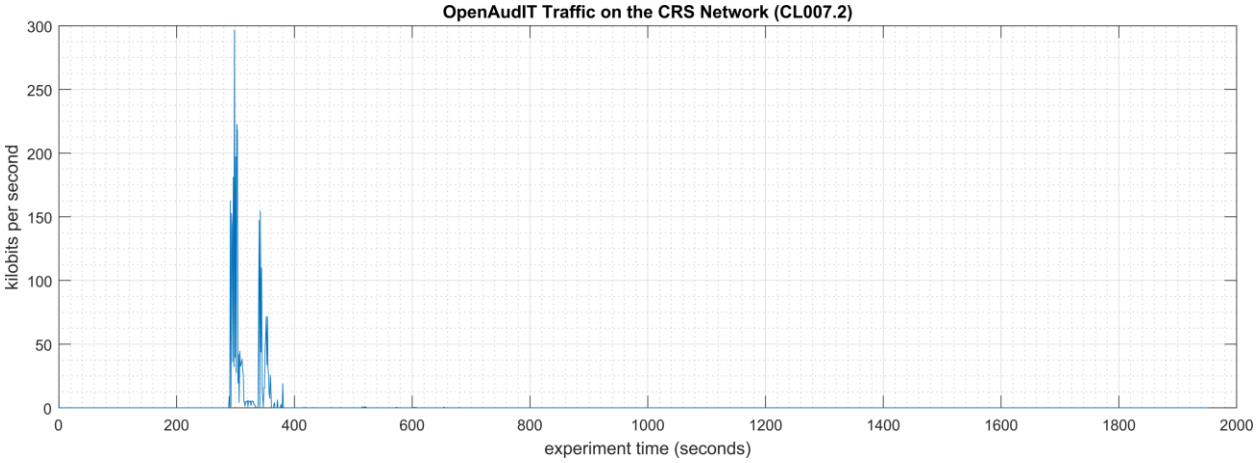


Figure 4-6 - Time series plot showing the rate of network traffic (in kilobits per second) transmitted and received by the Open-AudIT tool during the experiment time period, with the most prominent activity between 290 to 380 seconds.

Increased CPU utilization was observed on vController1 and vController2 between 340 to 420 seconds experiment time. CPU utilization for vController1 increased to an approximate average of 36% with a peak of 46% during the scan period (see Figure 4-7). A constant increase of the average CPU utilization was also observed on vController1 for the entire experiment, from the baseline value of approximately 2% to 8%. The cause of this increase is unknown at the time of publishing. CPU utilization for vController2 increased to an approximate average of 32% with a peak of 58% during the scan period (see Figure 4-8).

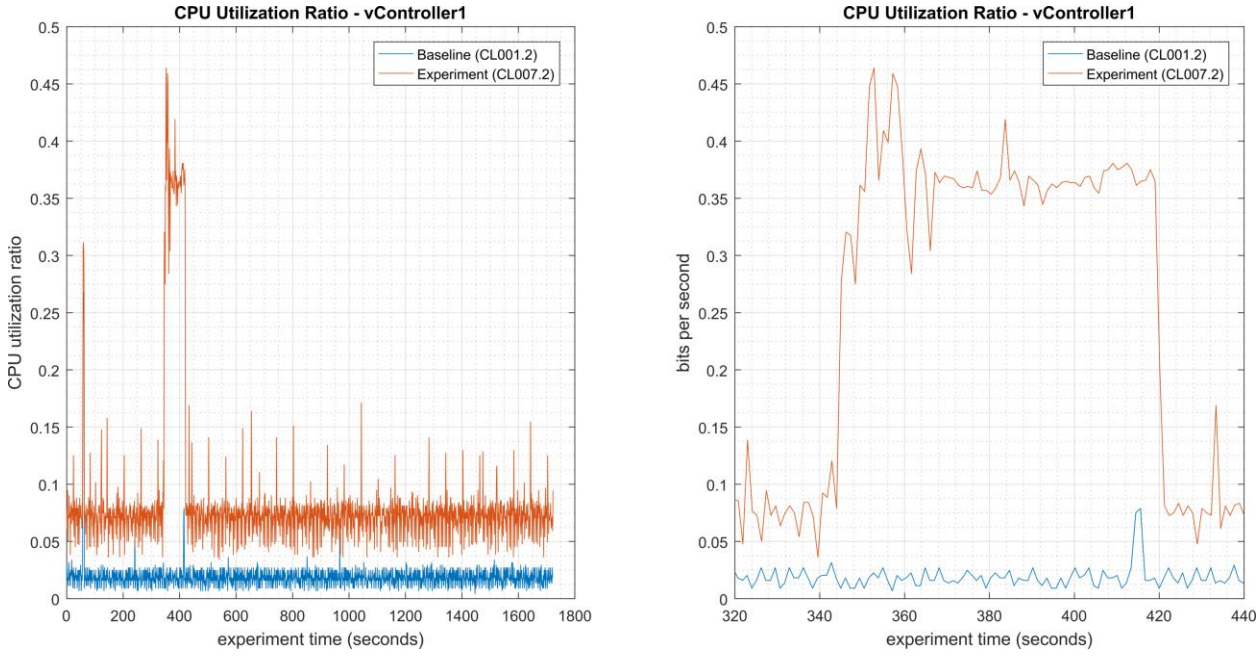


Figure 4-7 - Time series plots showing the CPU utilization ratio for vController1 during the experiment (left), and during the period of measured impact (right).

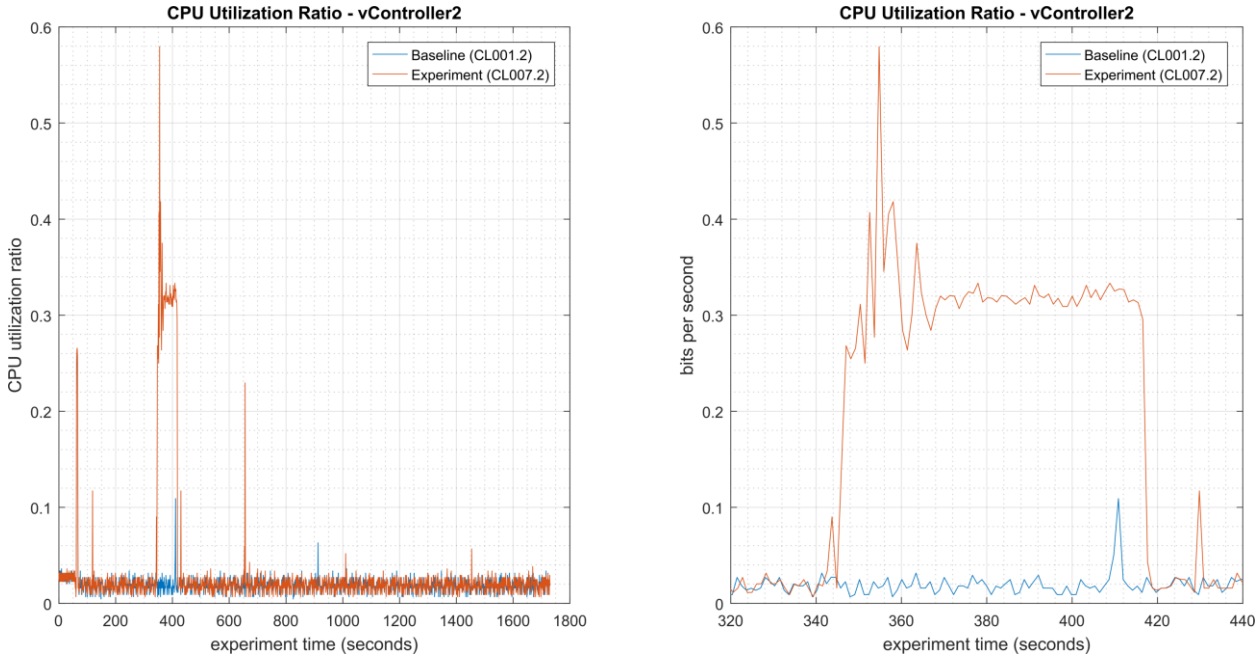


Figure 4-8 - Time series plots showing the CPU utilization ratio for vController2 during the experiment (left), and during the period of measured impact (right).

A slight increase of the part production time mean and variance was observed during this experiment, but they are not statistically significant.

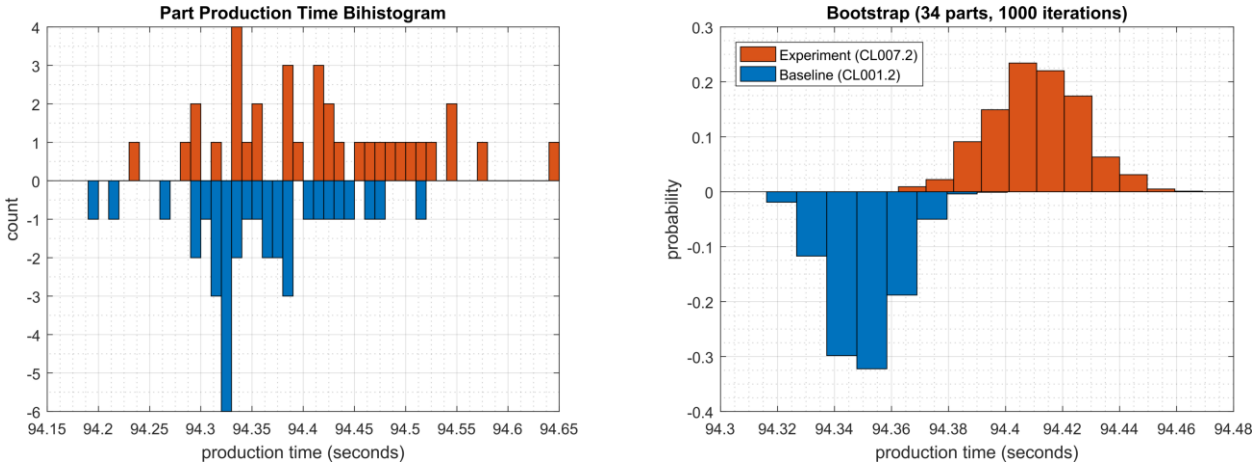


Figure 4-9 - Bihistograms showing the part production time (left) and estimated mean production time using the bootstrap method (right) using the measurements from baseline CL001.2 and experiment CL007.2.

4.2.7 Link to Entire Performance Measurement Data Set

- **CL007.1-OpenAudITNetworkScan.zip**
- **CL007.2-OpenAudITAuthenticatedNetworkScan.zip**

4.3 CSET

4.3.1 Technical Solution Overview

Cyber Security Evaluation Tool (CSET) is a tool provide by Department of Homeland Security for performing Cybersecurity evaluation against an organization. This evaluation is completely manual process of answering multiple questions to determine organizational security posture in regard to implemented current cybersecurity practices against current security status. This evaluation will help identify area within the organization that required more attention and resources.

4.3.2 Technical Capabilities Provided by Solution

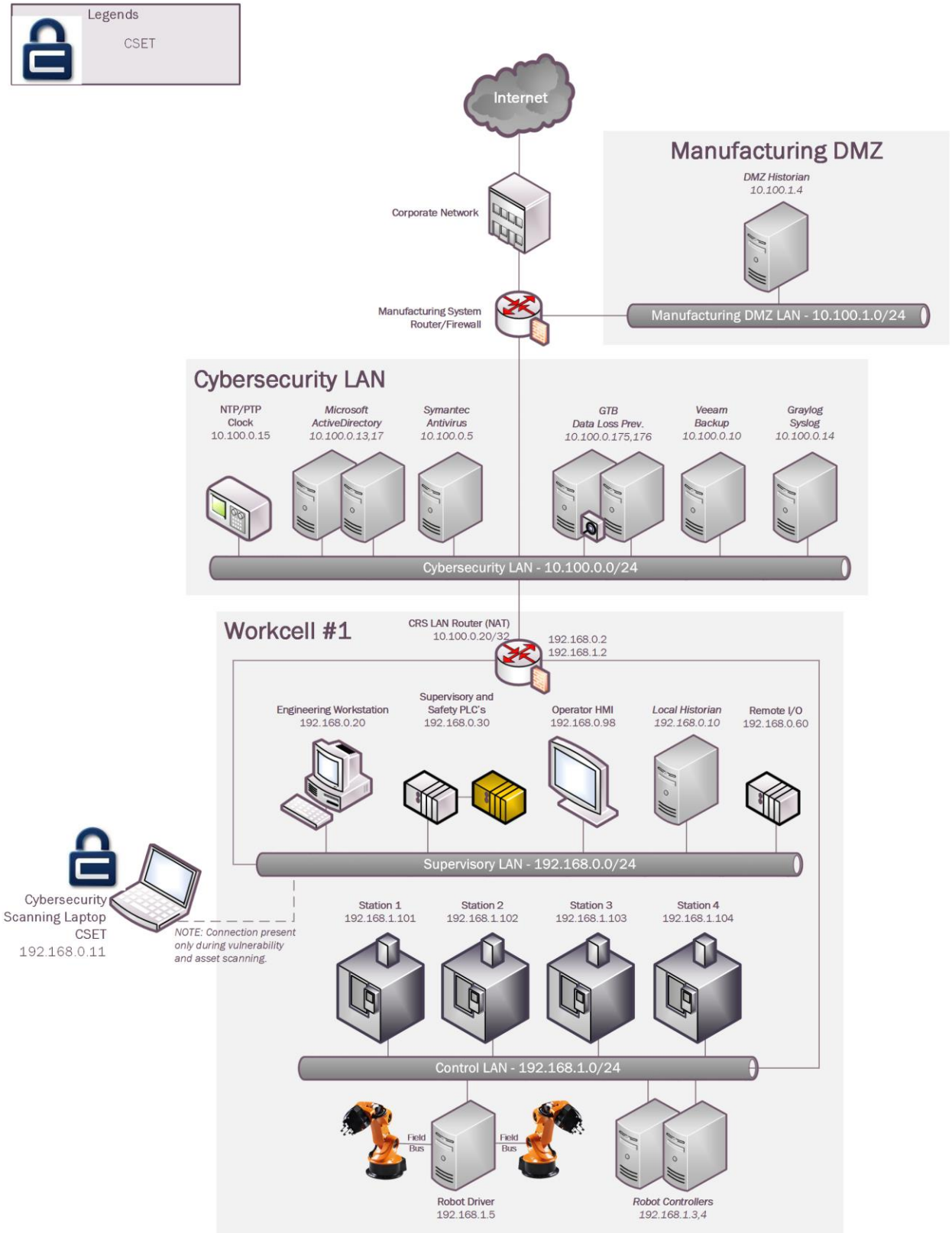
CSET provides components of the following Technical Capabilities described in Section 6 of Volume 1:

- Network Architecture Documentation
- Risk Assessment

4.3.3 Subcategories Addressed by Implementing Solution

ID.RA-1

4.3.4 Architecture Map of Where Solution was Implemented



4.3.5 Installation Instructions and Configurations

CSET Installation and Configuration

Download and Installation Instructions: Provided by DHS

Download CSET using the link at the bottom of this page or by clicking here. After clicking the link, you will be asked to identify yourself and will then be given the opportunity to download the file *CSET_x.x.iso (where x.x represents the download version)*.

The CSET download is in a file format known as "ISO." This file is an "image" of the equivalent installation files included on the CSET CD. Because of this format, it is necessary to process the download using one of the following methods:

1. **Decompressing the File** - Open the file using any one of the newer compression utility software programs.
2. **Mounting the File** - this method loads the ISO file using utility software to make the file appear like a virtual drive with the original CD loaded.
3. **Burning the file to CD** - this method uses CD-burn software and the ISO file to burn the files onto your own CD to create a physical disk identical to the CSET original.

These methods require separate software utilities. There are a variety of both free and purchased utility programs available through the Internet that will work with the ISO file format. As DHS does not recommend any specific application or vendor, it will be necessary for you to find a product that provides the necessary functionality. Step by step instructions for each method are provided below:

Decompressing the File

1. CLICK the "Download CSET" link at the bottom of this page and complete the requested information to download the ISO file.
2. SAVE the file to your hard drive of choice (i.e., your computer hard drive or USB drive) maintaining the file name and extension (.iso).
3. OPEN the ISO file with a compression utility program and SAVE the files to your hard drive of choice maintaining the original names and file extensions.
4. COMPLETE the *Installing the CSET Program* instructions below.

Mounting the File

1. CLICK the "Download CSET" link at the bottom of this page and complete the requested information to download the ISO file.
2. SAVE the file to your hard drive of choice (i.e., your computer hard drive or USB drive) maintaining the file name and extension (.iso).
3. RUN your ISO-specific utility program that is capable of mounting the file. COMPLETE the instructions within the utility software to create a virtual drive using the ISO file. If

you do not have an ISO utility application, you will need to find and install one before continuing with these instructions.

4. COMPLETE the *Installing the CSET Program* instructions below.

Burning the file to CD

1. CLICK the "Download CSET" link at the bottom of this page and complete the requested information to download the ISO file.
2. SAVE the file to the hard drive on your computer maintaining the filename and extension (.iso).
3. INSERT a blank, writable CD into the computer's CD drive.
4. RUN your CD-burn utility program. COMPLETE the instructions on your utility program to burn the ISO image to your DVD. (If you do not have an application that can do this, then you will need to find and install one before continuing with these instructions.)
5. COMPLETE the *Installing CSET Program* instructions below.

Installing the CSET Program

1. FIND the CSET_Setup.exe file in the folder, virtual drive, or CD containing the CSET files.
2. DOUBLE-CLICK the CSET_Setup.exe file to execute. This will initiate the installer program.
3. COMPLETE the instructions in the installation wizard to install the CSET program.
4. READ the material within the ReadMe document for a summary explanation of how to use the tool. Help is also available through the User Guide, screen guidance text, and video tutorials.

Video Tutorials

A number of video tutorials are available to help you better understand how to use this tool. They are designed to play within YouTube, therefore, you must have an active internet connection to view them. You can access these videos by navigating to the CSET YouTube channel (https://www.youtube.com/c/CSETCyberSecurityEvaluationTool).

To view close captioning in YouTube, click on the "cc" icon on the video window.

System Requirements

In order to execute CSET, the following minimum system hardware and software is required:

- Pentium dual core 2.2 GHz processor (Intel x86 compatible)
- CD-ROM drive if creating a physical CD
- 5 GB free disk space
- 3 GB of RAM

- Microsoft Windows 7* or higher
- A Microsoft Office compatible (.docx) document reader is required to view reports in .docx format
- A Portable Document Format (PDF) reader such as Adobe Reader is required to view supporting documentation. The latest free version of Adobe Reader may be downloaded from http://get.adobe.com/reader/
- Microsoft .NET Framework 4.6 Runtime (included in CSET installation)
- SQL Server 2012 Express LocalDB (included in CSET installation)

NOTE: For all platforms, we recommend that you upgrade to the latest Windows Service Pack and install critical updates available from the Windows Update website to ensure the best compatibility and security.

CSET Hash Values

SHA-256:
B7061B169E3461A298E58B99FADC9978D9F6CE22A0747669A538BDAF39C214ED

MD5: 53f2f71eb6e3bb54471e75318eaa64ee

SHA-1: f2b020e3a73db9b72ff85bd9b5e158449f6c003a

To download CSET, select the following link:

Download CSET

If you are unable to download or install CSET from the link, you may request a copy be shipped. To request a copy, please send an email to: cset@hq.dhs.gov. Please insert "CSET" in the subject line and include the following in your email request:

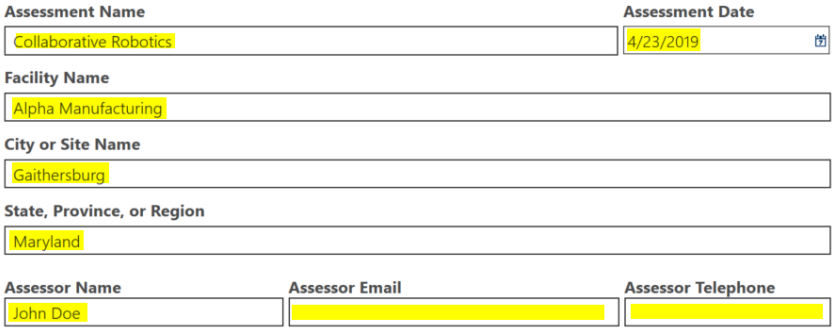
- Your name
- Organization name
- Complete street address (no P.O. boxes)
- Telephone number
- The error or installation issue you encountered when attempting the download

Running CSET for First time:

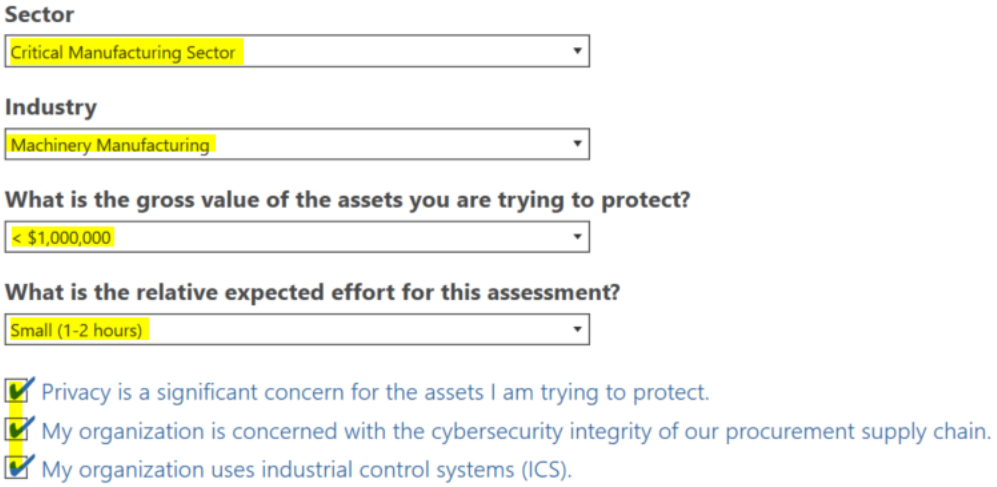
1. Once install of CSET has been completed find the application just installed and double click to run. 
2. Once program has launched you will see the home screen.
3. Click on File and select **"New Assetment"** 

4. Now, click on Start Here button in the lower right corner of program. 

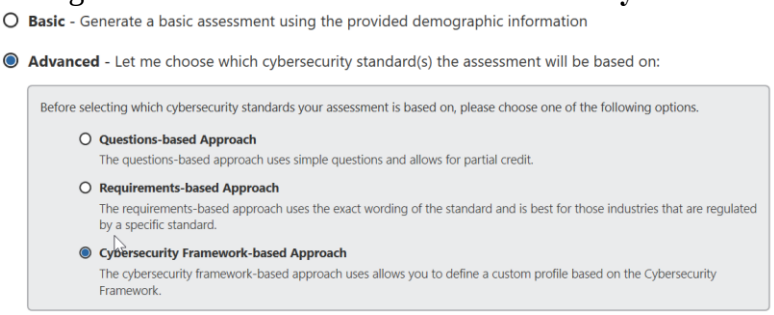
5. Next, enter all required information.



6. Click continue to proceed.
7. Now click on drop down menu and select the appropriate choices. Change any highlight options required.



8. Click continue to proceed.
9. If you want to create a network diagram click the button, otherwise click **"Continue"**.
10. Change Mode Selection to **"Advanced"** and **"Cybersecurity Frame-based Approach"**



11. Click continue.
12. Click continue to use default profile or create a new profile.
13. Click continue again.
14. Now answer the questions as they appear.
15. Complete all questions and generate a final report.

Lessons Learned:

- The tool is only as good as information entered. Make sure each answer is thought out before answering.
- Mark any answer for review as needed so there will be follow up.
- When completed your organization will receive a 0 to 100 score depending on readiness.

4.3.6 Highlighted Performance Impacts

No performance measurement experiments were performed for CSET due to its typical installation location (i.e., external to the manufacturing system).

4.3.7 Link to Entire Performance Measurement Data Set

N/A

4.4 GRASSMARLIN

4.4.1 Technical Solution Overview

GRASSMARLIN is an open source, passive network mapper dedicated to industrial networks and developed by the National Security Agency (NSA). GRASSMARLIN gives a snapshot of the industrial system including:

- Devices on the network
- Communications between these devices
- Metadata extracted from these communications

Points to consider:[11]

- Passive IP network mapping tool
- Hardware agnostic portable Java based tool
- Can only see and map hosts where you are capturing data from.

4.4.2 Technical Capabilities Provided by Solution

GRASSMARLIN provides components of the following Technical Capabilities described in Section 6 of Volume 1:

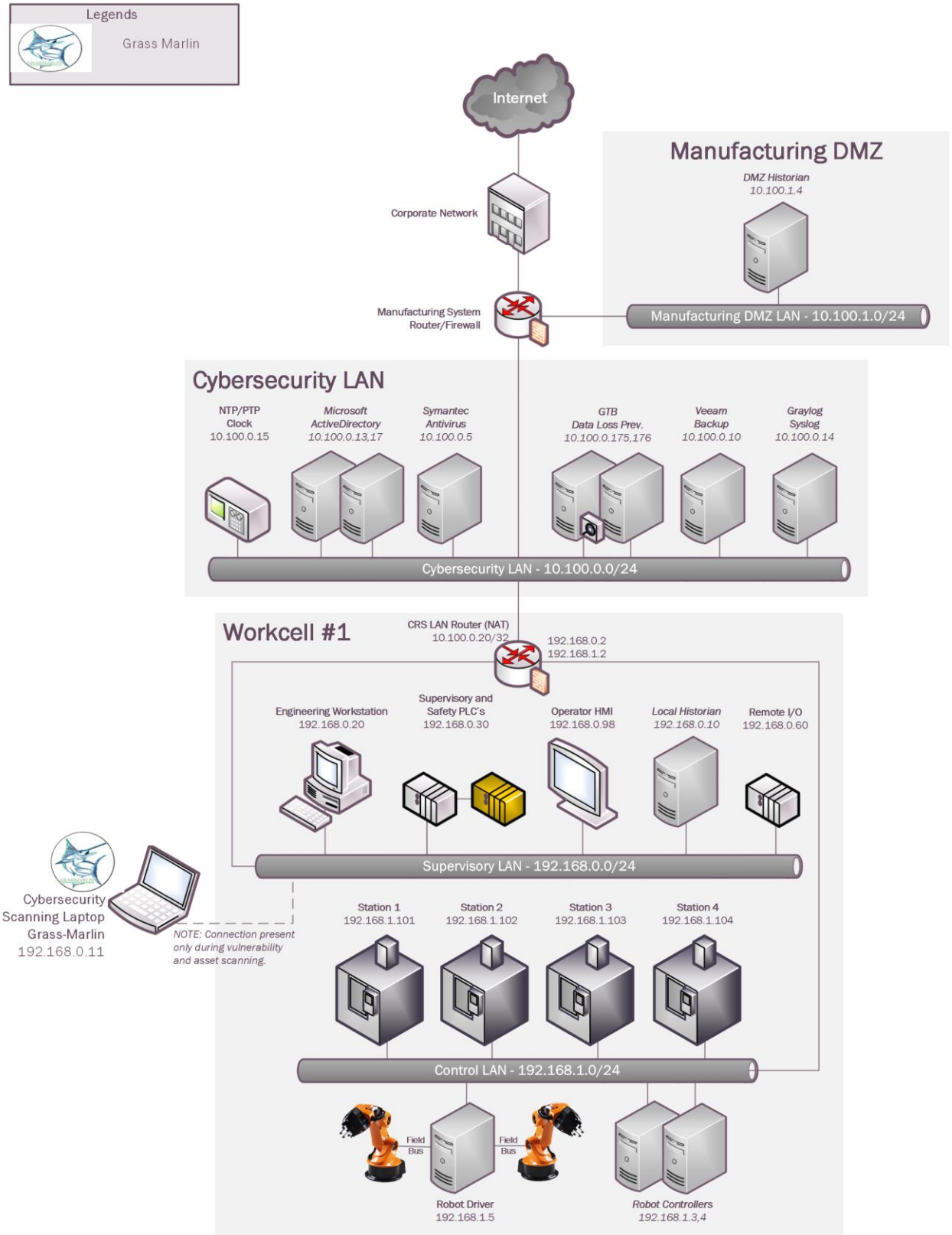
- Network Architecture Documentation
- Baseline Establishment
- Map Data Flows

4.4.3 Subcategories Addressed by Implementing Solution

ID.AM-3, ID.AM-4, PR.AC-5, PR.IP-1, PR.IP-3, PR.MA-1, DE.AE-1, DE.CM-7

[11] GRASSMARLIN Briefing Powerpoint 2017: https://github.com/nsacyber/GRASSMARLIN /blob/master/GRASSMARLIN_Briefing_20170210.pptx

4.4.4 Architecture Map of Where Solution was Implemented



4.4.5 Installation Instructions and Configurations

Details of the solution implemented:

Name	Version
GRASSMARLIN	3.2.1

Setup

- GRASSMARLIN is supported on the following platforms[12]
  Microsoft Windows (64bit, 7 8 and 10)
  Fedora Linux
  Ubuntu (14.04 ,15.10)
  Kali Linux 2.0
  CentOS (6,7)
  Debian (8)

  Download GRASSMARLIN from https://github.com/nsacyber/GRASSMARLIN/releases as per the OS version of your system. Upon download, run the installer. The installer will install additional programs such as Java and Wireshark during the setup.
- GRASSMARLIN can operate in a real time passive mode by sniffing the live traffic or by importing a recorded pcap file. Data in GRASSMARLIN is stored in a Session. The Session contains imported files and visual state information.
- GRASSMARLIN was installed on the Cybersecurity Scanning Laptop running Windows 10.

Using the Software:

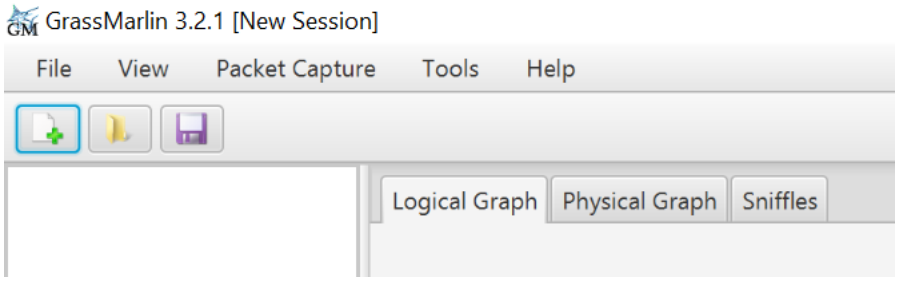
- A captured pcap file from the CRS system was imported in GRASSMARLIN to generate a network baseline. The pcap was captured by the running the tcpdump command on a Linux system which had a network connection from a Network aggregator device. This Aggregator was configured with mirror port connections in coming from the different network segments such as Supervisory LAN and Control LAN.

  tcpdump -i <mirror-port interface> -w mypcap.pcap

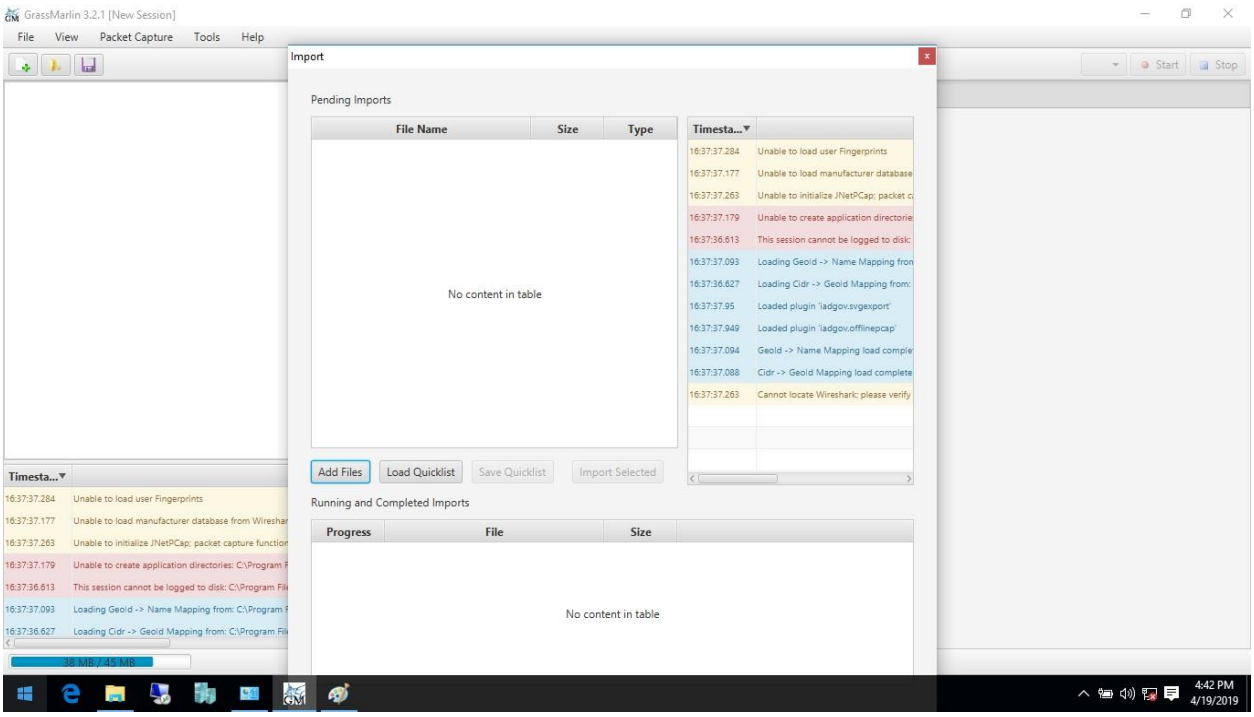
  For example: tcpdump -i eth1 -w /home/icssec/robotics.pcap
  Where eth1 is our mirror port connection

[12] GRASSMARLIN User Guide: https://github.com/nsacyber/GRASSMARLIN

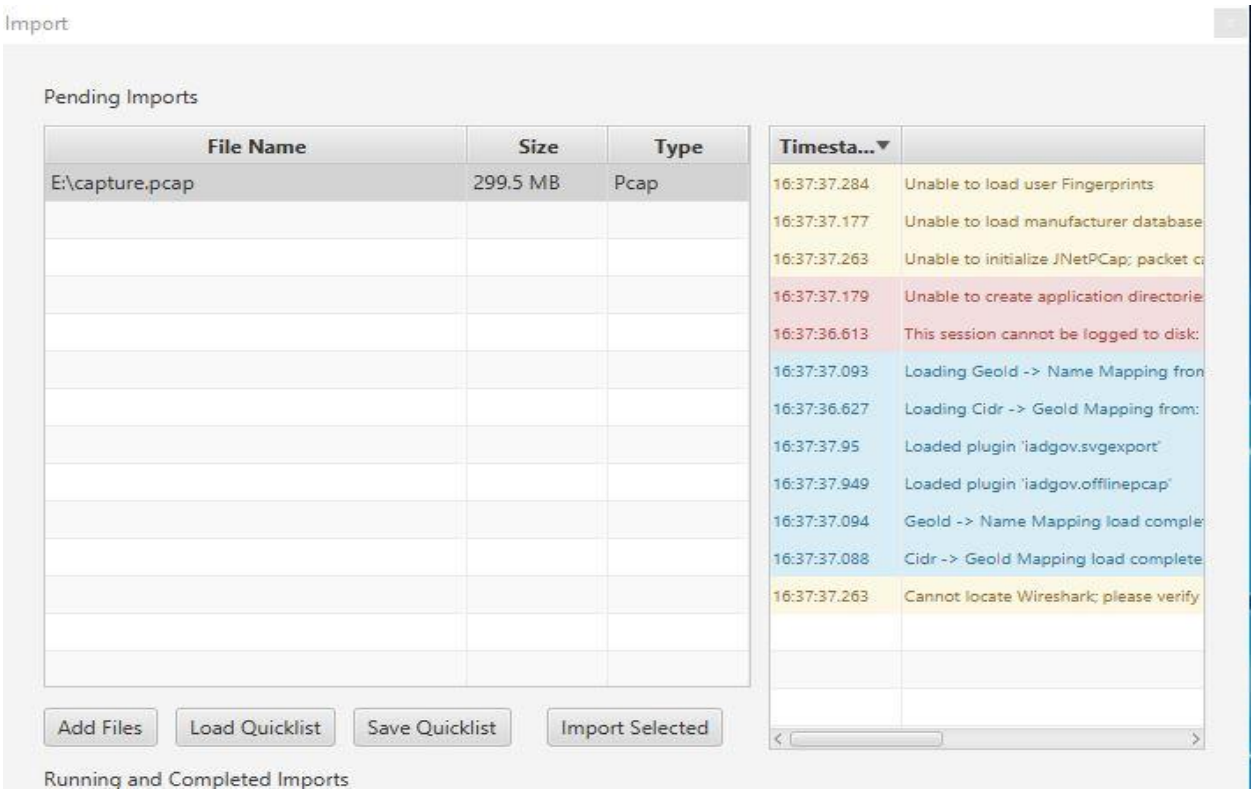
- To run GRASSMARLIN on a Windows or a Linux system with a Desktop, simply double click on the "GRASSMARLIN" shortcut or icon from the Programs Menu. To run it on a Linux system without a Desktop, type the command "**GRASSMARLIN**" or "**sudo GRASSMARLIN**" and the interface should load up.
- To Import a pcap in GRASSMARLIN, click on the **Import** icon in the toolbar (or select **Import files** from the File Menu)



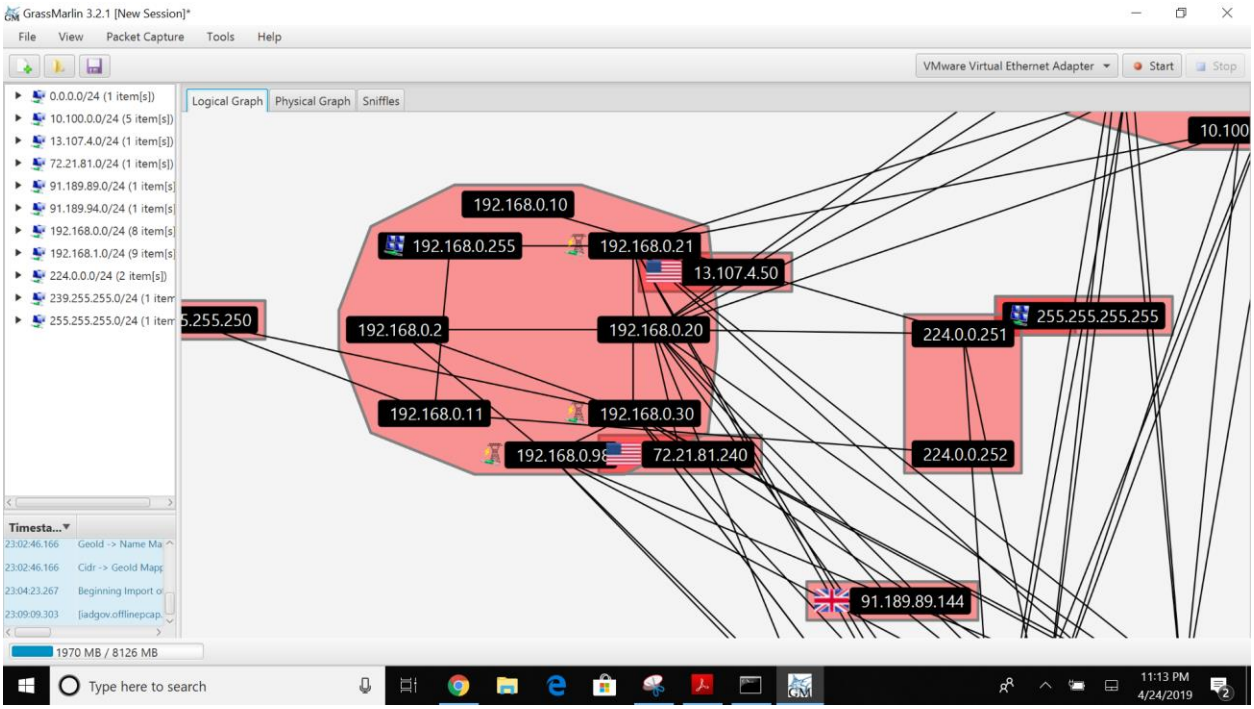
- Click on **Add Files.** Browse to the PCAP



- The Pcap will now show up under Pending Imports**.** Select the file and click on **"Import Selected".** Hit the **Close** button at the bottom of the page. The Import process can take several minutes to **hours** depending on the size of the pcap file.

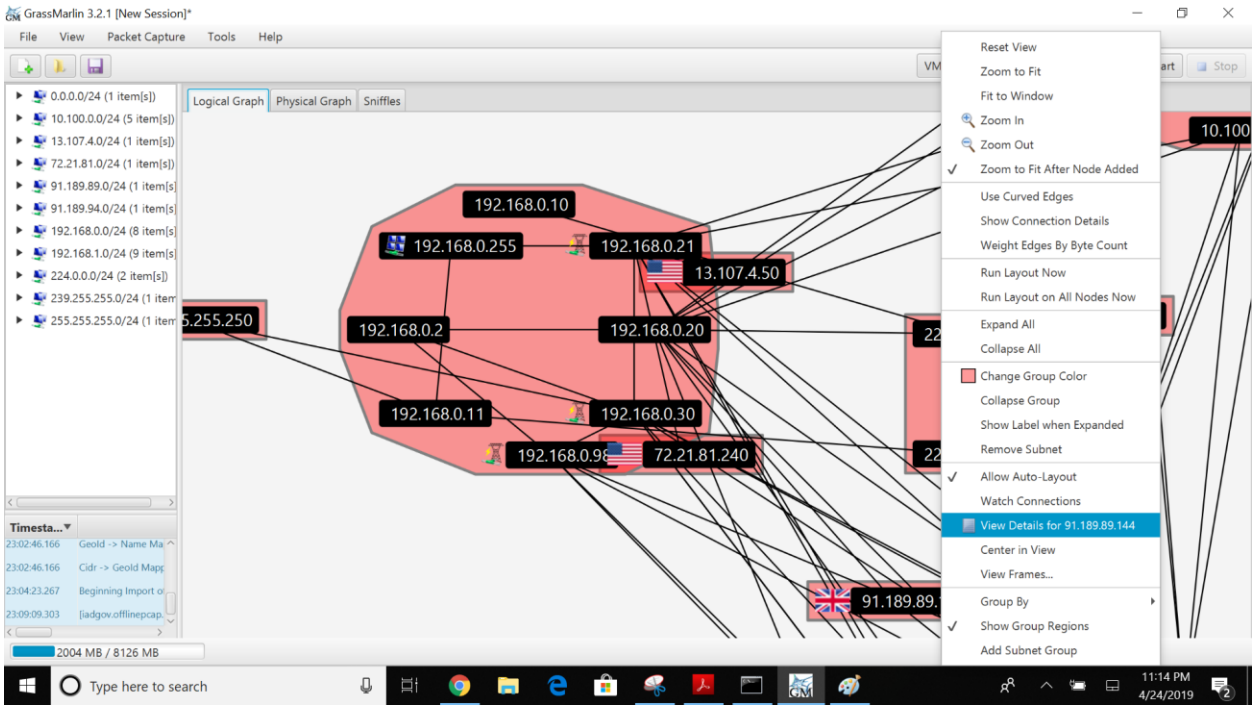


- Once complete, the screen will display a Logical Graph of the network topology.



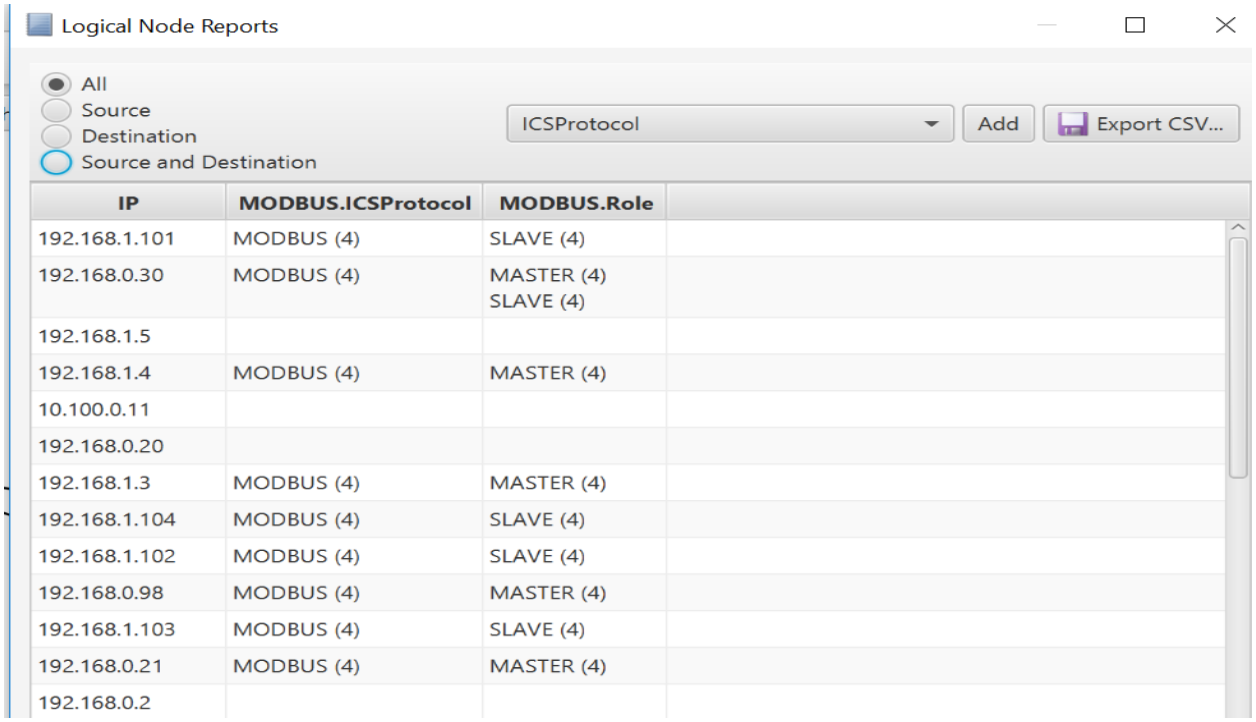
Take a moment to review the logical graph. Any public IP address will be highlighted with their respective Country's flag. This can be useful in finding out information about any external IP's that your network is communicating with.

Right-click on any external node IP address in question >> **View Details for <IP address>**

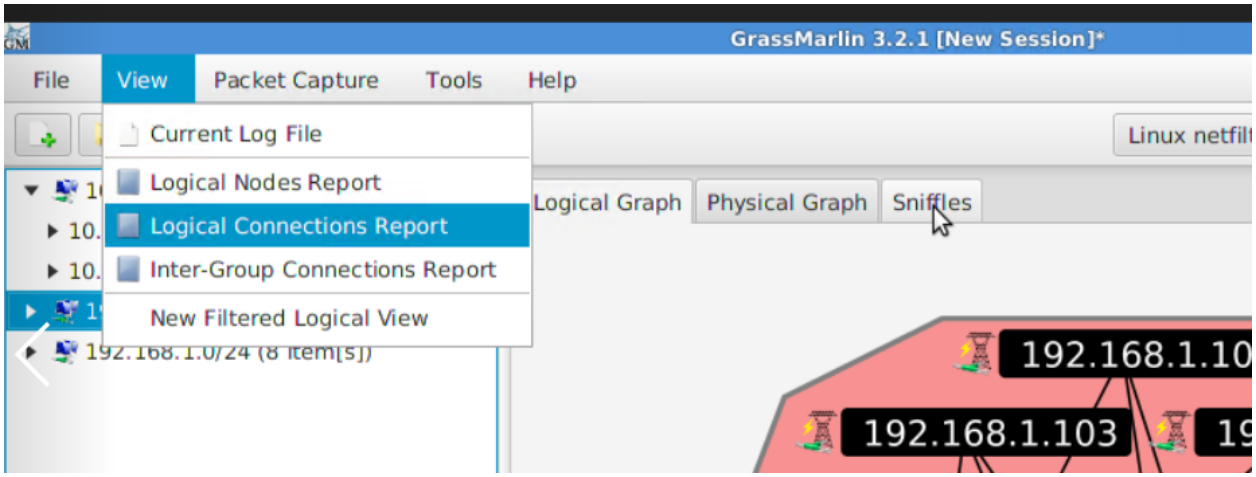


- To Generate a list of all nodes in the Logical Graph, click on **View** (Top Menu) >> **Logical Nodes Report.** By default, only a single column (IP) is present, although additional columns can be added with any Property present in the set of Nodes.

  To add a column, select the Property Name from the drop-down and click the Add button.

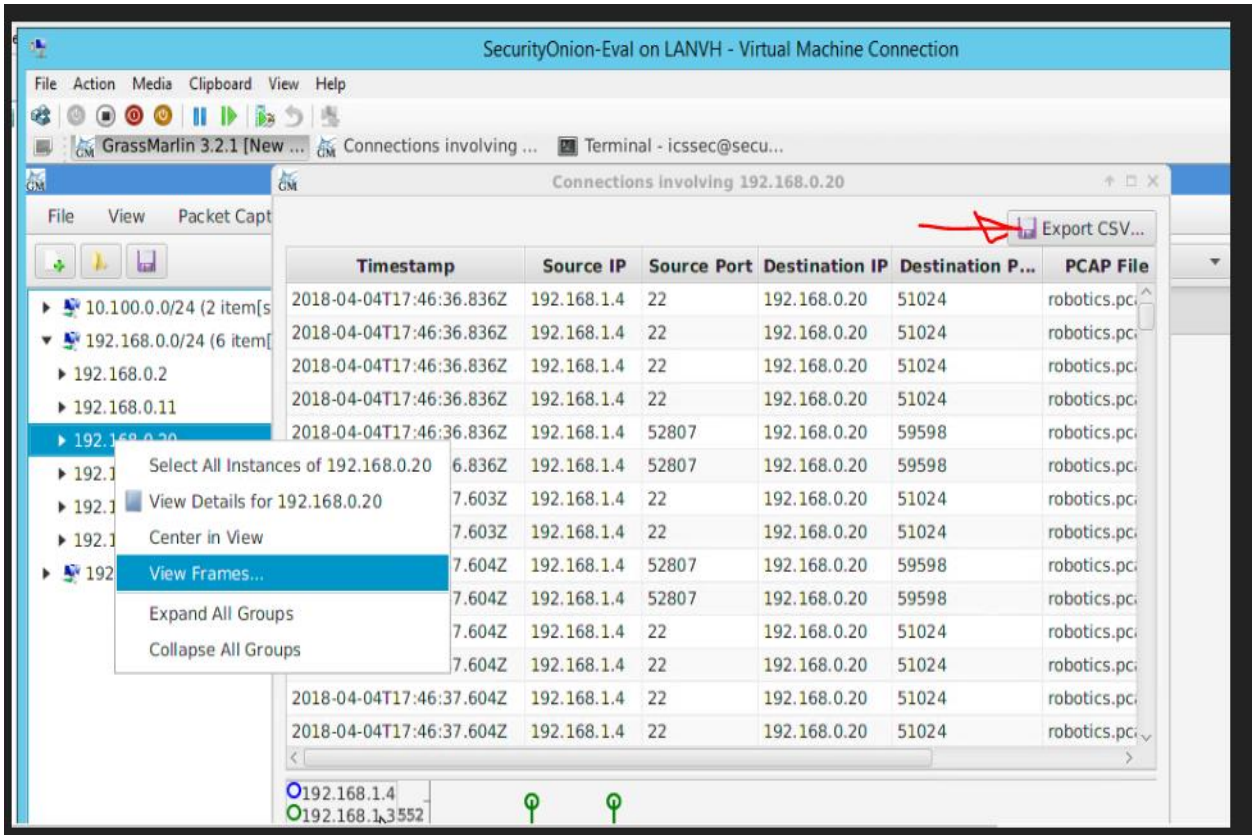


- Click on **View** >> **Logical Connections Report** to view a summary of all connections captured by the pcap file.

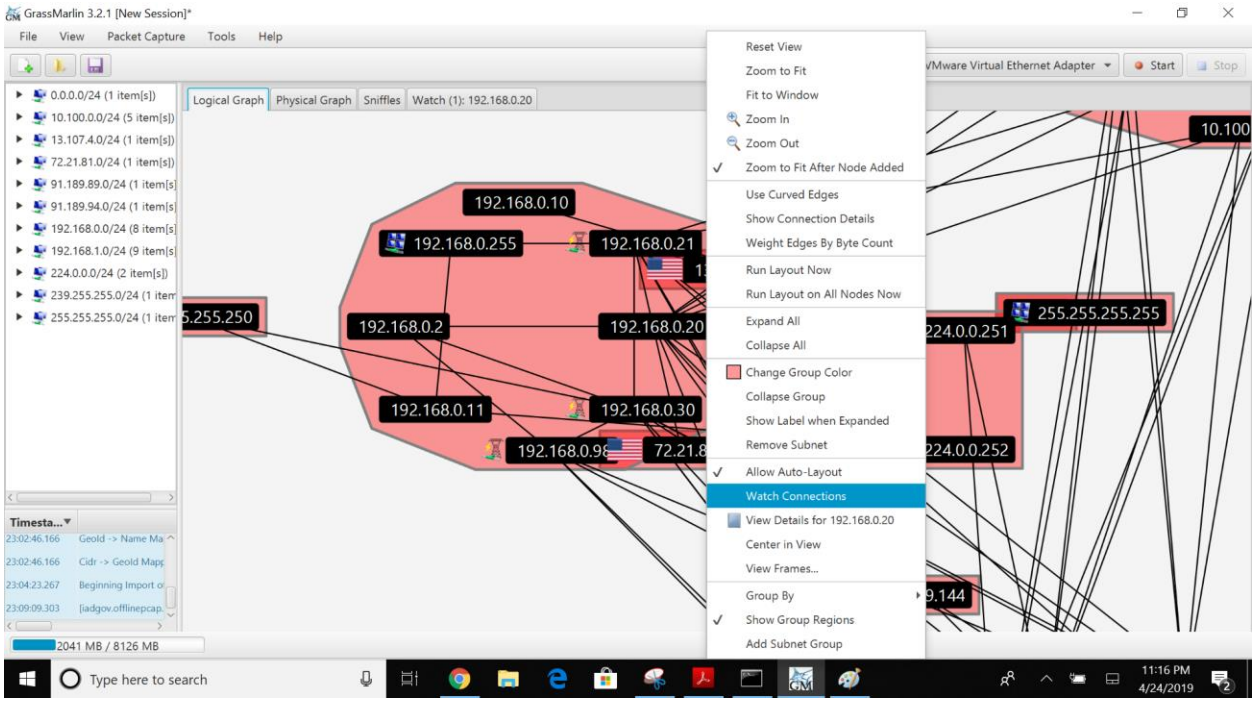


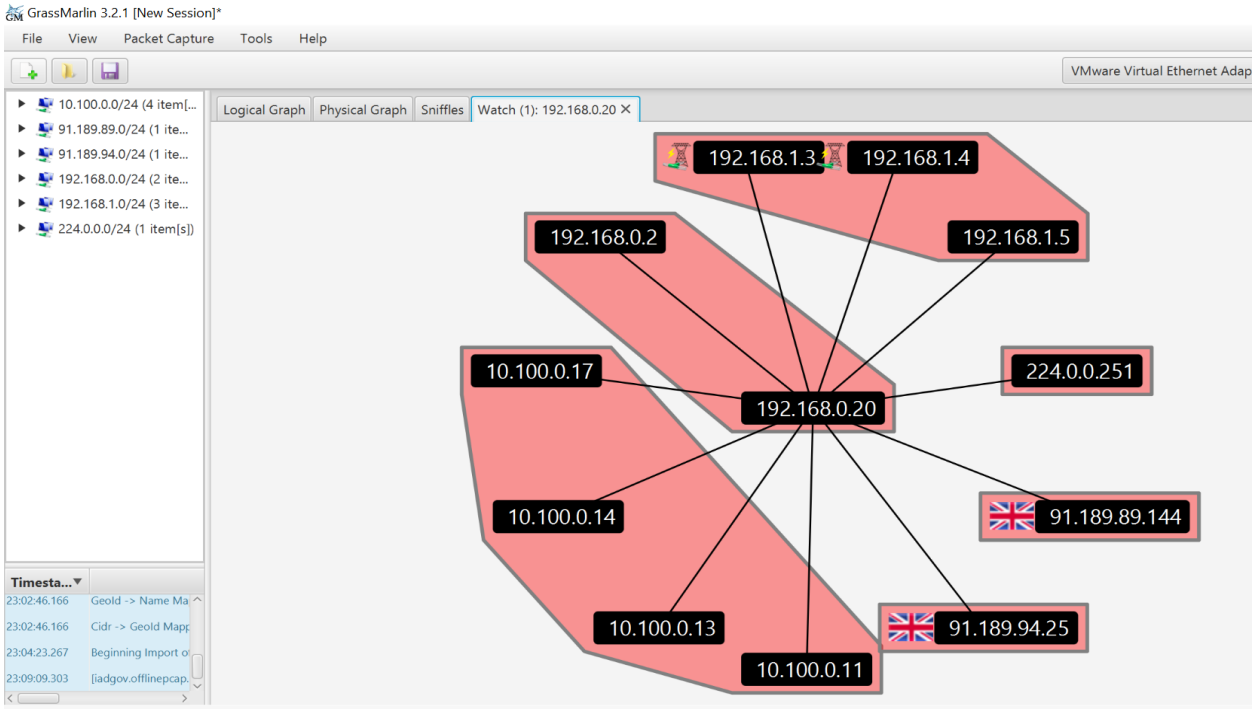
- To view all the logical communications for a specific host for capturing a baseline, Right-click on a **Node** >> **View Frames**. This opens a new screen as shown below displaying all the different IP addresses including ports and protocol information that the selected node is communicating with. You may click further on "**Export CSV**" button to export this data to a csv file.

Note: This process needs to be repeated on every host to capture a baseline of entire network.



- Another interesting feature is Watch-Graphs. A Watch Graph is a subset of Logical graph, created for a particular node and shows all the different nodes connected to it. This can be generated using **Watch-connections** menu. Right-click a node >> select **Watch Connections**. This will generate a graph in a new window "**Watch <IP address>**"


GrassMarlin 3.2.1 [New Session]*
File
View
Packet Capture
Tools
Help
Logical Graph
Physical Graph
Sniffles
Watch (1): 192.168.0.20
Reset View
Zoom to Fit
Fit to Window
Zoom In
Zoom Out
Zoom to Fit After Node Added
Use Curved Edges
Show Connection Details
Weight Edges By Byte Count
Run Layout Now
Run Layout on All Nodes Now
Expand All
Collapse All
Change Group Color
Collapse Group
Show Label when Expanded
Remove Subnet
Allow Auto-Layout
Watch Connections
View Details for 192.168.0.20
Center in View
View Frames...
Group By
Show Group Regions
Add Subnet Group
192.168.0.10
192.168.0.255
192.168.0.21
192.168.0.2
192.168.0.20
192.168.0.11
192.168.0.30
255.255.255.255
224.0.0.251
224.0.0.252
2041 MB / 8126 MB
Type here to search
11:16 PM
4/24/2019


GrassMarlin 3.2.1 [New Session]*
File
View
Packet Capture
Tools
Help
Logical Graph
Physical Graph
Sniffles
Watch (1): 192.168.0.20
192.168.1.3
192.168.1.4
192.168.1.5
192.168.0.2
10.100.0.17
224.0.0.251
192.168.0.20
10.100.0.14
91.189.89.144
10.100.0.13
91.189.94.25
10.100.0.11

4.4.6 Highlighted Performance Impacts

No performance measurement experiments were performed for the use of GRASSMARLIN due to its installation location and how it was used (i.e., the software performed offline analysis of PCAP files captured by other software).

4.4.7 Link to Entire Performance Measurement Data Set

N/A

4.5 Wireshark

4.5.1 Technical Solution Overview

Wireshark is a free and open-source packet analyzer. It is user friendly, simple to implement, just need to ensure network connection plugged in is configured to display traffic correctly i.e. Port mirroring.

4.5.2 Technical Capabilities Provided by Solution

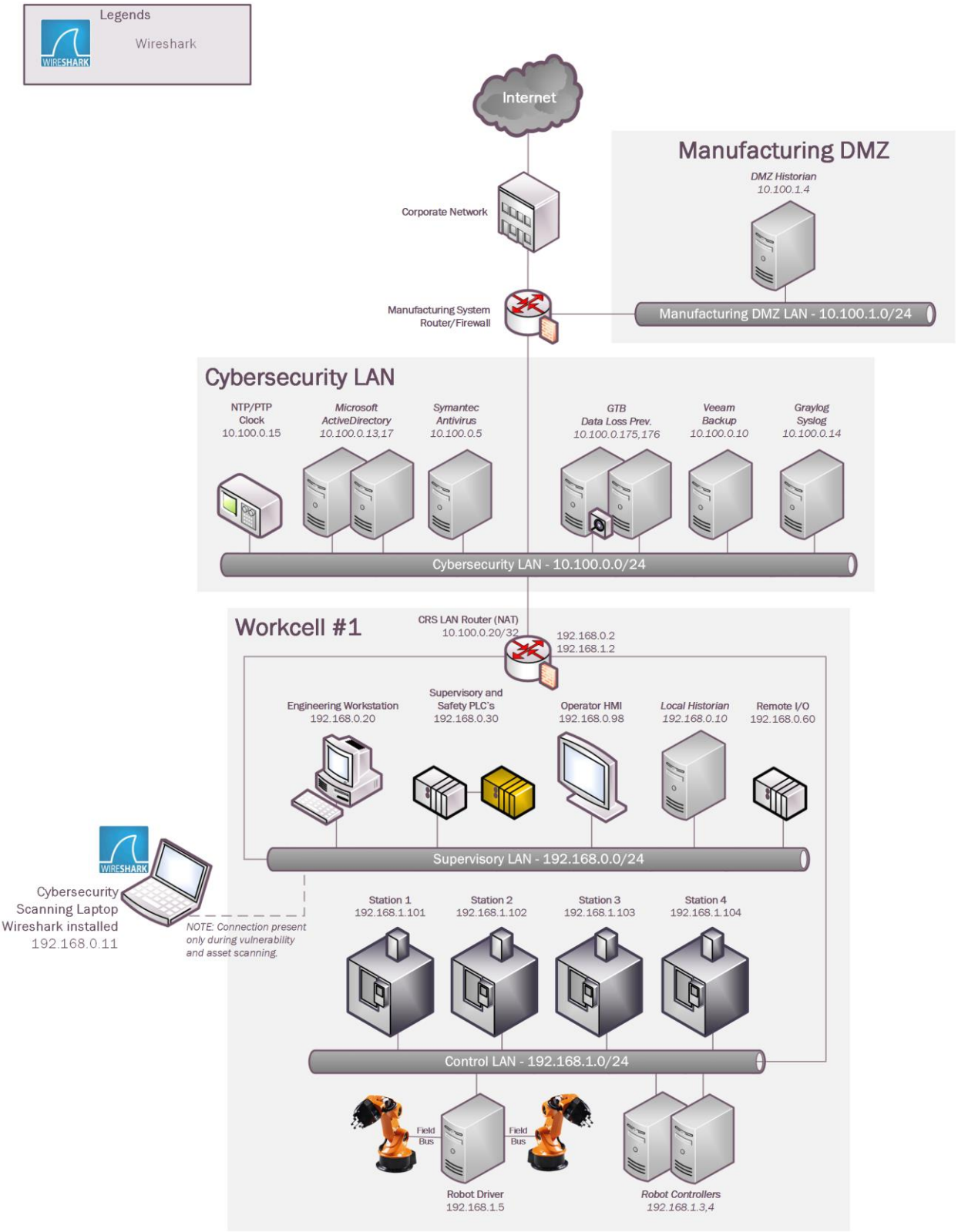
Wireshark provides components of the following Technical Capabilities described in Section 6 of Volume 1:

- Network Architecture Documentation
- Baseline Establishment
- Map Data Flows
- Forensics

4.5.3 Subcategories Addressed by Implementing Solution

ID.AM-3, ID.AM-4, PR.AC-5, PR.IP-1, PR.IP-3, PR.MA-1, DE.AE-1, DE.AE-2, DE.CM-7, RS.AN-3

4.5.4 Architecture Map of Where Solution was Implemented

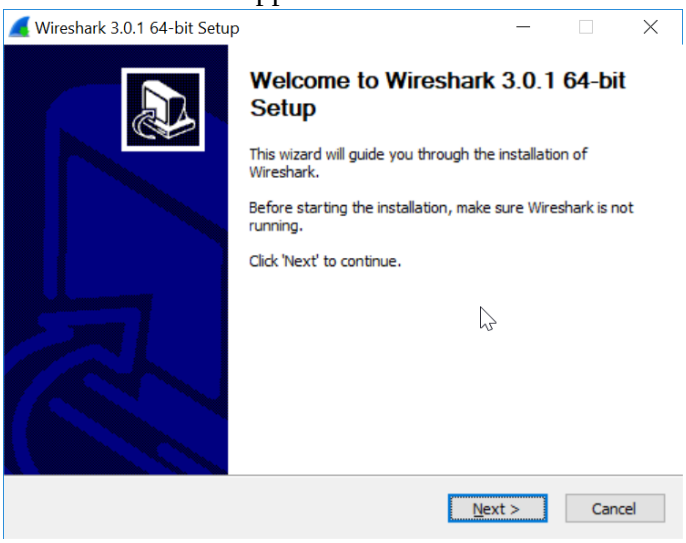


4.5.5 Installation Instructions and Configurations

Steps for installing Wireshark

Download and Installation instructions:

1. Only download Wireshark from https://www.wireshark.org **(Select 32bit or 64 bit)**
2. Once download has completed locate the executable just downloaded and double click to start install process. C:\Users\johndoe\Downloads\Wireshark-win64-3.0.1.exe
3. If prompted for password enter administrator account on local machine.
4. When first Screen appears click **"NEXT"**

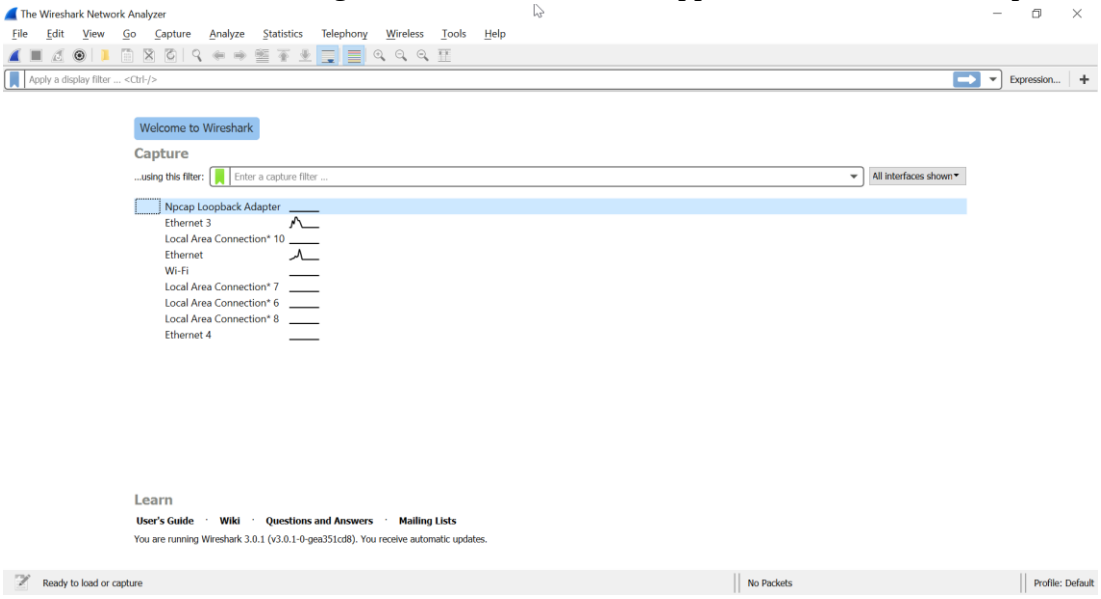


5. Click **"Agree"** to continue.
6. Leave default selected and click **"Next"** five times to continue install. (Make changes if all features aren't required. This will be uncommon)
7. When prompted for Npcap install click **"I Agree"** to continue.
8. Leave default and click **"Install"**.
9. Now click **"Next and Finish"** to start process.
10. Click next and then select **"Reboot Now"** or **"I want to manually reboot later"**
11. Click **"Finish"** to complete.

Running Wireshark and configure

1. Click start button and find program labeled **"Wireshark"**.
2. Once Wireshark is found right click on icon and select **More→Run as Administrator (Windows 10)** Older operating system can just hold down **"Shift + Right Click"** menu will appear for run as, select administrator to continue.
3. Wireshark requires administrative privileges to be fully functional, otherwise there will be undesired results.

4. Once Wireshark is running the initial interface will appear that the screen shot provided.

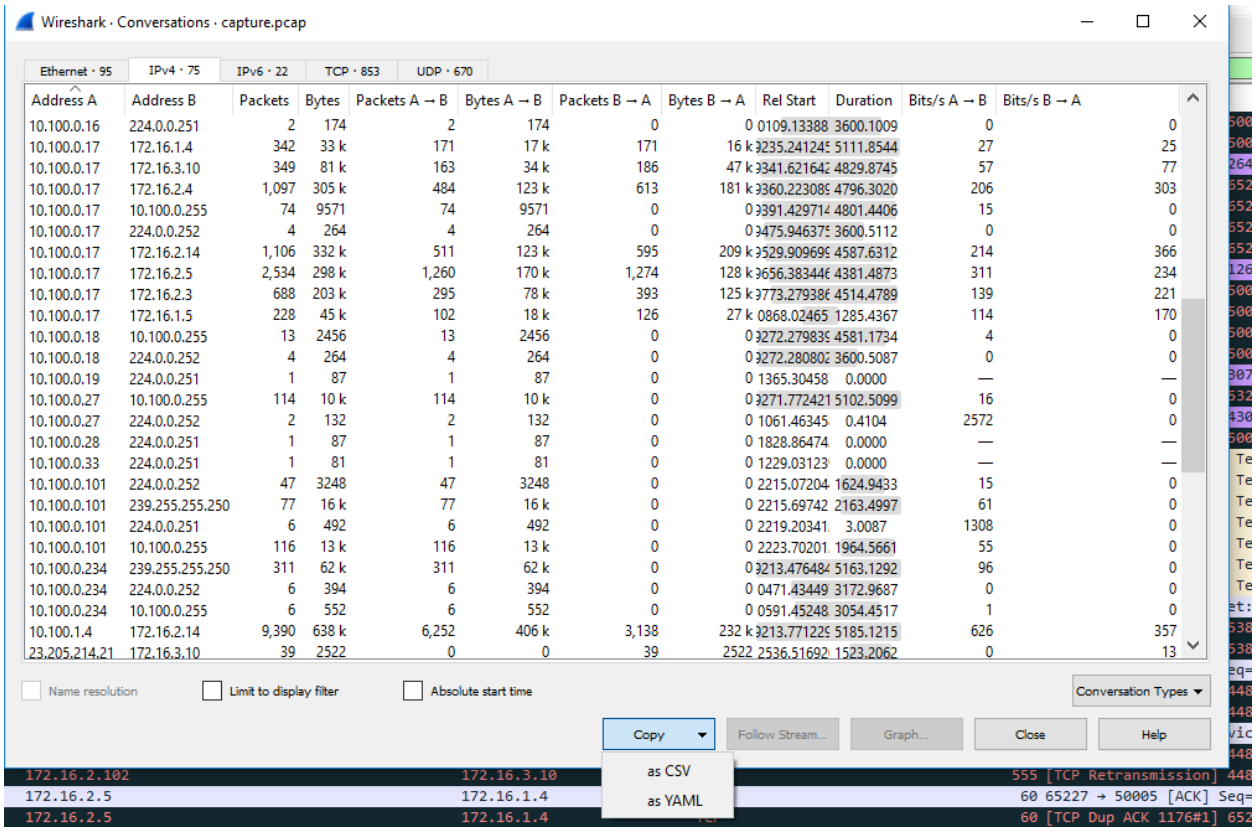


5. Select the interface to be monitored.

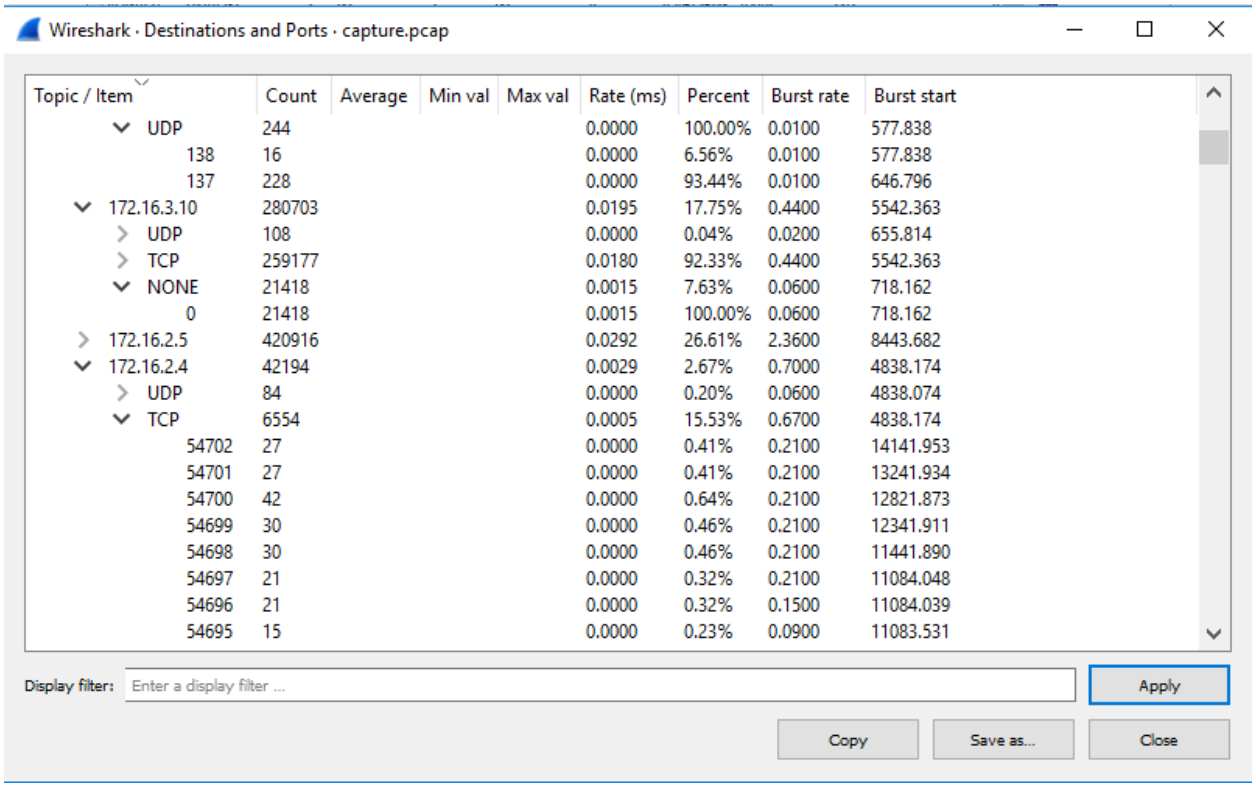
Wireshark provide lots of information and can be hard to decipher https://www.wireshark.org provides documentation along with searches for additional command syntax.

Capturing Network Baseline using Wireshark

1. Launch Wireshark. Click **Open** to load a previously captured pcap file or run a **"Start Capture"** as explained in the previous section to record traffic.
2. Upon loading the pcap or capturing live traffic; click on **Statistics** >> **Conversations**
3. This will generate a window similar to the one below which will list all the different types of communications happening between all endpoints in your traffic. Click **COPY** >> **as Csv** to save this data as a Csv file for further analysis.



4. To get a list of ports used, Click on **Statistics** >> **IPv4 Statistics** >> **Destination and Ports.** This will generate a list of ports used by all the IP addresses in the traffic. Click **Copy**, to copy the results to a word document or click **Save as** to save as a plain text file. Hit **Close** when done.



4.5.6 Highlighted Performance Impacts

No performance measurement experiments were performed for the use of Wireshark due to its typical usage (i.e., the software performs passive capturing of network packets using existing mirror/SPAN ports or bump-in-the-wire network taps, and the software was installed a laptop that is attached to the network only during maintenance and engineering activities).

4.5.7 Link to Entire Performance Measurement Data Set

N/A

4.6 Veeam Backup and Replication

4.6.1 Technical Solution Overview

Veeam Backup and Replication is a proprietary backup and incident recovery software developed by Veeam for virtual environments. It is built on VMware vSphere and Microsoft Hyper-V hypervisors. The software provides backup, restore and replication functionality for virtual machines. Veeam® Backup and Replication suite delivers availability for all workloads - virtual, physical, cloud (including VMware vSphere and Microsoft Hyper-V) -from a single management console. It provides fast, flexible and reliable recovery of your applications and data, and brings backup and replication together into a single software solution [1].

The Veeam Backup Free Edition lets you back up your VMs on the fly and provides you with flexible storage options, including file-based (NFS) primary storage, for easy archiving and quick recovery. Veeam also has products such as “Veeam agent for Windows” and “Veeam agent for Linux” for backing up physical Windows and Linux servers respectively.

Points to consider:

- Free backup edition available for virtual and physical servers.
- Support for file level backups as well as system image type of backups.
- Backups can be run without having to shut down the system. This can be very critical in ICS/SCADA environments.
- Tech support available for Free edition users.
- Easy to setup and use. Lot of documentation available online to get started.

4.6.2 Technical Capabilities Provided by Solution

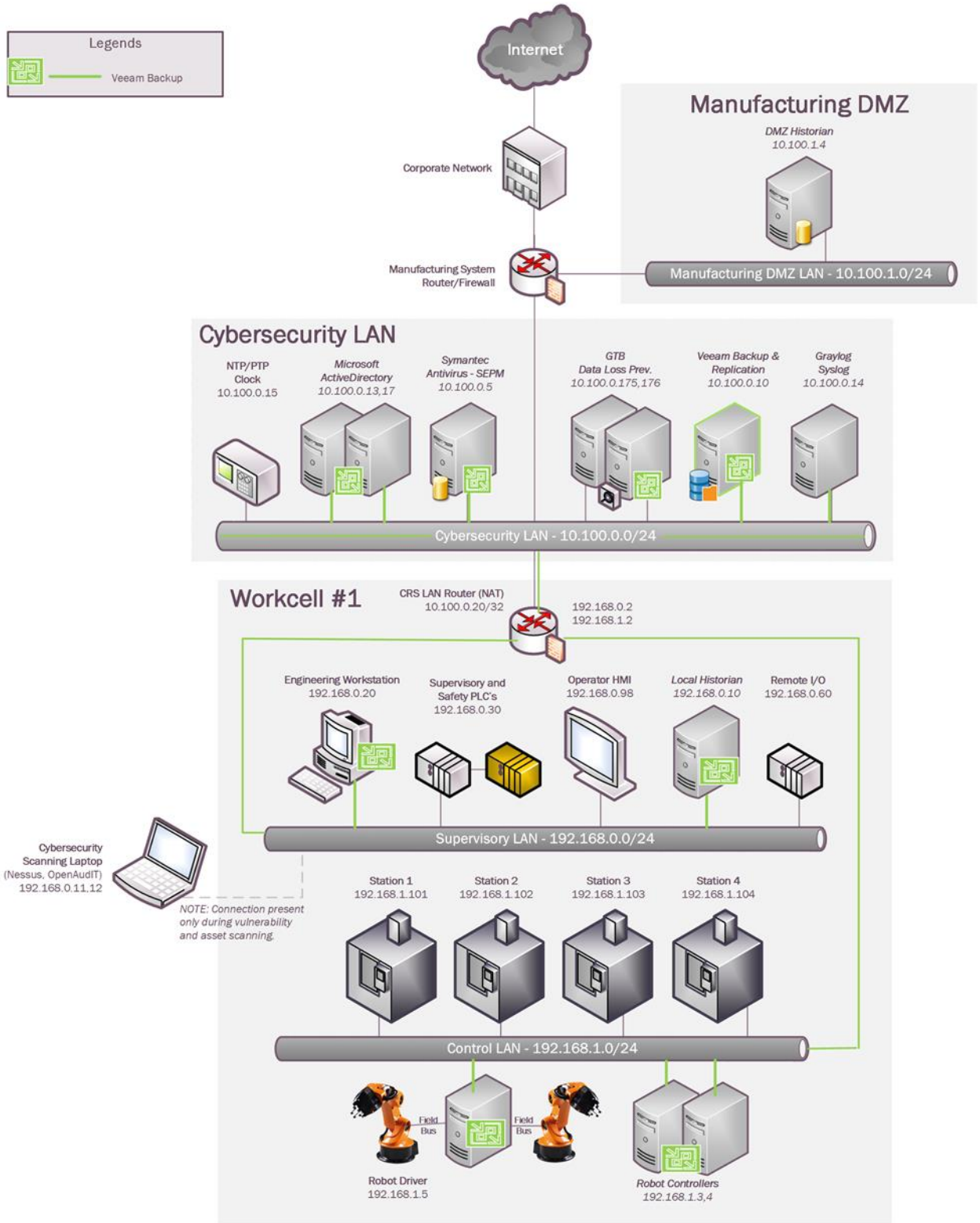
Veeam Backup and Replication provides components of the following Technical Capabilities described in Section 6 of Volume 1:

- Data Backup
- Data Replication

4.6.3 Subcategories Addressed by Implementing Solution

PR.IP-4

4.6.4 Architecture Map of Where Solution was Implemented



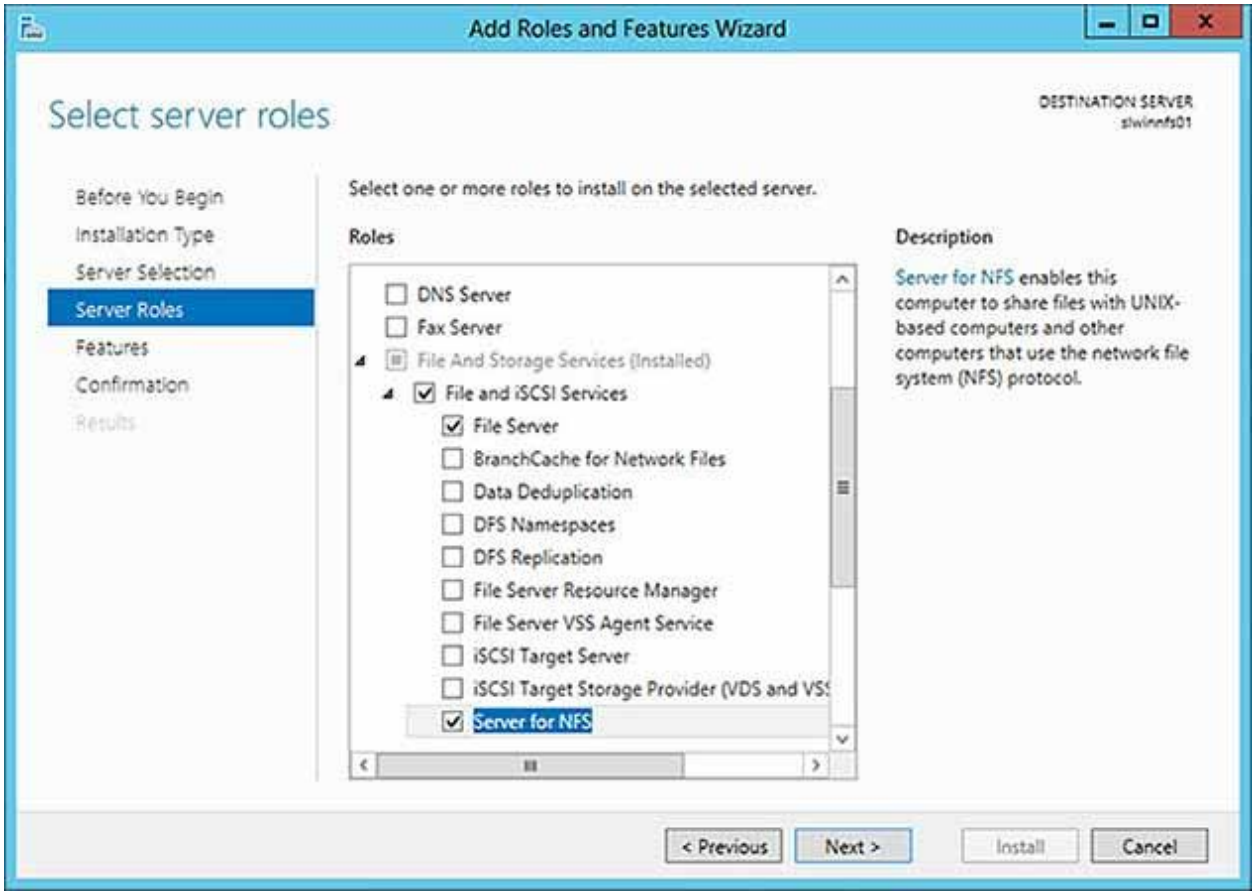
4.6.5 Installation Instructions and Configurations

Setup

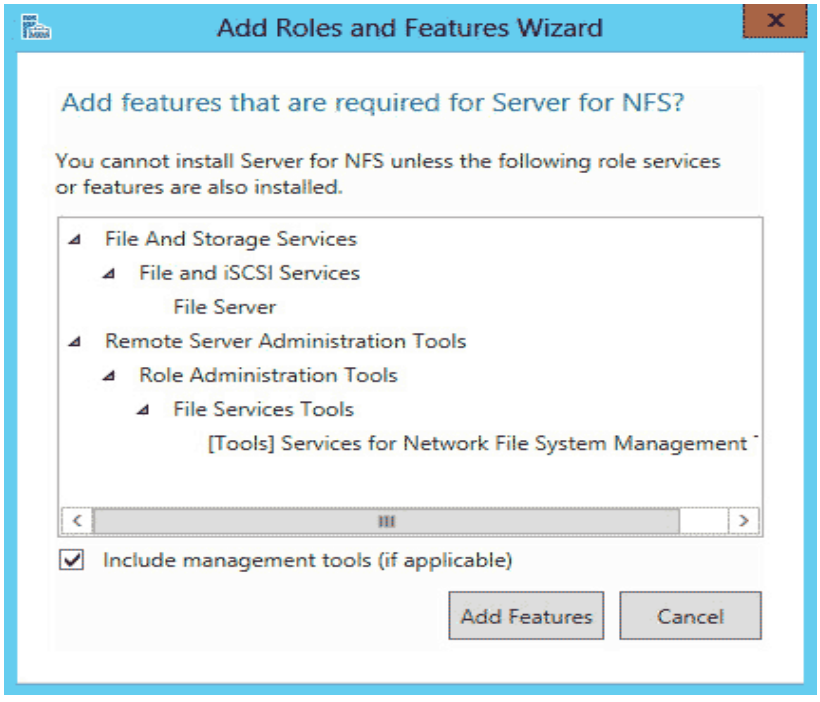
- The following products from Veeam were implemented

Name	Purpose	Version
Veeam Backup and Replication	Veeam Backup Server and Repository	9.5
Veeam Agent for Linux (Free version)	For backup/recovery of Physical Linux Systems in Robotics Network	3.0.0.865

- A Windows 2012 R2 Virtual Machine was setup in the Cybersecurity LAN for installing Veeam Backup and Replication Server. Around 4TB of storage was allocated to this VM for backup storage.
- The Free Edition of Veeam Backup and Replication lets you manage virtual machine backups from the Central Veeam BandR Console. However, any physical servers configured for backup using the Veeam agent cannot be managed from the Central console in the Free edition. These need to be managed locally on the endpoint or client system itself.
- A NFS share folder was setup on the same 4TB drive for saving backups. This NFS directory would then be mounted on the Linux clients of the Robotics system. NFS Shares can be hosted on Windows 2012 by installing the Role/Feature "**Server for NFS**" under "**File and iSCSI Services**" as shown below

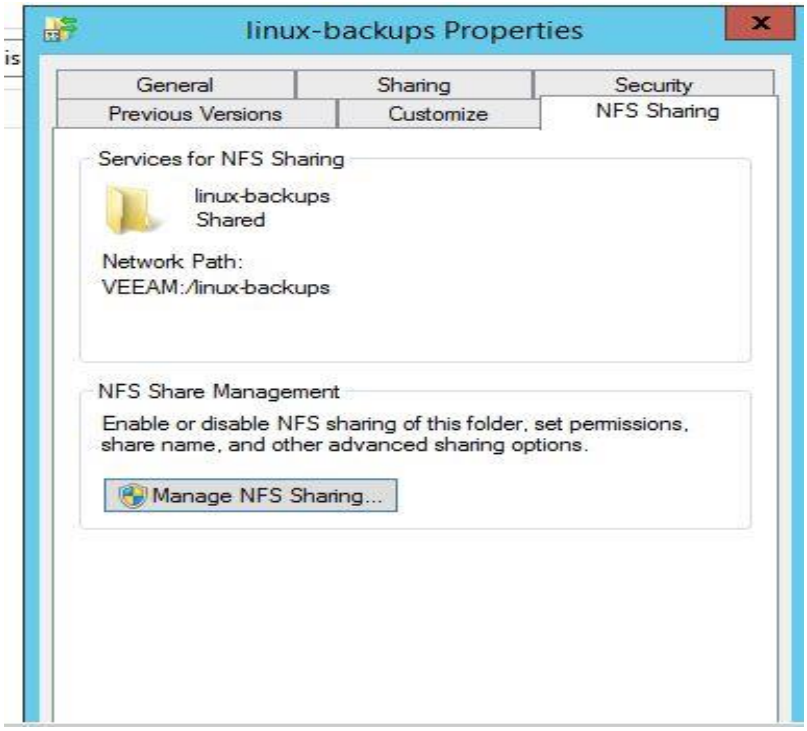


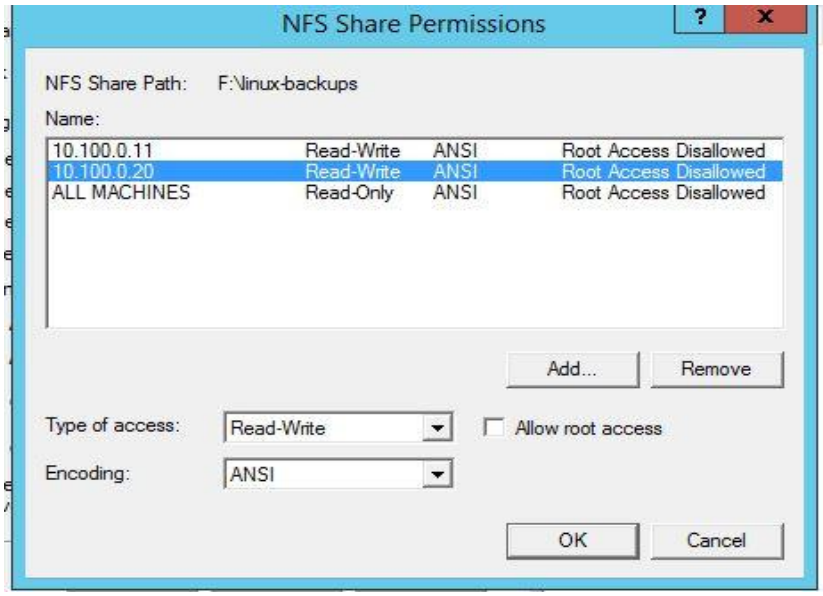
3187
3188



3189
3190

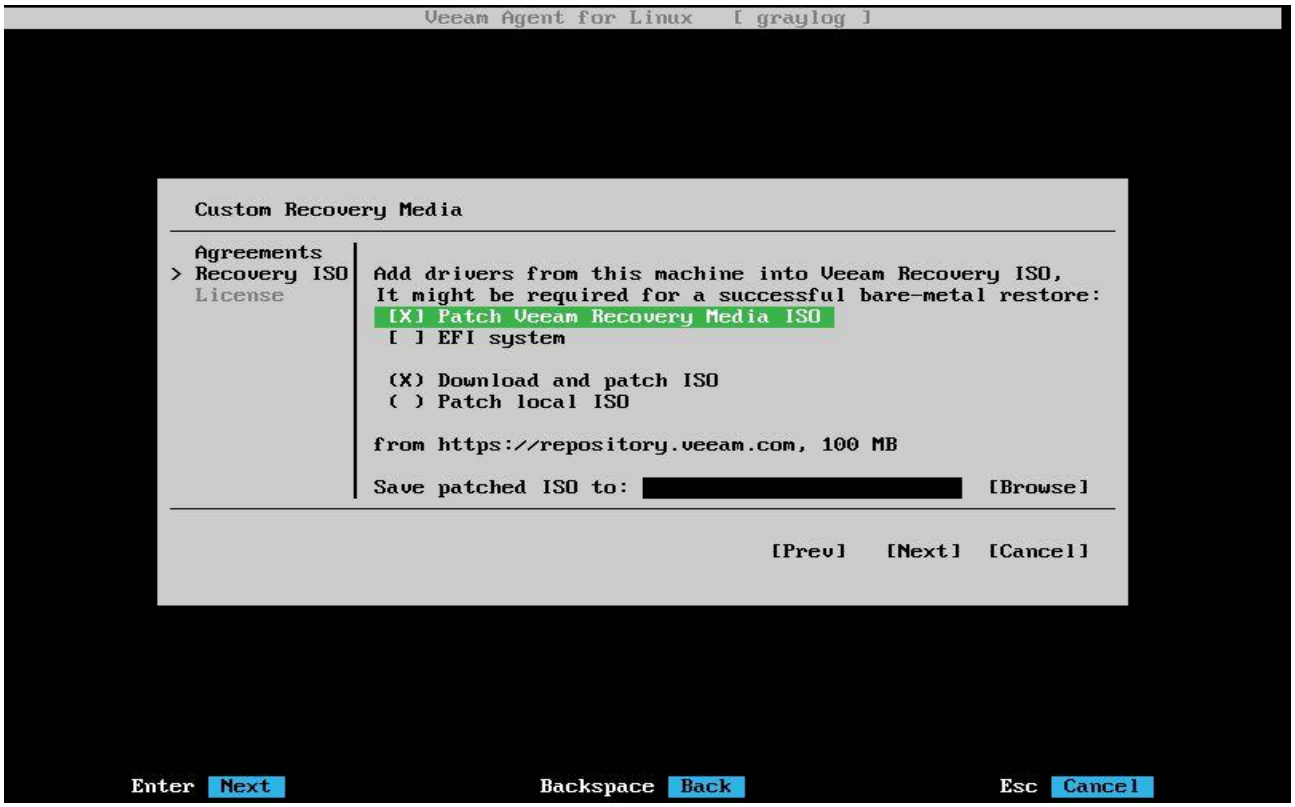
- Next, a directory named **linux-backups** was created. The below two images shows the NFS share permissions configured on this directory. The IP address **10.100.0.20** is the NAT IP address of the traffic coming out of Robotics Systems. Ensure to not select "Allow Root access" for security reasons.
  Right-click on the Directory >> Select **NFS-Sharing tab** >> **Manage NFS Sharing**



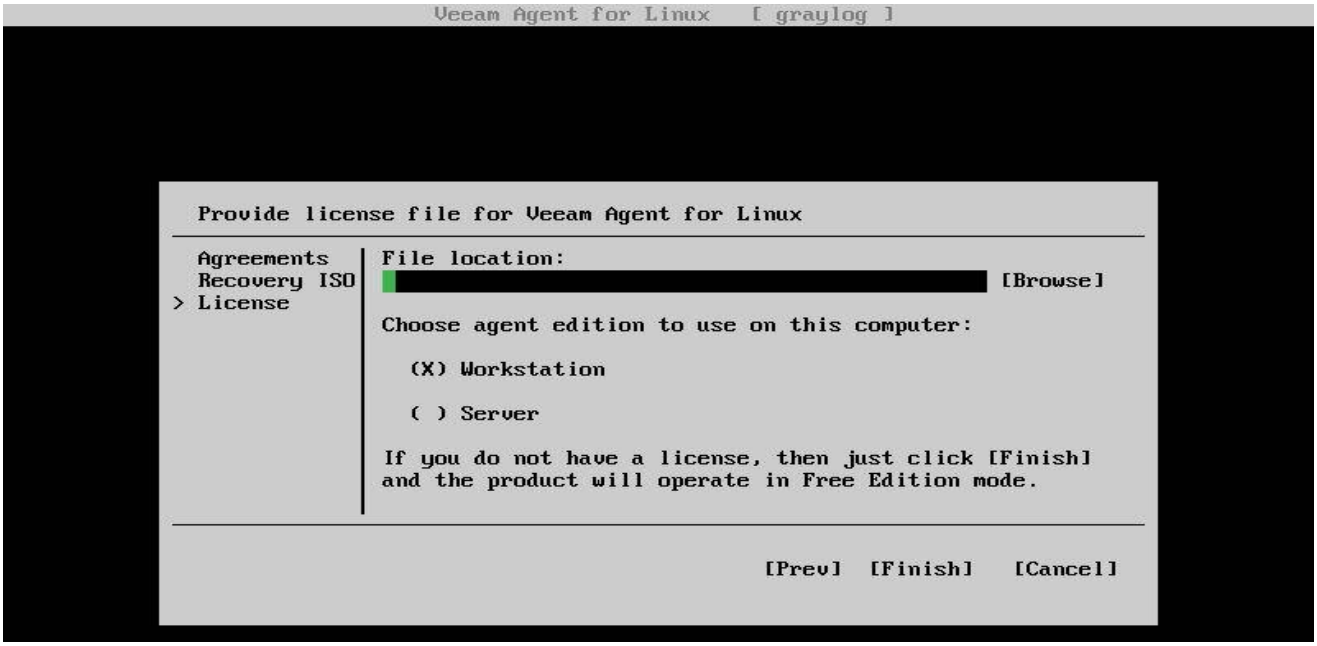


Configuring Backups

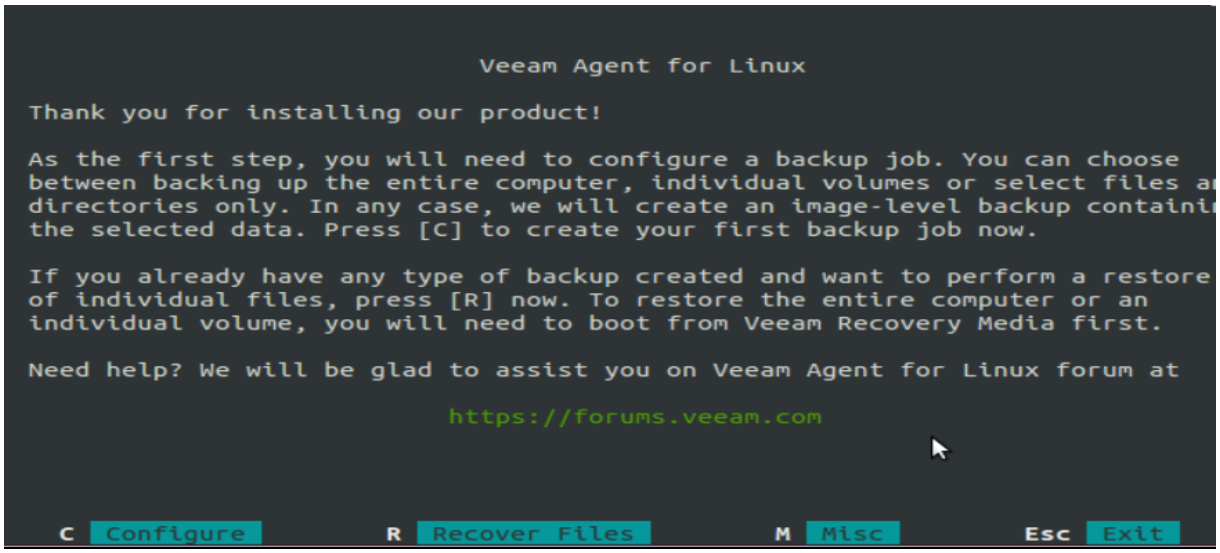
- All Linux systems in Collaborative Robotics system were configured for Backup using Veeam Agent for Linux [2].
- The **Offline Mode** of Agent installation was followed using the below instructions as the Linux systems did not have internet connectivity https://helpcenter.veeam.com/docs/agentforlinux/userguide/installation_offline.html?ver=30
- Network connectivity between the Linux clients and the Veeam server was verified using telnet for NFS ports. If using NFS to connect to Veeam server, ensure to test if the NFS mount folders can be accessed and written to from the Linux client.
- A backup or restore operation needs to be initiated from the client system. Once the agent is installed, run a **sudo veeam** command to launch the Veeam Control Panel utility. The initial screen will look as shown below. Accept the **End User Agreement** and click on **Continue**.
- Under **Recovery ISO** You can either select "**Patch Veeam Recovery media ISO**" and "**Download and patch ISO**" if the Linux system has internet connectivity else both of these options can be unchecked and proceed. The Veeam Recovery Media for Linux can also be downloaded manually from the Veeam website.



- Under License, just Click **FINISH** for Free Edition Mode

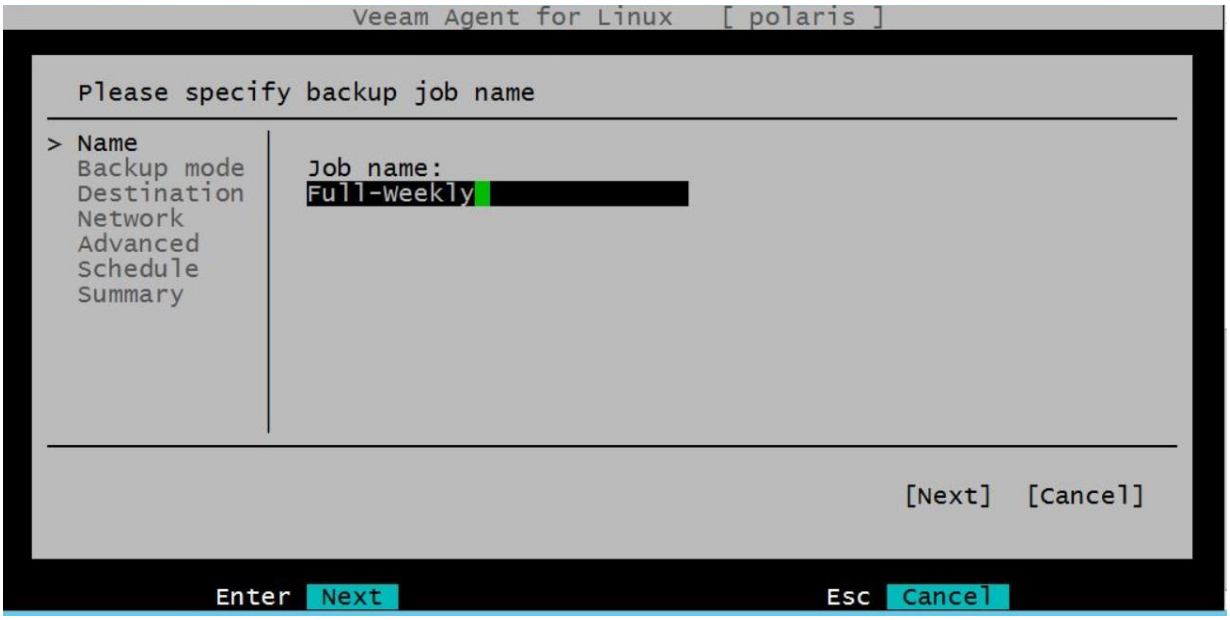


- Press “C” to Configure a new backup job.



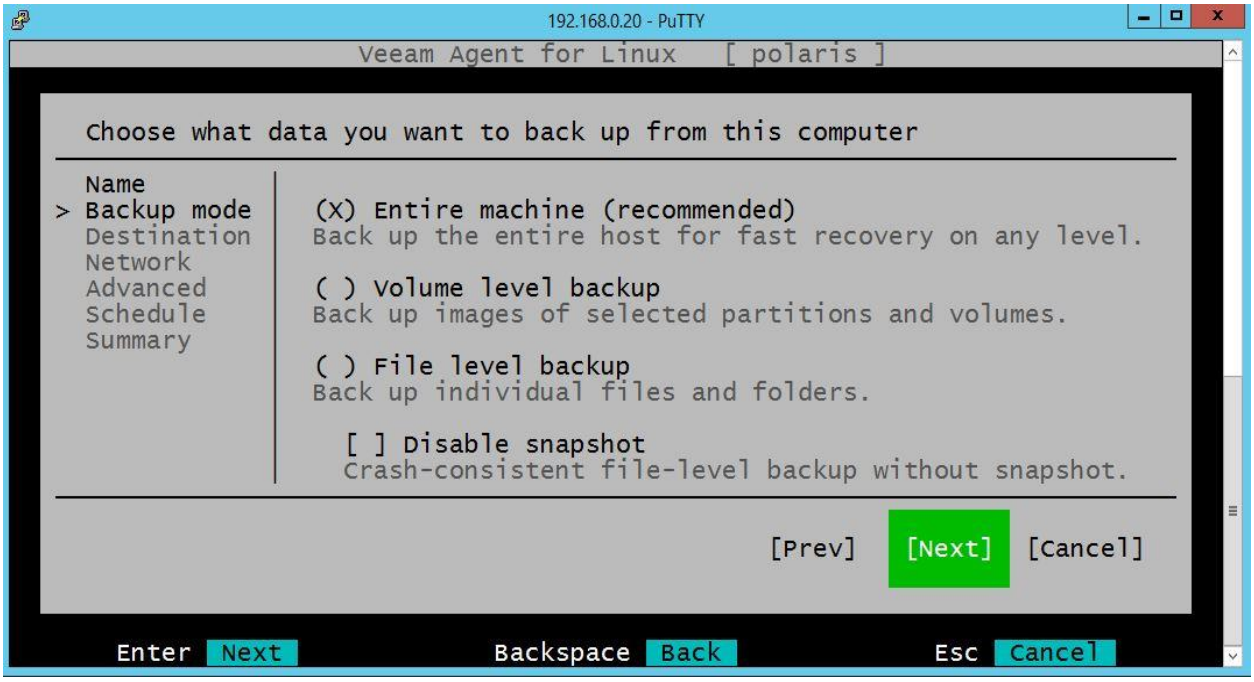
- Enter an appropriate Job name. Hit Next button

3235



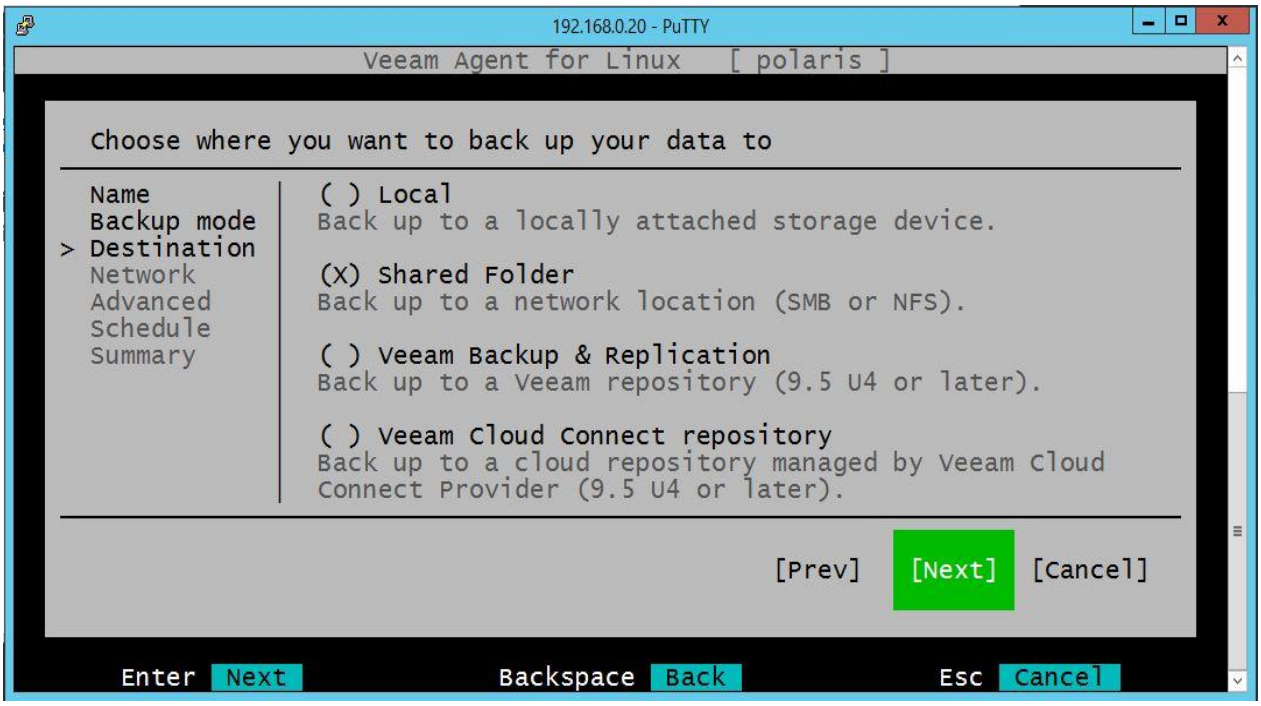
3236

3237 • Next under "**Backup Mode**", choose the type of backup to perform and hit Enter. For
3238 instance, to capture a full system image select Option #1 "Entire Machine" and hit Next.
3239

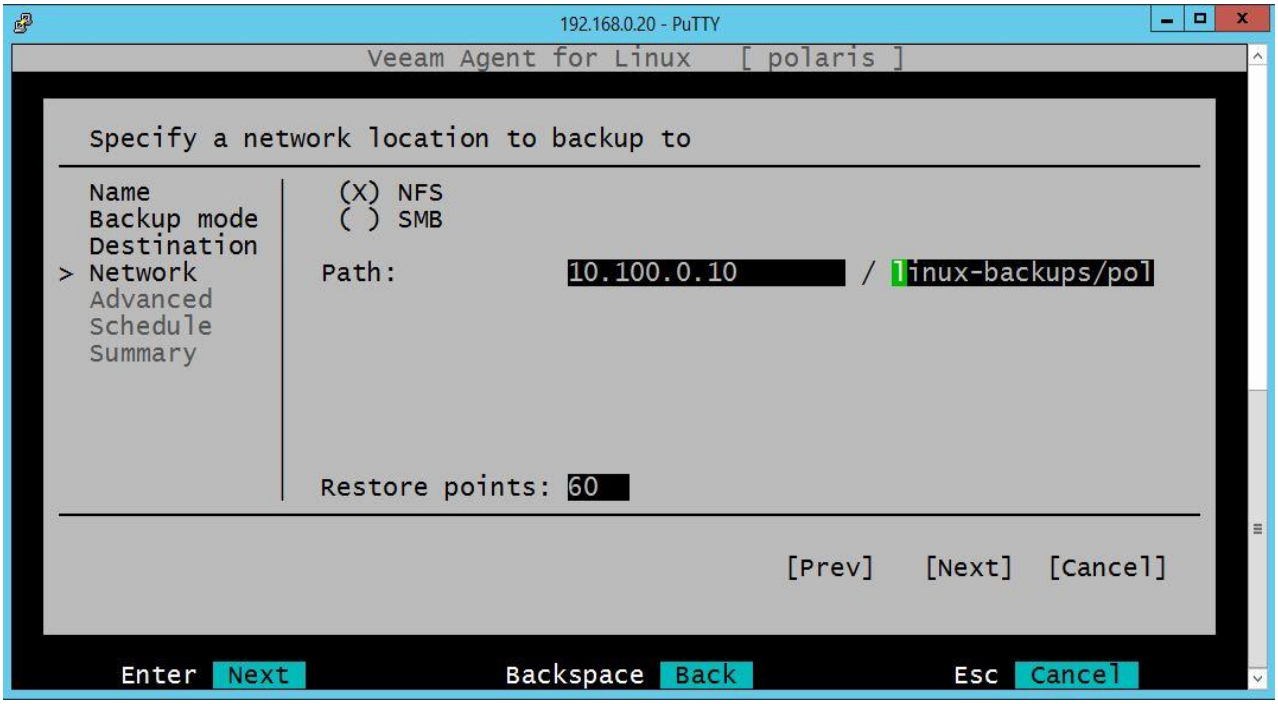


3240
3241

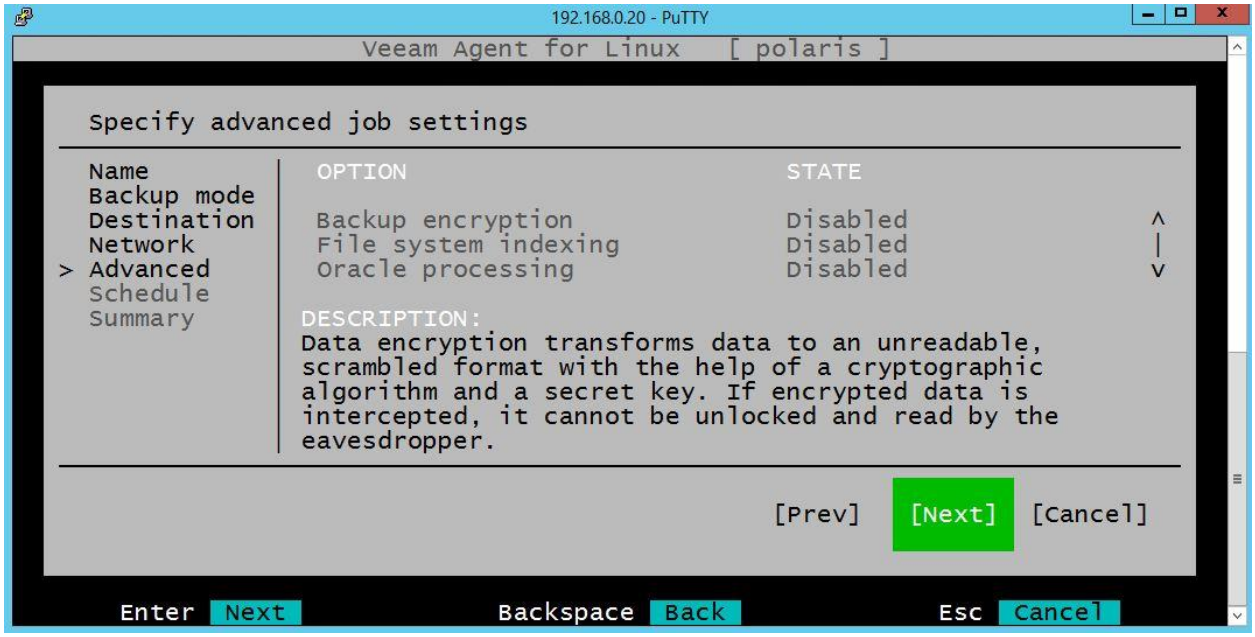
3242 • Under **Destination**, select Option # 2 "Shared Folder" to enable saving backup to the NFS
3243 folder created earlier on the Veeam Storage server. The Option #1 "Local" can be used to
3244 save the backup to a directly connected external USB device.



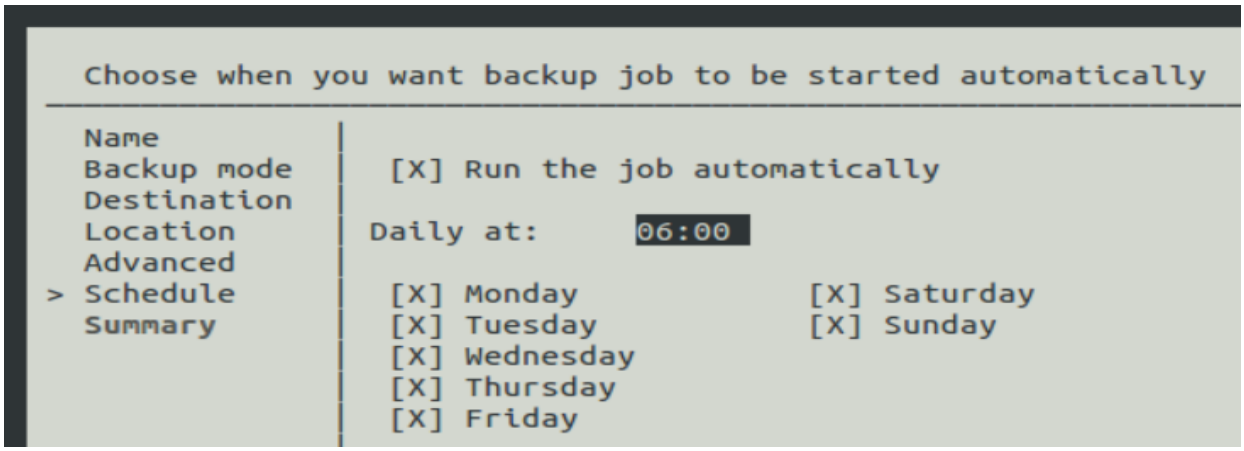
- Select "NFS" and enter the network path of the NFS mount point that was setup earlier. For instance, the image below shows the NFS-target IP address and folder from our setup.



- Under **Advanced,** Enable the options as required. For security purposes**,** Enable the **"Backup Encryption"**



- Under **Schedule**, you can either configure an automated job to run daily/weekly or uncheck "Run the job automatically" option to run a onetime manual backup.

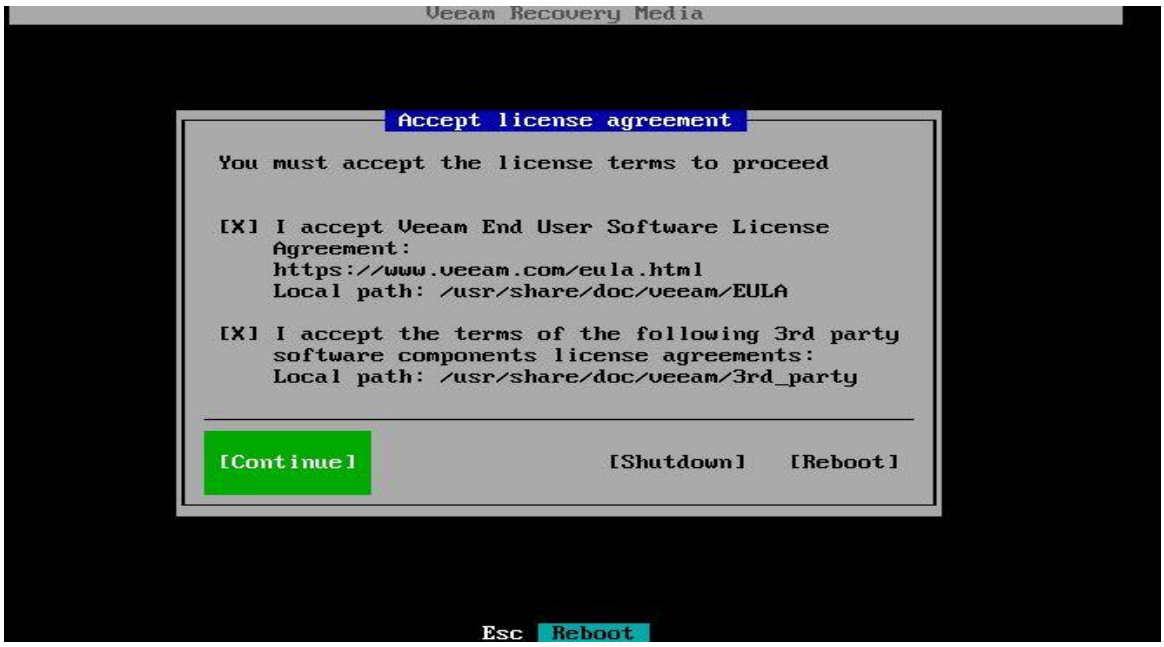


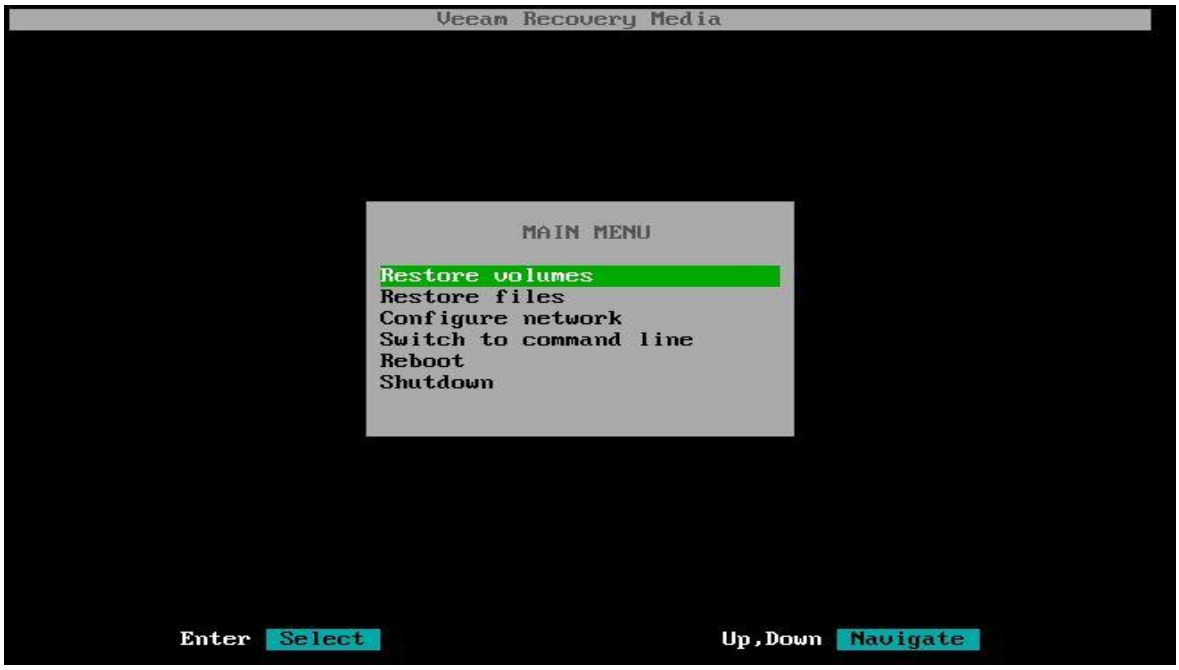
- Verify the settings on the Summary Screen and hit Next to kick off the job. Hit FINISH when done.

  Note: The free edition allows to schedule only one Backup job at a time. To change the backup mode, delete any existing job and re-run the configure wizard.

Recovery:

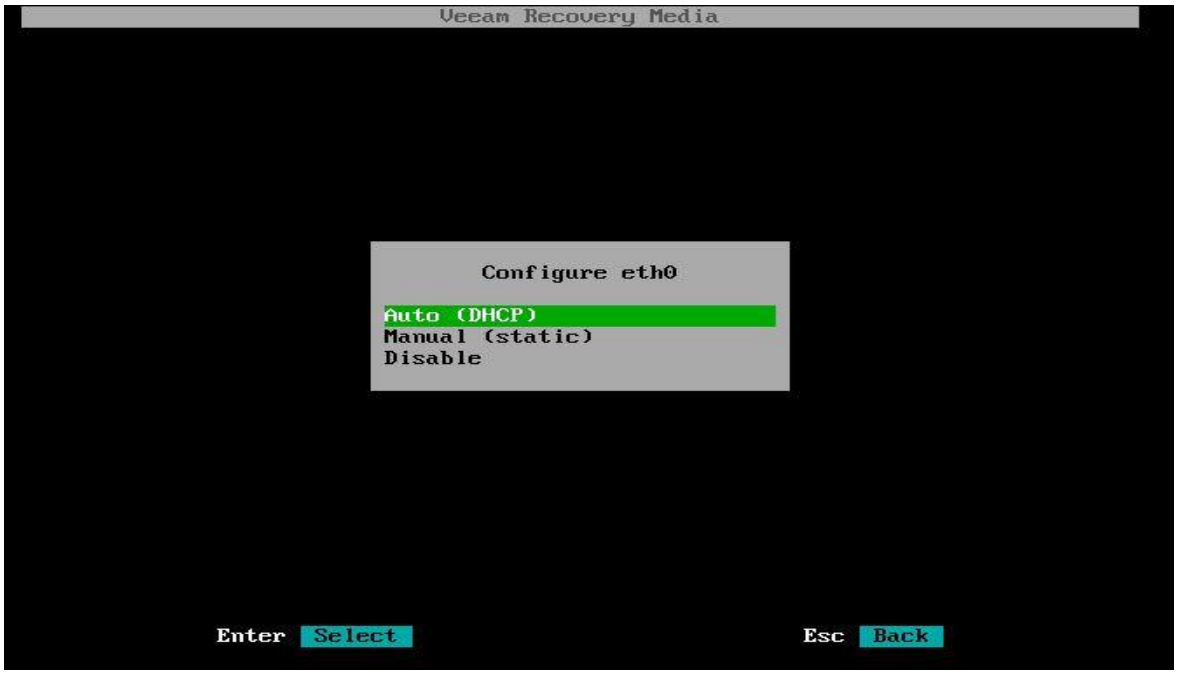
- A Restore operation is also initiated from the client and requires the Veeam Recovery Media to begin with. This media is available for download on the Veeam website
- Download the ISO and boot the server off it. The initial screen(s) will look like this:



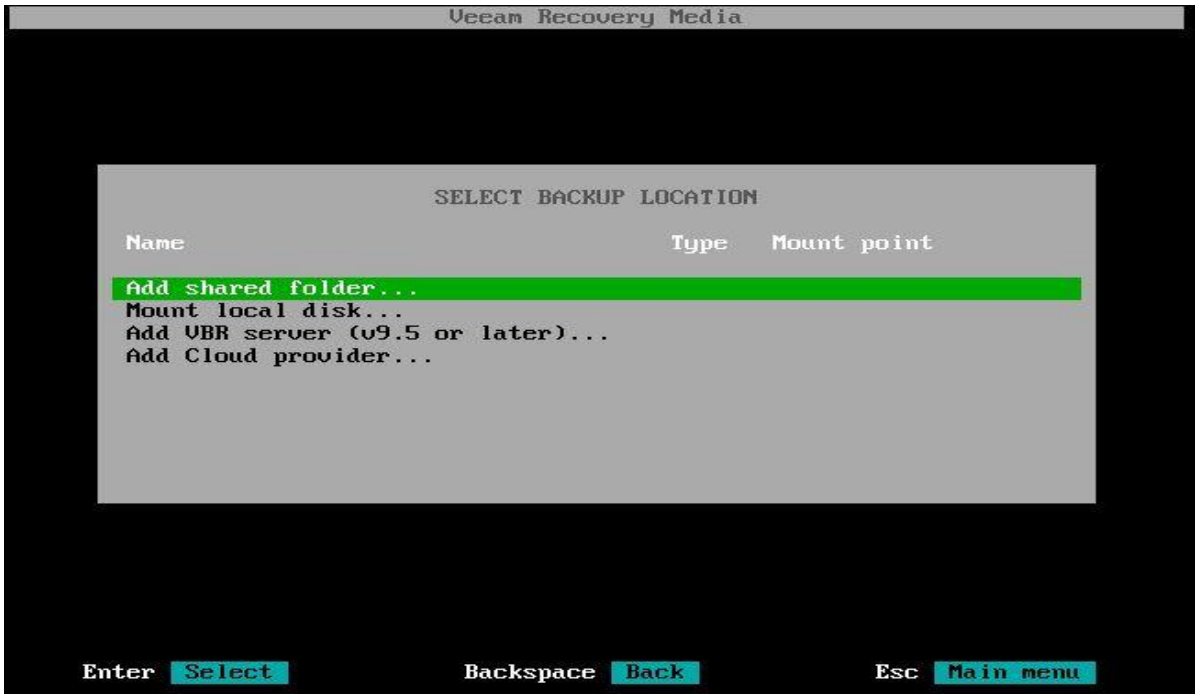


- If restoring from a Network drive (NFS or SMB), select the option "**Configure Network**" to first assign an IP address to the system. The Media supports both Static and DHCP method

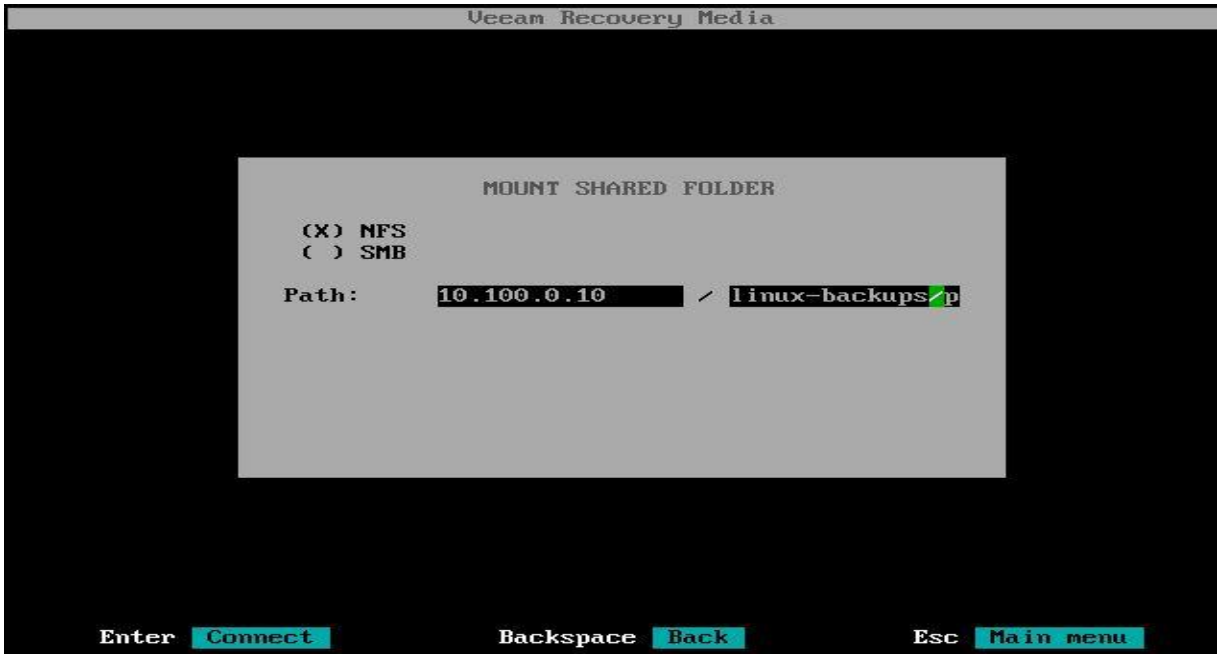
for obtaining an IP address as shown below. Once done, Hit **ESC** to go Back. Click on "**Restore Volumes**" to proceed.



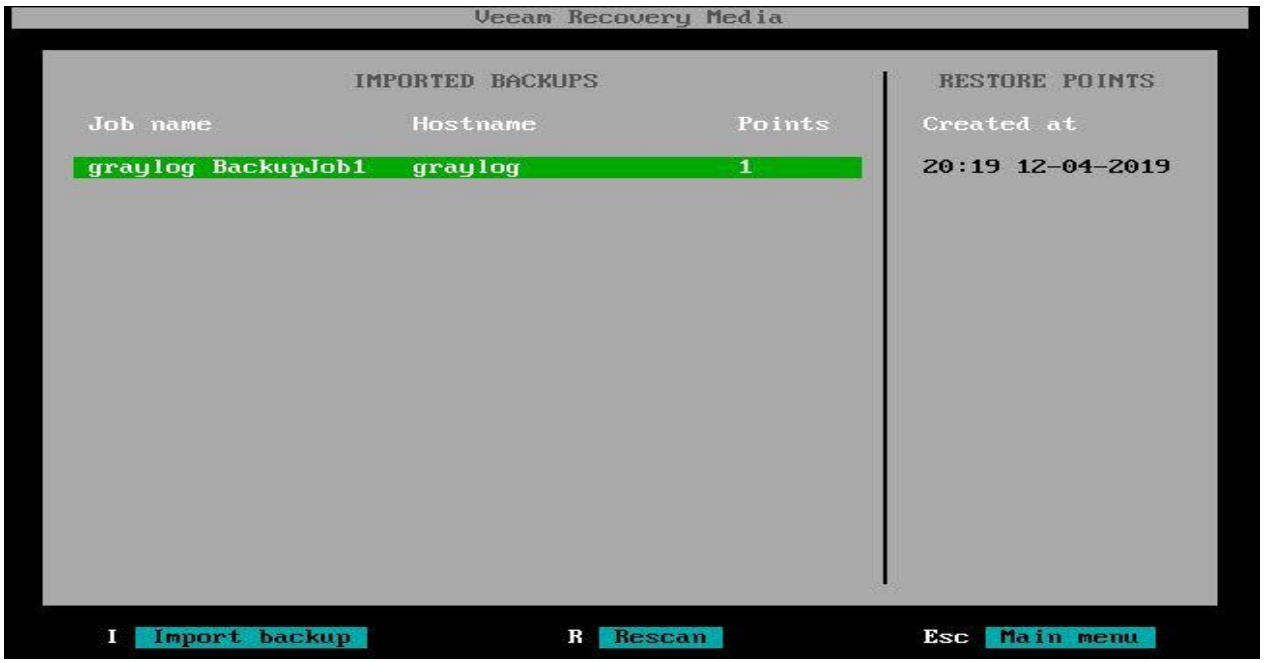
- Click on **Add Shared folder** for restoring from a Network Share Drive using NFS/SMB as in our case. If restoring from an External USB drive, Click on **Mount Local Drive**.



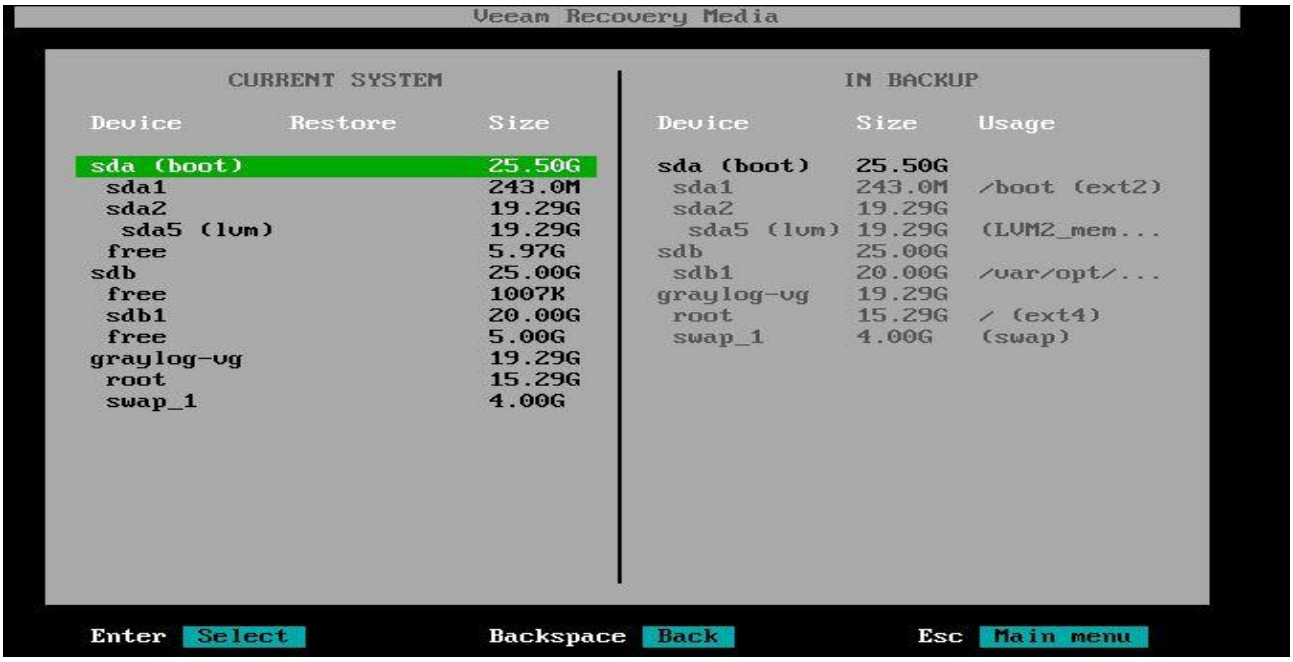
- Configure the Network Path of the backup target as required. Below image shows the Path set to connect to Veeam backup server using NFS.



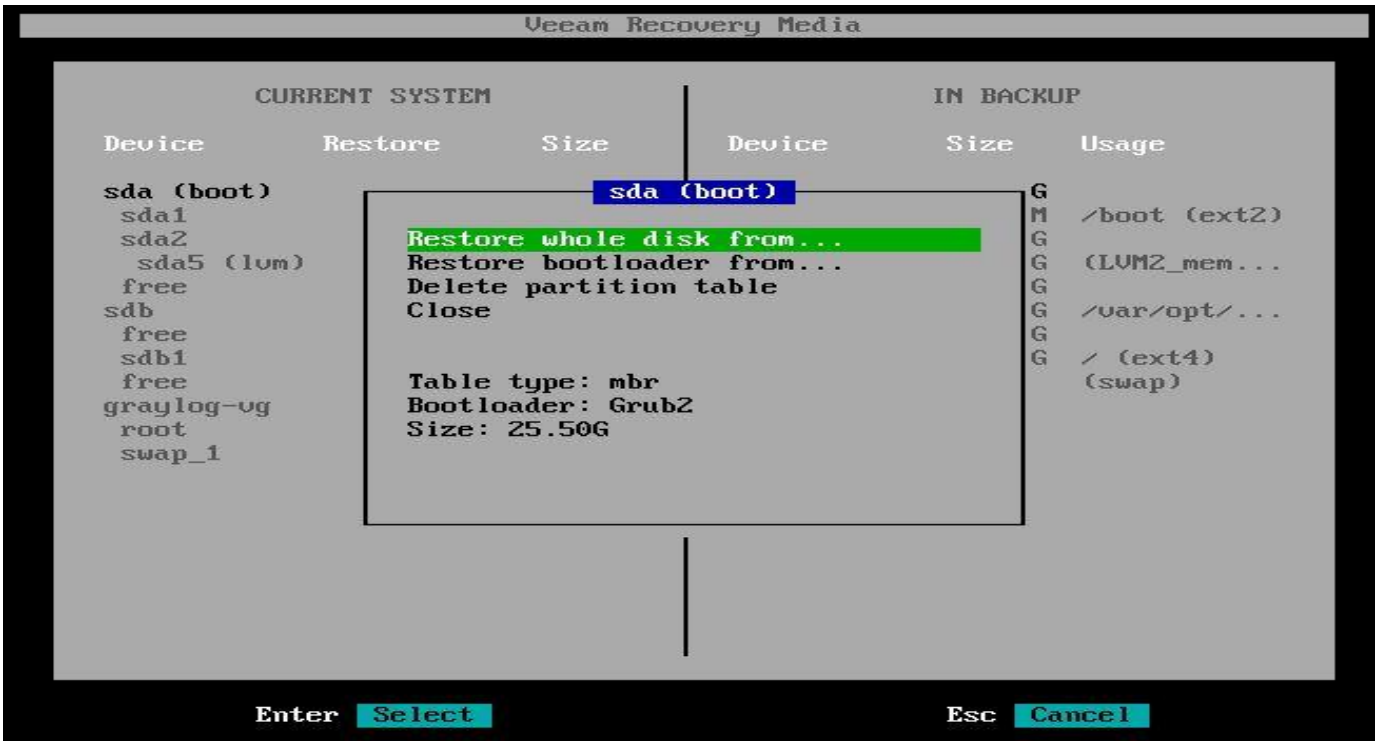
- Next, assuming the client can connect to the Veeam server or the Backup location successfully the wizard will then auto populate Restore points based off the backup jobs saved previously. Select a **Restore Point** from the Right and Hit **I** for **Import Backup** For instance:



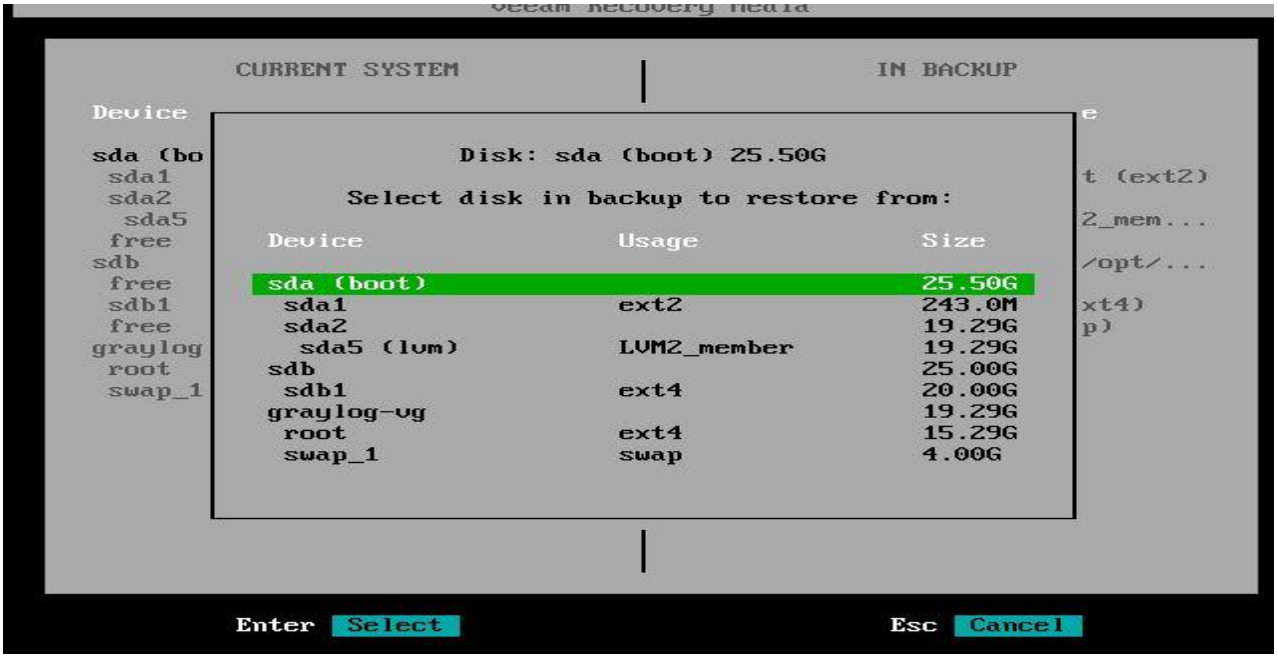
- The wizard will then display a comparison of the filesystem layout that's currently on the Linux server versus to what it currently has on that Backup Restore point. Select the Appropriate volume/disk to Restore and hit **Enter**. This will confirm your selection



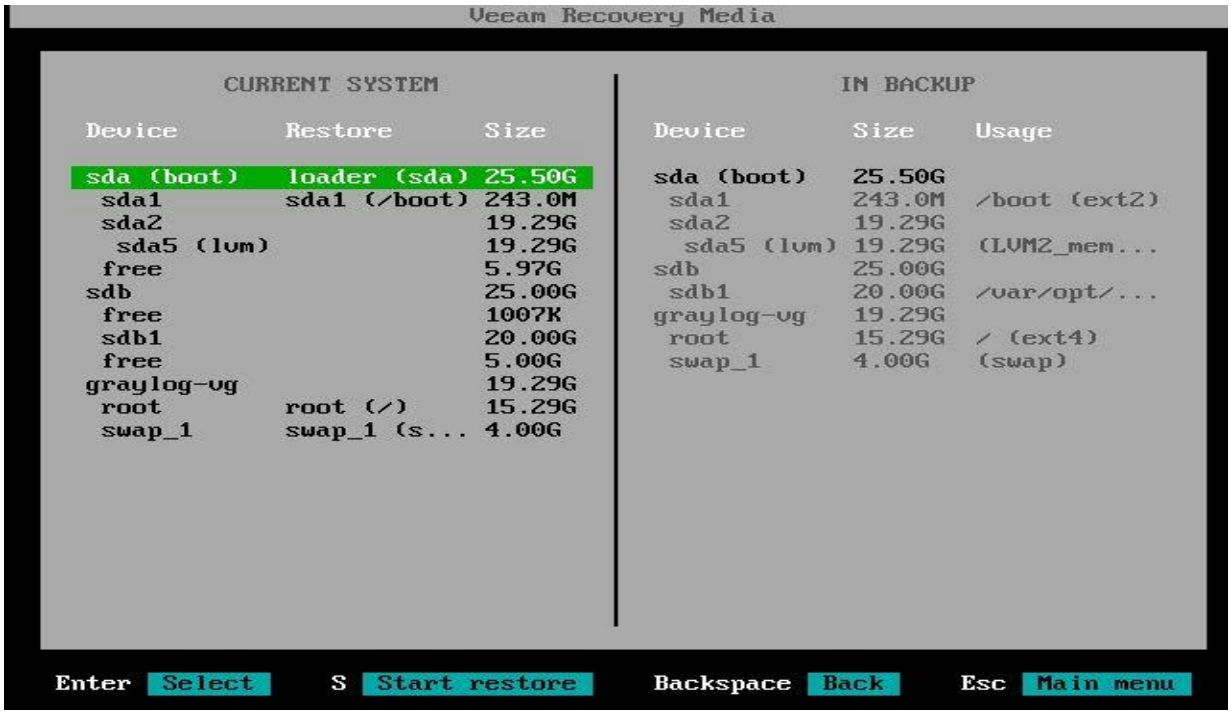
- Select the "**Restore Whole Disk from**" if restoring an Entire Volume / System Image or other options as shown in the list.
  Basically, you are telling the system to restore the image of **/sda** volume to the local **/sda** that's currently only the system.



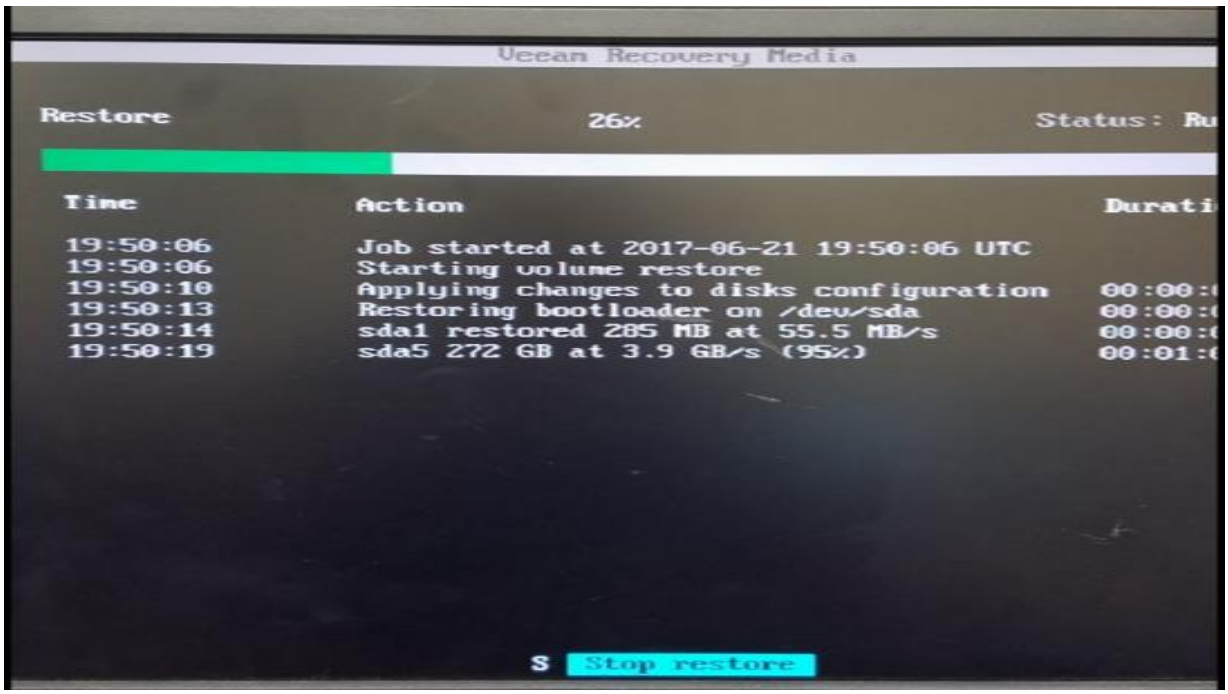
- The next screen lets you choose the disk from backup to restore from. Select the appropriate disk and hit Enter.



- On the Next screen, Hit S to Start the restore.



- Next the Recovery Summary screen will confirm the filesystem changes. Hit Enter to start the Recovery
- The restore process will now run and show a success message once complete. Eject the Veeam Recovery Media once restore completes and Reboot the server.



Changing backup job type:

- The free version of Veeam allows for one type of backup job to be scheduled at a time. The below shown commands can be run to delete an existing backup job and recreate a new one.

```
sudo veeamconfig job list

sudo veeamconfig job delete - -  name <job name>

sudo veeamconfig job delete - - id < id >
```

- Once deleted, run **sudo veeam** command to launch the Veeam Config Menu as shown below. Hit **C for Configure** to create a new job.

References:

[1] Veeam Backup and Replication https://www.veeam.com/vm-backup-recovery-replication-software.html

[2] Veeam agent for Linux Free edition https://www.veeam.com/linux-backup-free.html

4.6.6 Highlighted Performance Impacts

Three performance measurement experiments were performed for the Veeam tool while the manufacturing system was operational:

1. CL004.1 - Veeam agent is installed and running on predetermined CRS hosts.
2. CL004.2 - A full image backup is performed on CRS hosts.
3. CL004.3 - A directory backup (i.e., incremental backup) is performed on CRS hosts.

4.6.6.1 Experiment CL004.1

No performance impact to the manufacturing process was measured during the experiment.

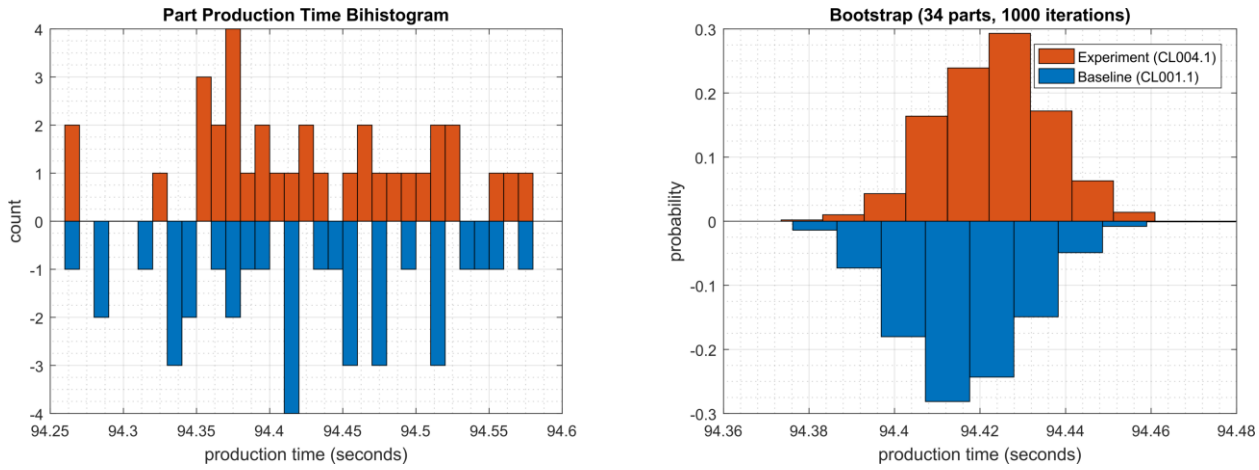


Figure 4-10 - Bihistograms showing the part production time (left) and estimated mean production time using the bootstrap method (right) using the measurements from baseline CL001.1 and experiment CL004.1.

4.6.6.2 Experiment CL004.2

A full image of three CRS hosts was performed during the experiment:

- Engineering Workstation (POLARIS, on the CRS Network),
- Robot Controller vController1 (on the hypervisor over Management Network), and
- Robot Controller vController2 (on the hypervisor over Management Network).

The imaging of POLARIS was performed from 210 sec. to 1023 sec. (experiment time), and all data was transferred over the CRS network. The vController1 and vController2 imaging was performed from 1050 sec. to 1710 sec. (experiment time) from the hypervisor, and all data was transferred over the Management network. The network traffic generated by the imaging of POLARIS is shown in Figure 4-11.

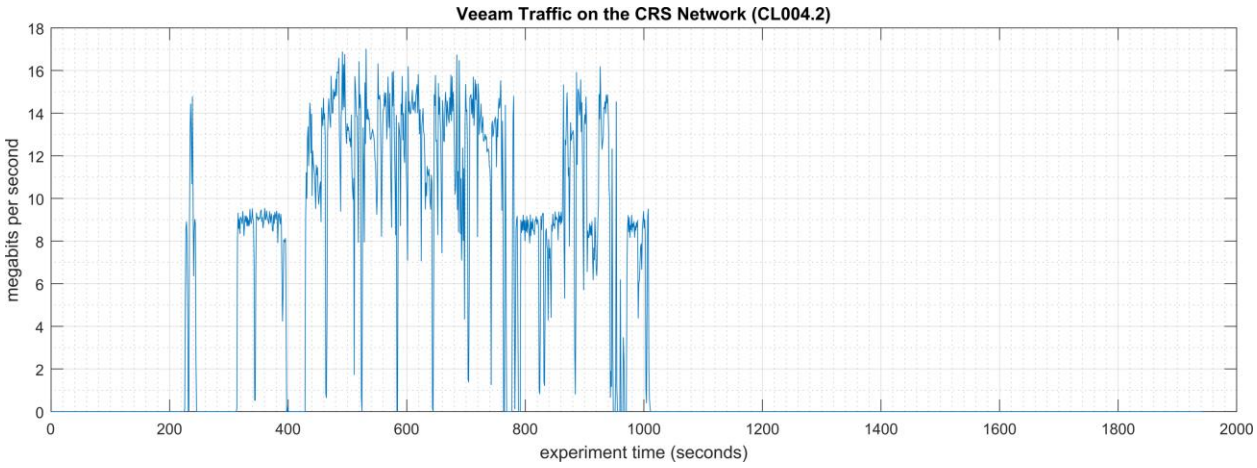


Figure 4-11 - Time series plot showing the rate of network traffic (in megabits per second) transmitted and received by the Veeam tool during the CL004.2 experiment. Network traffic transmitted and received by the vControllers are not shown in this plot.

Loss-of-view events were observed on the HMI multiple times during the experiment, as evident by the large inter-packet delay measurements between the HMI and Station 1 shown in Figure 4-12. The longest loss-of-view event occurred over 130 sec. in length. Based on the large inter-packet delay measurements, it is hypothesized that the loss-of-view events can also be classified as loss-of-control incidents, although this was not tested during the experiment. All the observed incidents occurred while the Veeam tool was imaging the POLARIS host.

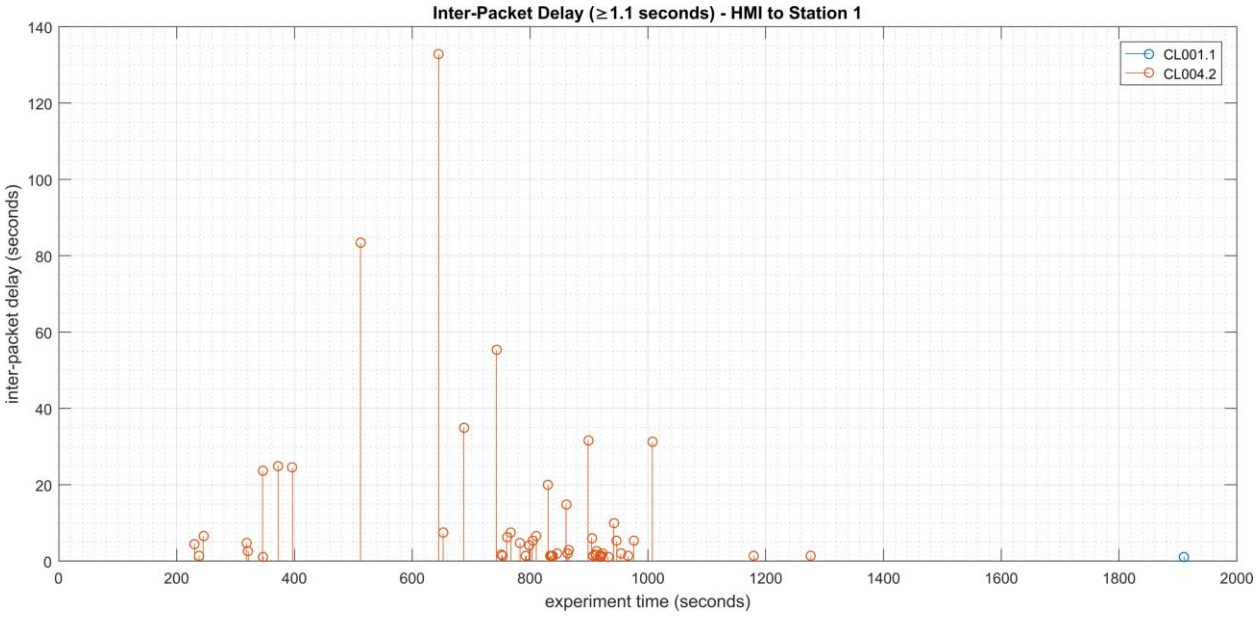


Figure 4-12 - Stem plot displaying the inter-packet delays (greater than or equal to 1.10 seconds) of Modbus TCP traffic between the HMI and Station 1, as measured during the baseline CL001.2 and experiment CL004.2. Note the large inter-packet delays measured between experiment time 400 to 1000 sec., resulting in multiple HMI loss-of-view events of over 15 seconds, and the largest event over 130 seconds in length.

The loss-of-view events were likely caused by the large round-trip (RTT) times (shown in Figure 4-13) observed between the HMI and Station 1 while the Veeam tool was imaging the POLARIS host, which were larger than the configured connection timeout value on the HMI (100 msec.). Measurements of the packet path delay (shown in Figure 4-14) show a similar increase, suggesting that one or more of the CRS network devices may have been overloaded while Veeam was active.

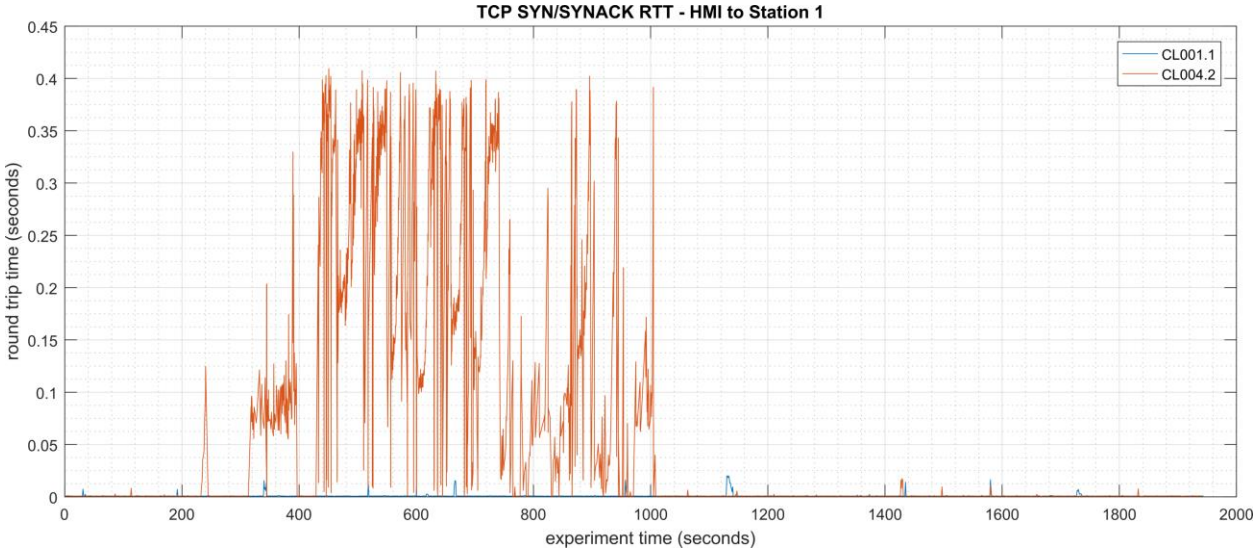


Figure 4-13 - Time-series plot showing the measured round-trip time of SYN and SYN-ACK packets sent between the HMI and Station 1 during the experiment. Large round-trip times (>350 msec.) occurred regularly from 400 seconds to 1000 seconds (experiment time).

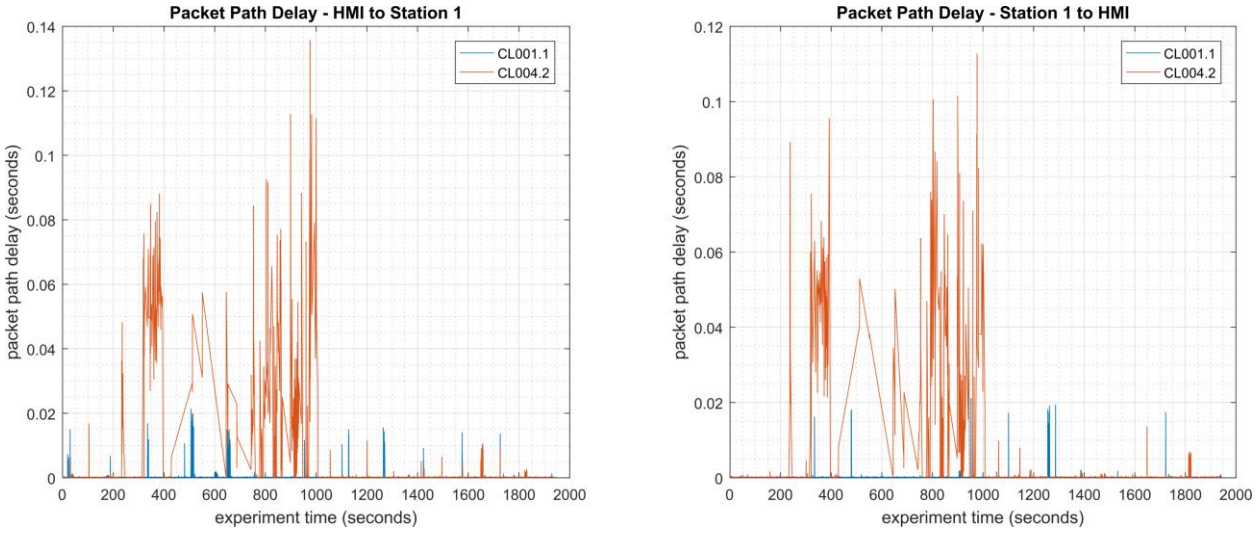


Figure 4-14 - Time-series plots showing the measured packet path delay Modbus TCP packets sent from the HMI to Station 1 (left) and sent from Station 1 to the HMI (right) during the experiment.

An increase in the robot job actuation time was observed on Robot 1 for Job 102 (see Figure 4-15). No other increases were observed for any of the other jobs. The two increases were measured while the Veeam tool was imaging the two vControllers.

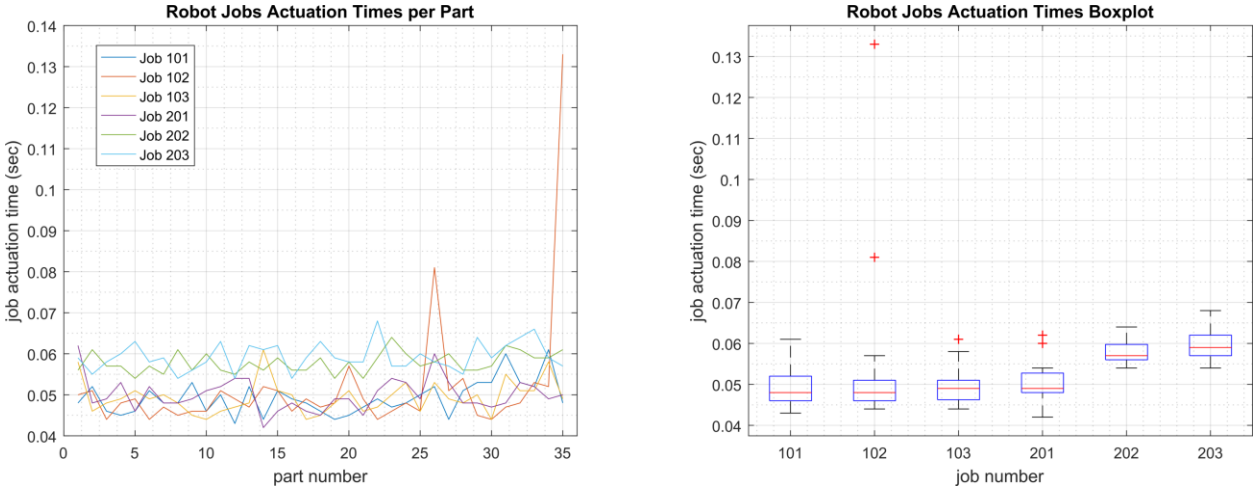


Figure 4-15 - Time-series (left) and boxplot (right) showing the job actuation times for each job during the CL004.2 experiment. Note the two increased actuation times for job 102, which occurred while the Veeam tool was imaging the vControllers.

A slight increase of the part production time variance was observed during this experiment, but it is not statistically significant.

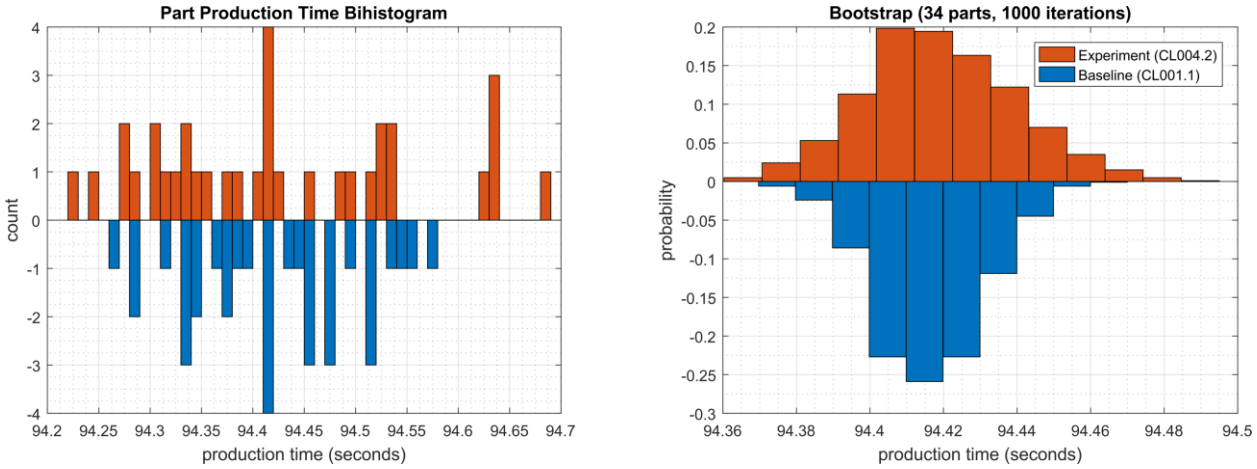


Figure 4-16 - Bihistograms showing the part production time (left) and estimated mean production time using the bootstrap method (right) using the measurements from baseline CL001.1 and experiment CL004.2.

4.6.6.3 Experiment CL004.3

A directory backup of the /opt/ directory on the Engineering Workstation (POLARIS) host was performed for this experiment. The backup was performed from 347 sec. to 1052 sec. (experiment time), and all data was transferred over the CRS network. The network traffic generated by the backup is shown in Figure 4-17.

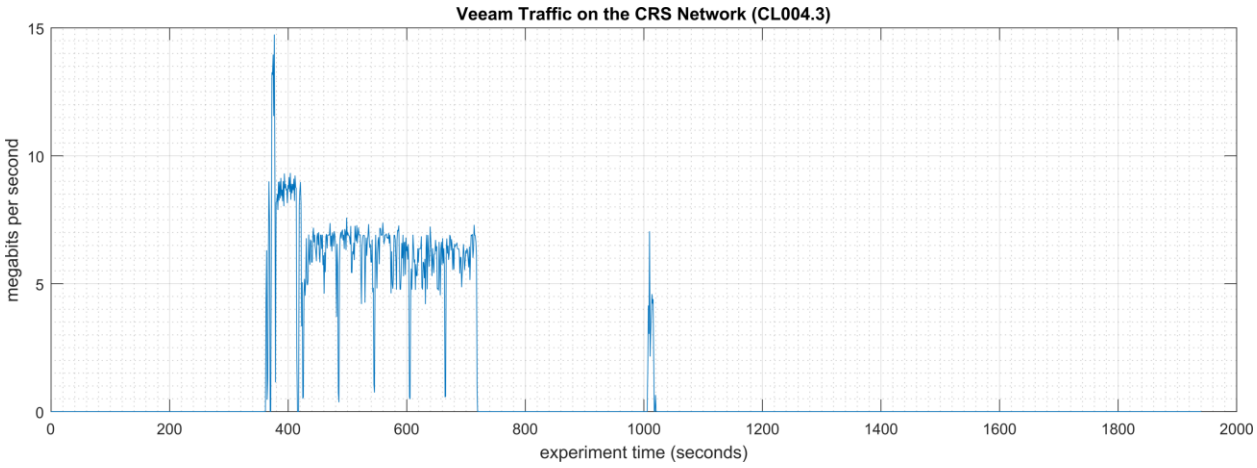


Figure 4-17 - Time series plot showing the rate of network traffic (in megabits per second) transmitted and received by the Veeam tool during the CL004.3 experiment.

Loss-of-view events with Station 3 and Station 4 were observed on the HMI multiple times during the experiment. Large inter-packet delay measurements between the HMI and Station 1 are shown in Figure 4-18. The longest loss-of-view event occurred over 9 sec. in length. Based on the large inter-packet delay measurements, it is hypothesized that the loss-of-view events can also be classified as loss-of-control incidents, although this was not tested during the experiment. All the observed incidents occurred while the Veeam tool was actively backing up POLARIS.

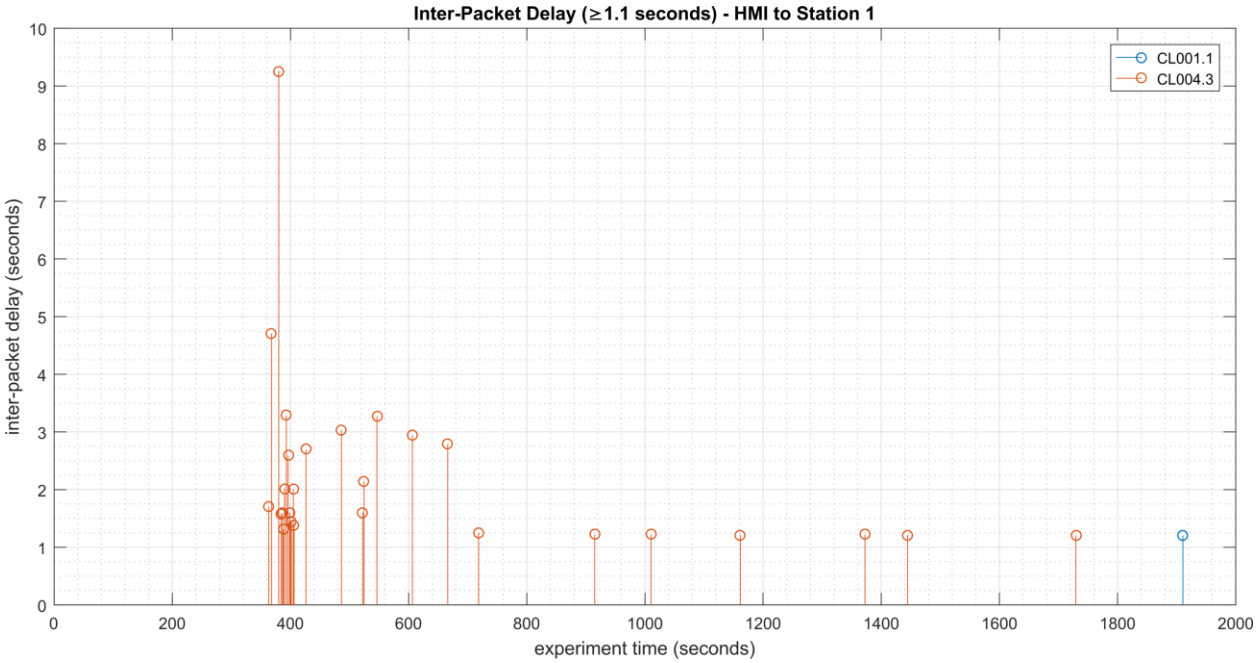


Figure 4-18 - Stem plot showing the inter-packet delays (greater than or equal to 1.10 seconds) of Modbus TCP traffic between the HMI and Station 1, as measured during the baseline CL001.2 and experiment CL004.3. Note the large inter-packet delays measured between experiment time 370 to 700 sec., resulting in multiple HMI loss-of-view events of over 2 seconds, and the largest event over 9 seconds in length.

The loss-of-view events were likely caused by the large round-trip (RTT) times (shown in Figure 4-19) observed between the HMI and Station 1 while the Veeam tool was active, which were larger than the configured connection timeout value on the HMI (100 msec.). Measurements of the packet path delay (shown in Figure 4-20) show a similar increase, suggesting that one or more of the CRS network devices may have been overloaded while Veeam was active.

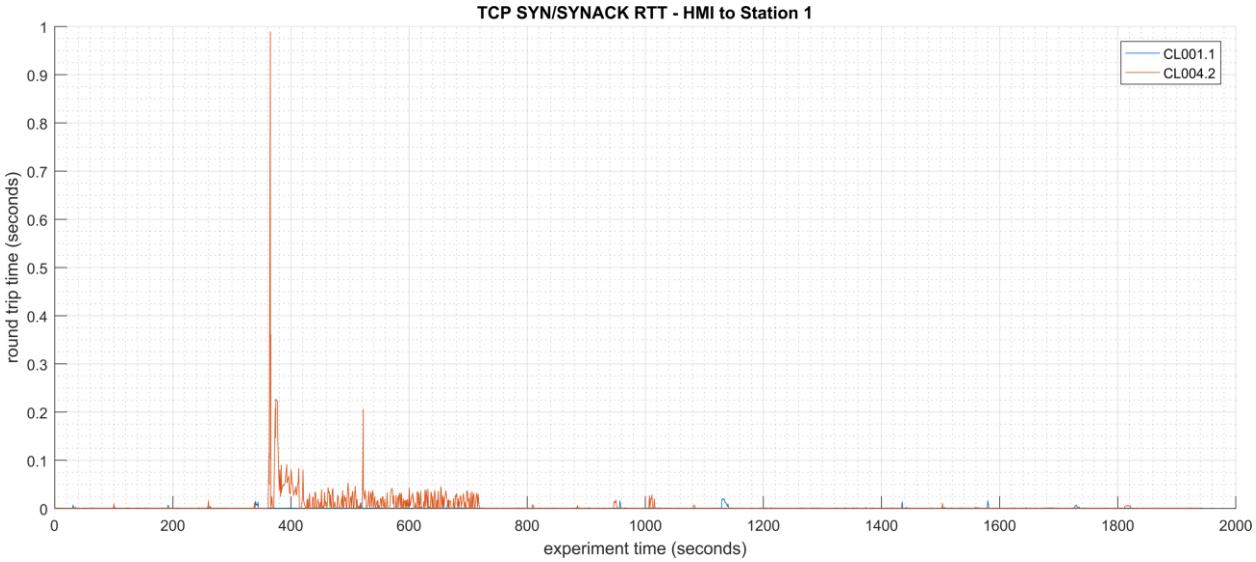


Figure 4-19 - Time-series plot showing the measured round-trip time of SYN and SYN-ACK packets sent between the HMI and Station 1 during the experiment.

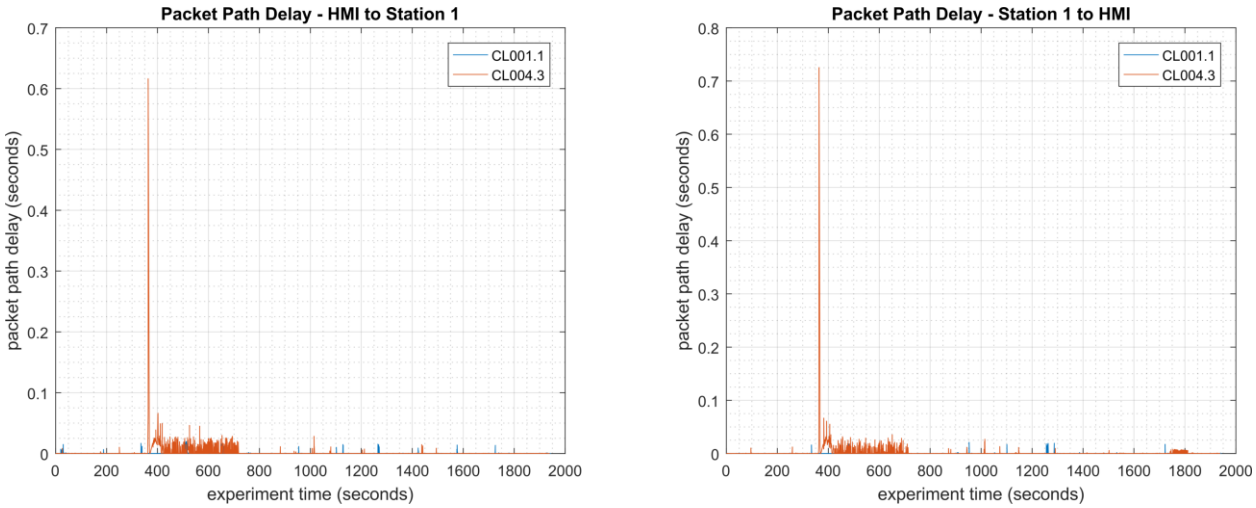


Figure 4-20 - Time-series plots showing the measured packet path delay Modbus TCP packets sent from the HMI to Station 1 (left) and sent from Station 1 to the HMI (right) during the experiment. Note the large path delay of over 600 msec. around 350 sec., followed by consistent delays of around 20 msec. until around 700 sec.

A slight increase of the part production time mean was observed during this experiment but it is not statistically significant.

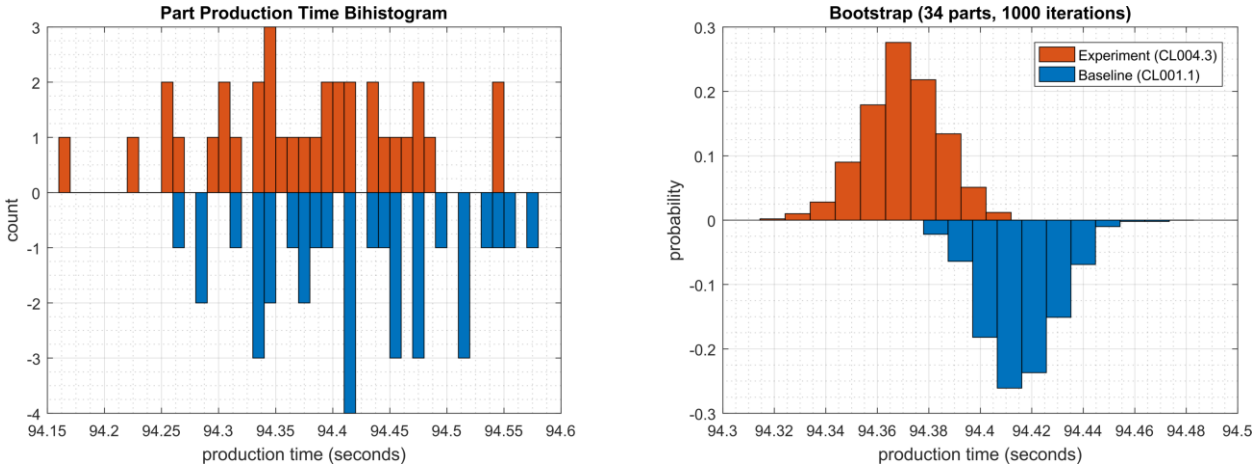


Figure 4-21 - Bihistograms showing the part production time (left) and estimated mean production time using the bootstrap method (right) using the measurements from baseline CL001.1 and experiment CL004.3.

4.6.7 Link to Entire Performance Measurement Data Set

- **CL004.1-HostBackups.zip**
- **CL004.2-FullImageBackup.zip**
- **CL004.3-DirectoryBackup.zip**

4.7 TeamViewer

4.7.1 Technical Solution Overview

TeamViewer is a Remote Desktop sharing tool. TeamViewer provides Secure Remote Access and Support Solutions for Entrepreneurs, Small Businesses, and Large Enterprises. Some of its features include Cross Platform Support Access such as PC-PC, PC-Mobile, Mobile-Mobile, etc. Multi User Support Sessions and Remote Device Control [1]

4.7.2 Technical Capabilities Provided by Solution

TeamViewer provides components of the following Technical Capabilities described in Section 6 of Volume 1:

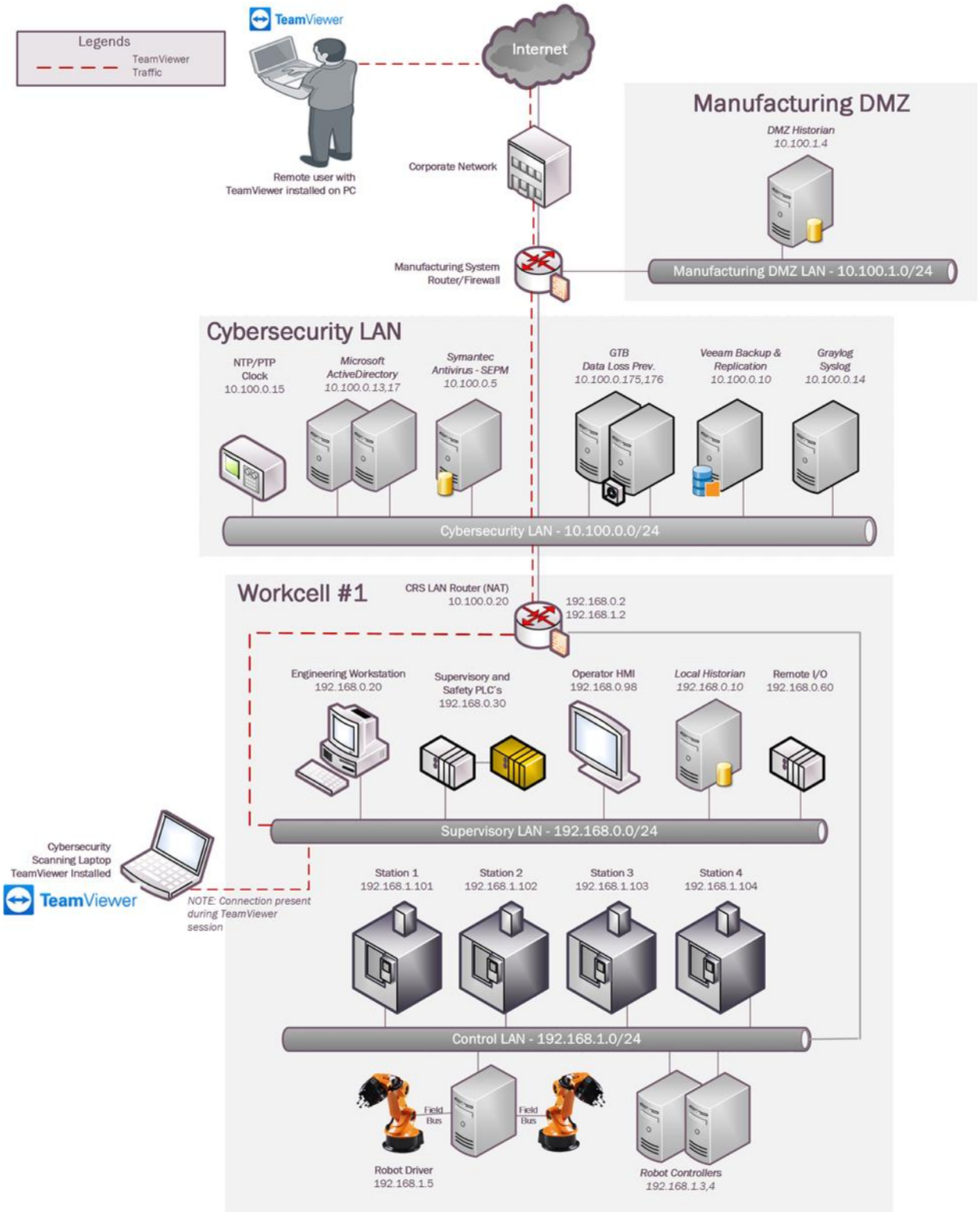
- Secure Remote Access

Secure Remote Access

4.7.3 Subcategories Addressed by Implementing Solution

PR.MA-2, PR.AC-5

4.7.4 Architecture Map of Where Solution was Implemented



4.7.5 Installation Instructions and Configurations

Setup for Robotics System:

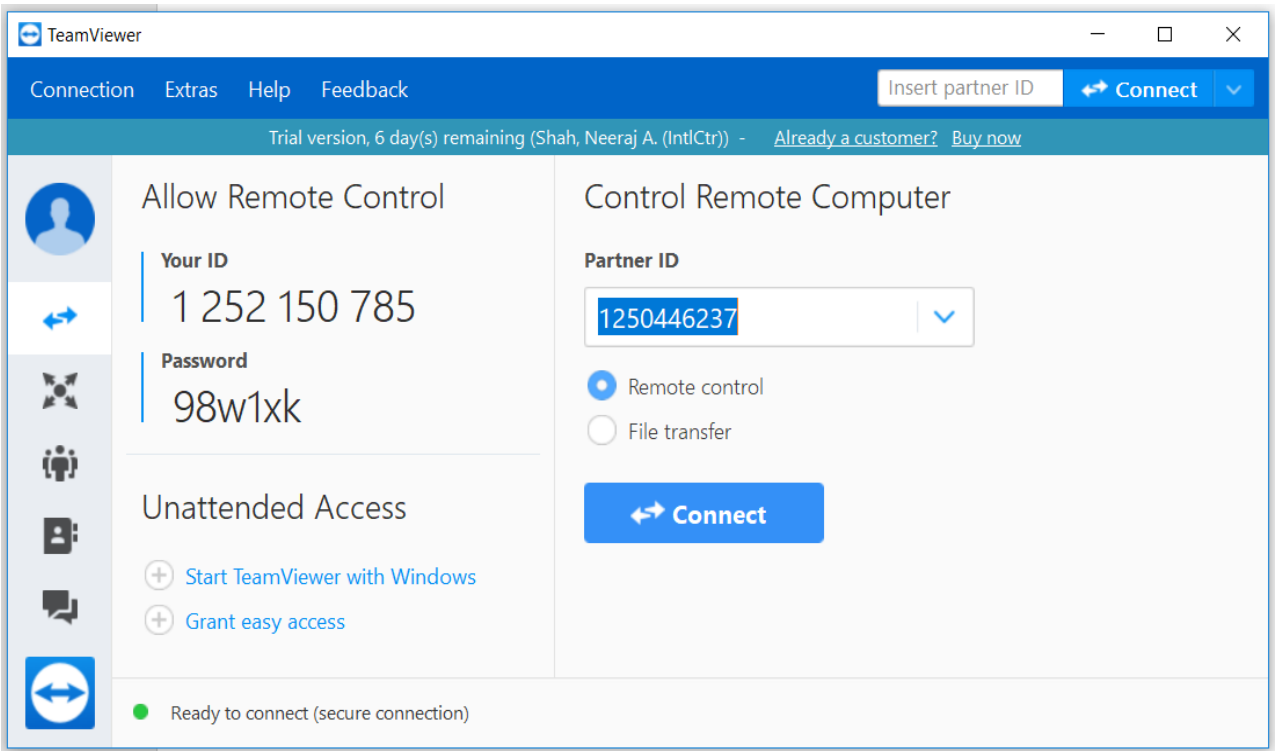
Secure Remote Access was setup for the CRS system using TeamViewer. The Cybersecurity scanning laptop was used a jump box for installing TeamViewer and connecting remotely to the Work Cell network within.

Configuration:

- TeamViewer v14 was downloaded and installed on the Cybersecurity scanning laptop. The person connecting remotely needs to have Team viewer installed on their system too.

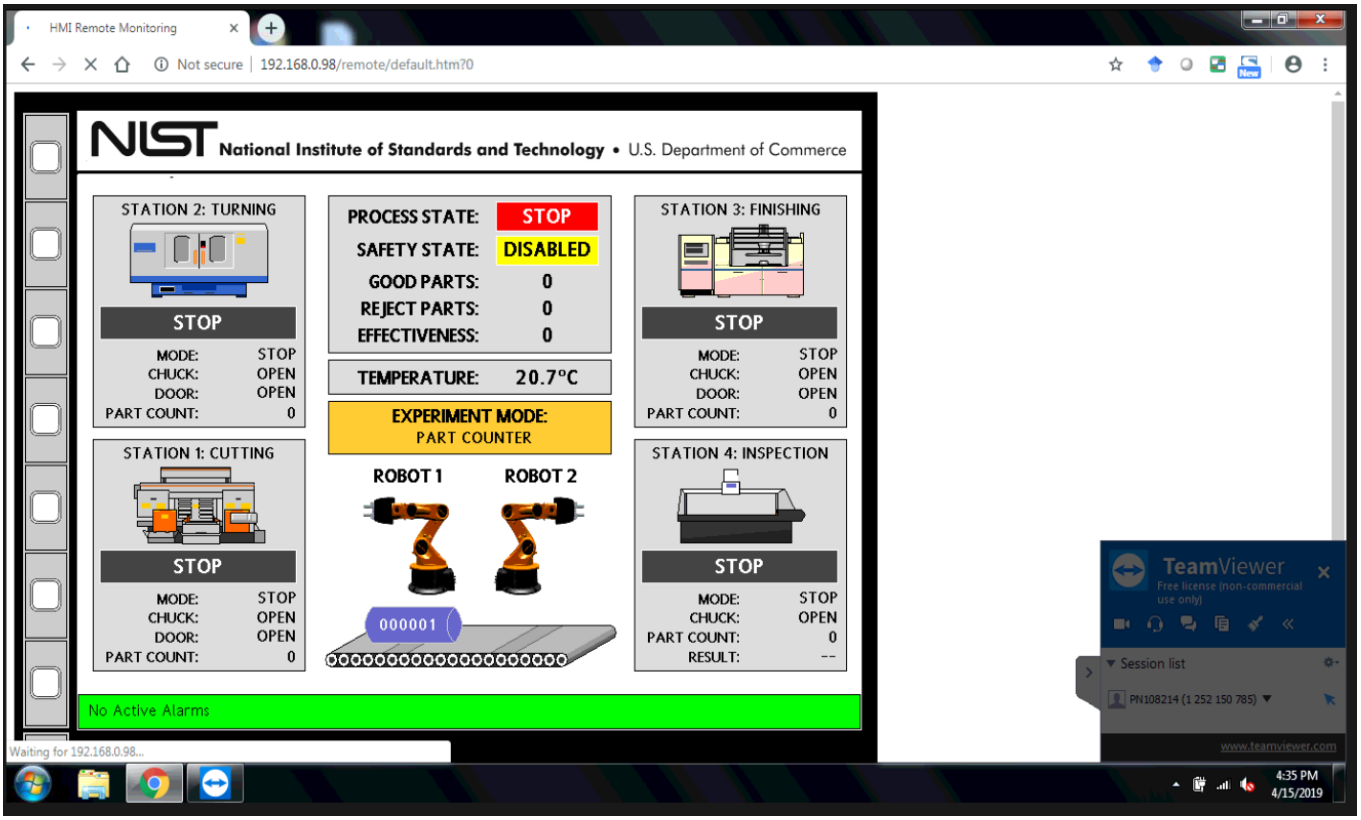
- The scanning laptop had internet access via wireless and at the same time access to the Work cell network by connecting a physical Ethernet connection coming from the core switch. A Static IP was assigned to the system on the Ethernet interface.

- The person connecting remotely needs to know your ID and password to punch in. Both of these are displayed on the TeamViewer panel itself.



- The remote person needs to enter your ID in the **Partner ID** box, select **Remote Control** and hit **Connect** button to initiate a session. Next, Enter the password as prompted.

- Once the connection was established, the HMI Panel was accessed off a browser on the Cybersecurity Scanning laptop to perform maintenance on the HMI.



- Two factor authentication was configured by using the procedure mentioned here: https://community.teamviewer.com/t5/Knowledge-Base/Two-factor-authentication-Activation-and-Deactivation/ta-p/66

References:

[1] Team Viewer: https://www.teamviewer.com

4.7.6 Highlighted Performance Impacts

No performance measurement experiments were performed for the use of Team Viewer due to its intended usage (i.e., Team Viewer was installed on a laptop that is attached to the network only during maintenance and engineering activities).

4.7.7 Link to Entire Performance Measurement Data Set

N/A

4.8 Microsoft Active Directory

4.8.1 Technical Solution Overview

Active Directory (AD) is a directory service developed by Microsoft for Windows domain networks. A directory is a hierarchical structure that stores information about objects on the network. A directory service, such as Active Directory Domain Services (AD DS), provides the methods for storing directory data and making this data available to network users and administrators. For example, AD DS stores information about user accounts, such as names, passwords, phone numbers, and so on, and enables other authorized users on the same network to access this information. A server running Active Directory Domain Services (AD DS) is called a domain controller [1]. It authenticates and authorizes all users and computers in a Windows domain type network—assigning and enforcing security policies for all computers and installing or updating software. Active Directory uses Lightweight Directory Access Protocol (LDAP) versions 2 and 3, Microsoft's version of Kerberos and DNS.[13]

Points to consider

- Cost of infrastructure can get high.
- Requires expertise to setup and maintain. Setup involves detailed planning.
- It is prone to being hacked.

4.8.2 Technical Capabilities Provided by Solution

Microsoft Active Directory provides components of the following Technical Capabilities described in Section 6 of Volume 1:

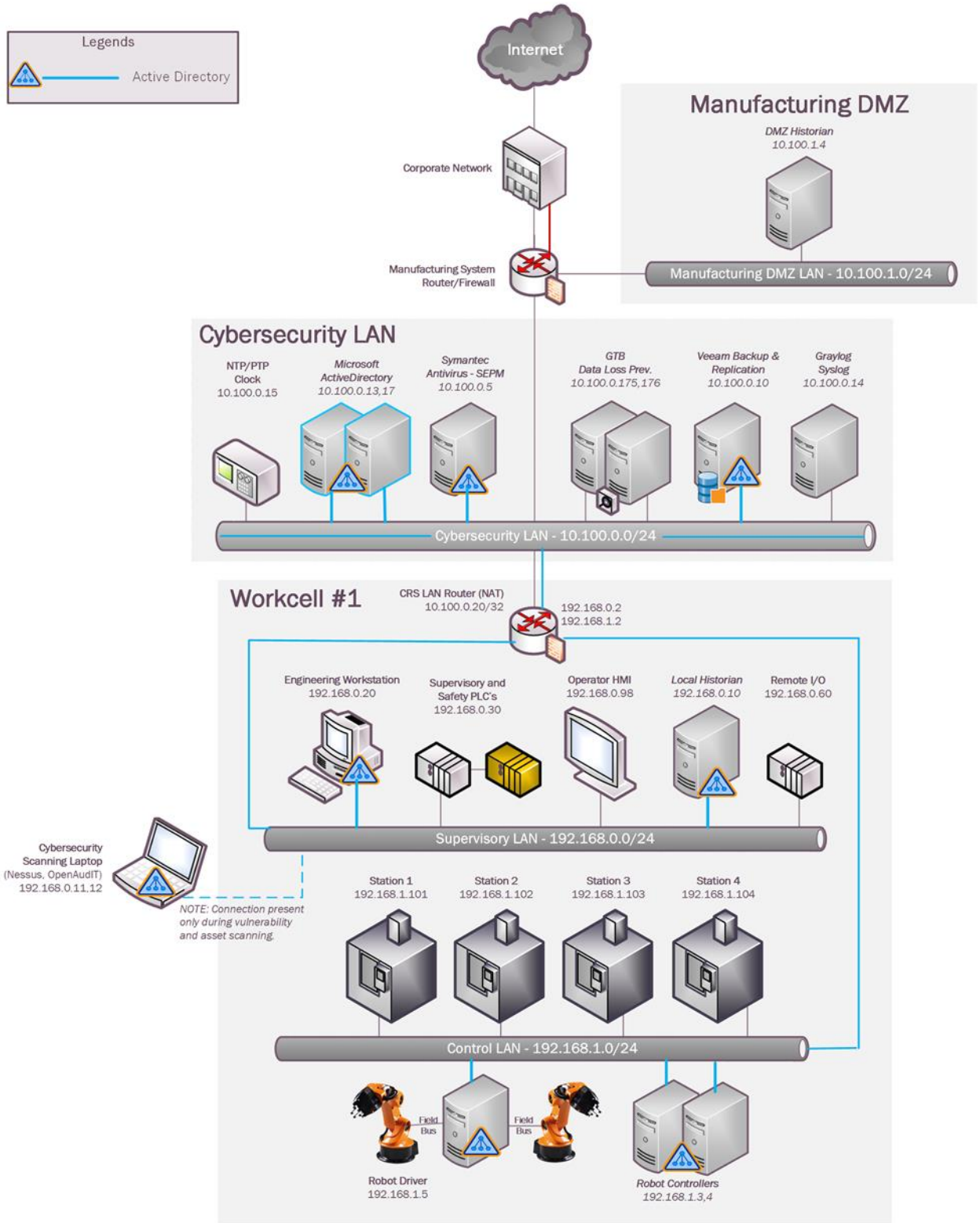
- Credential Management
- Authentication and Authorization

4.8.3 Subcategories Addressed by Implementing Solution

PR.AC-1, PR.MA-1, PR.MA-2, PR-PT-3, PR.PT-4, DE.CM-3

[13] https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview

4.8.4 Architecture Map of Where Solution was Implemented



4.8.5 Installation Instructions and Configurations

Setup:

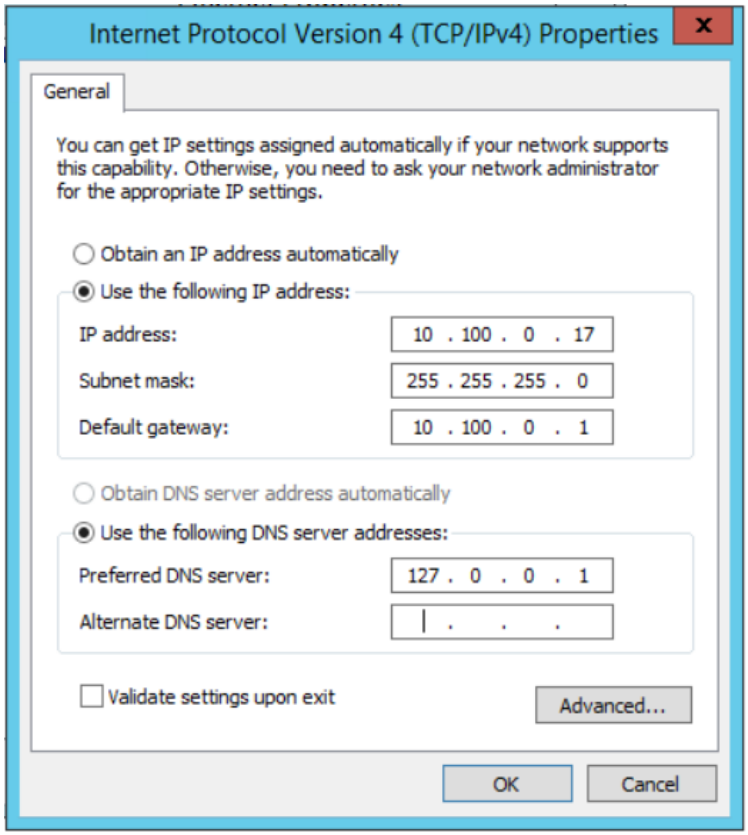
The setup consists of two virtual machines running Active Directory services in the Cybersecurity LAN. The server "**LAN-AD**" is the Primary DC and DNS server while "**LAN-AD-02**" one is the backup DC and DNS server.

Details of the AD-servers

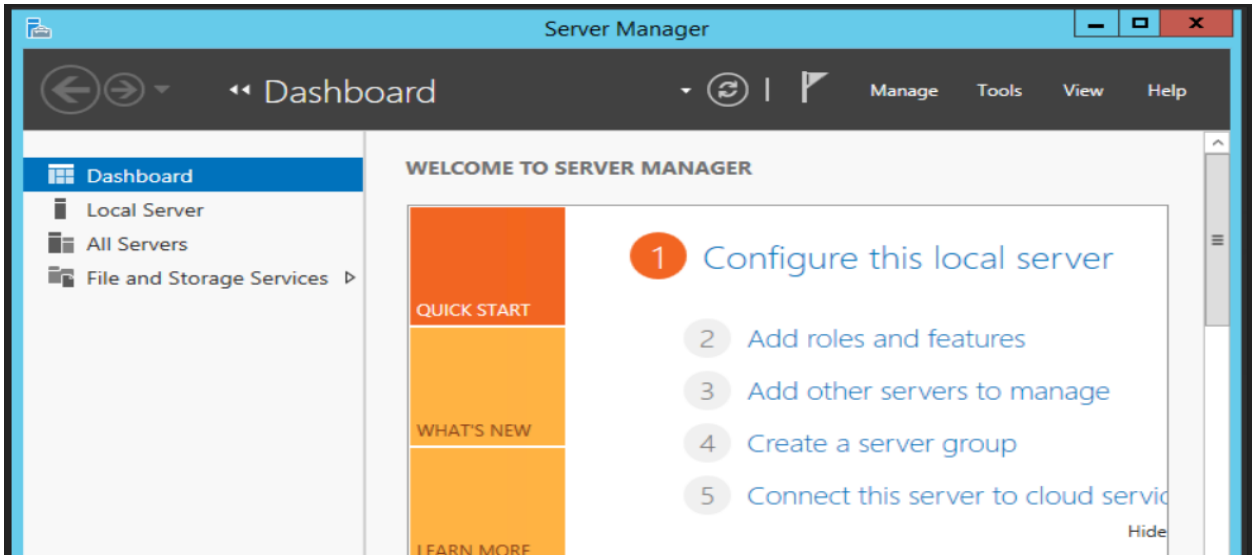
Hostname	IP address	Roles	Domain Name
LAN-AD	10.100.0.17	Active Directory, DNS, Network Policy Server (Radius)	LAN.lab
LAN-AD02	10.100.0.13	Active Directory, DNS, Network Policy Server (Radius)	LAN.lab

Installation:

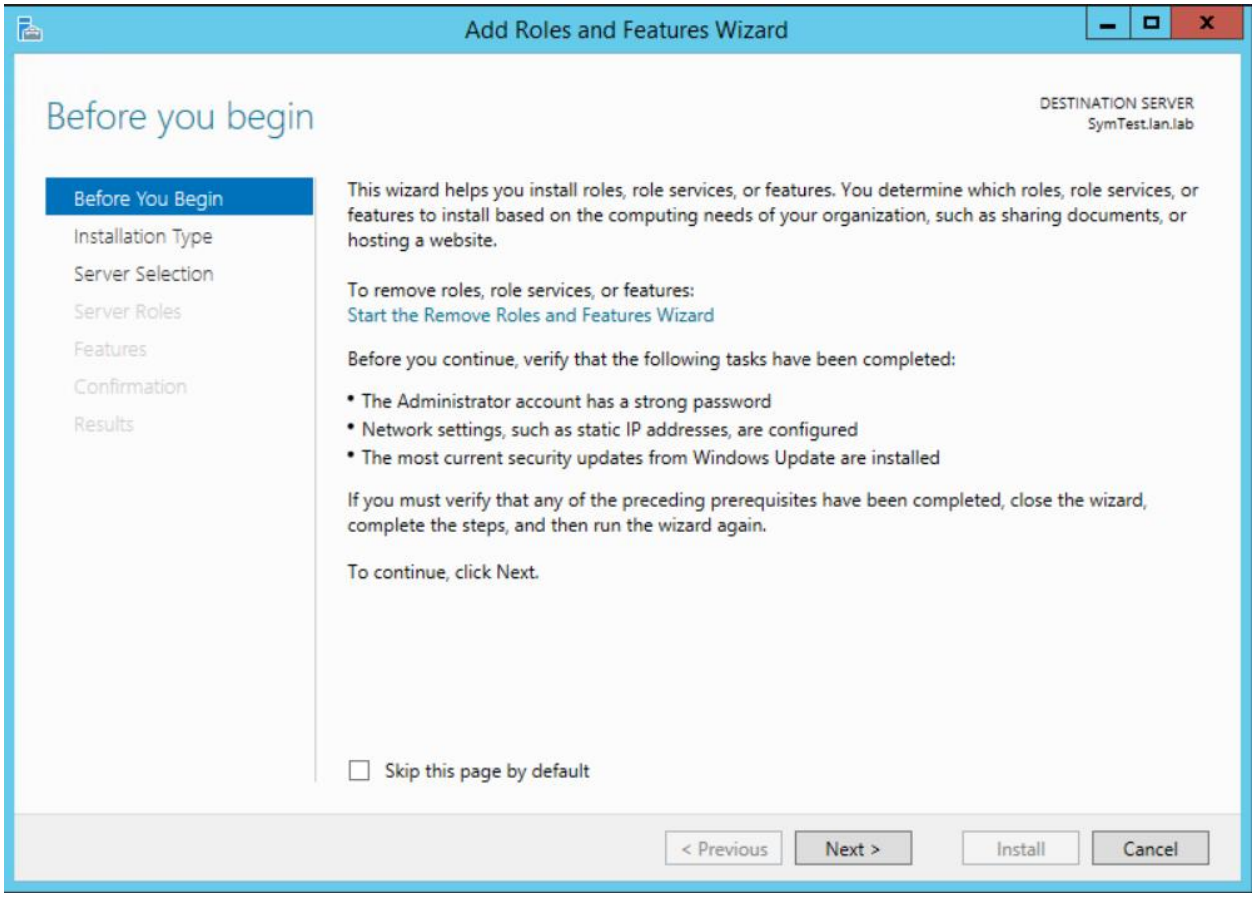
- Below are high level instructions for installing Active Directory services (ADDS) on a Windows 2012 R2 server.
- It is recommended to have 2 servers running AD for redundancy. Ensure the servers are up to date with patches and have meaningful hostnames as per their role. Begin by configuring a static IP address on the network interface of your server. Since the server will also act as DNS server, for DNS server field you can use local host address 127.0.0.1



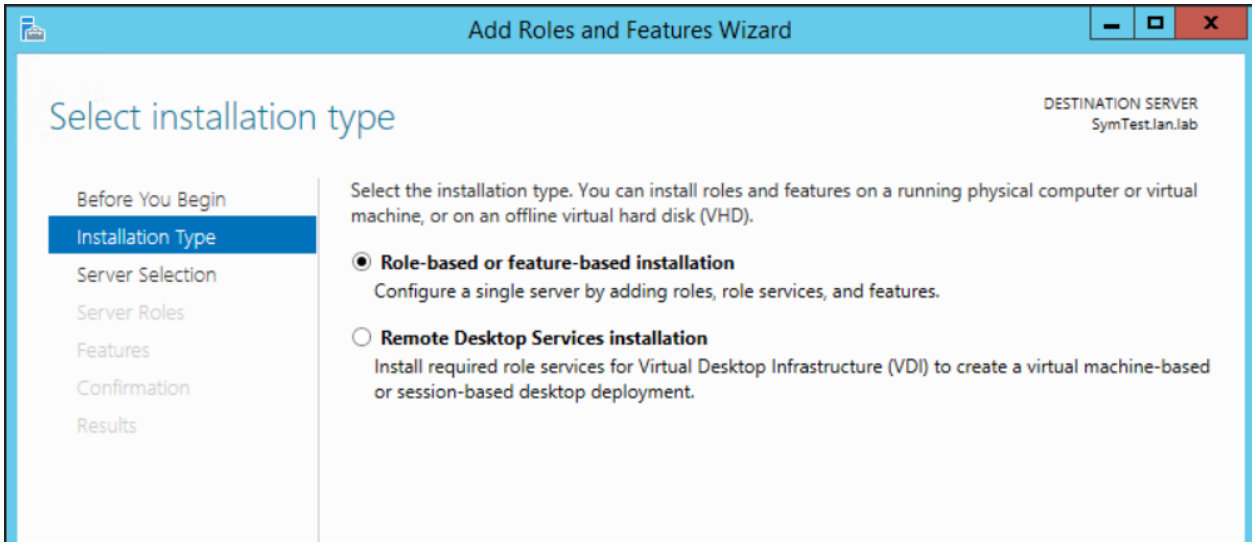
- Launch "Server Manager" and click on "Add Roles and Features"



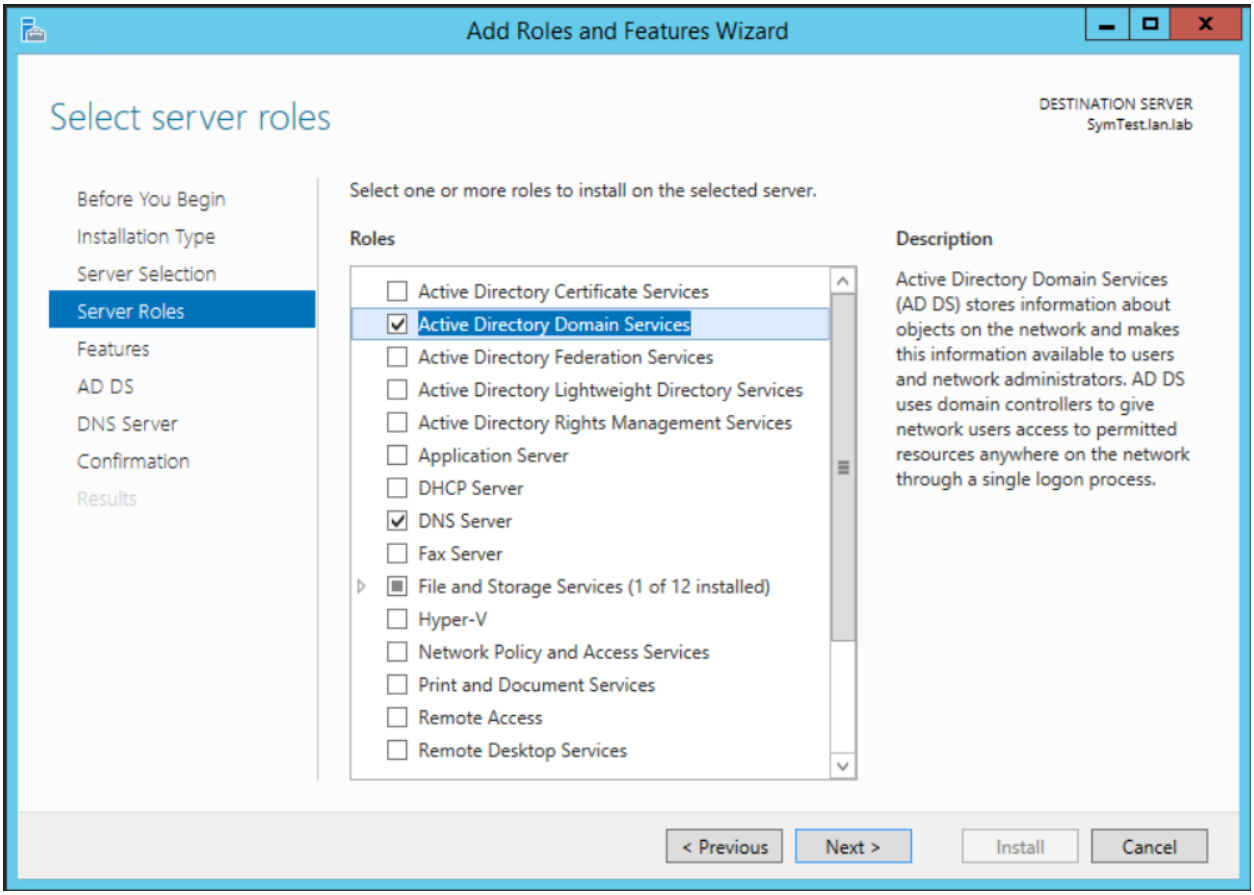
- Click "**Next**" at the first page



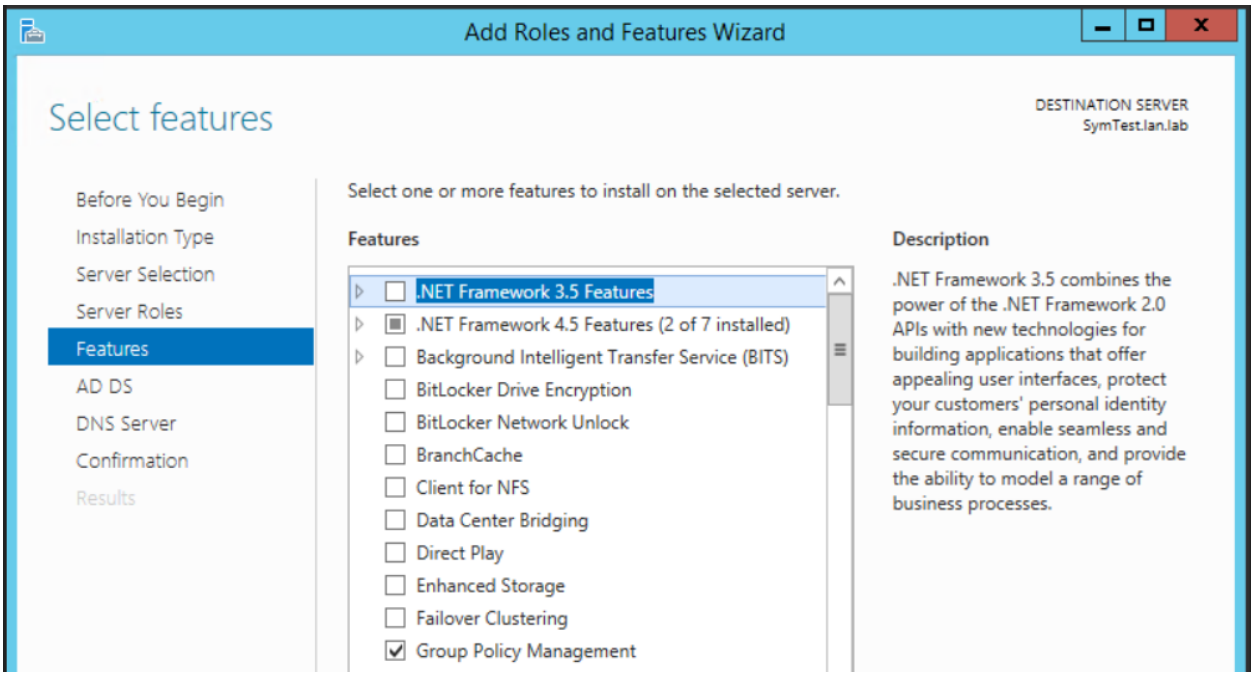
- Select "**Role Based or Feature Based Installation**" under Installation Type



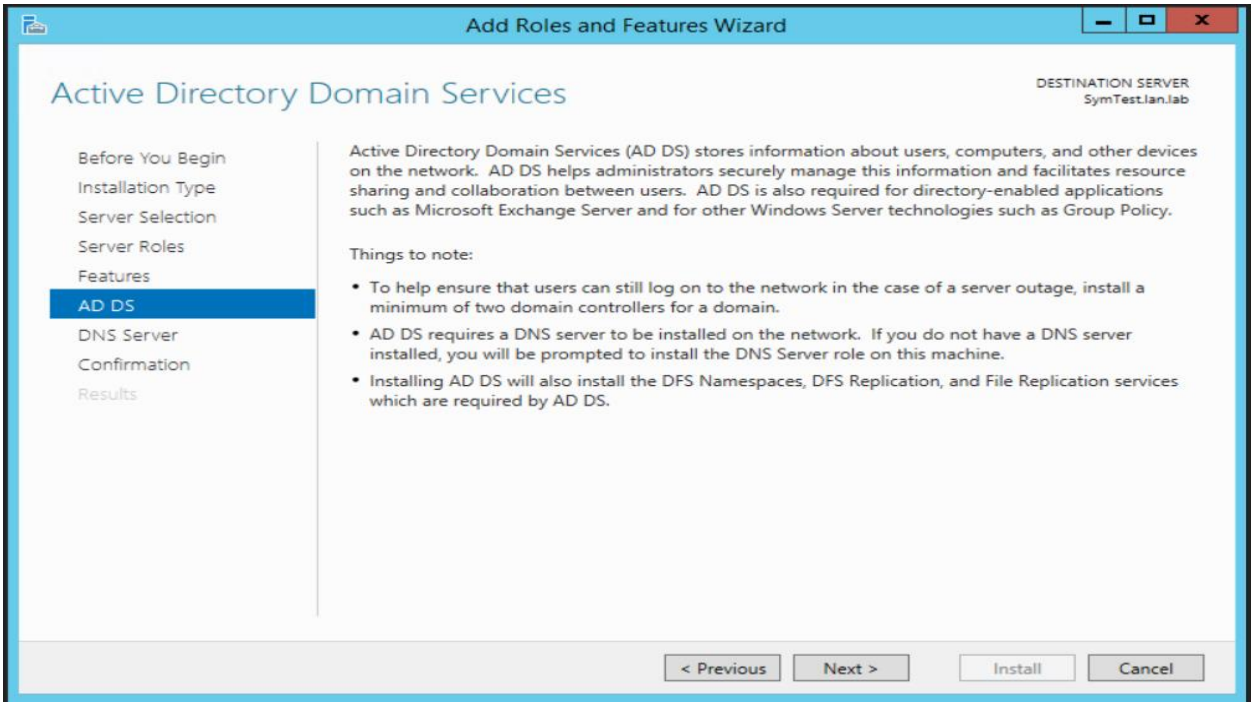
- Select "**Active Directory Domain Services**" and **"DNS Server**" to install. Click Next



- Under "**Features**", leave the default options selected and click **Next.**

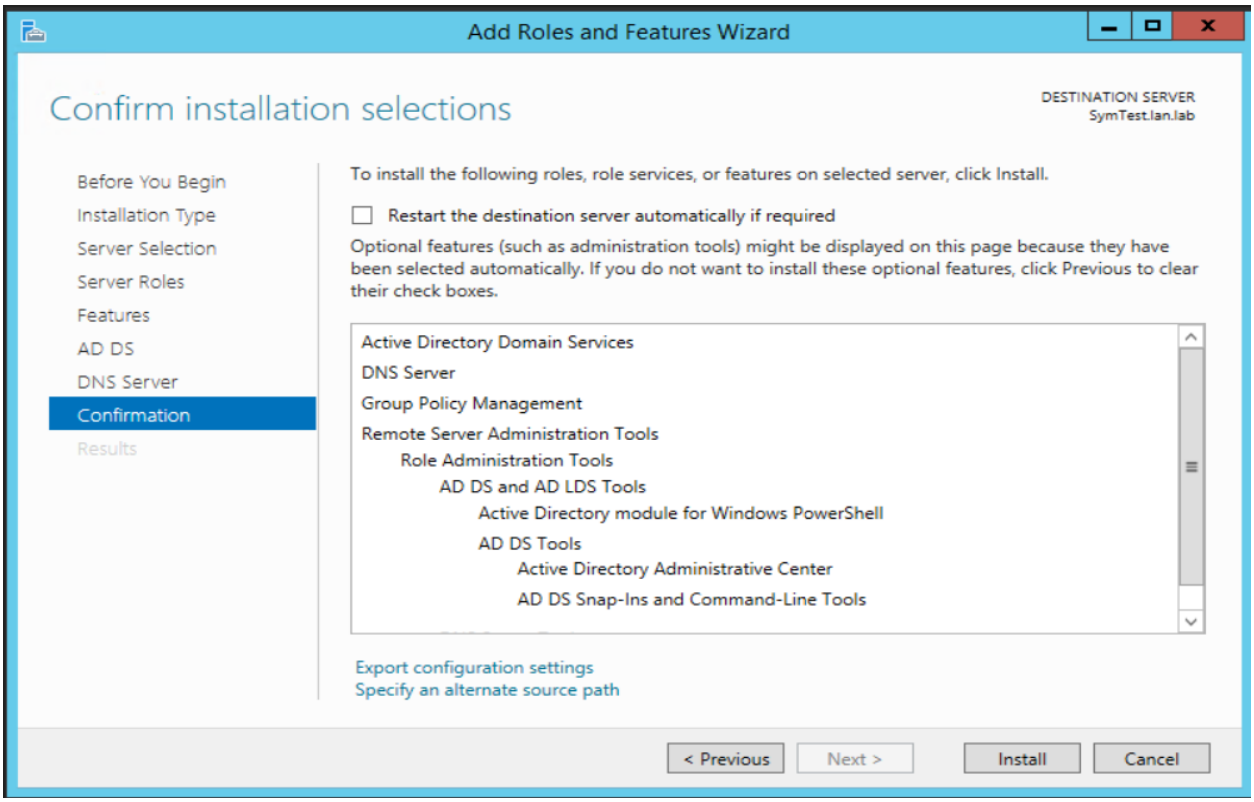


3555 • On the "**AD DS**" page, click **Next**. Likewise, on the "**DNS Server**" page click **Next** as well.



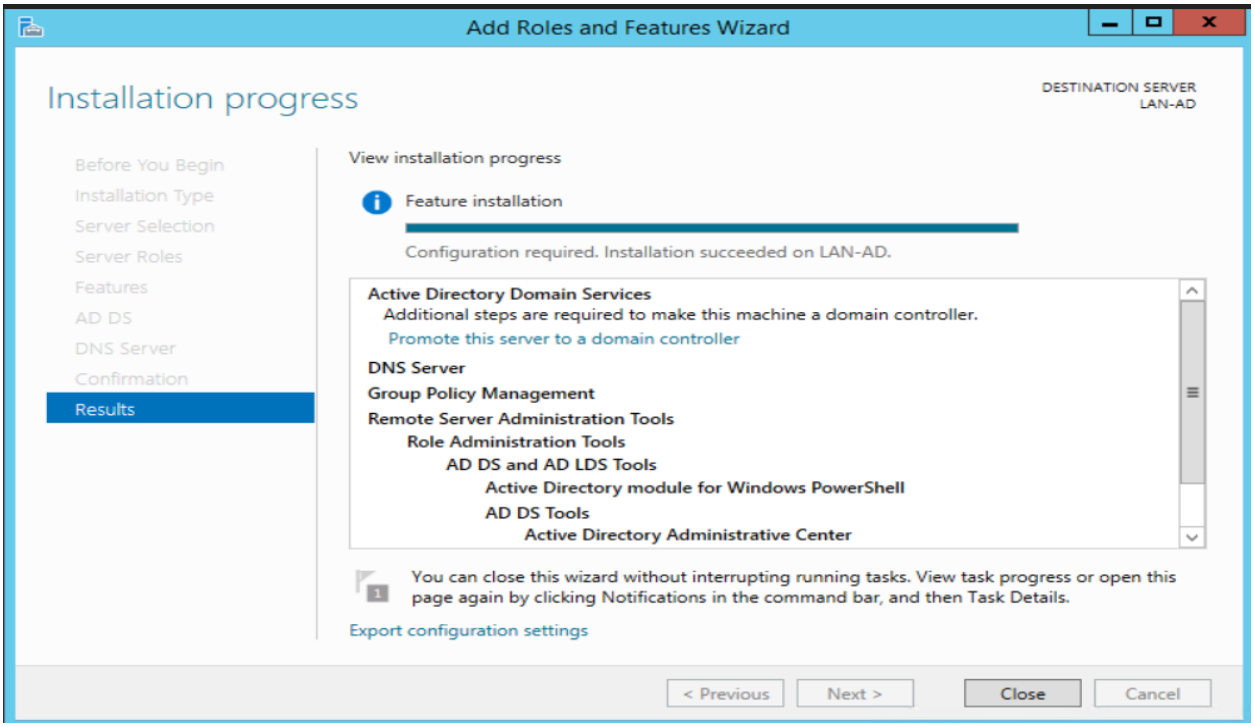
3556

3557 • Verify your settings on the "**Confirmation**" page. Click **Install** to proceed.

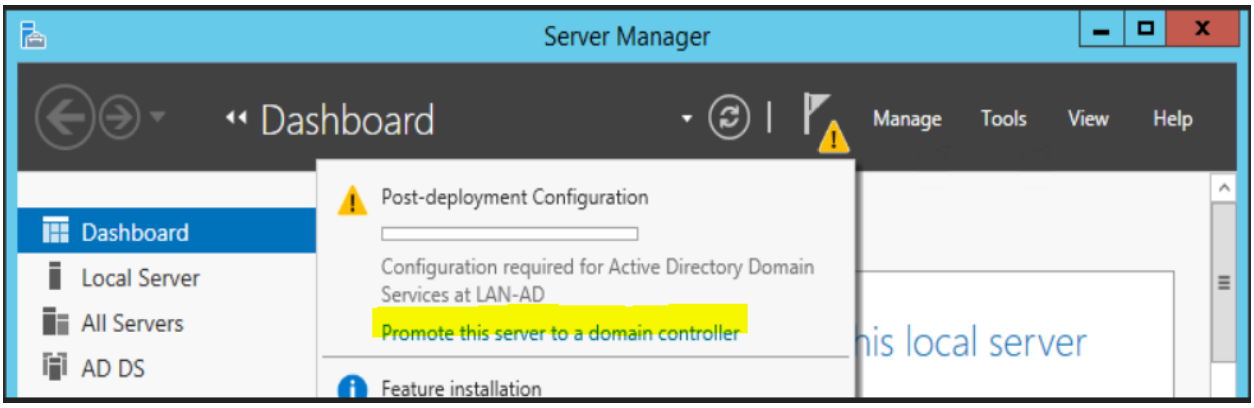


3558

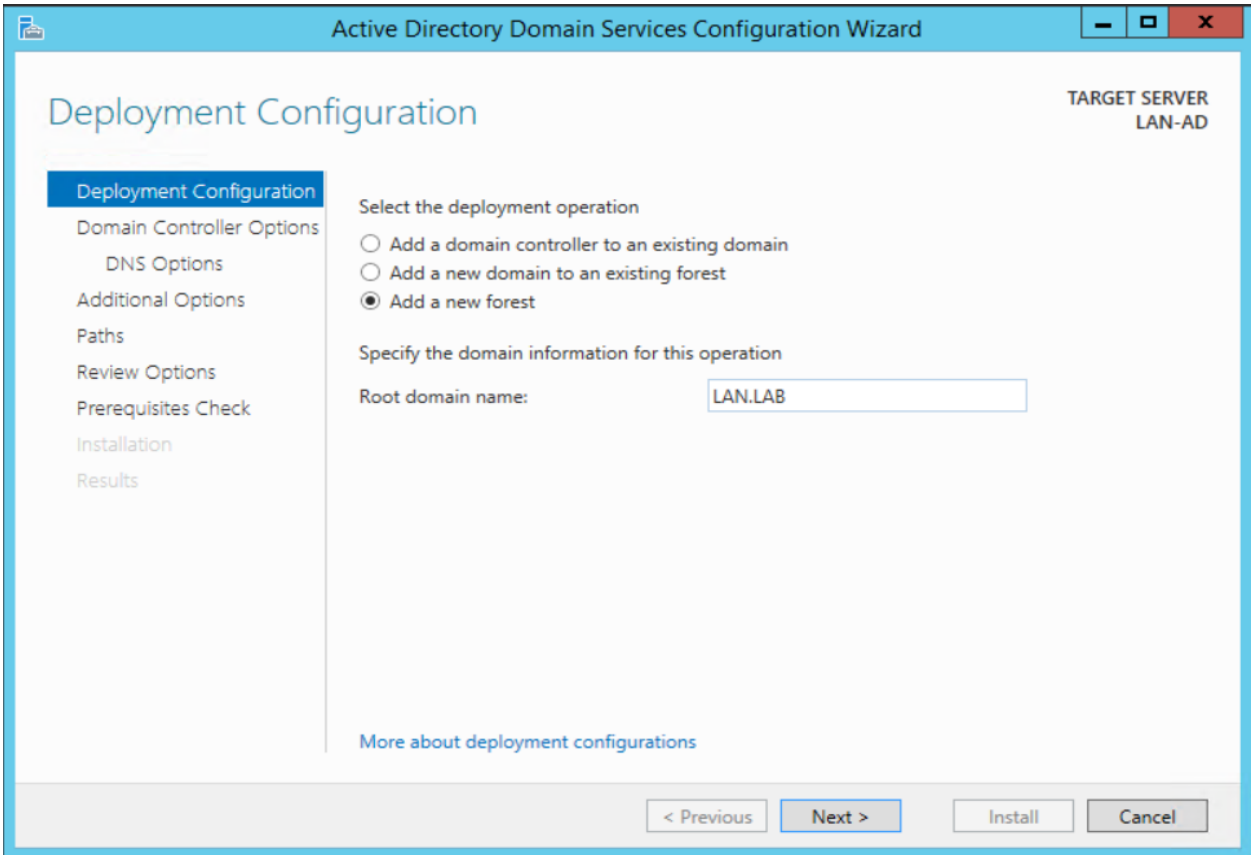
- The installation process will run and will show an "Installation succeeded" message upon completion. Hit **Close** button.



➢ Launch "**Server Manager**" again and click on "**Promote this server to a domain controller**"

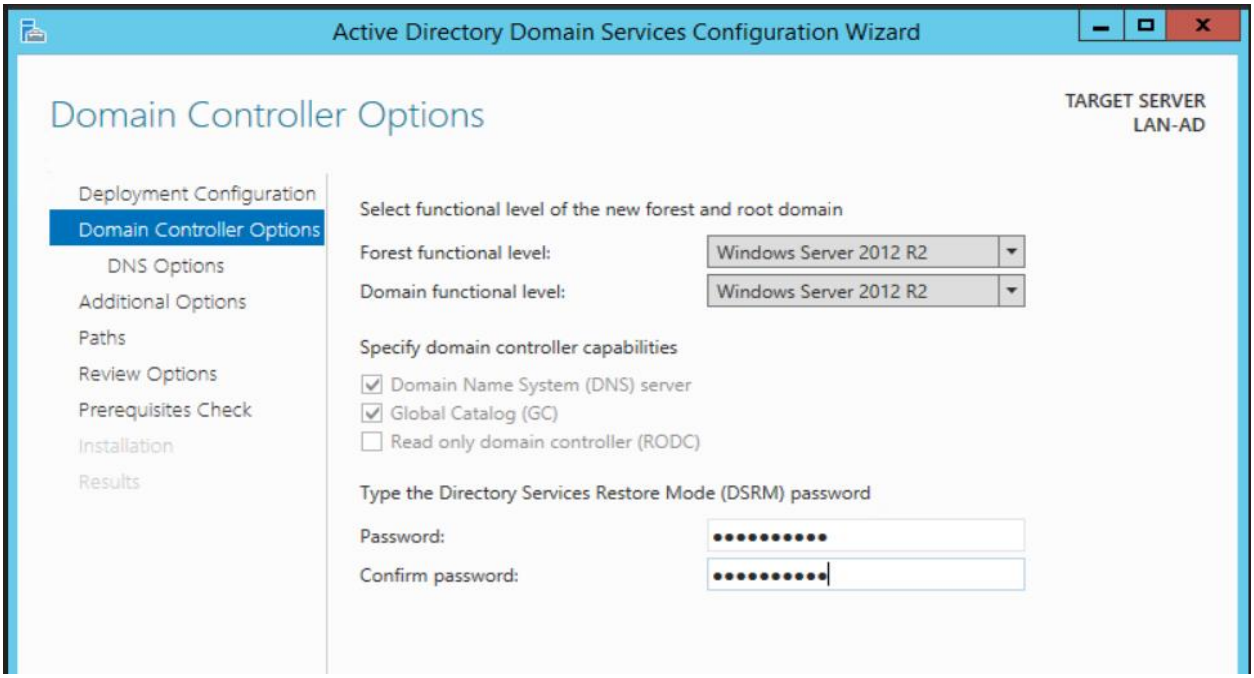


- On the "Deployment Configuration" step, select "**Add a new forest**" as this would be a new domain controller in a new forest. Mention a Root Domain name as applicable to your environment.



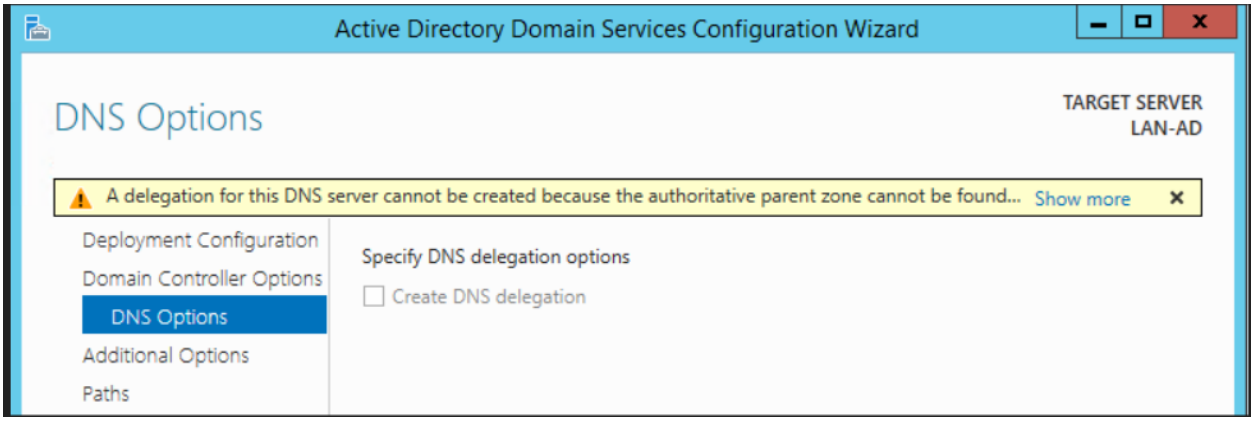
3568

3569 • Set a Directory Services Restore Mode password in the next step. Click **Next**



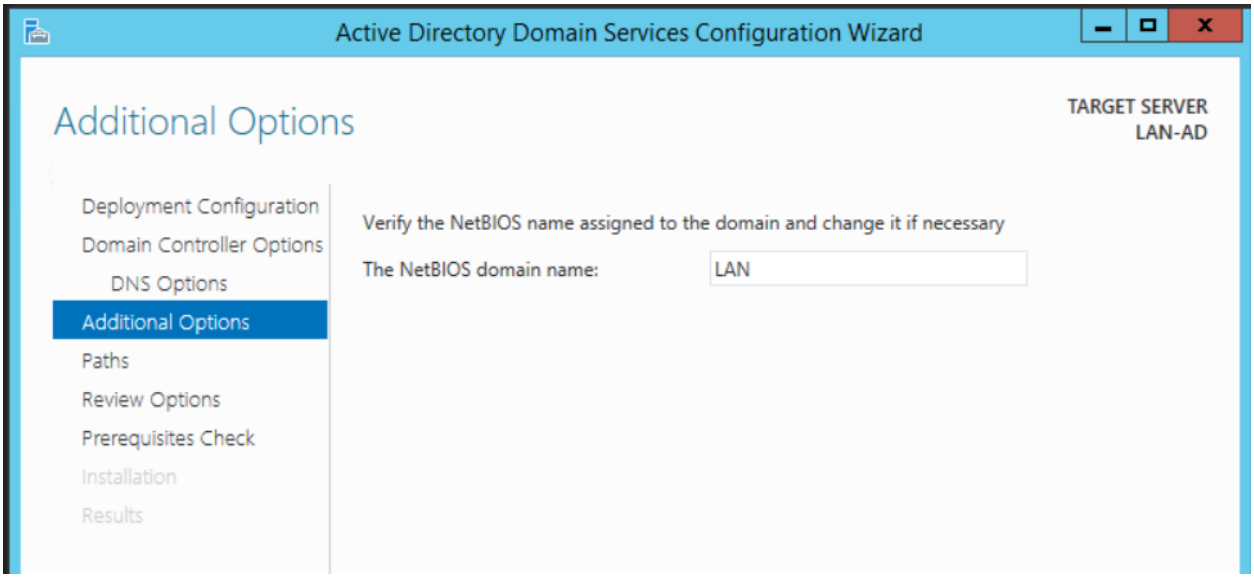
3570

3571 • Under "**DNS Options**" leave the default options selected. Click **Next**



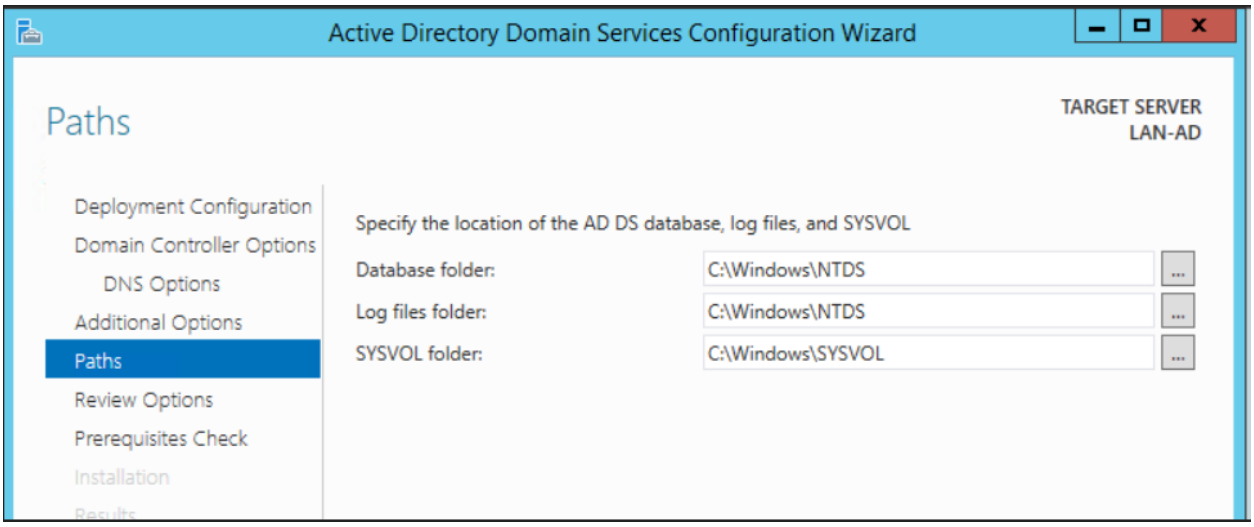
3572

3573 • Under "**Additional Options**", confirm the NETBIOS domain name. Click **Next.**



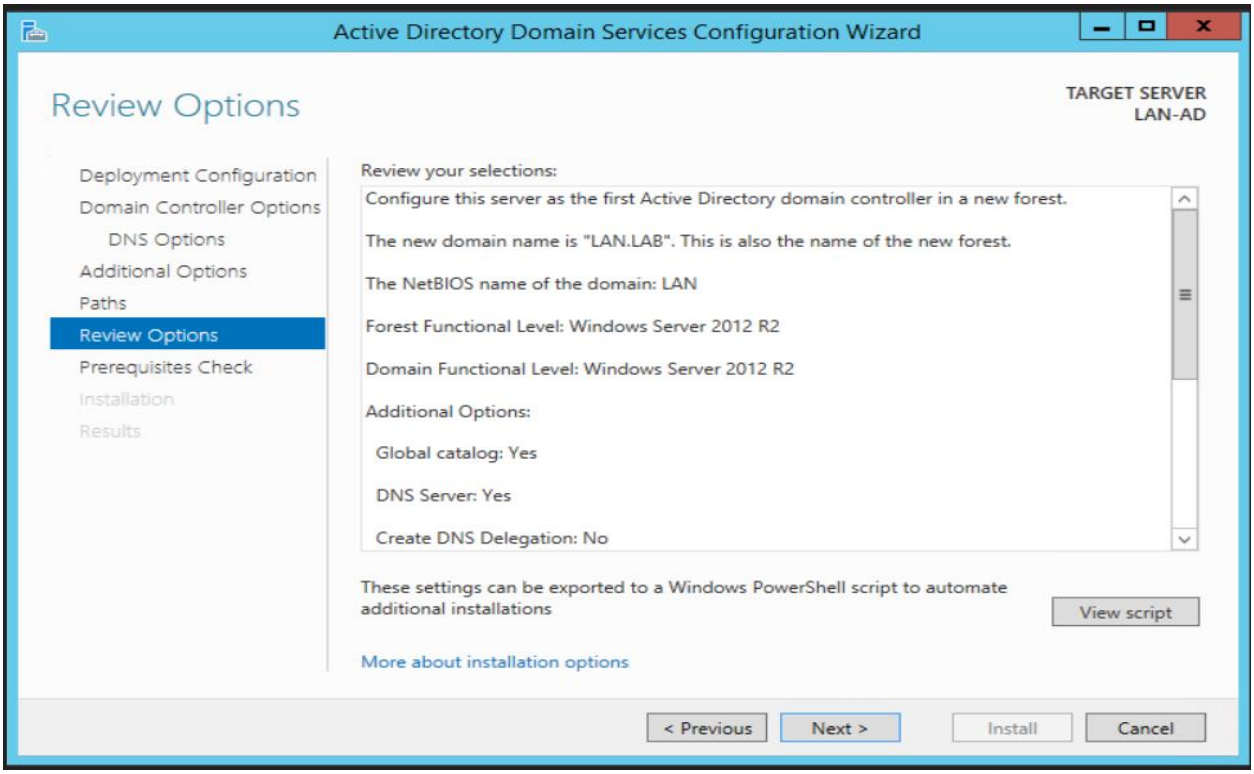
3574

3575 • Under "**Paths**", leave the default folder paths as it is. Click **Next**



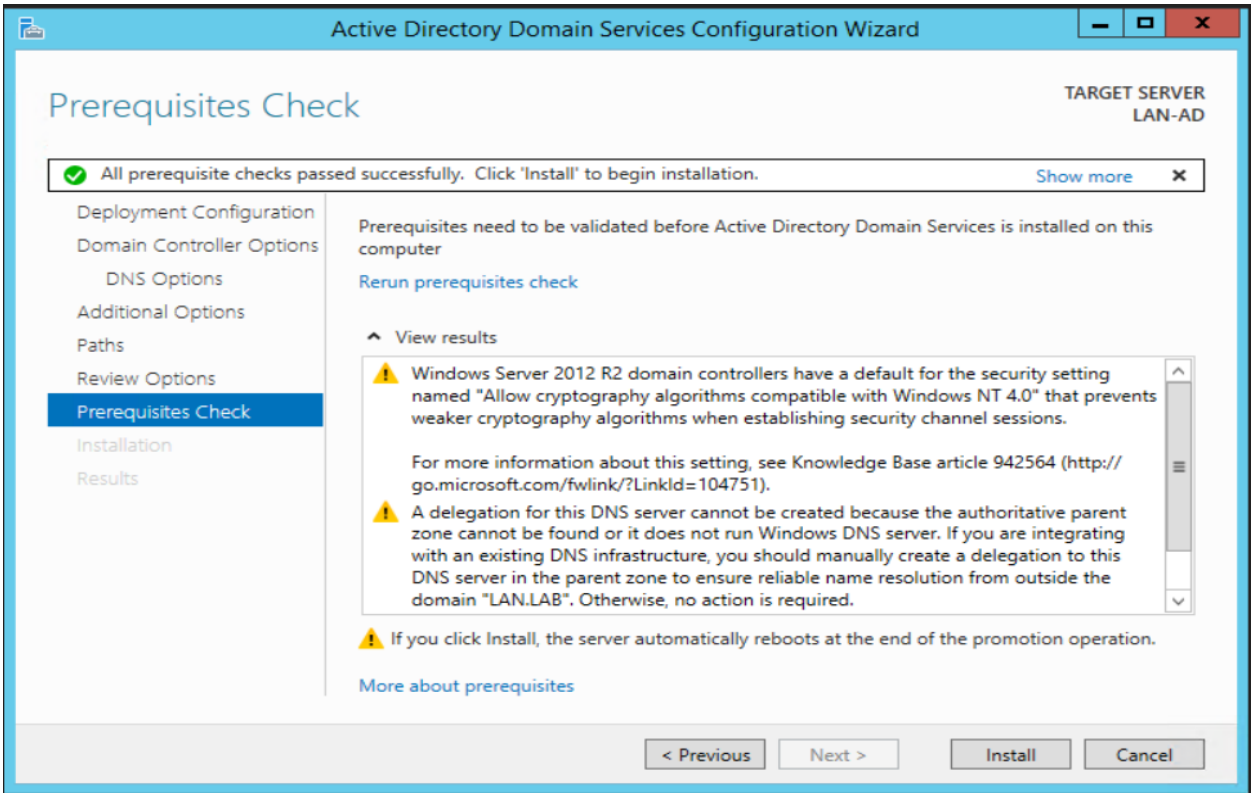
3576

3577 • On the "**Review Options**" page, confirm all the settings and click **Next**.

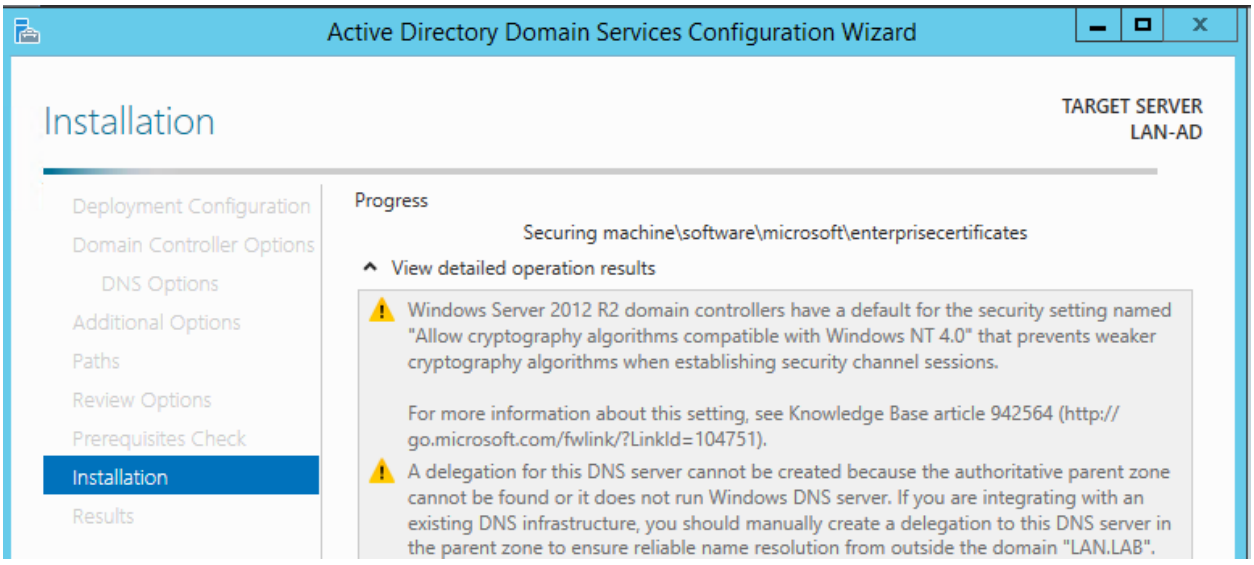


3578

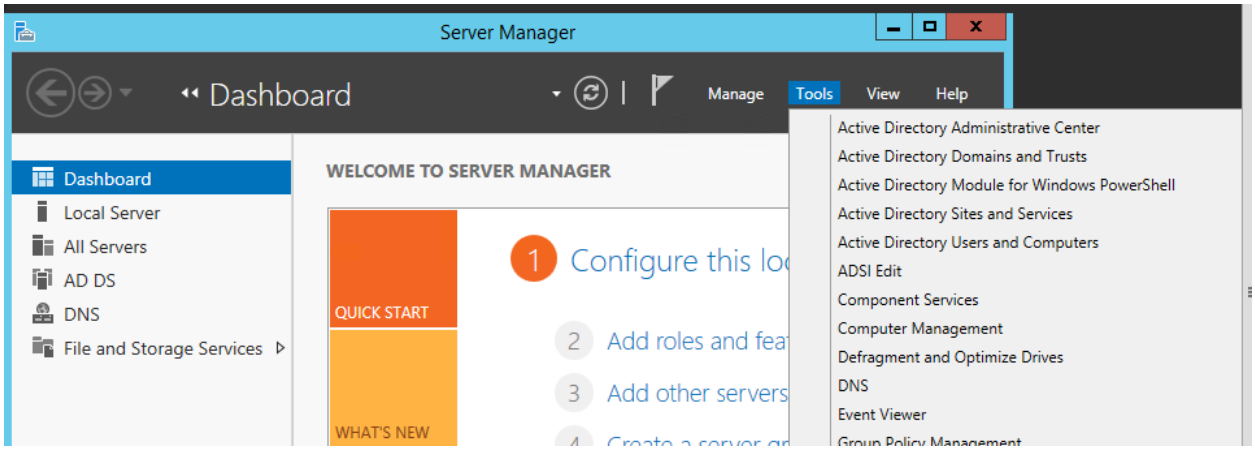
3579 • On the "**Prerequisites Check**", click Install to launch the installation process.



- The installation process will now run displaying the Progress bar. Upon completion, the server should auto reboot.



- Upon reboot, login with domain administrator credentials. Open "Server Manager" and click on "Active Directory Users and Computers" under Tools to manage your AD.



Configuration:

- All of the Linux systems from the Robotics System were joined to the AD domain **lan.lab** using **Centrify Express** [2]. The initial domain join process is a onetime task and involves a system restart.

- The procedure to join Ubuntu Linux Systems to Active Directory domain using Centrify can be found in the section below "CentrifyDC Installation"

- In addition, DNS records for each Linux host were manually created on the Active Directory server.

CentrifyDC Express Installation

Pre-requisites: Connectivity between your Linux server and AD server.

Ensure you can ping the AD Domain Controller from your Linux host. Configure the DNS settings on its network interface to point to the IP address of the AD server and set the search domain to whatever domain name you have created in your AD. Once done, you can verify the DNS-settings by checking the /etc/resolv.conf file of your Linux server.

- The free Centrify Express (Centrifydc) package can be downloaded either from https://launchpad.net or https://www.centrify.com/express/linux/download/ . Ensure to select the correct OS version and CPU architecture that matches your Linux host.
- Upload the downloaded file to any Ubuntu Linux server which you want to join to AD.
- Run the command "**dpkg -i <package_name>** "to install it. It may prompt you to install some dependencies. Ensure the dependencies have been installed prior.

```
root@rigel:/home/icssec# dpkg -i /media/CDROM/centrifydc_5.1.1-831-0ubuntu1_amd6
4.deb
Selecting previously unselected package centrifydc.
(Reading database ... 270726 files and directories currently installed.)
Unpacking centrifydc (from .../centrifydc_5.1.1-831-0ubuntu1_amd64.deb) ...
Setting up centrifydc (5.1.1-831-0ubuntu1) ...
Processing triggers for man-db ...
Processing triggers for ureadahead ...
Processing triggers for libc-bin ...
ldconfig deferred processing now taking place
root@rigel:/home/icssec#
```

- Run the command "**adlicense --express**" to activate the free express mode.

```
root@rigel:/home/icssec# adlicense --express
The mode is express.
root@rigel:/home/icssec#
```

- Next run the "**adjoin –workstation domain-name**" command. This will prompt you to enter the Domain Administrator password.

```
root@rigel: /home/icssec
root@rigel:/home/icssec# adjoin --workstation lab.local
```

- If the above step completes successfully, run "adinfo" command to verify the domain join status as follows

```
root@rigel: /home/icssec
root@rigel:/home/icssec# adinfo
Local host name:   rigel
Joined to domain:  lan.lab
Joined as:         rigel.lan.lab
Pre-win2K name:    rigel
Current DC:        lan-ad.lan.lab
Preferred site:    default-first-site-name
Zone:              Auto Zone
Last password set: 2017-06-22 10:28:38 EDT
CentrifyDC mode:   connected
Licensed Features: Disabled
root@rigel:/home/icssec#
```

- You can now login to your Linux host using your AD credentials.

- For example: ssh username.domain-name@hostname.domain-name
- OR directly via Desktop as shown below: Domain-Name\Username

- **Enabling sudo for administrators**

To make an AD Domain Group a sudoer; edit the file /etc/sudoers file (using the command visudo) and add the following line:

```
%adgroup        ALL=(ALL) ALL
```

Where, **adgroup**, is a group from your active directory. The group names from active directory are transformed into all lower case letters with underscores replacing spaces, so you can use %domain_admins for the Domain Admins group.

4.8.6 Highlighted Performance Impacts

One performance measurement experiment was performed for the Active Directory service while the manufacturing system was operational:

1. CL002.1 - The Active Directory service is installed and running on CRS hosts.

4.8.6.1 Experiment CL002.1

No performance impact to the manufacturing process was measured during the experiment.

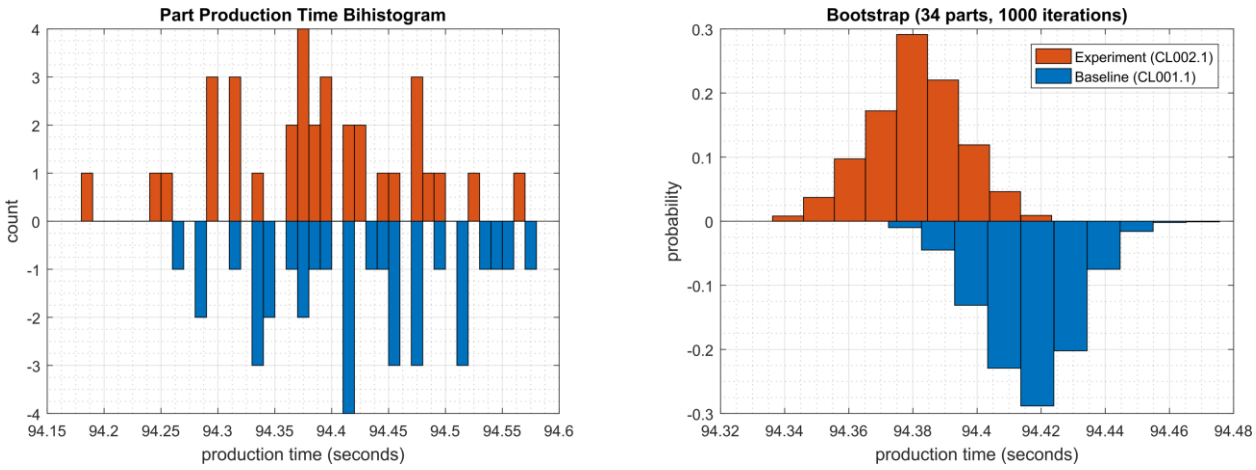


Figure 4-22 - Bihistograms showing the part production time (left) and estimated mean production time using the bootstrap method (right) using the measurements from baseline CL001.1 and experiment CL002.1.

4.8.7 Link to Entire Performance Measurement Data Set

- **CL002.1-ActiveDir.zip**

4.9 Symantec Endpoint Protection

4.9.1 Technical Solution Overview

Symantec Endpoint Protection:
Symantec Endpoint Protection (SEP) is a complete endpoint protection solution from Symantec. It delivers superior, multilayer protection to stop threats regardless of how they attack your endpoints. SEP integrates with existing security infrastructure to provide orchestrated responses to address threats quickly. Its lightweight SEP agent offers high performance without compromising end-user productivity. SEP also defends against ransomware and other emerging threats with multilayered protection that fuses signatureless technologies like advanced machine learning, behavior analysis and exploit prevention with proven protection capabilities like intrusion prevention, reputation analysis and more.[14]

Points to Consider:

- Next Generation Antivirus / Endpoint protection solution to prevent against virus attacks and emerging cyber threats such as zero-day attacks, ransomware etc.
- OS Platform independent: The endpoint agents are supported on Windows and Linux.
- Comes with a lightweight agent and virus definition sets that require minimal network bandwidth.
- Diverse Feature set: Core capabilities include Antivirus, Host Firewall, Intrusion Prevention, Host Integrity, System lockdown, Application White listing and USB Device Control.
- Centralized Management: All endpoints, rule sets, policies can be centrally managed from the Symantec Endpoint Manager console.
- The Symantec Manager component is supported only on Windows OS.
- The Linux agent requires the OS kernel on Linux systems to be at a certain level for installation. In addition, the Linux agent is a 32-bit installer. If installing on a 64-bit Linux system, it requires certain 32-bit packages/libraries to be installed as a pre-requisite. This may conflict with some of the existing packages on the system.
- The endpoint agent on each system by default needs to communicate outbound with a range of public IP addresses for its Reputation analysis and Global Threat intelligence feature. It is recommended to allow this traffic from your firewall to leverage the advanced features of the product.
- **Important**: System reboot is required to complete the installation process on clients/endpoints. Plan ahead of time.

[14] Symantec Endpoint Protection: https://www.symantec.com/content/dam/symantec/docs/data-sheets/endpoint-protection-14-en.pdf

4.9.2 Technical Capabilities Provided by Solution

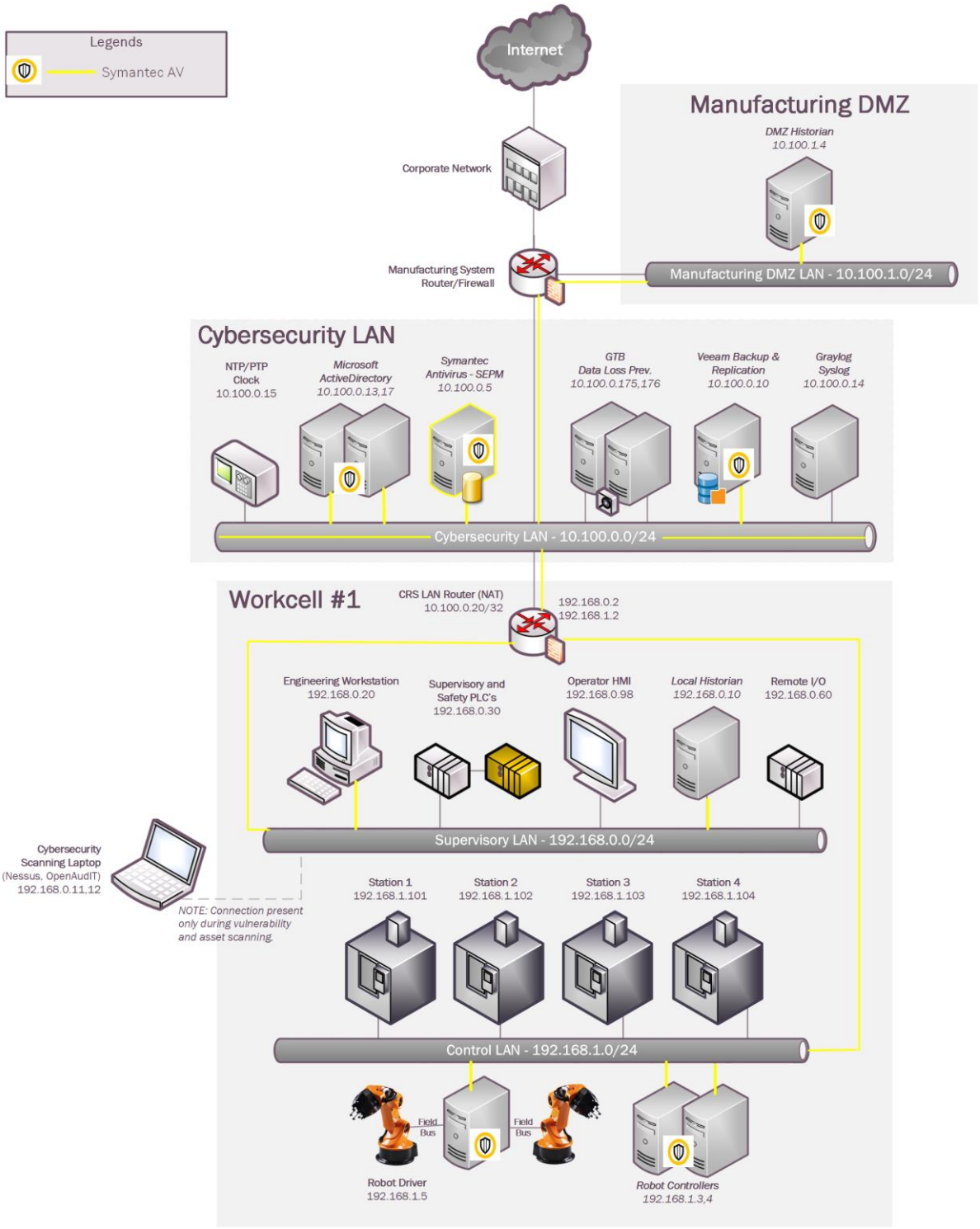
Symantec Endpoint Protection provides components of the following Technical Capabilities described in Section 6 of Volume 1:

- Anti-virus/malware

4.9.3 Subcategories Addressed by Implementing Solution

PR.AC-1, DE.CM-3, DE.CM-4

4.9.4 Architecture Map of Where Solution was Implemented



4.9.5 Installation Instructions and Configurations

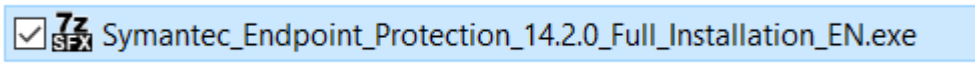
Setup Overview:

Setup consists of a single Symantec Endpoint Protection Manager (SEPM) instance in the Cybersecurity LAN network. This central instance communicates with all the endpoint agents deployed on to the Process Control systems. Likewise, all endpoints report their status to the Manager server. The communication ports required to be opened are different for Windows clients as compared to Mac/Linux clients. Detailed list of firewall ports can be obtained from Symantec website. The SEP Manager server downloads its daily signature updates from the Symantec cloud servers, so this necessary traffic was allowed to pass thru the Manufacturing System Firewall.

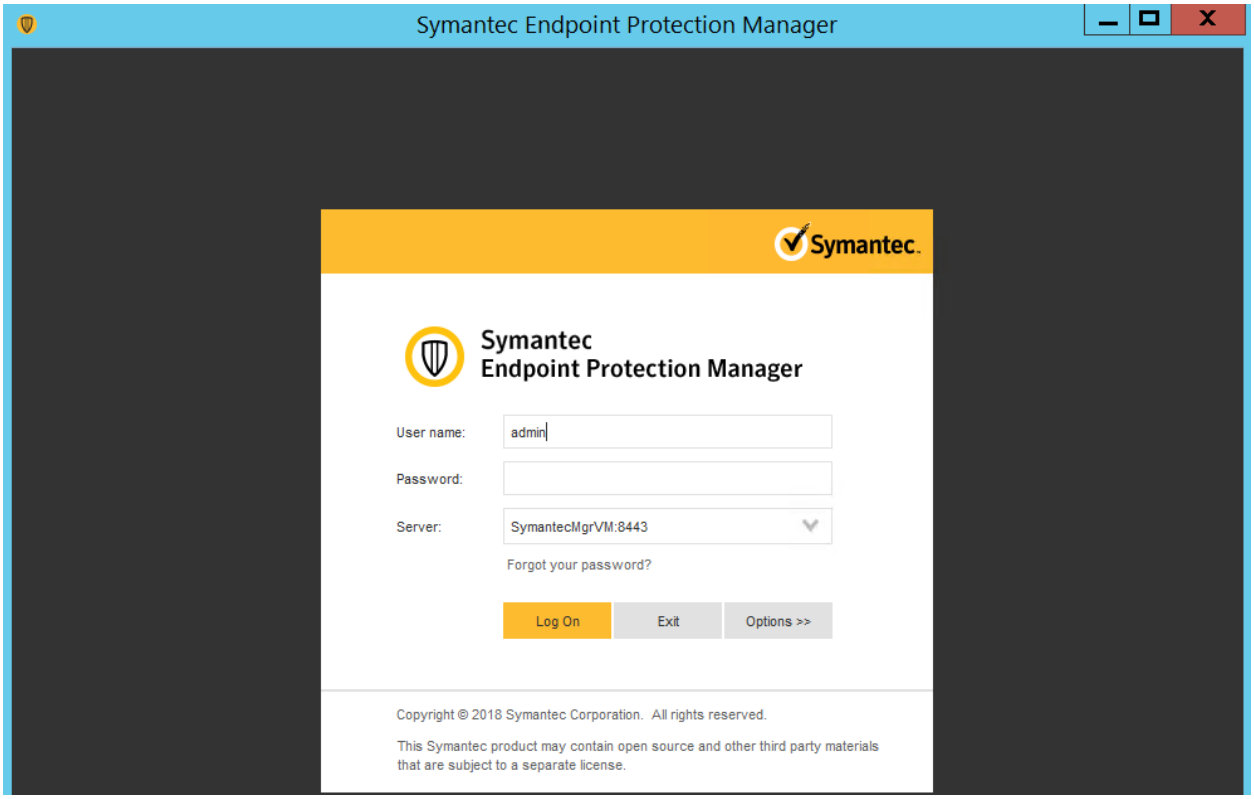
Details of the software used

Product Name	Version
Symantec Endpoint Protection Manager (SEPM)	14.2 Build 758
Symantec Endpoint agent for Linux (Client)	14.2.758.0000

Installation of SEP Manager:

- SEPM is supported only on Windows server platforms. A Windows Server 2012 R2 virtual machine was setup in the Cybersecurity LAN to install the SEPM component.
- Upon purchase, there will be a license file emailed to you along with the link to download the install binaries. Download the zip bundle from the Symantec website. Extract the zip file which will be like the one below depending on whatever is the latest version available.
  - 

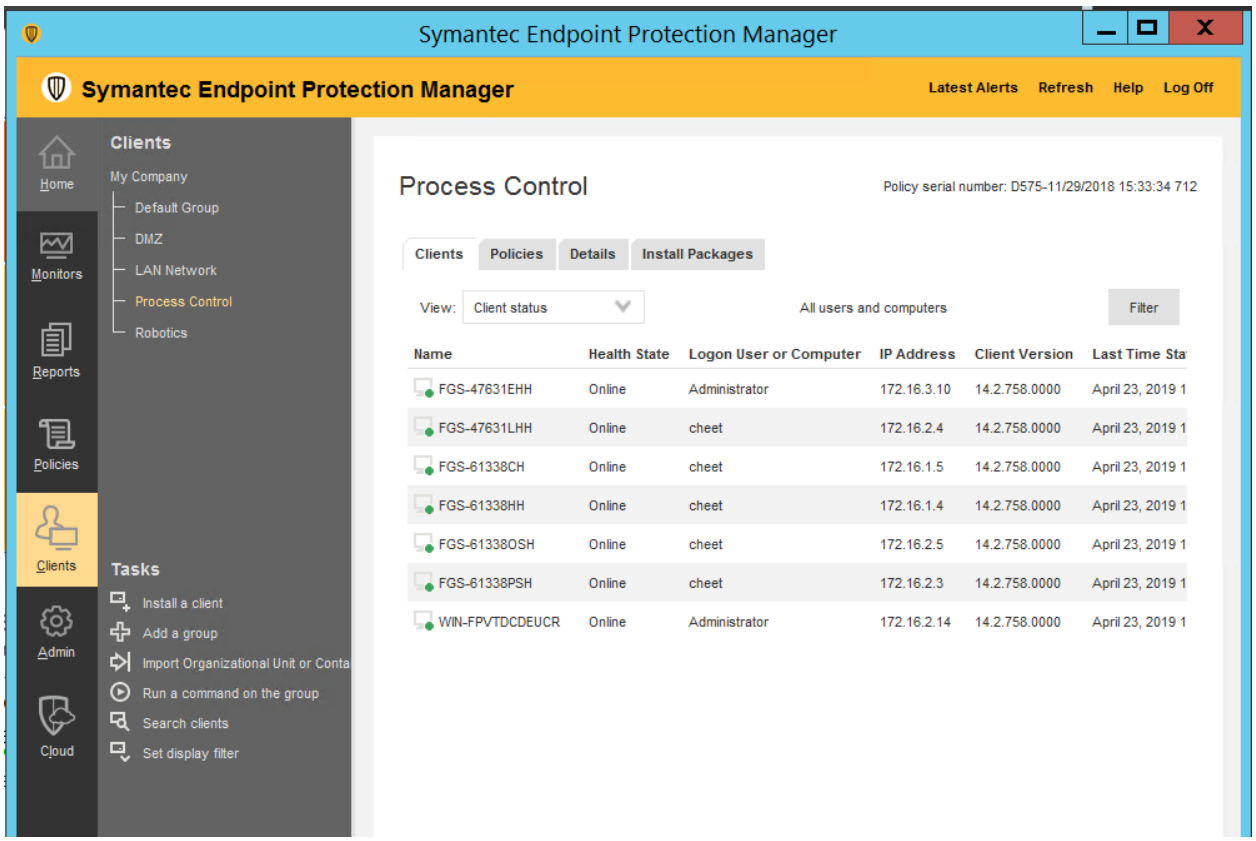
- Open the extracted folder and run the **Setup.exe** file. Mid-way during the setup, the install wizard will prompt to select a password for the admin user. Enter a strong password and hit **Next**.
- On the **Backed Database** selection page, there are two options - "**Embedded**" and "**MS SQL Server**". Choose the **Embedded database** if you do not have a MS SQL Server. Follow the on-screen instructions and complete the installation wizard. Reboot the server once done.
- Launch the SEP Manager console and login with the admin user created earlier.



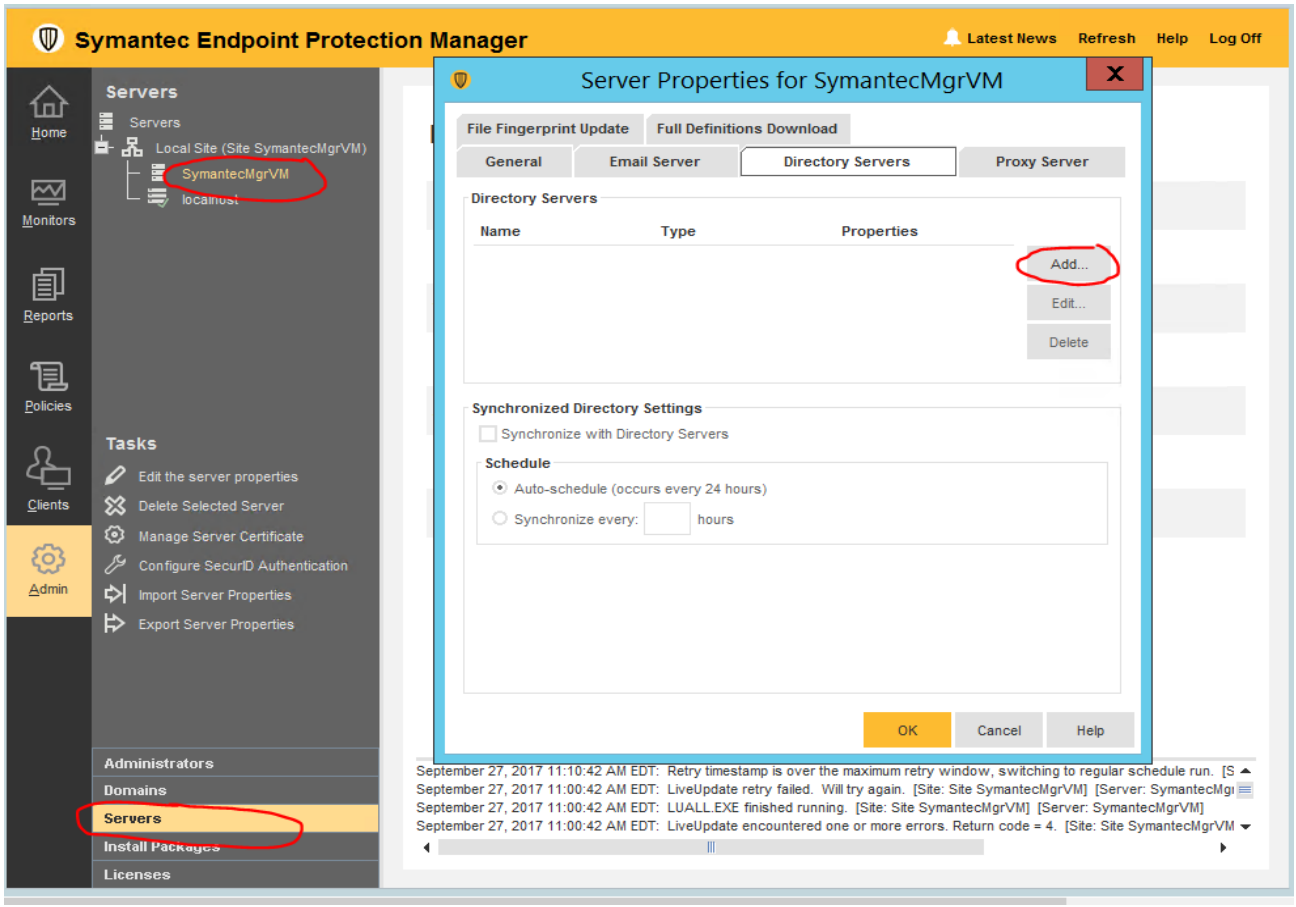
- Upon completing the installation of Symantec Endpoint Manager, the next steps are to activate the license, configuring client groups to group devices and installing the antivirus agent on each endpoint/client system.
- Link to Official Symantec Endpoint Protection v14 installation guides - https://support.symantec.com/en_US/article.DOC9449.html
- Ensure to open the necessary ports on the firewall for communication between the SEPM server and endpoints. A complete list of ports is available at https://support.symantec.com/en_US/article.HOWTO81103.html

Custom Configuration of SEPM server

- The following client groups were created to group devices from each of the systems. Upon installing the AV agent on the endpoints, the devices were moved to their respective groups.



- For integrating SEP Manager with AD/LDAP server, click on **ADMIN** >> **Servers** >> **Local Site** >> **<Server Name>** >> **Edit Server Properties** >> **Directory servers.** Click further on "**ADD**" button as shown below to configure domain details. Once done, logout and try logging in back with your AD credentials.



- Similarly, Email server can be configured by clicking on the "Email Server" tab.

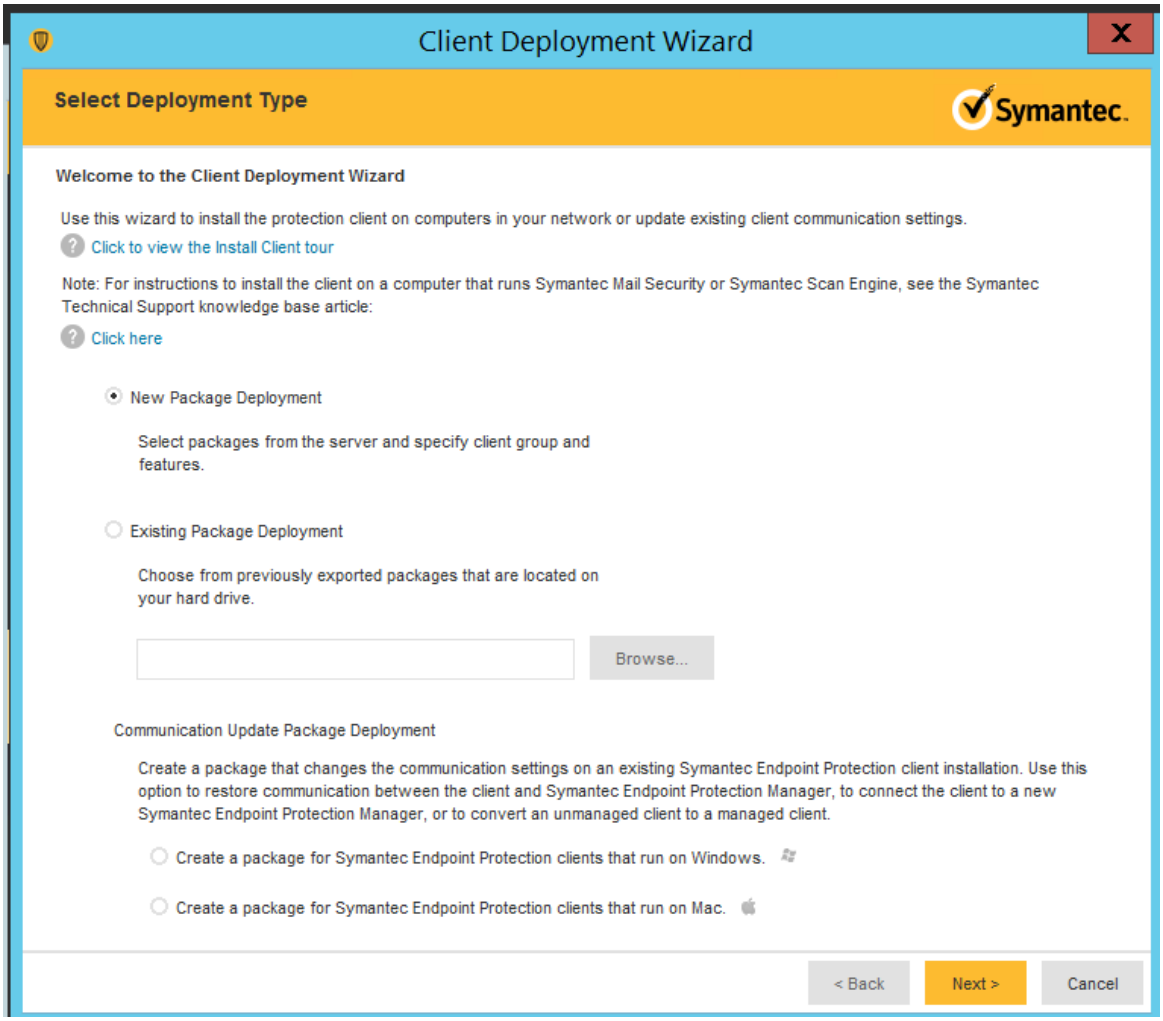
<u>Getting started with Endpoint installs</u>

High level steps:

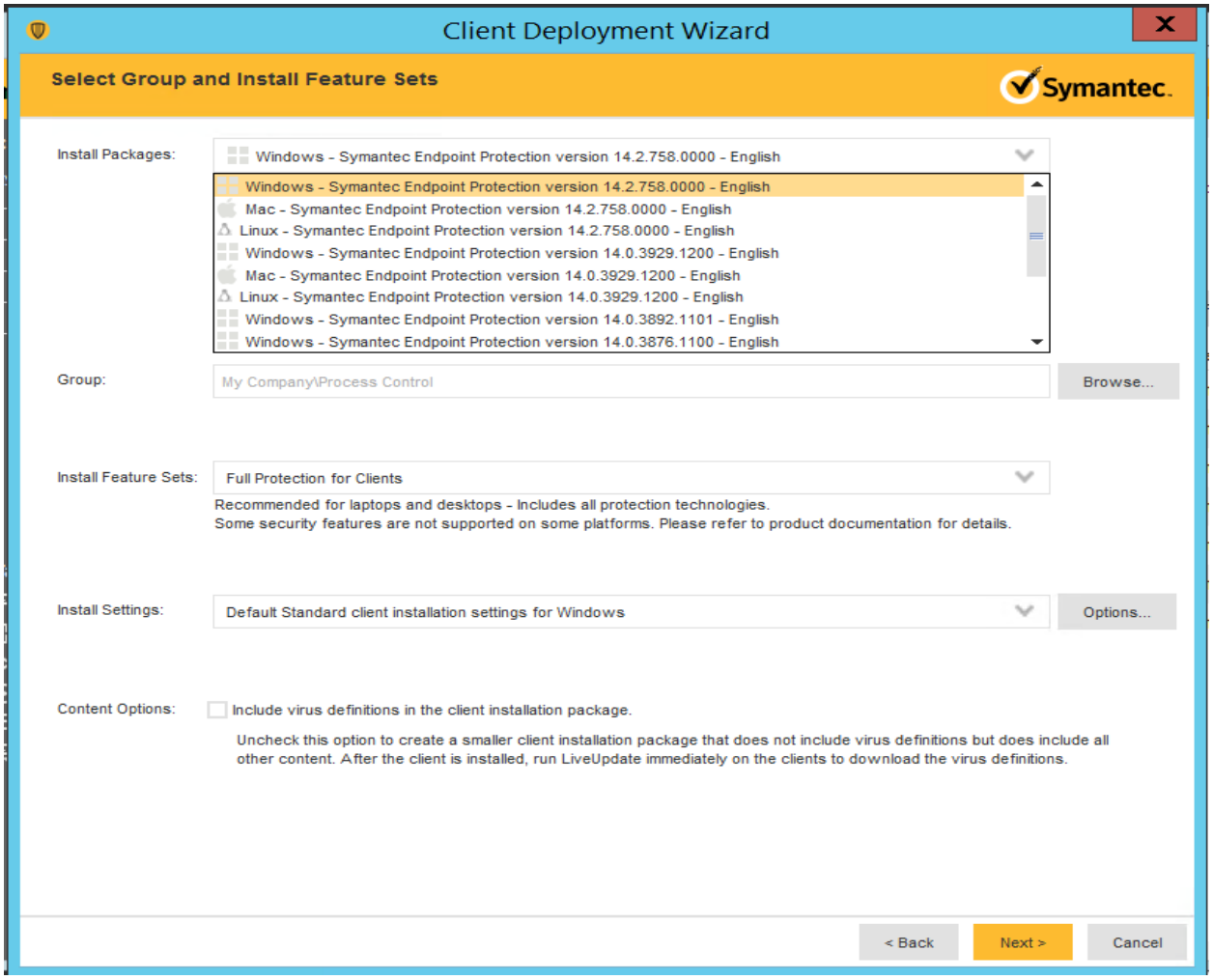
- Create a deployment package specific for a client group
- Deploy the package from the SEPM server to the endpoint using Network Deployment options or manually copy over the package to the endpoint for installation.
- Restart the endpoint. Verify the device shows up in the SEPM console.

Creating a deployment package:

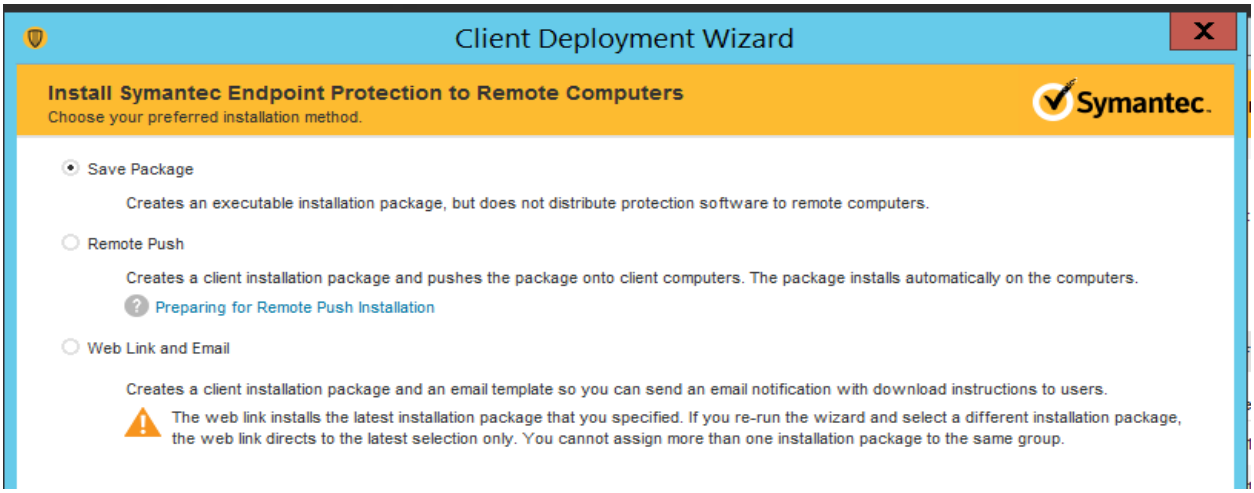
- Login to the Symantec Manager console, click on **CLIENTS** >> **<Group Name>** where the device needs to be in >> Click on **Install client under TASKS**. For instance, to create a deployment package for the group "**Process Control**", click on that group name followed by **Install Client** option.
- Select "**New Package Deployment**" if this is your first agent installation of that group. If you have already deployed the agent on other systems of this group, you can re-use the same package and skip this wizard completely.



- Click "**Next**" >> Choose the appropriate OS Platform as per the endpoint OS, from the dropdown list of **Install Packages**. You will notice the Group Name is already pre-populated. This ensure the client will be placed directly in that group upon install. Under **Content Options**; Select "**Include virus definitions in the client installation package**" [optional]. Click **Next**.



- On the next page, choosing the "**Save Package**" will create a local installer which needs to be copied over the target machine manually and the "**Remote Push**" will make the SEPM server perform a network deployment to the target machine(s). Choose your preferred option and hit **Next**.



Installing the AV on Robotics Systems

- A new deployment package was created for the "**Robotics**" group with OS as Linux. This will create a **.rpm** package for Red Hat systems and **.deb** package for Debian based systems. The package with (.deb) extension was copied over manually to each Ubuntu Linux server in the Robotics system.

- Symantec AV on Linux requires the below 32-bit packages to be installed as a pre-requisite[15]. A Full backup of all Linux systems in Robotics was taken prior to installing these.
    - libc6:i386
    - libx11-6:i386
    - libncurses5:i386
    - libstdc++6:i386

- If installing it on a 64-bit server, ensure to enable/check if multi-architecture mode is enabled as follows, prior to installing those 32-bit libraries. For instance, on a Debian /Ubuntu system; run the following commands.

- Verify if the system has 64-bit architecture by running

```
dpkg --print-architecture
```

- If the output is something like the one shown below, it means you are okay

```
amd64
```

- Verify that you have multi-arch mode enabled by running the following command. Multi-architecture mode lets us install 32-bit packages on a 64-bit system.

Type:

```
dpkg --print-foreign-architectures
```

The output is:

```
i386
```

If you don't have multi-arch support you have to enable it.

- Run this command to enable multi-arch support:

```
sudo dpkg --add-architecture i386
```

This will allow us to install those 32-bit packages.

[15] https://support.symantec.com/en_US/article.TECH228118.html

```
sudo apt-get install libc6:i386 libx11-6:i386 libncurses5:i386 libstdc++6:i386
```

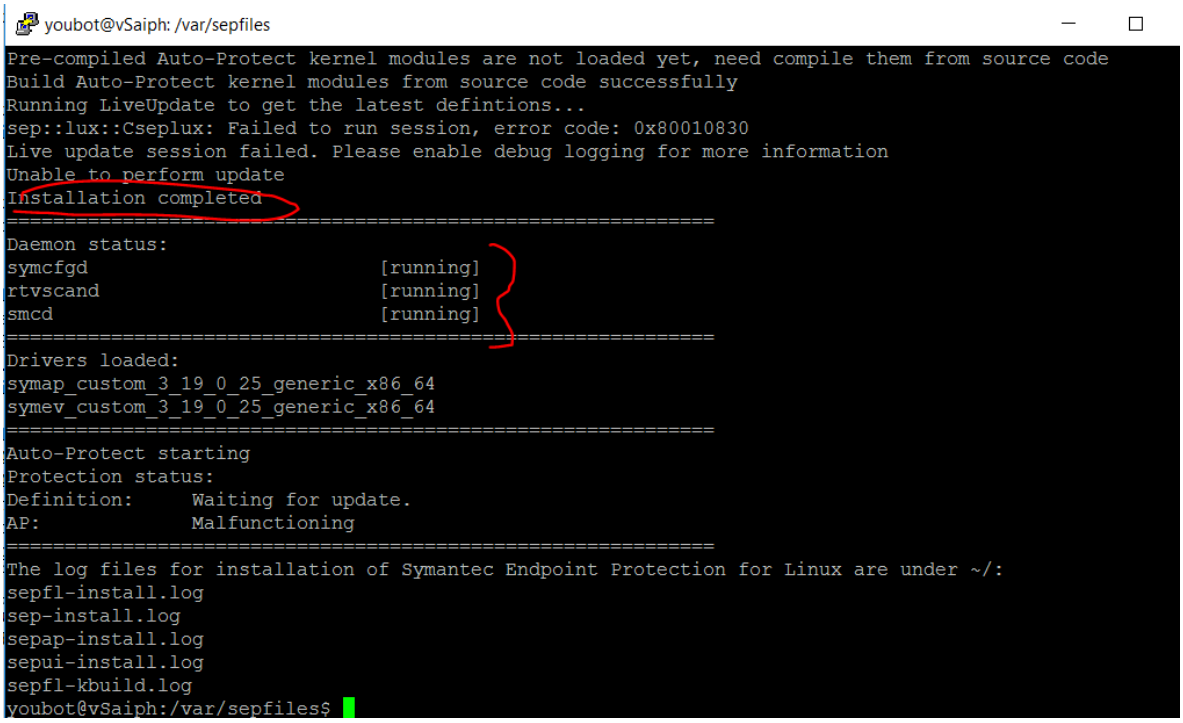
- The zip file containing the .deb package was extracted on the Linux client. The following command was run to grant execute permissions to the "install.sh" file found in the extracted folder.

```
chmod u+x install.sh
```

- Next, the install.sh script was run as

```
sudo ./install.sh -i
```

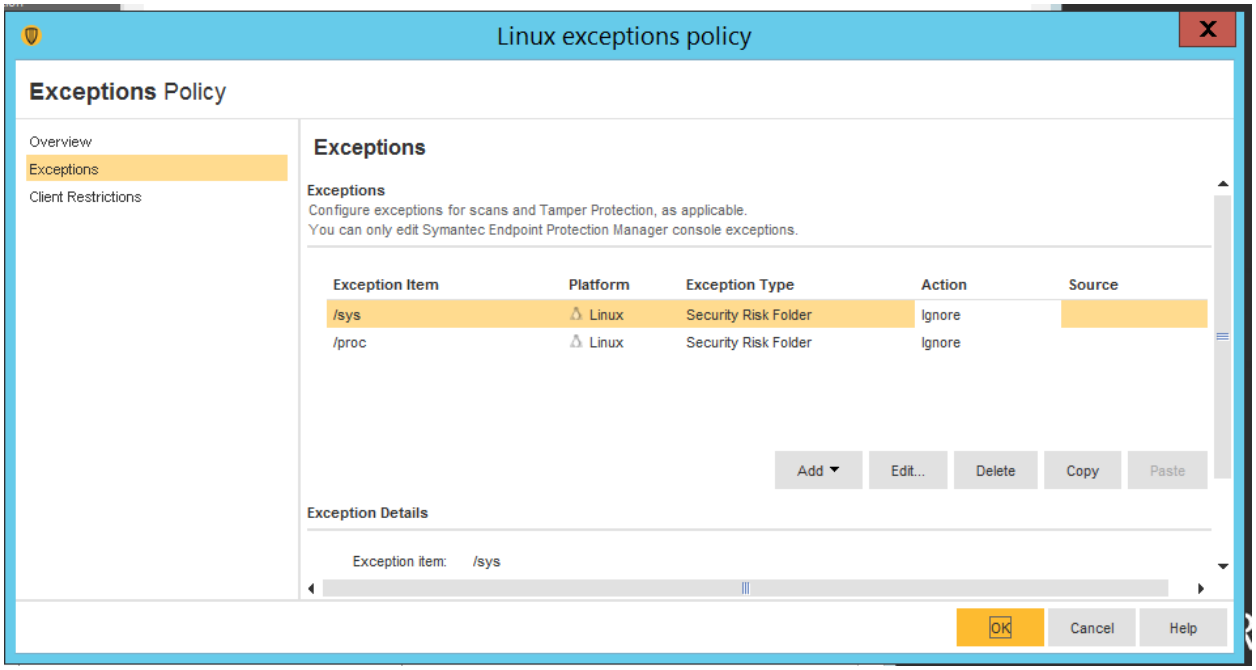
- Upon successful install, it showed an output like the one below



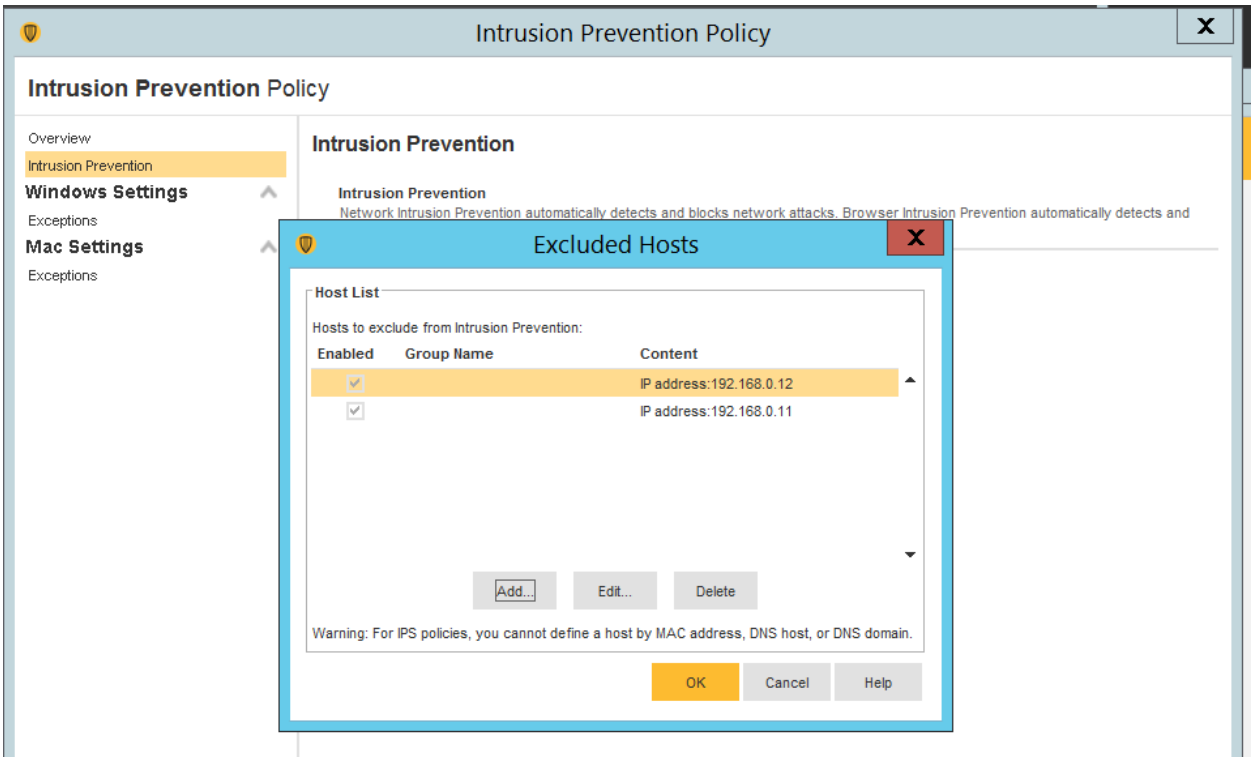
- The client was rebooted, and its status was verified to be green ONLINE in the SEPM console. The process was repeated for all other Linux machines.

Additional Configuration

- An "**Exceptions**" policy was created for excluding the /sys and /proc directories from scanning. Click on **Policies** >> **Exceptions** >> Default policy or create your own >> **Exceptions** >> Click **Add** to add folders to exclude from scanning.



- Symantec AV on each system by default blocks any port scan related traffic. If you have a vulnerability scanner or security tools in your environment, ensure those IP addresses are whitelisted in the SEPM console. The recommended way to do this is by creating a policy under **Policies** >> **Intrusion Prevention** >> **Excluded Hosts** and linking it to the appropriate client group. The image below shows our Nessus server and Open-AudIT servers were excluded to permit these hosts perform their respective scans.



Lesson learned

- Installation on Linux systems: Have a proper backup of the Linux machine prior to installing the endpoint agent. The Linux agent being a 32bit binary requires some 32-bit packages to be installed as a pre-requisite.[16] On 64bit Linux systems, this will install 32bit packages alongside their 64bit counterparts. This can cause issues/conflicts with some of existing packages such as python libraries especially if you are on older versions of Linux such as Ubuntu 12.04.
- On newer versions of Linux, ensure "Multiarch" mode is enabled to allow 32bit apps to install on 64bit systems.[17] On our Ubuntu 12.04 servers, wherein we couldn't get the agent to install due to these package conflicts, we ended up applying other compensating controls.

[16] https://support.symantec.com/en_US/article.TECH228118.html

[17] https://wiki.debian.org/Multiarch/HOWTO

4.9.6 Highlighted Performance Impacts

Two performance measurement experiments were performed for the Symantec tool while the manufacturing system was operational:

1. CL005.1 - Symantec agent is installed, and real-time scanning is enabled on CRS hosts.
2. CL005.2 - A full system scan is performed on predetermined CRS hosts.

4.9.6.1 Experiment CL005.1

The Symantec agent was installed and real-time scanning enabled on following CRS hosts: the robot driver (MINTAKA), robot controller vController1, and robot controller vController2.

CPU utilization increased from around 2% to 7% on vController1 during the experiment (see Figure 4-23). However, this CPU increase was not observed on vController2 (see Figure 4-24), which performs all of the same functions as vController1. At the time of publishing, it is unknown if this CPU increase on vController1 was caused by the Symantec agent.

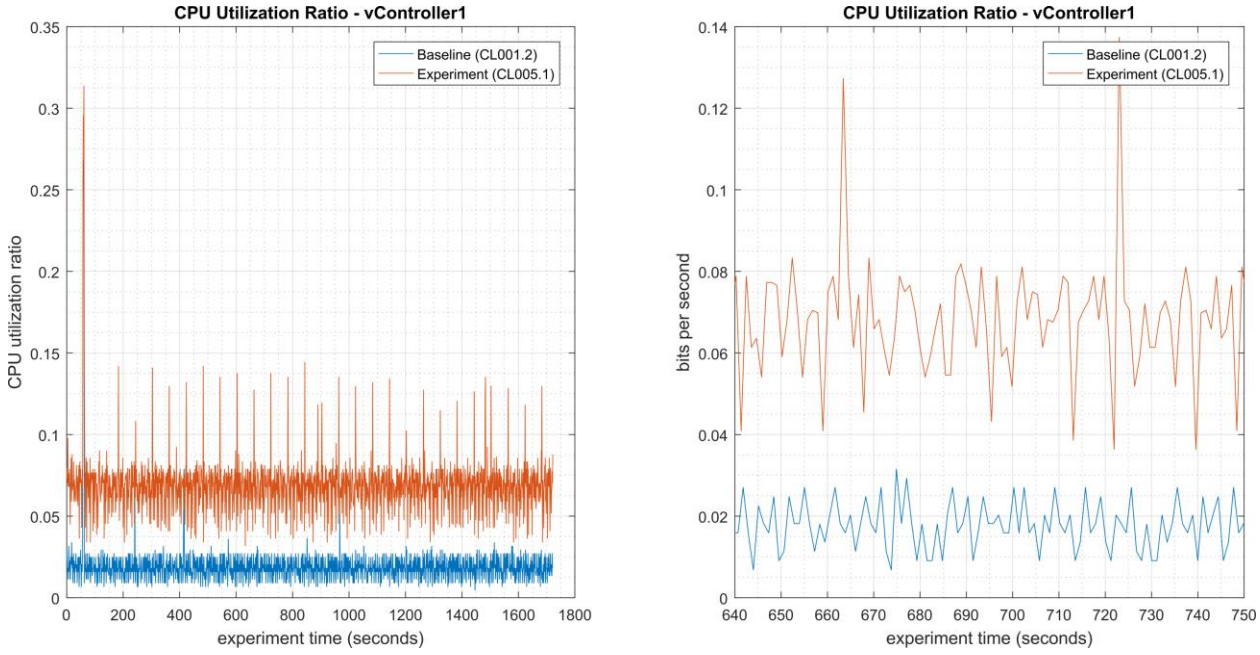


Figure 4-23 - Time series plots showing the CPU utilization ratio for vController1 during the CL005.1 experiment and CL001.2 baseline (left), and during the period of measured impact (right).

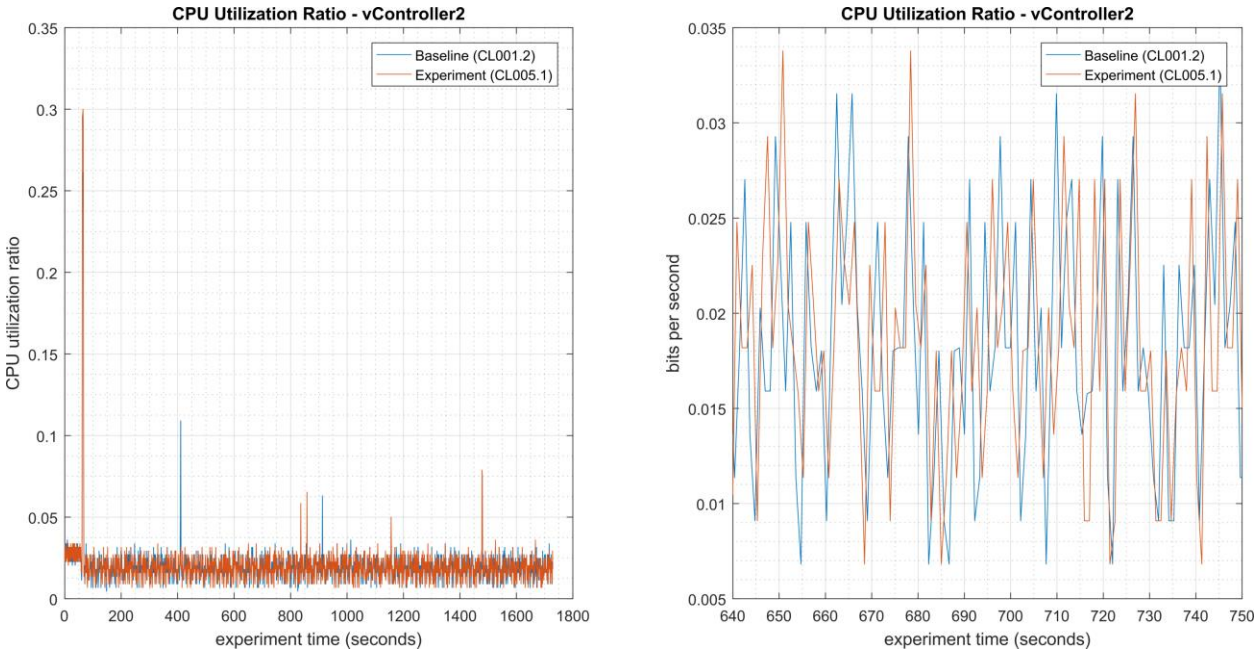


Figure 4-24 - Time series plots showing the CPU utilization ratio for vController2 during the CL005.1 experiment and CL001.2 baseline (left).

A slight increase of the part production time mean was observed during this experiment, but is not statistically significant.

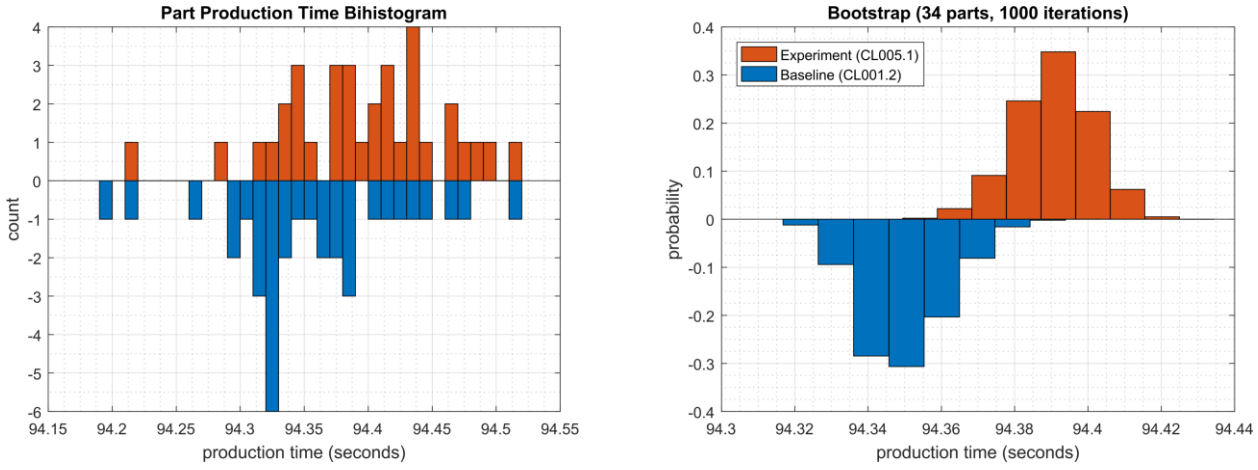


Figure 4-25 - Bihistograms showing the part production time (left) and estimated mean production time using the bootstrap method (right) using the measurements from baseline CL001.2 and experiment CL005.1.

4.9.6.2 Experiment CL005.2

A full system scan of the robot driver (MINTAKA), robot controller vController1, and robot controller vController2 were initiated at 106 sec., 140 sec., and 309 sec. experiment time, respectively. The tool did not report when the scanning ended, so it was not recorded. The host MINTAKA does not run a performance logger, so data from this host is not available.

The CPU utilization increased during the scan period on both vController1 and vController2. CPU utilization on vController1 (see Figure 4-26) increased from 7% to 29% while the scan was executing (from 140 sec. to 750 sec. experiment time), with a peak of 78%. CPU utilization on vController2 (see Figure 4-27) increased from 2% to 26% while the scan was executing (from 300 sec. to 920 sec. experiment time), with a peak of 33%.

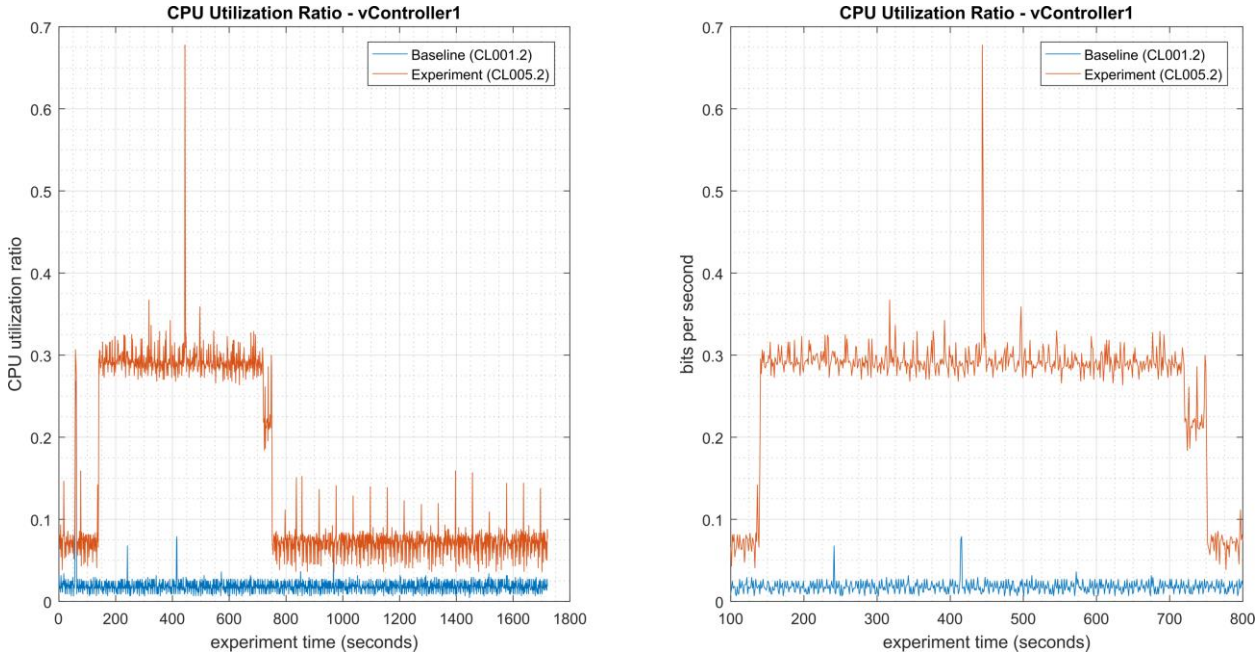


Figure 4-26 - Time series plots showing the CPU utilization ratio for vController1 during the CL005.2 experiment and the CL001.2 baseline (left), and during the period of measured impact (right).

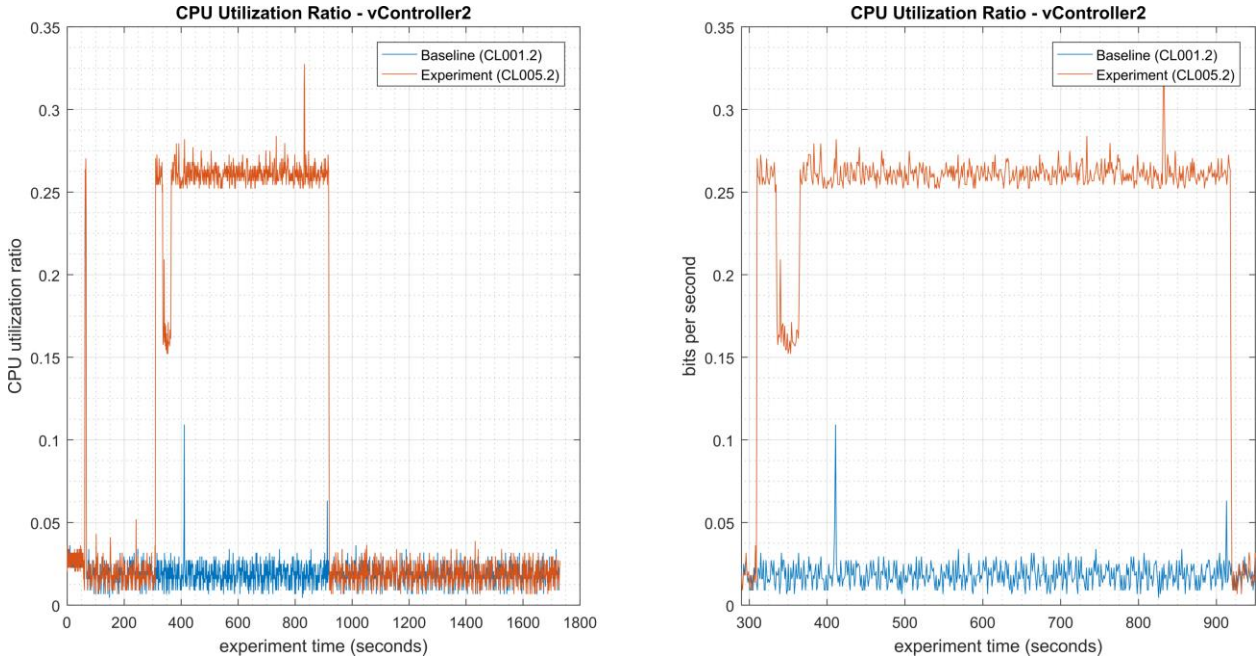


Figure 4-27 - Time series plots showing the CPU utilization ratio for vController2 during the CL005.2 experiment and the CL001.2 baseline (left), and during the period of measured impact (right).

Network activity increased for a short time on both vController1 and vController2 while the scan was active, but the activity occurred at different times. Network activity on vController1 (see Figure 4-28) increased at the end of the scan (from 720 sec. to 750 sec. experiment time), while network activity on vController2 (see Figure 4-29) increased towards the beginning of the scan (from 335 sec. to 365 sec. experiment time). Sustained network bitrates over 2 Mbps for around 30 seconds total were measured on both vControllers.

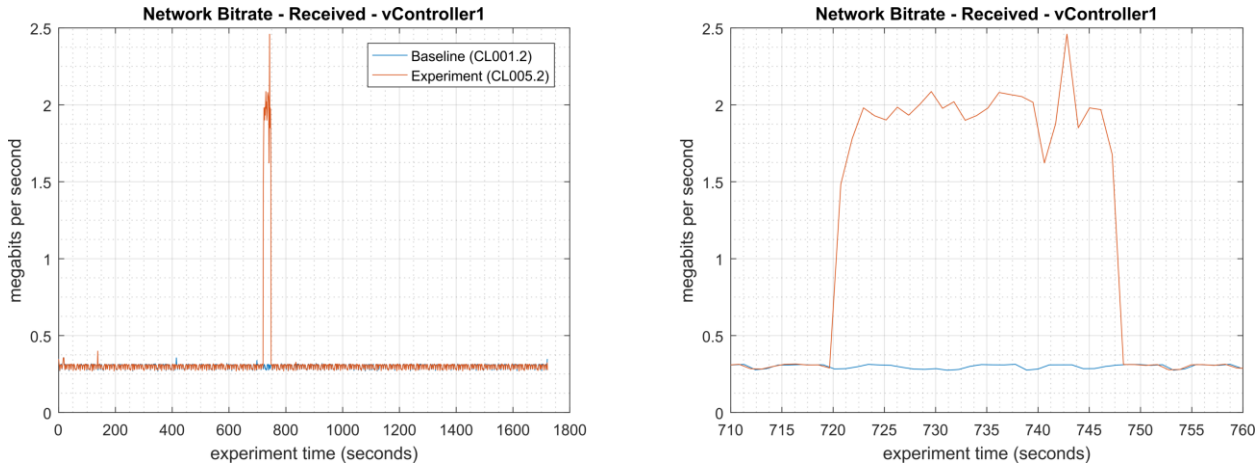


Figure 4-28 - Time series plots showing the quantity of network traffic received by vController1 during the experiment (left), and during the period of measured impact (right). The peak in traffic shown between 720 sec. to 750 sec. occurred while the scan was active.

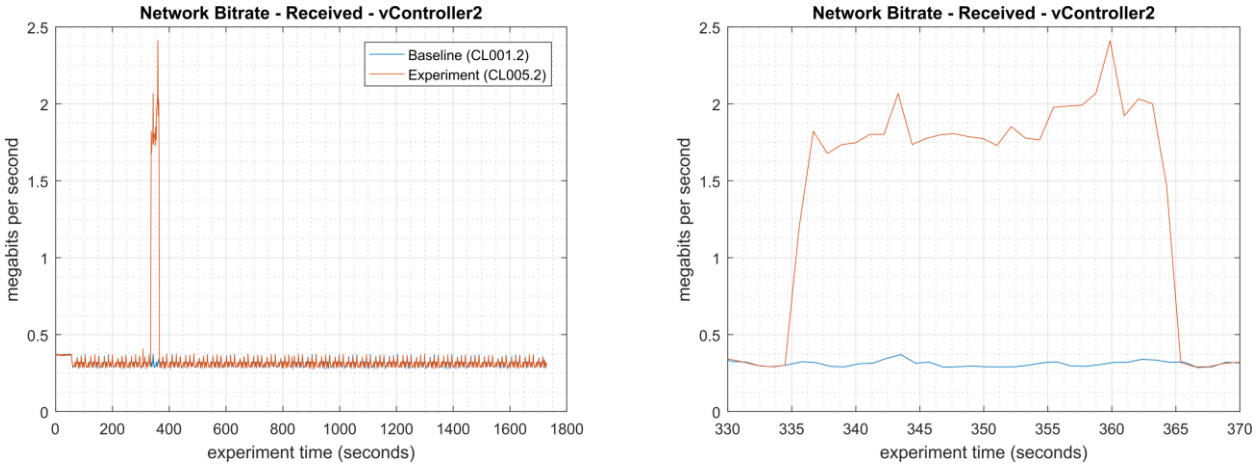


Figure 4-29 - Time series plots showing the quantity of network traffic received by vController2 during the experiment (left), and during the period of measured impact (right). The peak in traffic shown between 330 sec. to 365 sec. occurred while the scan was active.

No performance impact to the manufacturing process was measured during the experiment.

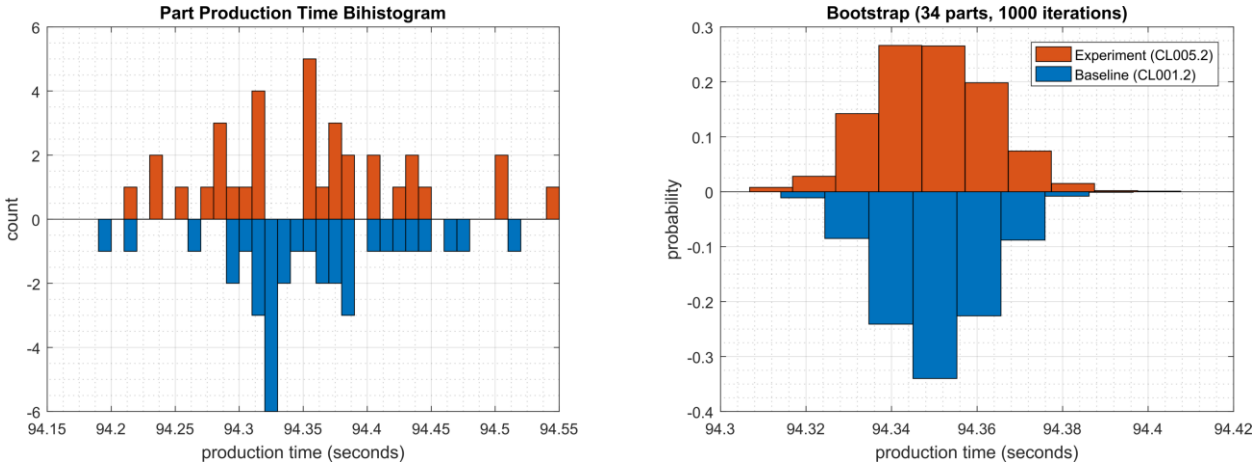


Figure 4-30 - Bihistograms showing the part production time (left) and estimated mean production time using the bootstrap method (right) using the measurements from baseline CL001.2 and experiment CL005.2.

4.9.7 Link to Entire Performance Measurement Data Set

- **CL005.1-AntivirusRealTimeScan.zip**
- **CL005.2-AntivirusFullScan.zip**

4.10 Tenable Nessus

4.10.1 Technical Solution Overview

Nessus Professional is a vulnerability assessment software from Tenable. It features high-speed asset discovery, configuration auditing, target profiling, malware detection, sensitive data discovery and more. Nessus supports technologies such as scanning operating systems, network devices, next generation firewalls, hypervisors, databases, web servers and critical infrastructure for vulnerabilities, threats and compliance violations.[18] It supports both authenticated and unauthenticated scans.

Points to consider:

- Easy to setup, User friendly dashboard, fast scanning and can be configured to work in a distributed environment.
- Support for Industrial Protocols such as MODBUS, DNP3 etc. It has the necessary plugins to detect vulnerabilities on ICS/SCADA systems making it ideal to use in OT environments.
- Comes with a variety of Out-of-box policy and configuration templates.
- No limit on number of IPs or number of assessments you can run.
- Support for scanning devices behind a firewall.
- No integration available with LDAP or AD in the Professional edition.
- Multiple user accounts not supported for logging in to the Web UI.

4.10.2 Technical Capabilities Provided by Solution

Tenable Nessus provides components of the following Technical Capabilities described in Section 6 of Volume 1:

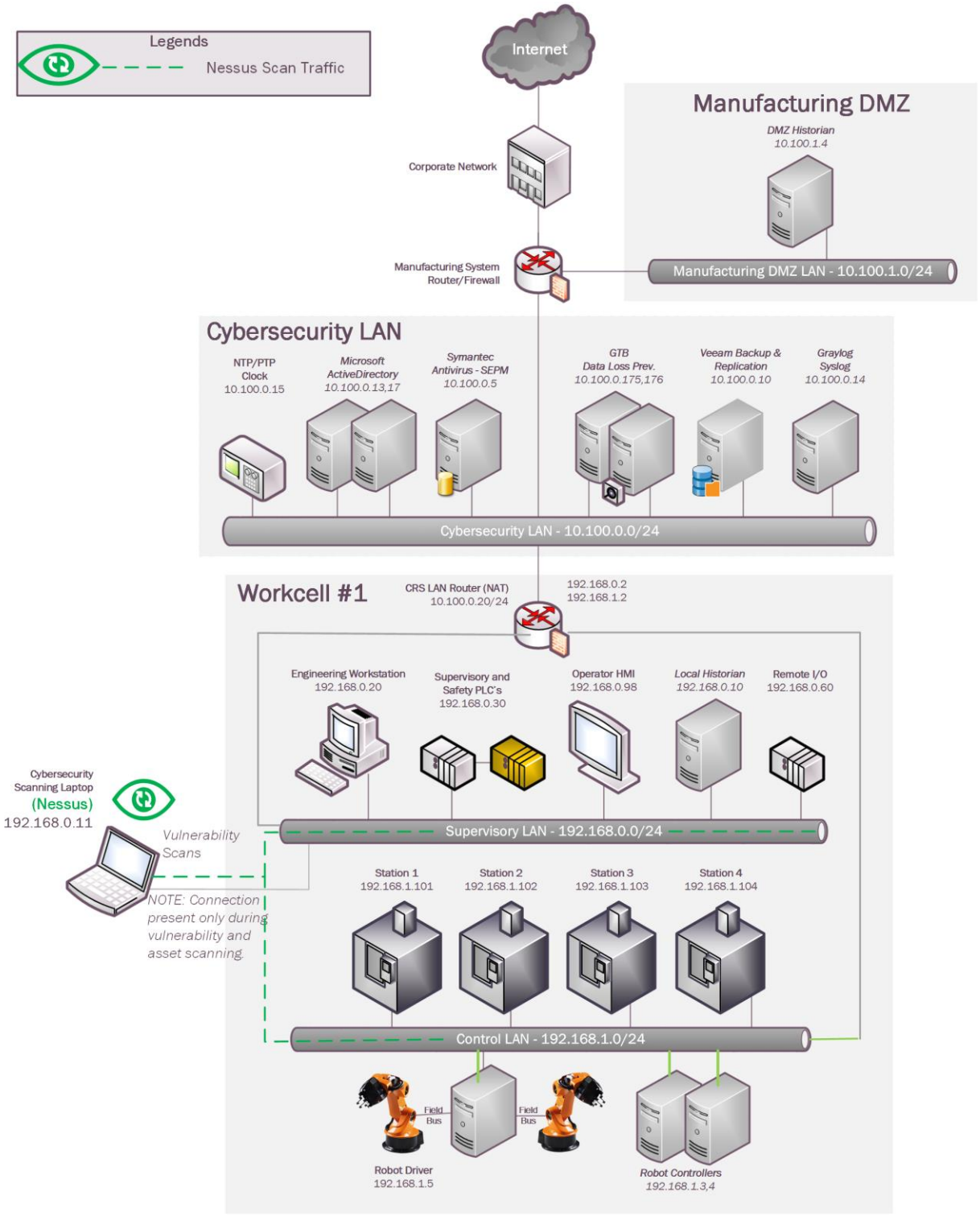
- Vulnerability Scanning
- Vulnerability Management

4.10.3 Subcategories Addressed by Implementing Solution

ID.AM-3, ID.AM-4, ID.RA-1, DE.CM-4, DE.CM-8

[18] Nessus Professional: http://info.tenable.com/rs/934-XQB-568/images/NessusPro_DS_EN_v8.pdf

4.10.4 Architecture Map of Where Solution was Implemented



4.10.5 Installation Instructions and Configurations

Details of the solutions implemented:

Name	Version
Nessus Professional	7.2.0

Setup Overview:

- The Robotics systems being behind a firewall (NAT) cannot be reached directly from the Cybersecurity LAN network. To work around this, a dedicated laptop was setup to assume the role of Nessus server and Nessus Professional 7.x was installed on it.[19] This laptop would be used on-demand to perform scans. A temporary network connection from the Supervisory LAN would be arranged as required and the system was assigned a static IP address.

- During the setup, the wizard will prompt for registration. The Registration process and updates can be configured either in online or offline mode. An online mode is suitable for environments where Nessus server is connected to the internet while an offline mode is for air-gapped environments. Detailed instructions for registering Nessus offline can be found in the product guide. Upon completion, Nessus can be accessed via https://<IP address of Nessus server>:8834

- The Nessus server needs to have network connectivity from whichever networks or subnets that are intended to be scanned. In addition, if performing authenticated scans then appropriate firewall rules should be in place to allow SSH, WMI or SNMP traffic depending on the type of hosts. If performing unauthenticated scan, the firewall should be allowed for any-any communication between the Nessus server and target network.

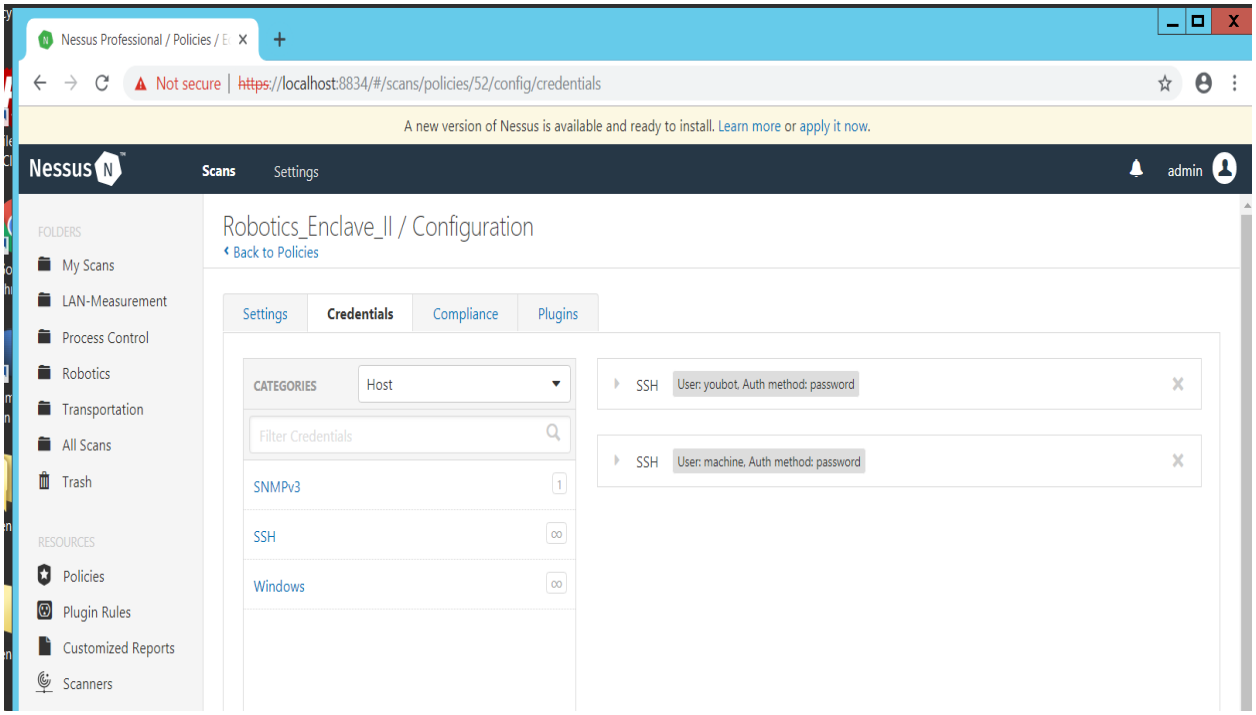
Configuration for Robotics System:

- Ensure to allow firewall rules for Nessus scanning. Port 22 was allowed on our firewall between the Nessus system and Supervisory, Control LAN networks.

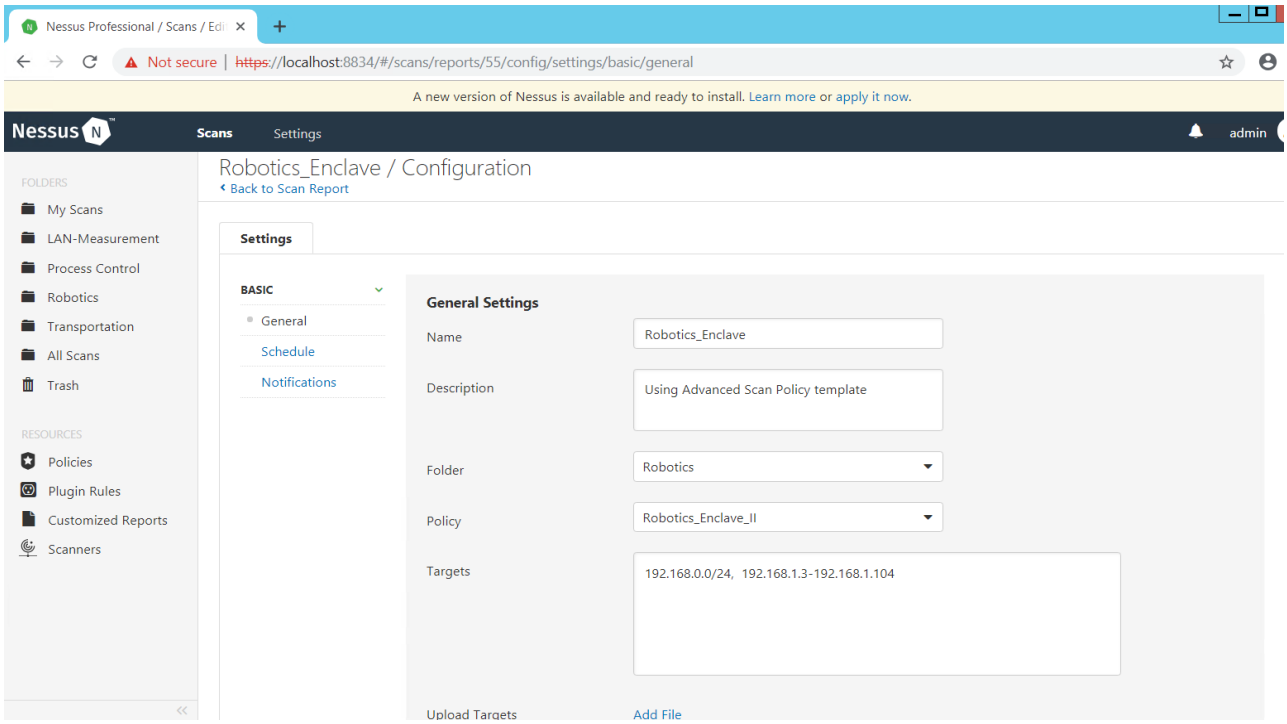
- It is important to not change the IP address on the Nessus server once setup is done, as it causes errors. This is because Nessus installer records all network settings during the install process. Any hardware change made post install is not recognized by Nessus.

[19] Nessus Official Documentation: https://docs.tenable.com/nessus/Content/GettingStarted.htm

- A new policy was created specific to the assets in Robotics and linked to a scan job. The scan was scheduled to be On-Demand. The figure below shows the Policy configured Robotics System



- The figure below shows the corresponding scan job settings which has the "**Robotics_Enclave_II**" policy assigned to it under **Policy**.



- To kick-off a manual on-demand scan, click on the launch button next to the scan.

4.10.6 Highlighted Performance Impacts

Two performance measurement experiments were performed for the Nessus tool while the manufacturing system was operational:

1. CL006.1 - A host discovery scan was performed on the CRS network.
2. CL006.2 - Credentialed checks were performed on predetermined CRS hosts.

4.10.6.1 Experiment CL006.1

A "host discovery" scan was performed on the two CRS networks: Supervisory LAN (192.168.0.0/24) and Control LAN (192.168.1.0/24). The Nessus GUI reported scanning was active between 452 to 1412 seconds (experiment time).

Multiple performance impacts were observed while the Nessus tool was actively scanning the HMI and machining stations. Loss-of-view events likely occurred (but were not directly observed) on the HMI multiple times during the experiment, as evident by the large inter-packet delay measurements between the HMI and Station 1 shown in Figure 4-32. Two large round-trip time transients (over 500 milliseconds) were observed on TCP traffic between the HMI and Station 1.

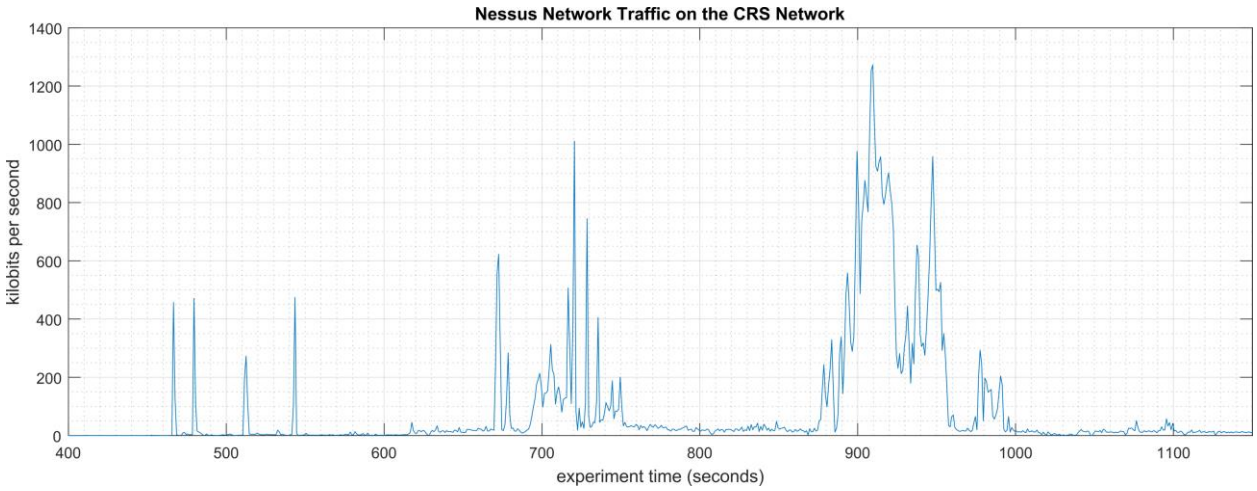


Figure 4-31 - Time series plot showing the quantity of network traffic transmitted and received by the Nessus tool during the experiment time period 400 to 1200 seconds, with the most prominent activity between 700 to 750 seconds and 875 to 1000 seconds. The Nessus GUI reported it was active between 450 to 1400 seconds experiment time.

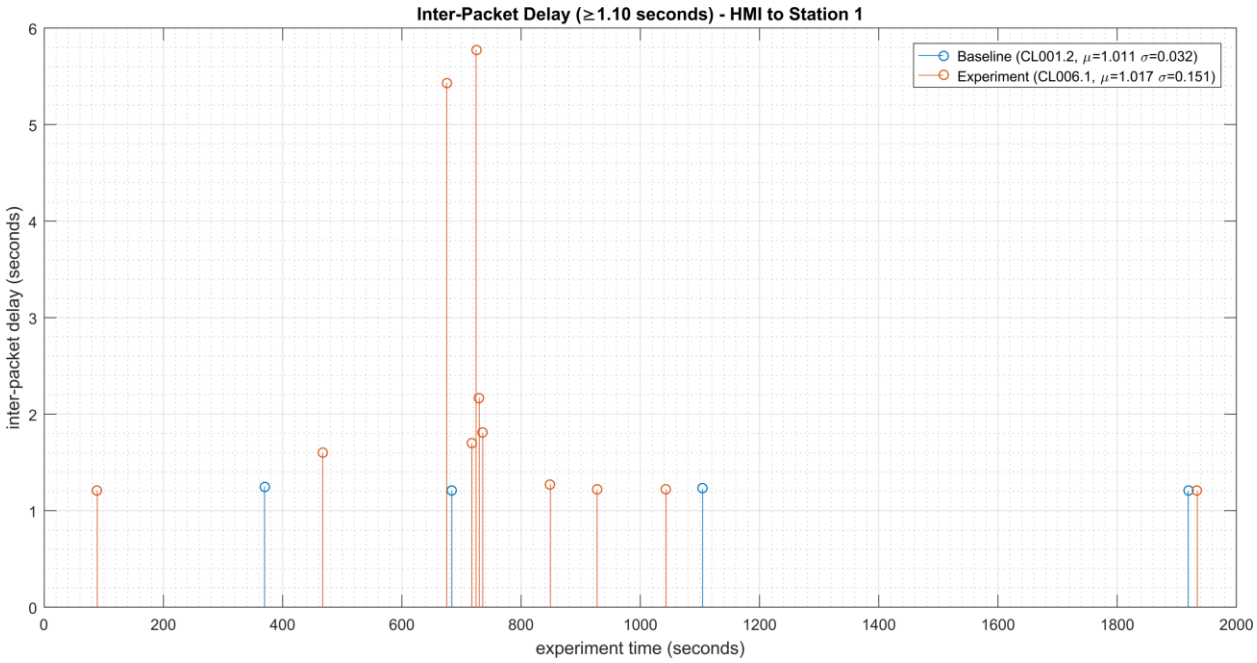


Figure 4-32 - Stem plot displaying the inter-packet delays (greater than or equal to 1.10 seconds) of Modbus TCP traffic between the HMI and Station 1, as measured during the baseline CL001.2 and experiment CL006.1. Note the large inter-packet delays between experiment time 600 to 800, resulting in HMI loss-of-view for over 5 seconds.

Performance impacts to the supervisory PLC task execution time were observed while the Nessus tool was actively scanning. Relatively large fluctuations of the average task execution time and the maximum task execution time were observed from 800 to 1000 seconds experiment

time. The largest maximum task execution time was observed at 930 seconds with a value of 2088 microseconds (a threefold increase above the average). Impacts to the measured inter-packet delay between the PLC and Station 2 were also observed during this period. Further analysis revealed Nessus was actively scanning the machining stations while these PLC impacts were observed. It is hypothesized that the impacts were caused by interruptions to Modbus TCP communications between the supervisory PLC and the machining stations, likely due to increased resource utilization on the machining stations.

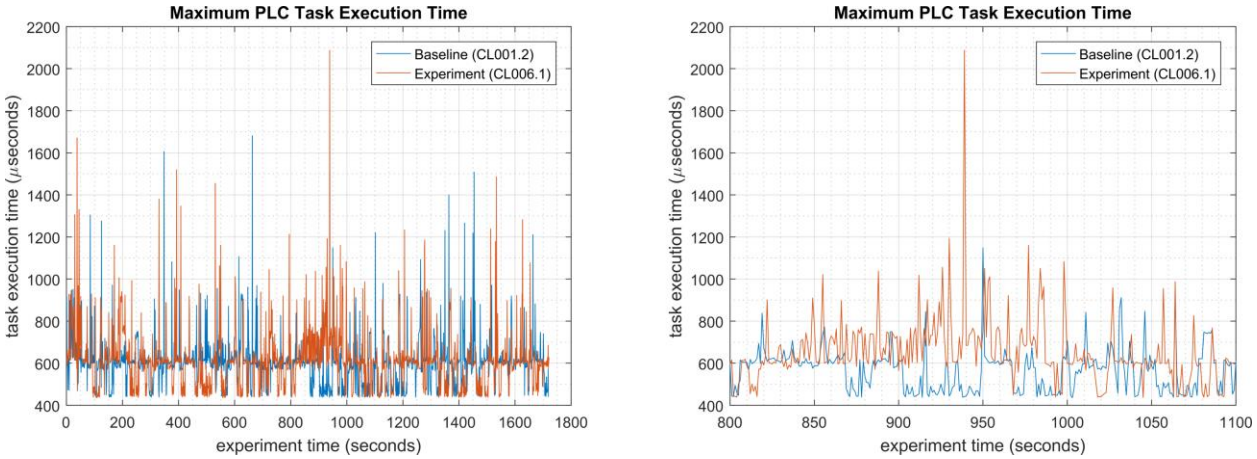


Figure 4-33 - Plots showing the maximum PLC task execution time during the experiment (left) and during the period of measured impact (right). While the Nessus tool was active, the PLC experienced periods of fluctuating and increased task execution time.

A slight increase of the part production time mean and variance were observed during this experiment, but they are not statistically significant.

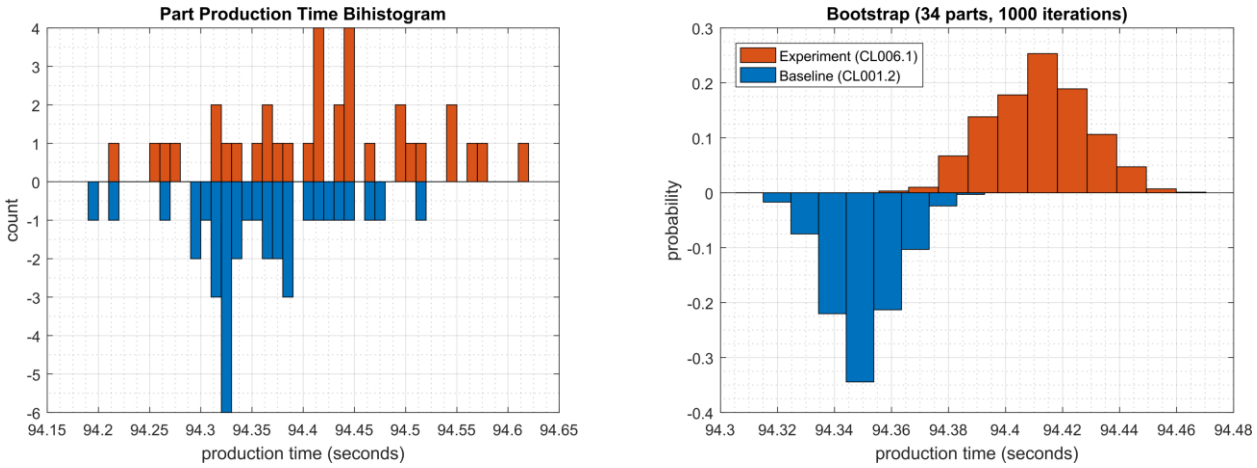


Figure 4-34 - Bihistograms showing the part production time (left) and estimated mean production time using the bootstrap method (right) using the measurements from baseline CL001.2 and experiment CL006.1.

4.10.6.2 Experiment CL006.2

"Credentialed checks" were performed on the two CRS networks: Supervisory LAN (192.168.0.0/24) and Control LAN (192.168.1.0/24). The credentials gave Nessus access to the following hosts and ICS devices: the engineering workstation (POLARIS), the robot driver (MINTAKA), the robot controller vController1, and the robot controller vController2, and the four machining stations.

The Nessus GUI reported scanning was active between 200 to 1500 seconds (experiment time).

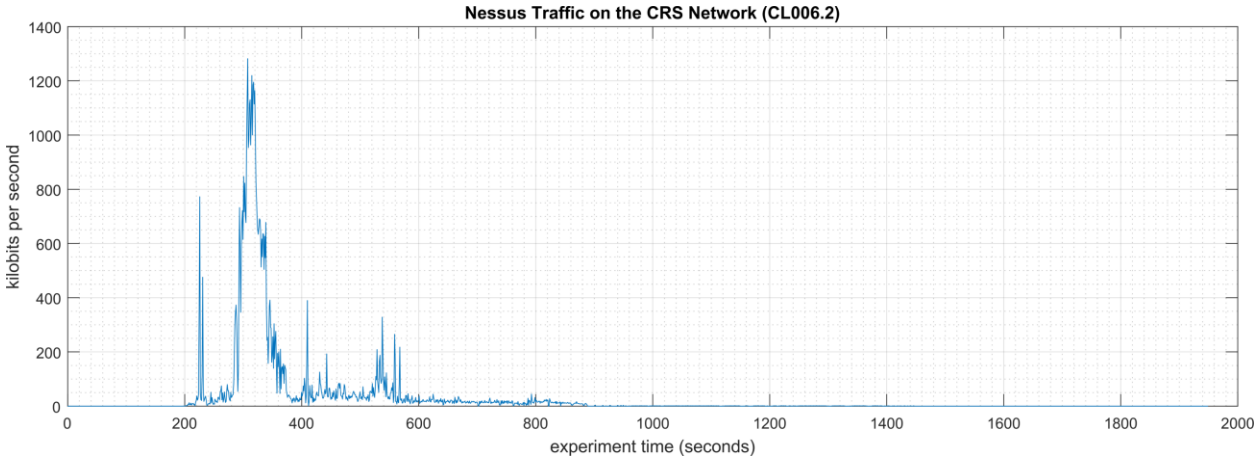


Figure 4-35 - Time series plot showing the quantity of network traffic transmitted and received by the Nessus tool during the experiment, with the most prominent activity from 200 to 600 seconds.

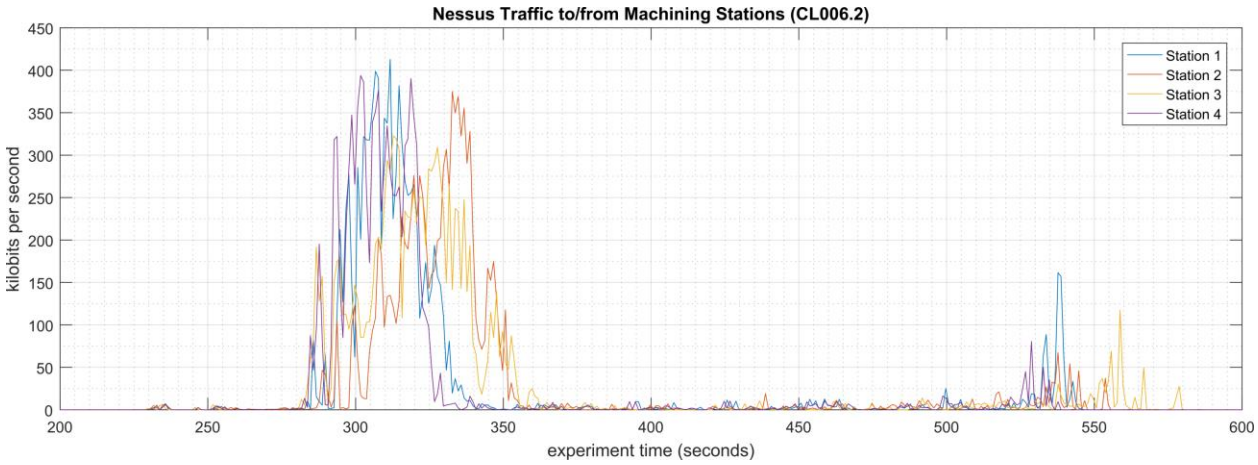


Figure 4-36 - Time series plot showing the quantity of network traffic transmitted and received by the Nessus tool and the machining stations during the experiment. Performance impacts to the PLC appear to correlate Nessus scanning the machining stations, likely due to the limited processing power of the devices.

Multiple performance impacts were observed while the Nessus tool was actively scanning the HMI and machining stations. Loss-of-view events likely occurred (but were not directly observed) on the HMI multiple times during the experiment, as evident by the large inter-packet delay measurements between the HMI and Station 1 shown in Figure 4-37. Two large round-trip

time transients (over 500 milliseconds) were observed on TCP traffic between the HMI and Station 1.

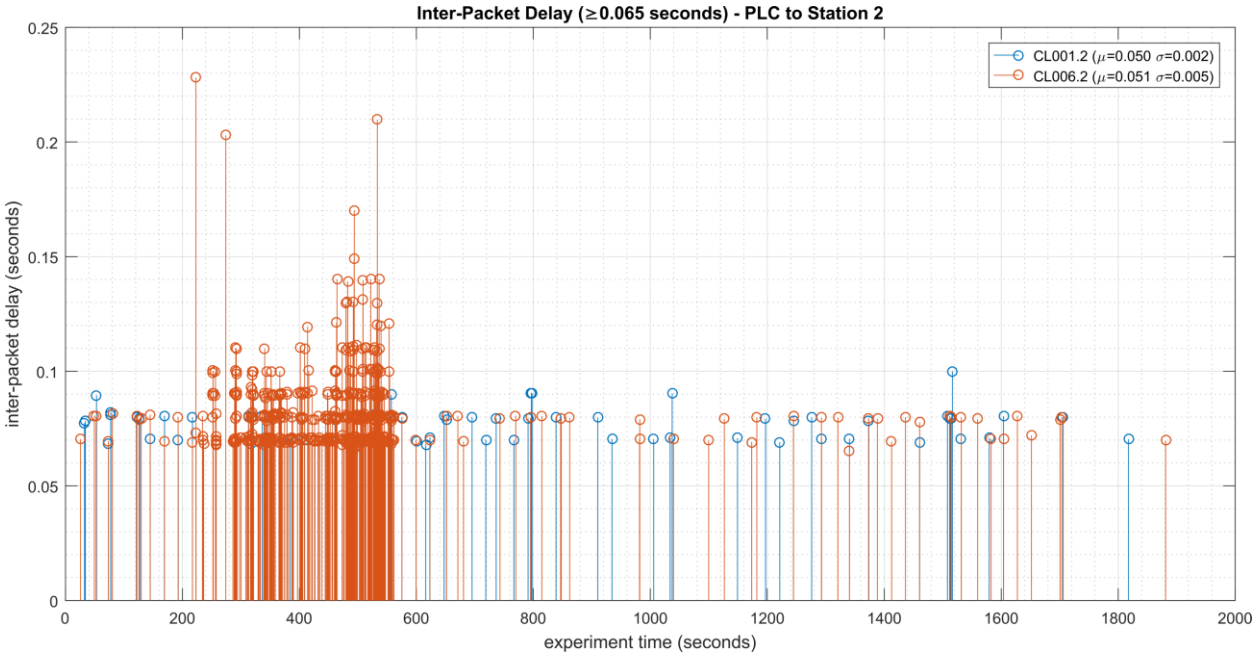


Figure 4-37 - Stem plot displaying the inter-packet delays (greater than or equal to 0.065 seconds) of Modbus TCP traffic between the PLC and Station 2, as measured during the baseline CL001.2 and experiment CL006.2. Note the large inter-packet delays between experiment time 250 to 600.

Performance impacts to the supervisory PLC task execution time were observed while the Nessus tool was actively scanning. Relatively large fluctuations of the average task execution time and the maximum task execution time were observed from 250 to 600 seconds experiment time (see Figure 4-38). Impacts to the measured inter-packet delay between the PLC and Station 2 were also observed during this period. Further analysis revealed Nessus was actively scanning the machining stations while these PLC impacts were observed. It is hypothesized that the impacts were caused by interruptions to Modbus TCP communications between the supervisory PLC and the machining stations, likely due to increased resource utilization on the machining stations.

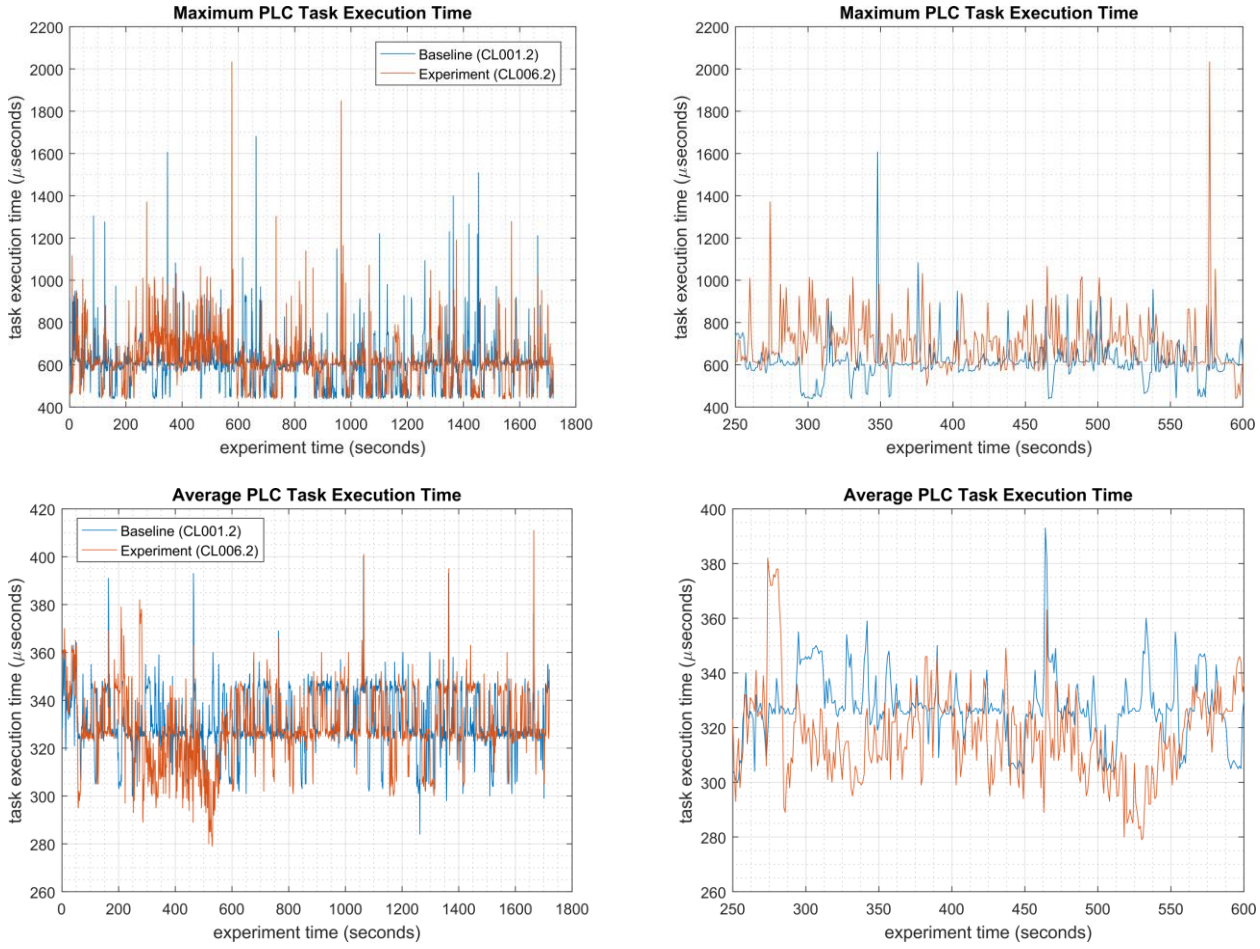


Figure 4-38 - Plots showing the maximum (top) and average (bottom) PLC task execution time during the experiment (left) and during the period of measured impact (right). While the Nessus tool was active, the PLC experienced periods of fluctuating and increased task execution time.

Since Nessus was configured to perform an authenticated scan, vController1 and vController2 both hosts experienced increased utilization of resources (i.e., CPU, disk, memory).

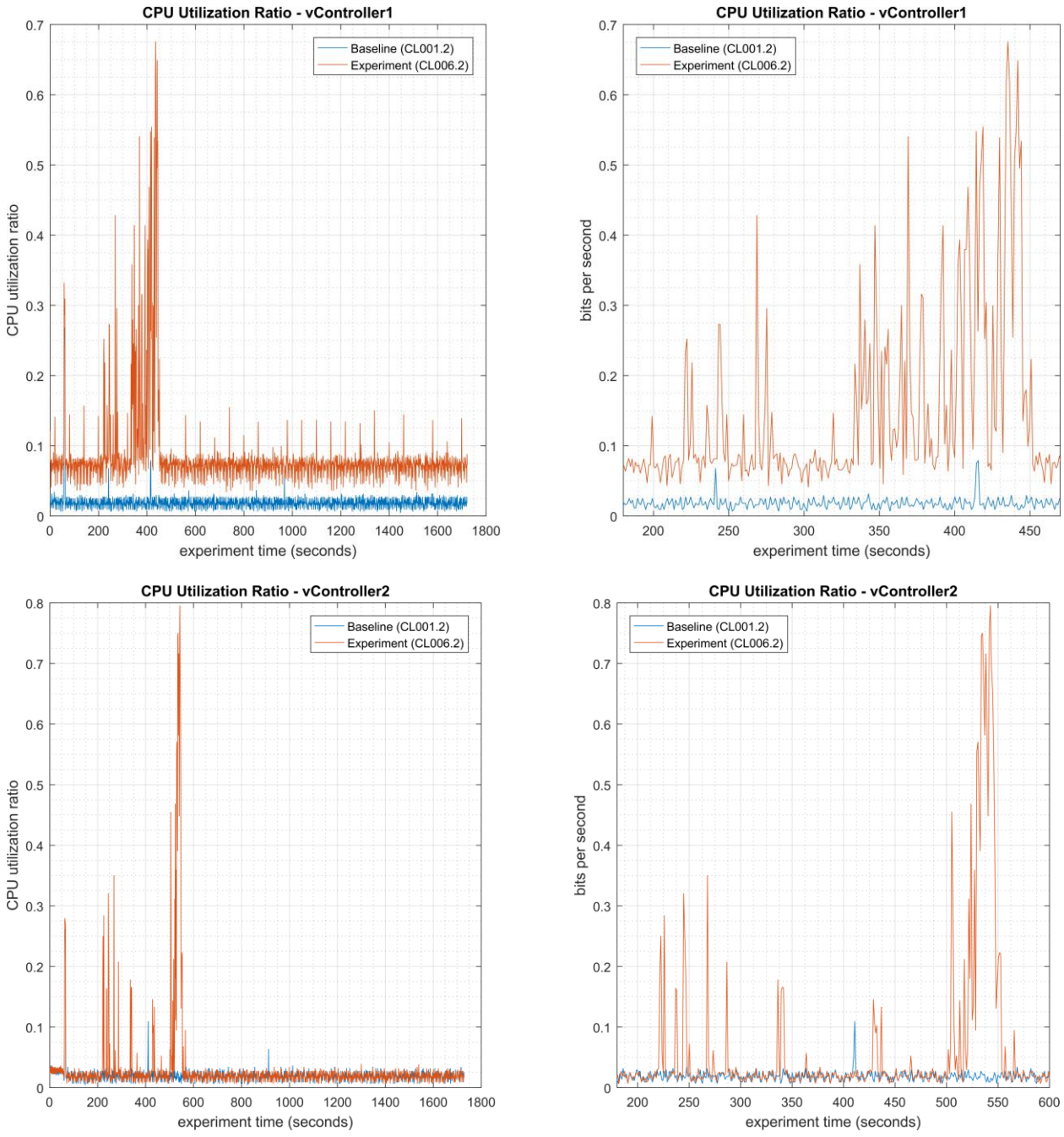


Figure 4-39 - Time series plots showing the CPU utilization of vController1 and vController2 during the CL006.2 experiment. vController1 experienced intermittent periods of increased CPU utilization from 200 sec. to 450 sec., with a maximum of 68% utilization. vController2 experienced intermitted periods of increased CPU from 225 sec. to 560 sec., and a maximum of 80% utilization.

A slight increase of the part production time variance was observed during this experiment, but it is not statistically significant.

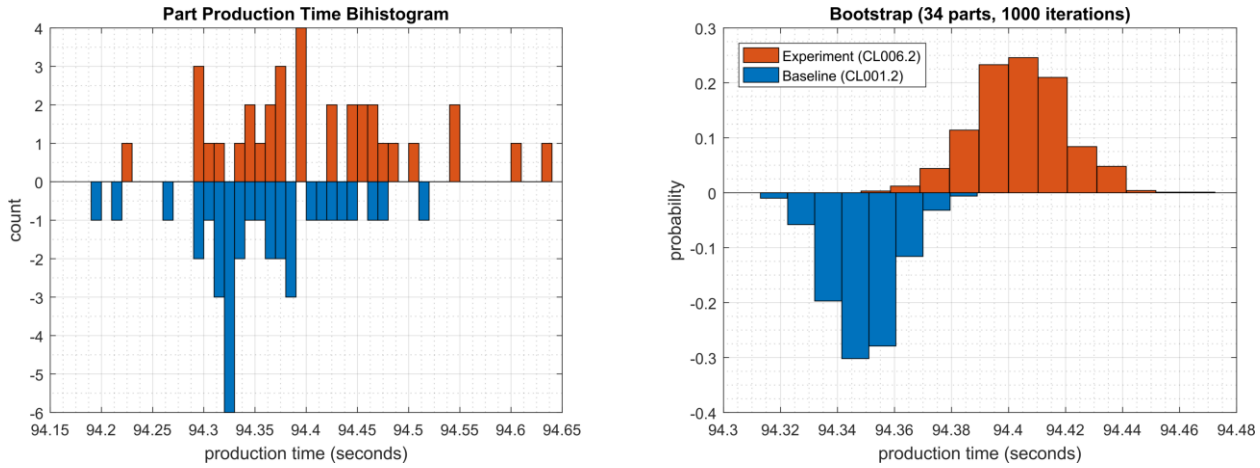


Figure 4-40 - Bihistograms showing the part production time (left) and estimated mean production time using the bootstrap method (right) using the measurements from baseline CL001.2 and experiment CL006.2.

4.10.7 Link to Entire Performance Measurement Data Set

- **CL006.1-NessusNetworkScan.zip**
- **CL006.2-NessusAuthenticatedScan.zip**

4.11 NamicSoft

4.11.1 Technical Solution Overview

NamicSoft Scan Report Assistant, a parser and reporting tool for Nessus, Burp, Nexpose OpenVAS and NCATS.[20]

4.11.2 Technical Capabilities Provided by Solution

NamicSoft provides components of the following Technical Capabilities described in Section 6 of Volume 1:

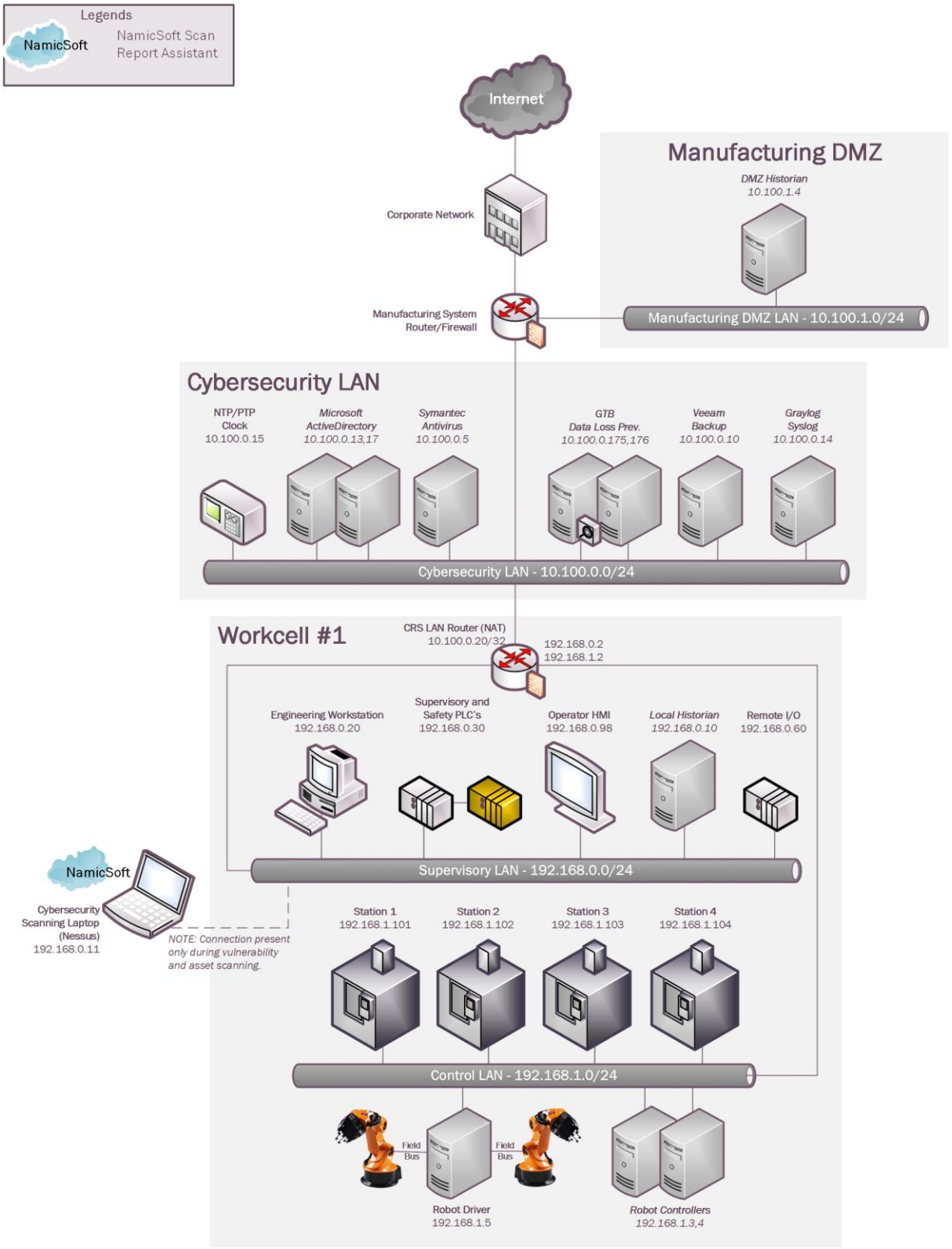
- Vulnerability Management

4.11.3 Subcategories Addressed by Implementing Solution

ID.RA-1, DE.CM-4, RS.MI-3

[20] Namicsoft https://www.namicsoft.com/

4.11.4 Architecture Map of Where Solution was Implemented



4.11.5 Installation Instructions and Configurations

Details of the solutions implemented:

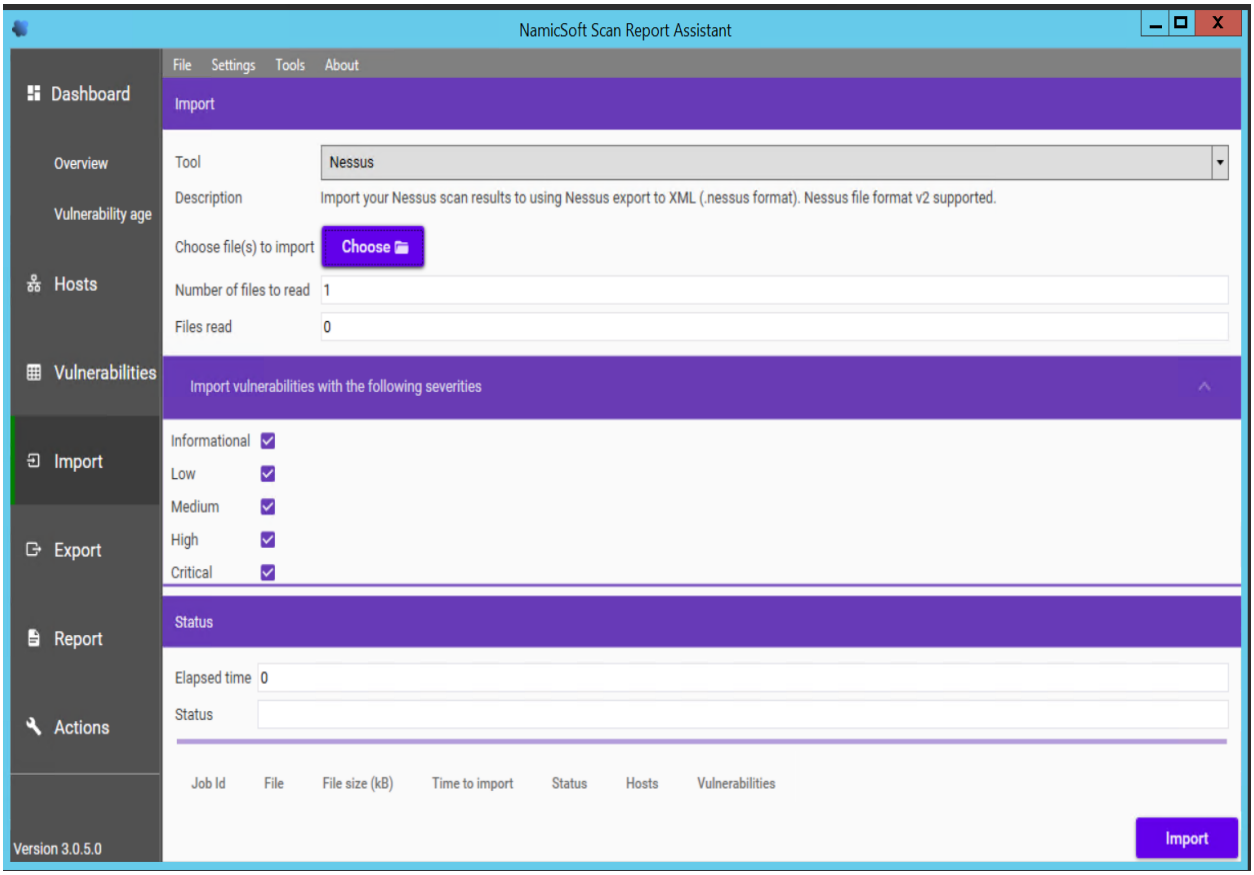
Name	Version
NamicSoft Scan Report Assistant	3.5.0

Setup:

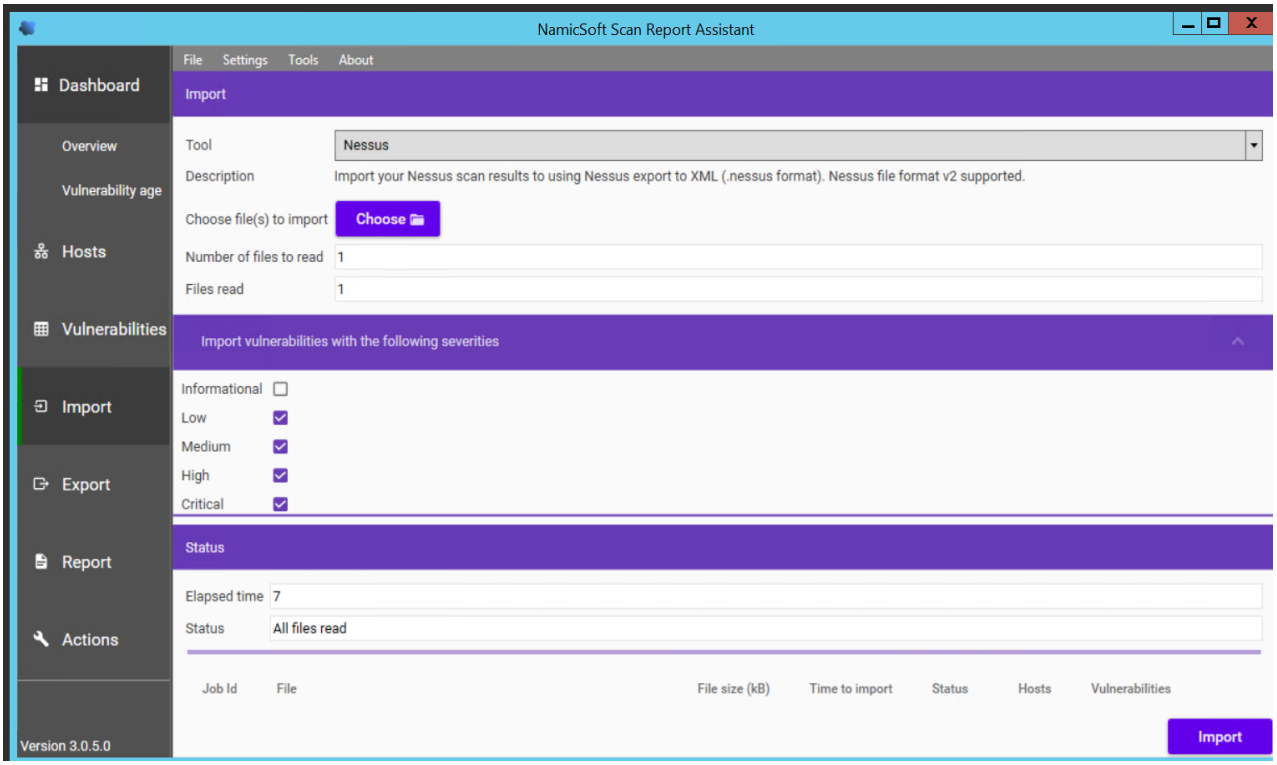
- Download NamicSoft from https://www.namicsoft.com and run the installer on a Windows PC. NamicSoft is currently supported on 64-bit Windows with .Net Framework 4.5 installed
- The installation is tied to a user account. Any changes made by a user would not be visible to a different user logging in to the same system.
- If using for the first time, the installation will prompt for a license file. If a license is not entered, it runs in free mode. The free mode is limited to five hosts.
- NamicSoft was installed on the Scanning laptop used for Nessus scanning.

Configuration for reporting Nessus scans:

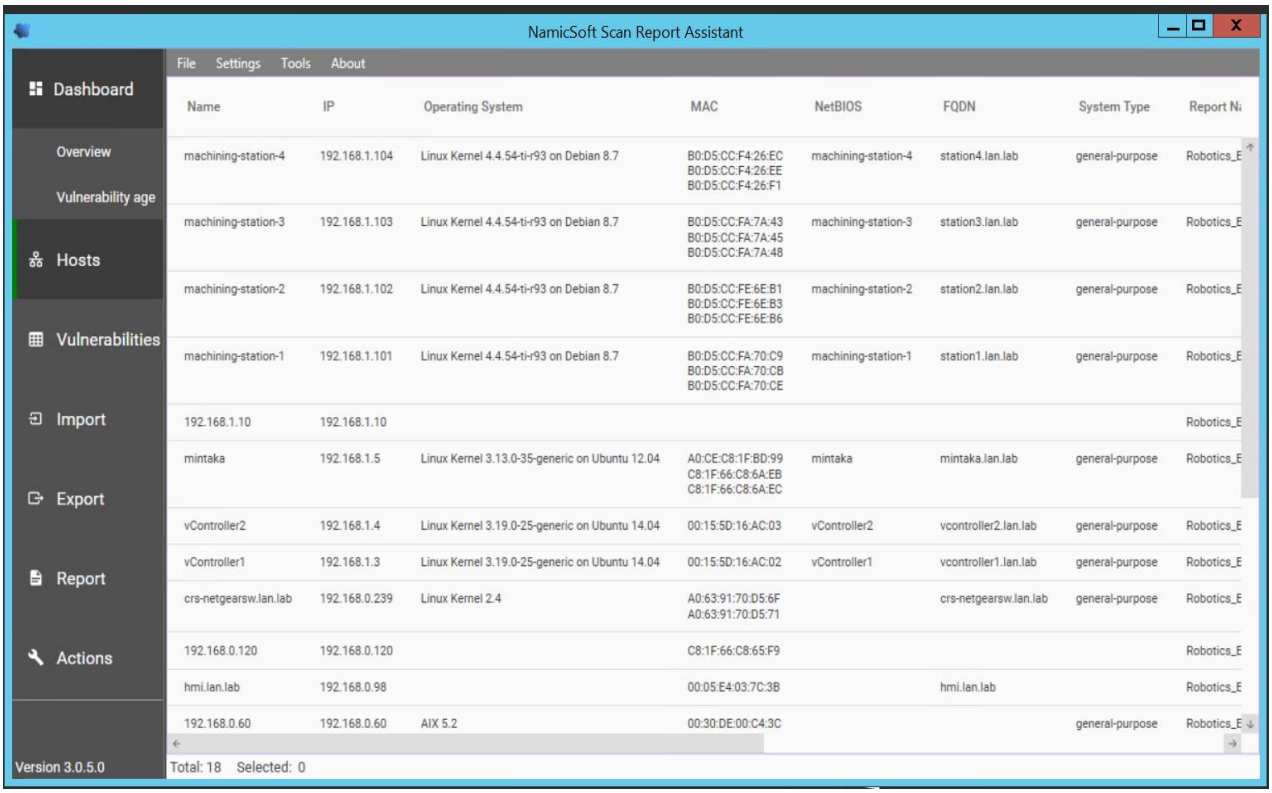
- Export a Scan Report of N**essus** format from the Nessus web interface.
- Launch NamicSoft Report Assistant. Click **Import** on left-side explorer, select **Nessus**
- Click on **Choose** button to import files



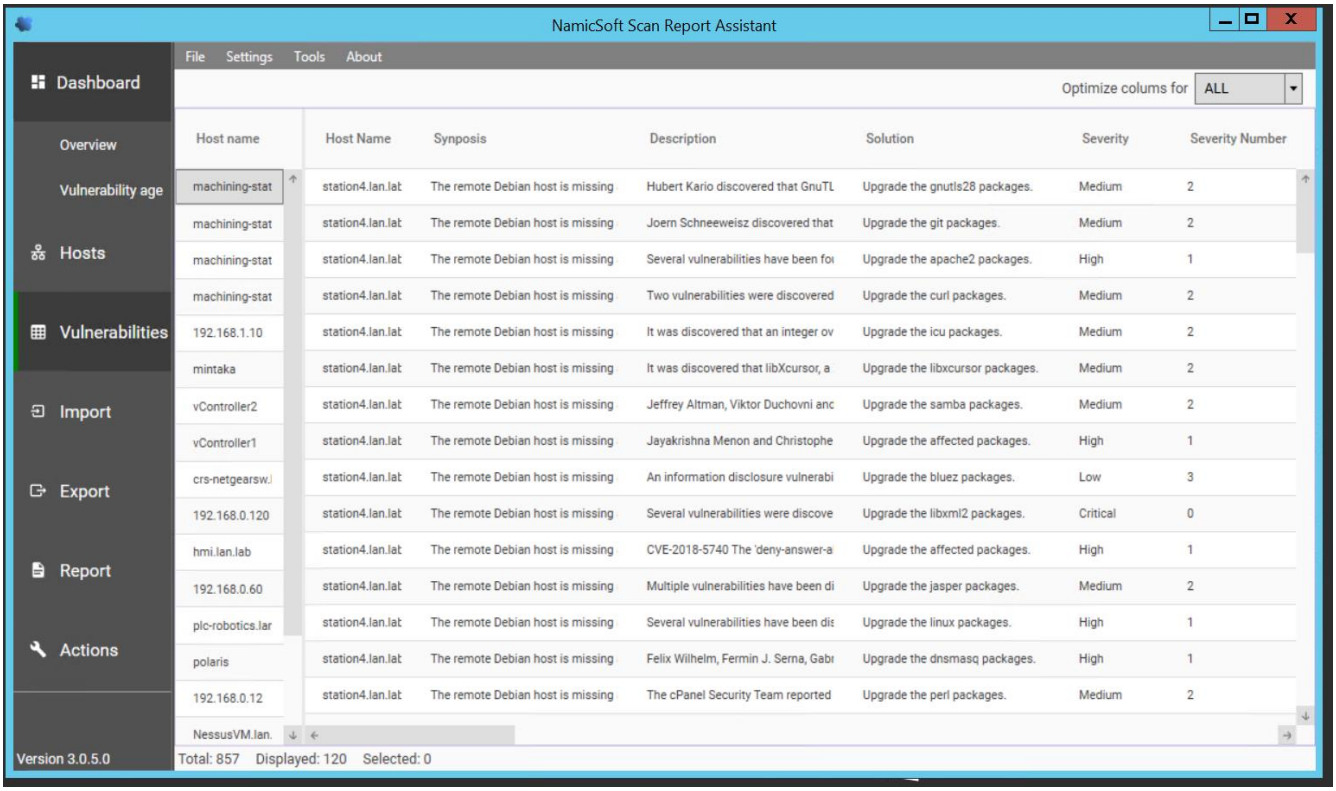
- Browse to the Nessus scan report. Under **Import Vulnerabilities with following vulnerabilities, C**heck / Un-check whichever severity of vulnerabilities you wish to be included in the report. Click **Import**
  The below image shows "Informational" type being excluded. When the **Import** finishes, the Status bar should display **All files read**



- Upon completion of Import, go to **Hosts** page to view all the hosts level summary. Similarly, clicking on **Vulnerabilities** page shows all the vulnerabilities

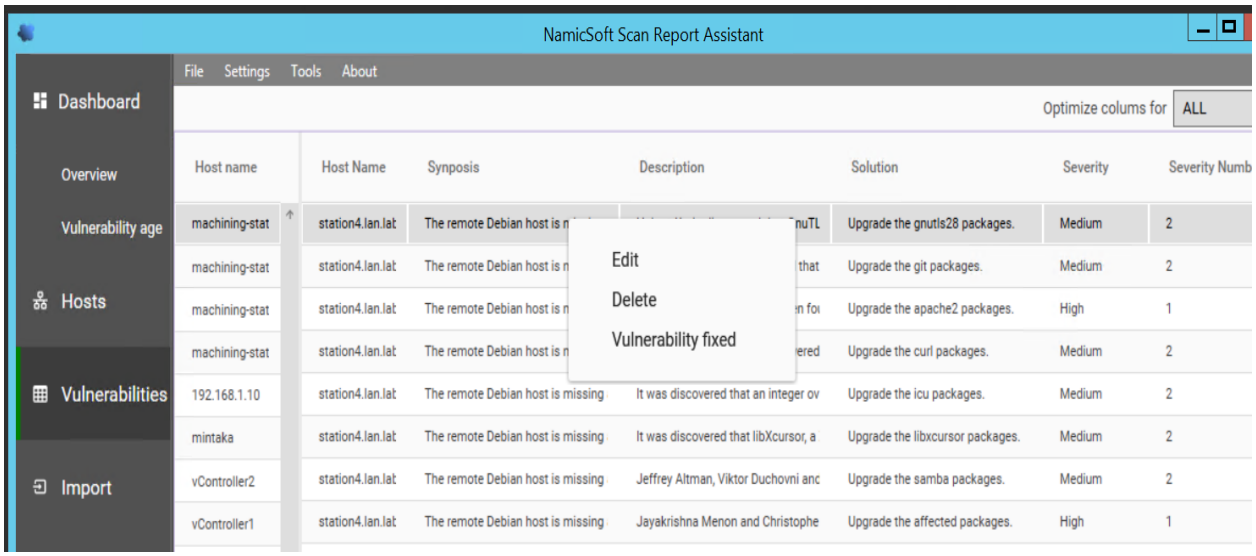


4128



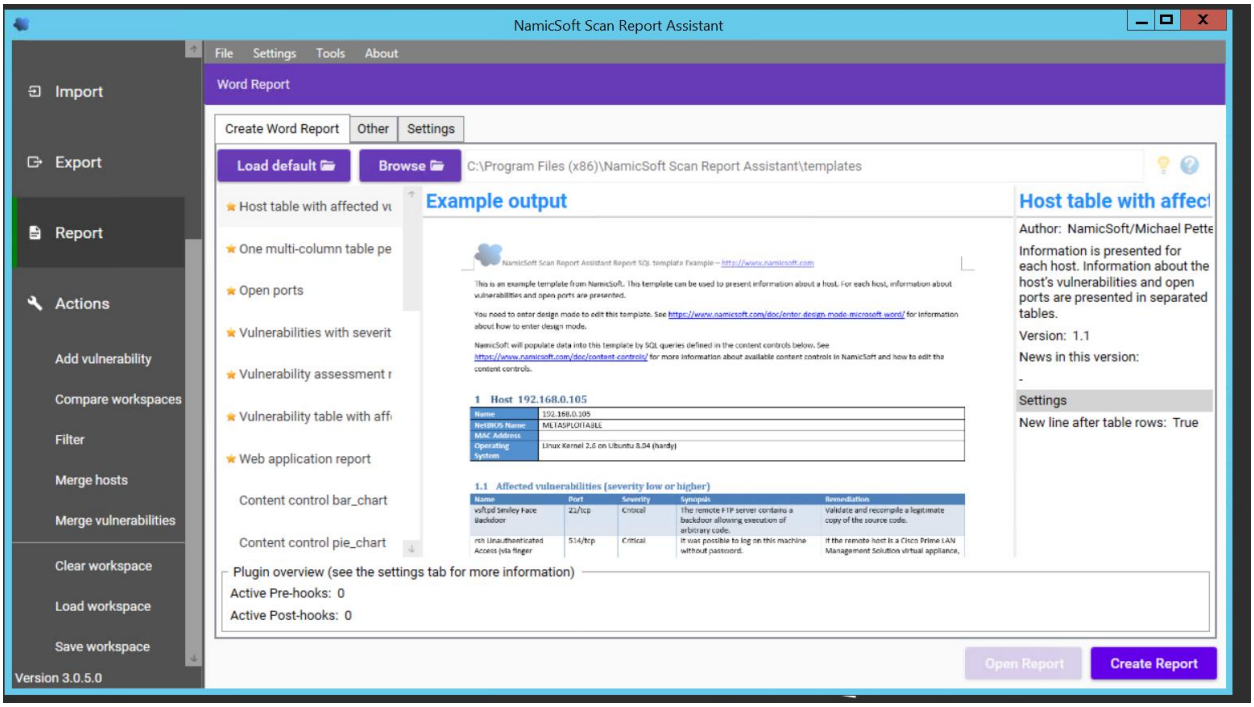
4129

4130 • To mark a Vulnerability as Fixed, select the Vulnerability >> Right Click >> Fixed.

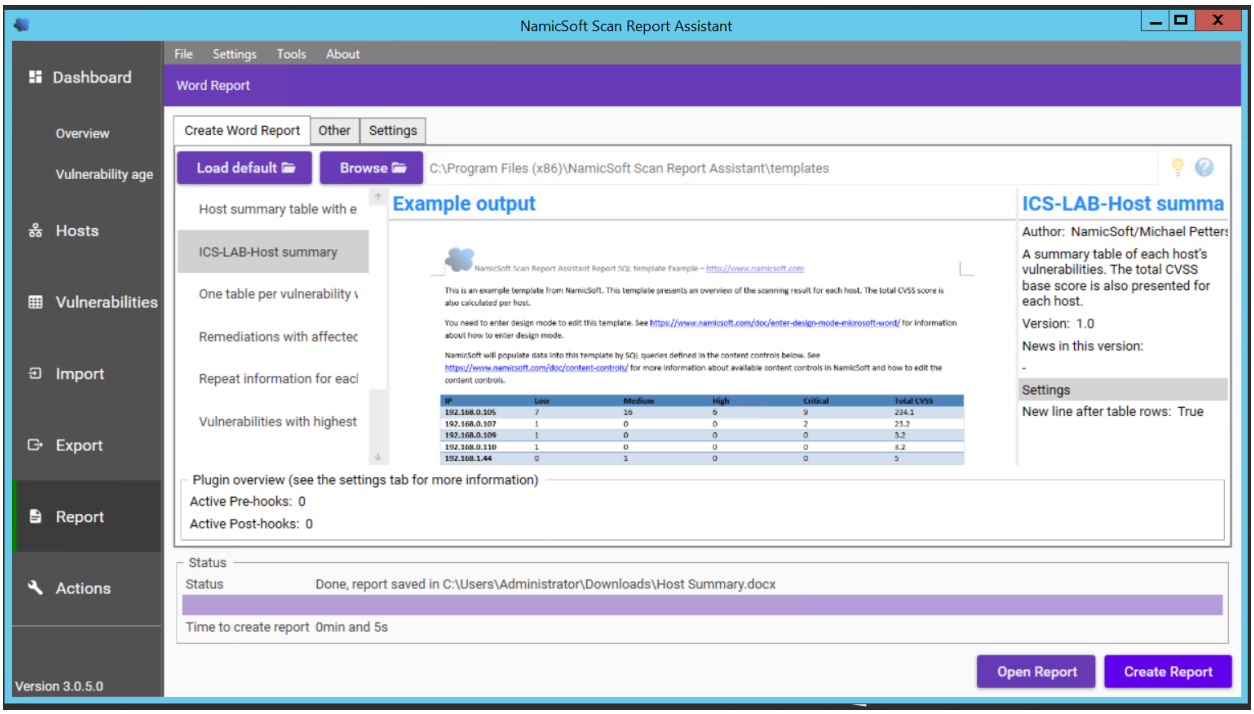


- Under **Actions**, click on **Save Workspace**. Ensure to Save your workspace after every change made. When running NamicSoft the next time, you can load this saved workspace file.

- To generate a Report, click on **Report.** You can select one of the default reporting templates from the list or create a custom one. To use a default template, select one from the list >> **Create Report.**

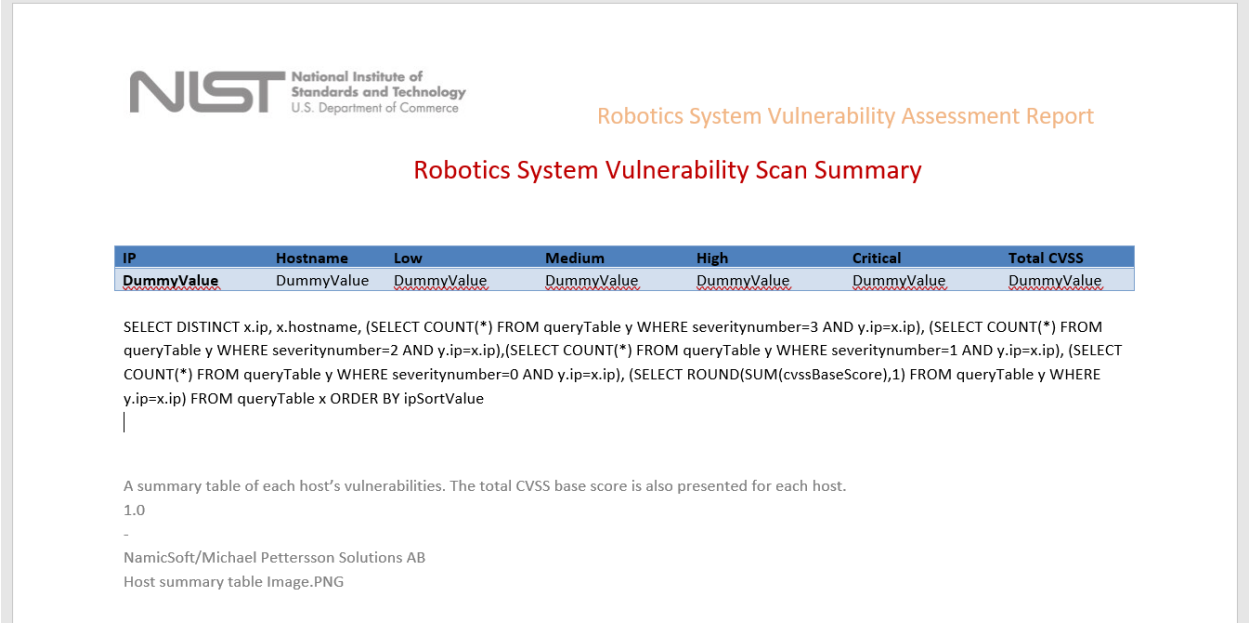


4142 • To view the Report, click **Open Report.**



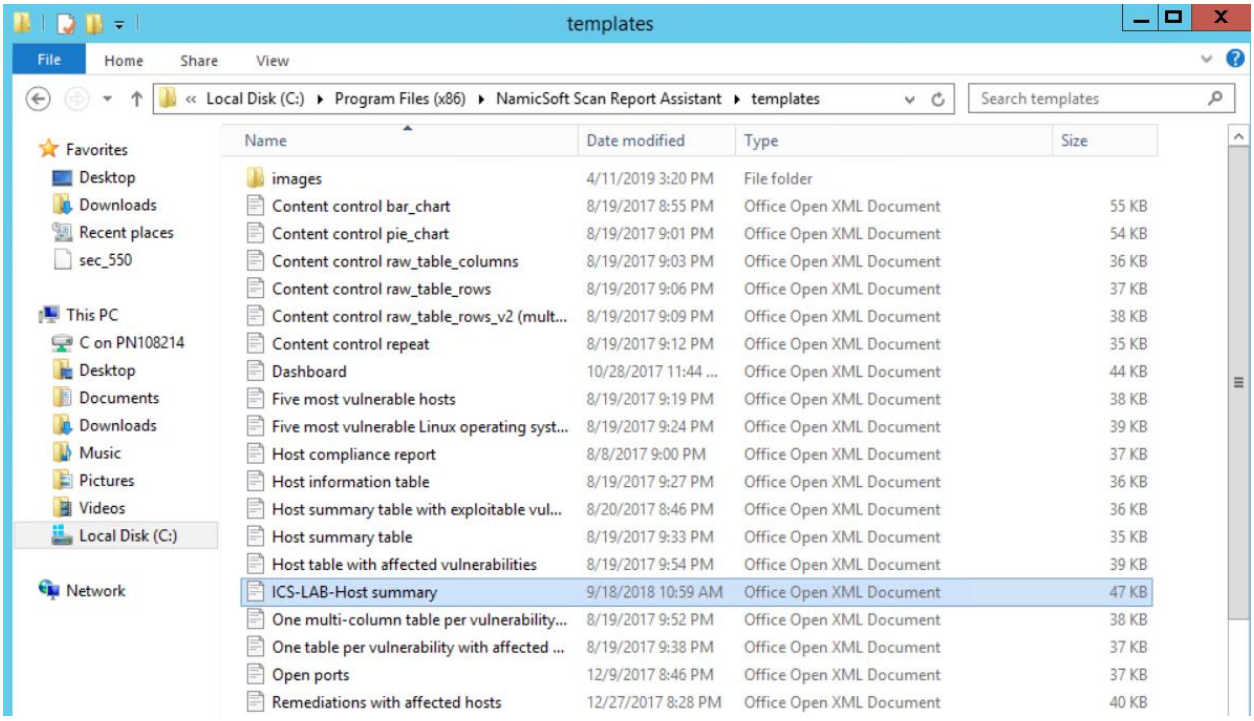
4143

4144 • To create a custom template, copy one of the template files located under **C:\Program**
4145 **Files(x86)\NamicSoft Scan Report Assistant\templates** and save it to a different folder.
4146 Open the copied file in MS Word to begin editing. The image below shows a customized
4147 template file created for CRS system. This report generates a summary of hosts and their
4148 respective vulnerabilities based on the Severity level.
4149

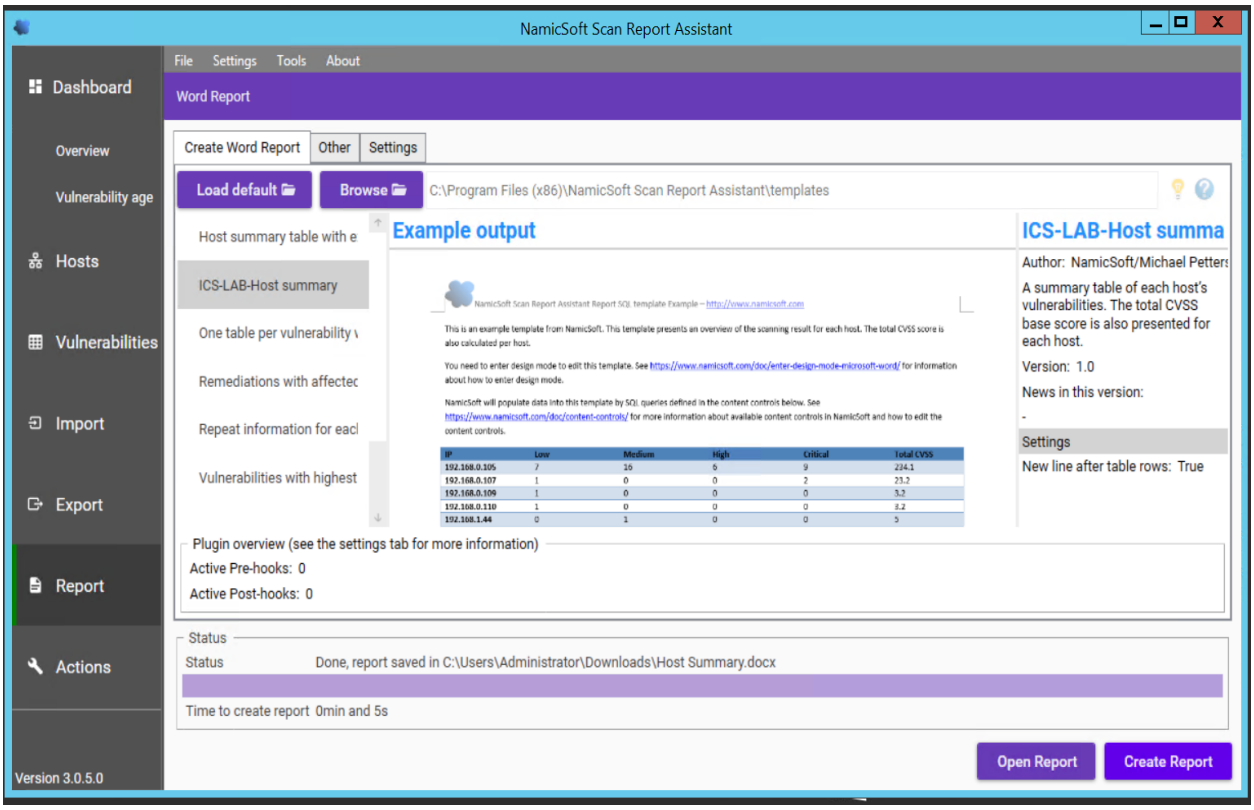


4150

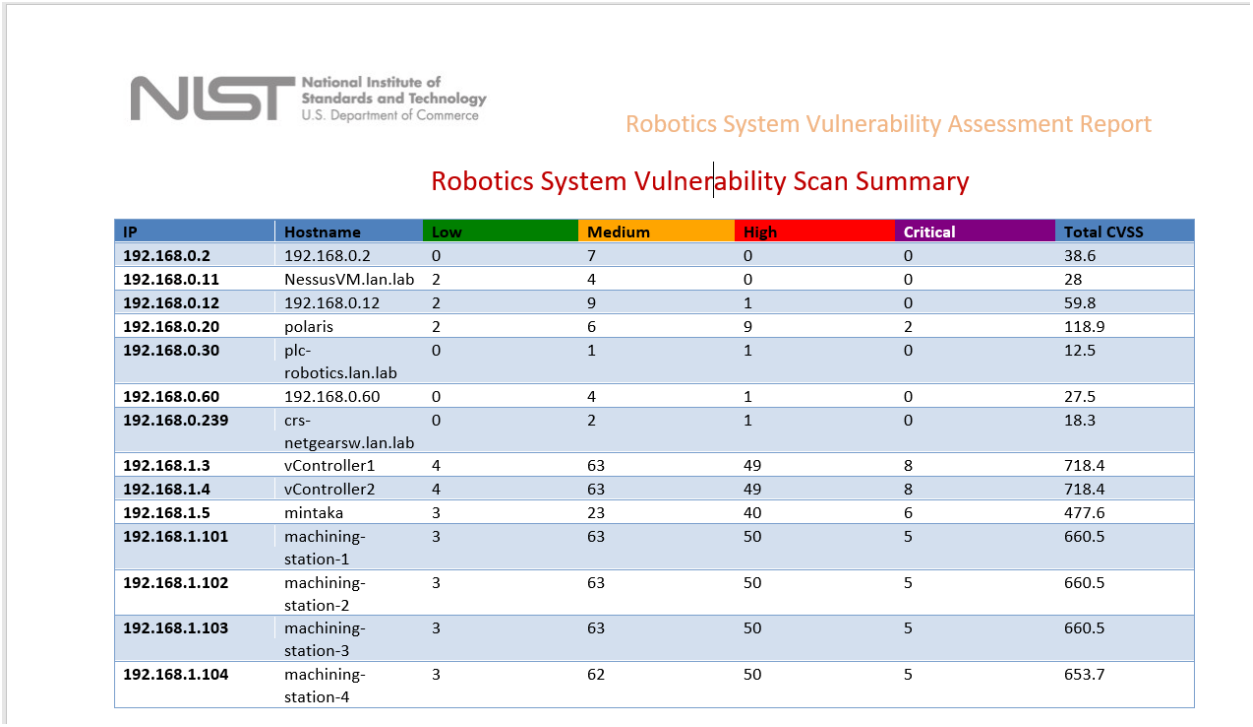
- Detailed instructions for creating custom reports are available on the NamicSoft website under https://www.namicsoft.com/doc/content-controls/
- Save your changes and give the file a suitable name. Copy this file back to the "Templates" directory. For instance, the below image shows our customized file – **ICS LAB Host Summary** copied back to the templates folder.



- Launch NamicSoft again. The custom report should now appear under the list. Select it and click on **Create Report.**



- The output should appear as per your changes.



National Institute of Standards and Technology
U.S. Department of Commerce

Robotics System Vulnerability Assessment Report

Robotics System Vulnerability Scan Summary

IP	Hostname	Low	Medium	High	Critical	Total CVSS
192.168.0.2	192.168.0.2	0	7	0	0	38.6
192.168.0.11	NessusVM.lan.lab	2	4	0	0	28
192.168.0.12	192.168.0.12	2	9	1	0	59.8
192.168.0.20	polaris	2	6	9	2	118.9
192.168.0.30	plc-robotics.lan.lab	0	1	1	0	12.5
192.168.0.60	192.168.0.60	0	4	1	0	27.5
192.168.0.239	crs-netgearsw.lan.lab	0	2	1	0	18.3
192.168.1.3	vController1	4	63	49	8	718.4
192.168.1.4	vController2	4	63	49	8	718.4
192.168.1.5	mintaka	3	23	40	6	477.6
192.168.1.101	machining-station-1	3	63	50	5	660.5
192.168.1.102	machining-station-2	3	63	50	5	660.5
192.168.1.103	machining-station-3	3	63	50	5	660.5
192.168.1.104	machining-station-4	3	62	50	5	653.7

- To report on Vulnerabilities remediated based off the previous vulnerability scans, use the "**Compare Workspaces**" feature under Action Menu

    - Load Nessus result from your previous scan. Save as a workspace.
    - Clear the workspace in the GUI (or restart NamicSoft)
    - Load Nessus results from the latest scan
    - Open Actions --> Compare workspaces. Choose **Compare** with current workspace and point Workspace 2 to your workspace saved earlier.
    - Choose Excel output file (target)
    - Click "Compare Workspaces"

4.11.6 Highlighted Performance Impacts

Two performance measurement experiments were performed for the vulnerability management technical capability while the manufacturing system was operational:

1. CL011.1 - Patches are installed on network hardware.
2. CL011.2 - Patches are installed on servers and ICS devices (e.g., PLC).

4.11.6.1 Experiment CL011.1

The firmware and operating systems for all three of the networking devices in the CRS (one router, two switches) were updated and patched to the most current versions. The firmware was updated while the CRS system was not operational.

A slight increase of the part production time mean was observed during this experiment but is not statistically significant.

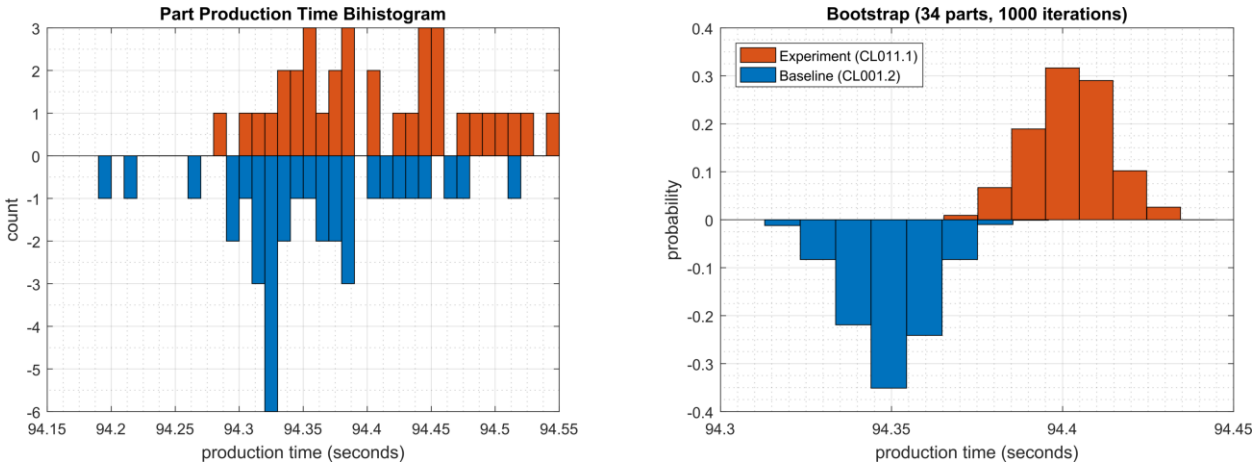


Figure 4-41 - Bihistograms showing the part production time (left) and estimated mean production time using the bootstrap method (right) using the measurements from baseline CL001.1 and experiment CL011.1.

4.11.6.2 Experiment CL011.2

The firmware and operating systems for each server (MINTAKA, POLARIS, vController1, and vController2) and each ICS device (HMI, PLC, and Engineering Laptop) were updated and patched to the most current versions. The firmware and operating systems were updated while the CRS system was not operational, and all of the devices were restarted after the updates completed.

A decrease in the average inter-packet delay (IPD) was observed on the PLC Modbus TCP communications to Station 2. Further analysis revealed that the performance impact also showed a relatively unstable IPD, as compared to the baseline (see Figure 4-42). These new performance characteristics were consistent throughout the experiment. An increase in the average IPD was also observed on the Modbus TCP communications between Robot 2 and the PLC. Again, further analysis revealed that the performance impact showed a relatively unstable IPD, as compared to the baseline (see Figure 4-43).

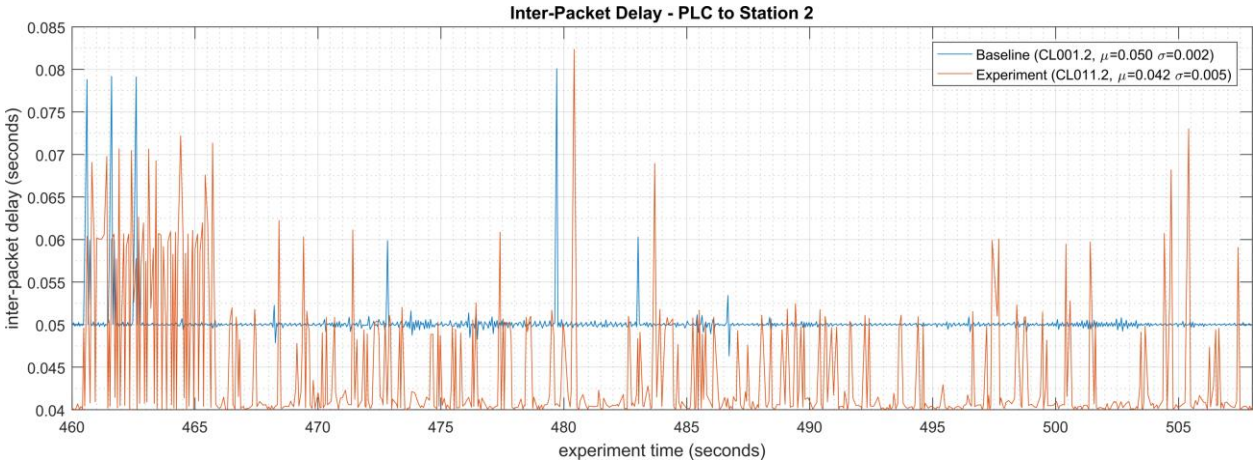


Figure 4-42 - Time series plot displaying the inter-packet delay of Modbus TCP traffic between the PLC and Station 2, as measured during the baseline CL001.2 and experiment CL011.2. Note the relatively constant baseline average delay of around 0.050 sec., while the experimental delay is decreased to an average of 0.042 sec. with large deviations.

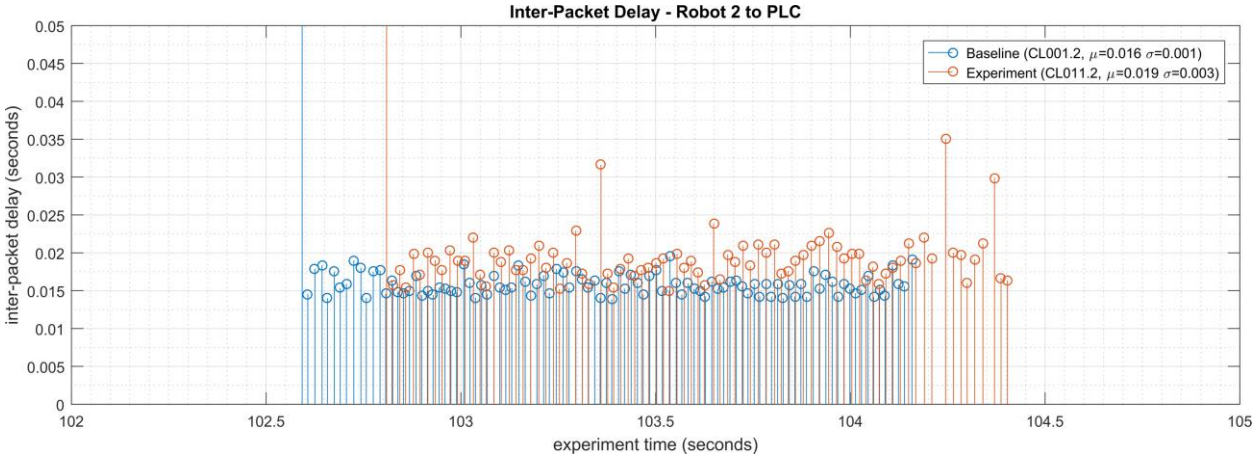


Figure 4-43 - Stem plot displaying the inter-packet delay of Modbus TCP traffic between Robot 2 and the PLC, as measured during the baseline CL001.2 and experiment CL011.2. Note the relatively constant baseline average delay of around 0.016 sec., while the experimental delay is increased to an average of 0.019 sec. and relatively unstable.

A small increase in the average robot job actuation time was observed on Robot 1 for Job 103 (see Figure 4-44). No other increases were observed for any of the other jobs. This added actuation time was also observed for all the experiments performed after CL011.2.

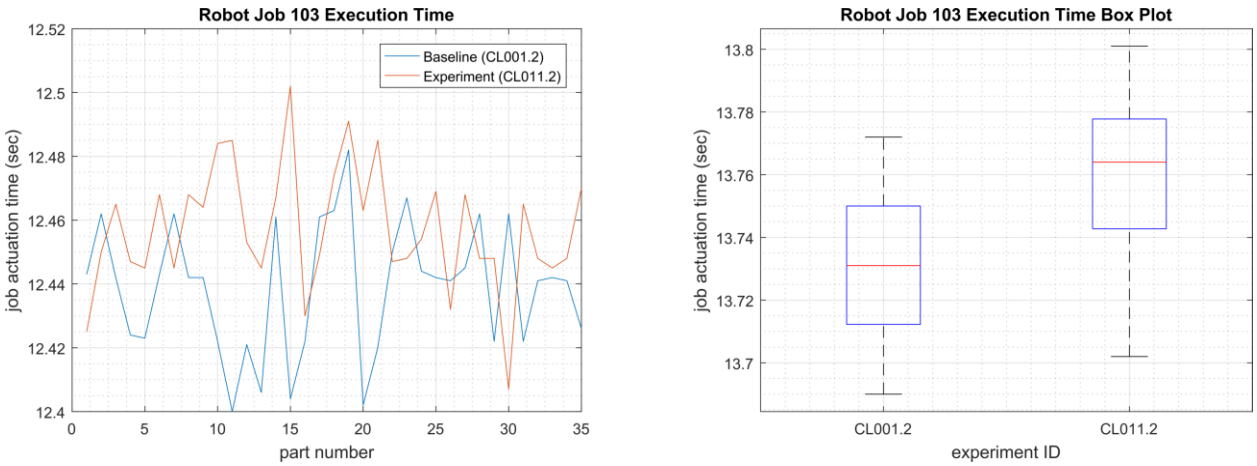


Figure 4-44 - Time-series (left) and boxplot (right) showing the job actuation times for Job 103 during the CL001.2 baseline and CL011.2 experiment.

Performance impacts to the supervisory PLC task execution time were observed after the PLC operating system was updated. The task execution time increased from an average of around 330 µsec. during the baseline to around 690 µsec., with the maximum task execution time now consistently exceeding 2000 µsec. (see Figure 4-45).

CPU utilization on vController2 also increased from an average of around 2% during the baseline to an average of around 7% during the experiment (consistent with the increase vController1 had experienced in previous experiments). This CPU increase was observed for all the experiments performed after CL011.2 but was not consistent with vController1, which measured a consistent average of 2% CPU utilization for CL011.2 and all subsequent experiments.

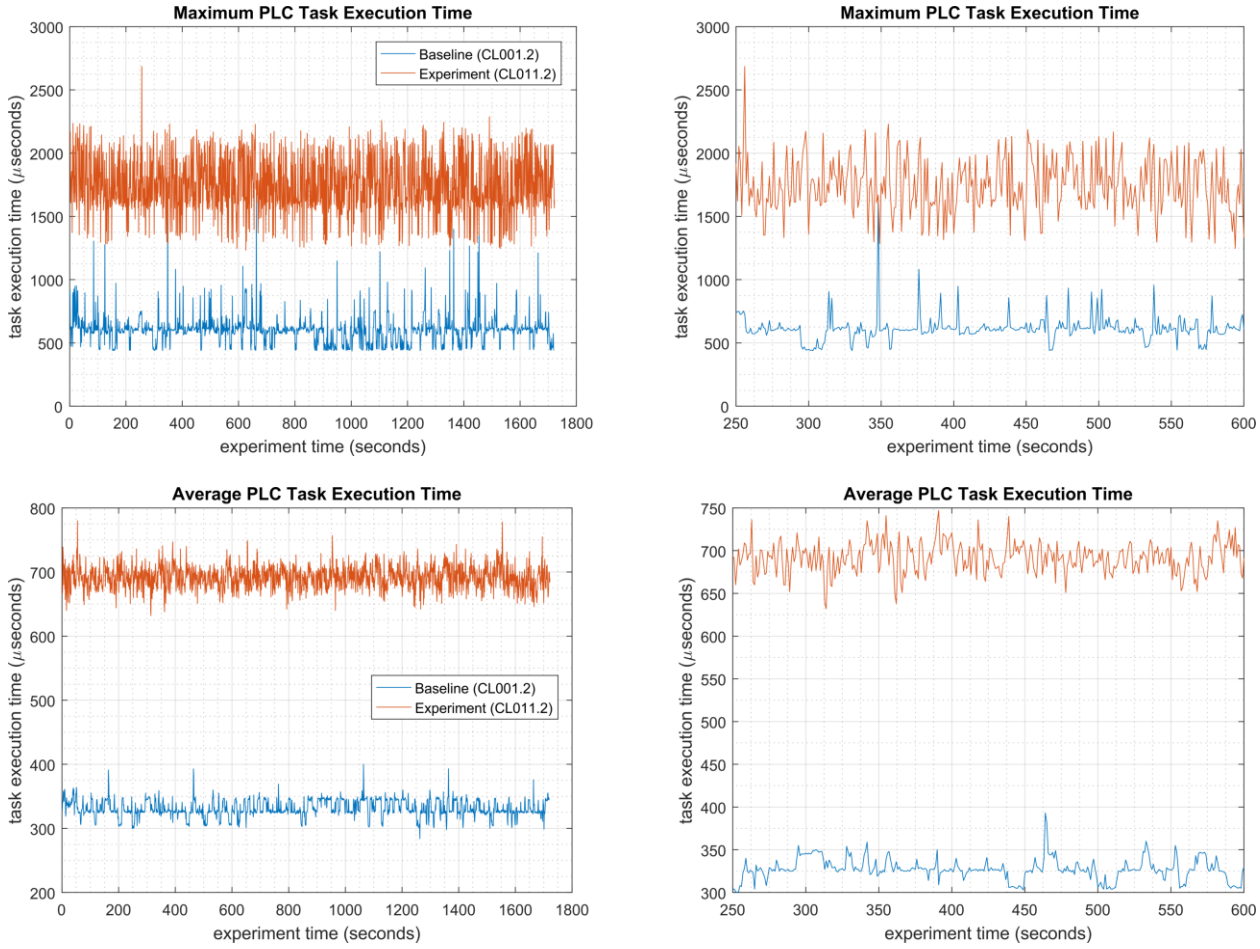


Figure 4-45 - Plots showing the maximum (top) and average (bottom) PLC task execution time during the experiment (left) and during the period of measured impact (right). The PLC task execution time characteristics changed considerably after patches were applied to the PLC and other ICS devices.

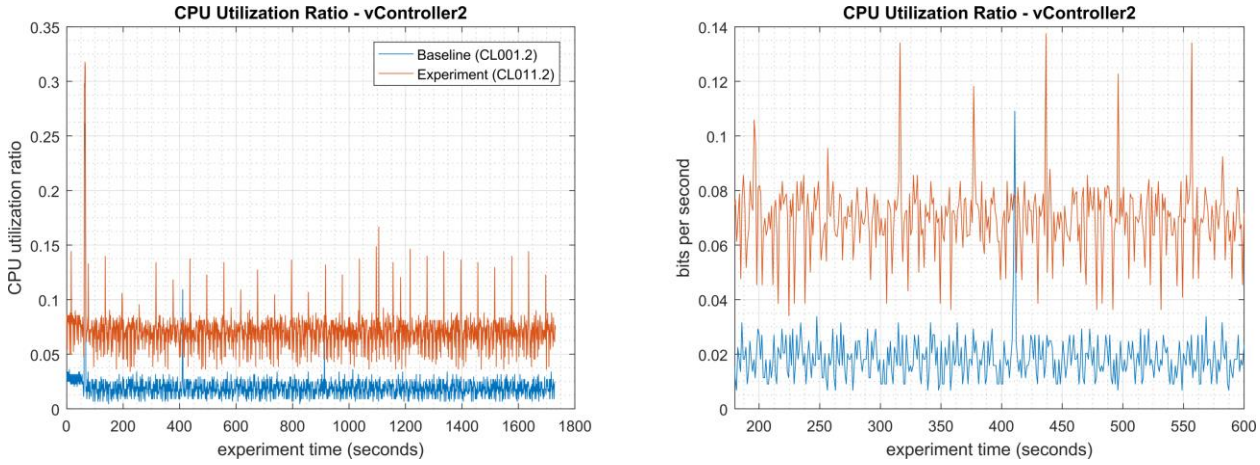


Figure 4-46 - Time series plots showing the CPU utilization ratio for vController2 during the CL011.2 experiment and the CL001.2 baseline (left), and a detailed view of the same data (right).

A slight increase of the part production time mean was observed during this experiment, but it is not statistically significant.

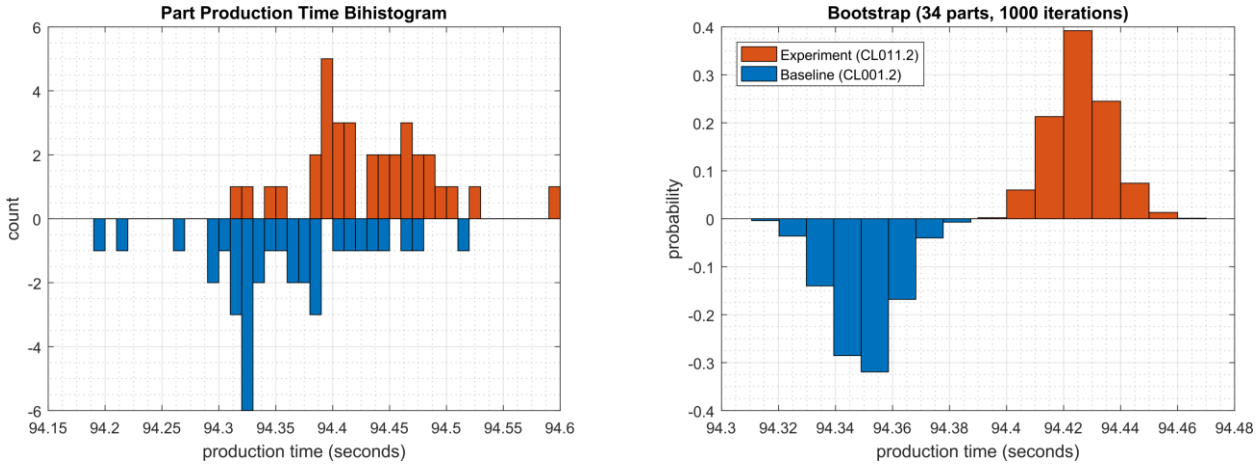


Figure 4-47 - Bihistograms showing the part production time (left) and estimated mean production time using the bootstrap method (right) using the measurements from baseline CL001.2 and experiment CL011.2.

4.11.7 Link to Entire Performance Measurement Data Set

- **CL011.1-PatchesNetworkHardware.zip**
- **CL011.2-PatchesServersICSDevices.zip**

4.12 GTB Inspector

4.12.1 Technical Solution Overview

GTB Inspector by GTB Technologies is a DLP solution that has been evaluated in our lab environment for low baseline manufacturing profile. GTB Inspector's built in ability to detect, log, and block network traffic trying to leave premise. Inspector detects and blocks FTP, Email, HTTP, HTTPS (SSL/TLS), Finger Printed files, USB protection, and other configured exfiltration methods. GTB Inspector is the main component that analyzes all network traffic and depending on the configuration Bridge (In-Line), Monitoring (OOL), TAP, Transparent Proxy (TPROXY), and Load Balancing if required. GTB Central Console which is the device Inspector reports back to, so there is always a log of violation that occurred. Central Console allows for groups and escalation paths depending on the alerting required.

GTB is configured within the corporate network. This option was chosen to ensure we could get the best protection for the entire environment.

All DLP products have a high cost to implement, but GTB Technologies provides a product that can grow as your company does.

Once installed and configured system requires little maintenance.

Install time within the lab was approximately 16 hours for configuration, but for simple data capture setup took about an hour.

4.12.2 Technical Capabilities Provided by Solution

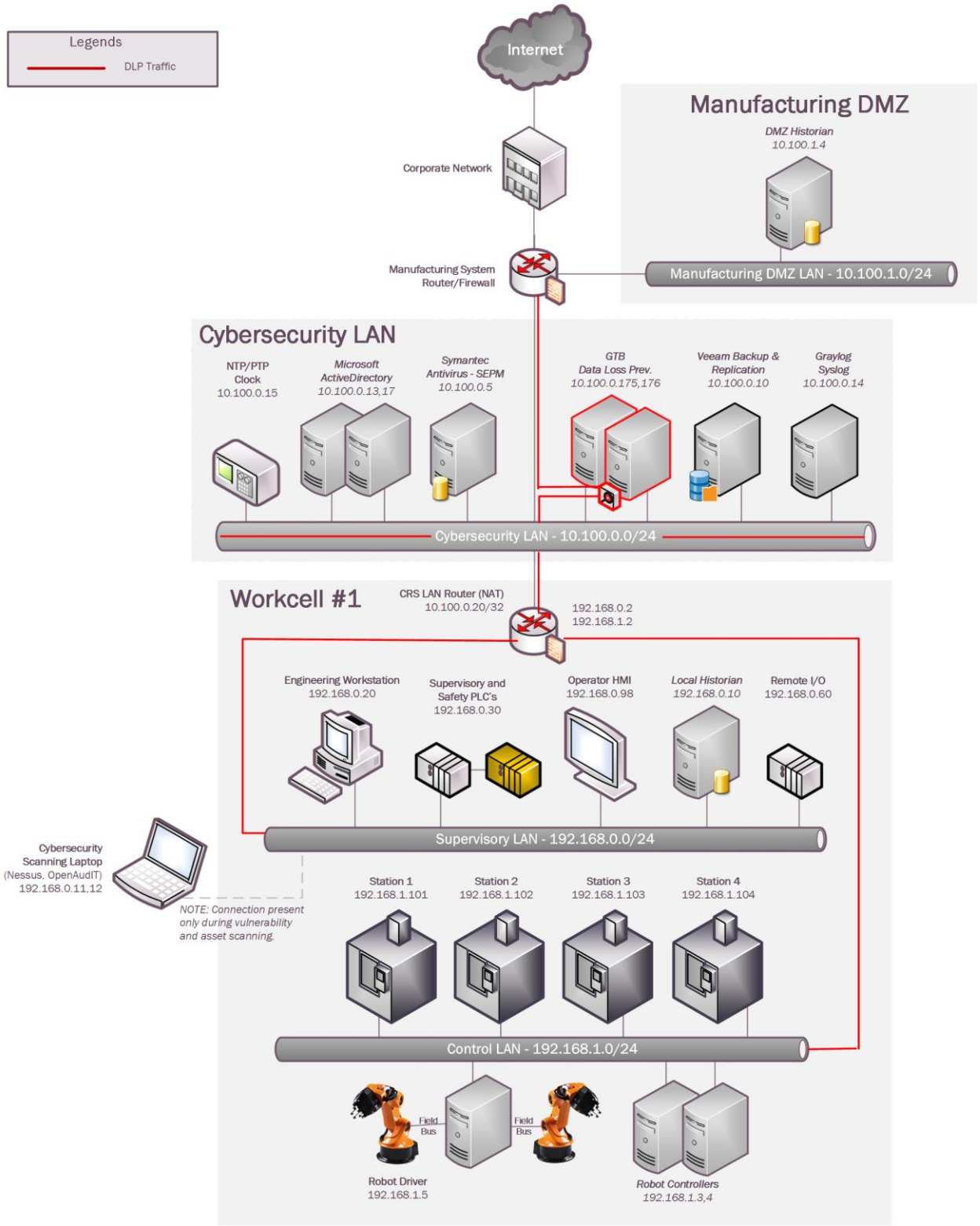
GTB Inspector provides components of the following Technical Capabilities described in Section 6 of Volume 1:

- Data Loss Prevention

4.12.3 Subcategories Addressed by Implementing Solution

PR.DS-5

4.12.4 Architecture Map of Where Solution was Implemented

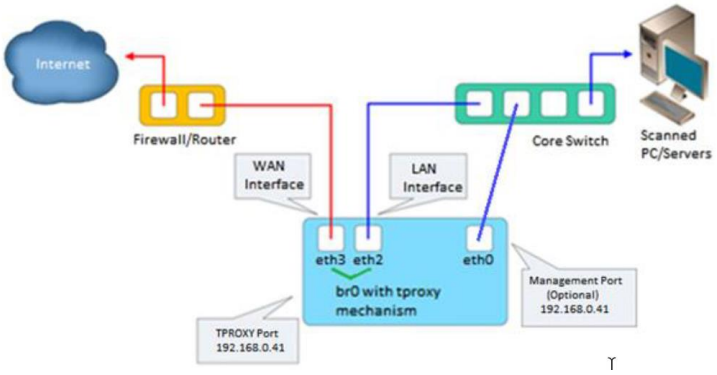


4.12.5 Installation Instructions and Configurations

Steps for installing GTB Central Console and Inspector

- Both products are virtual machines and downloadable from https://gttb.com/downloads/ select desired product for download.
- Once downloaded extract each zip file to its own folder.
- Inside newly created folders there'll be a "**installation guide"** along with the extracted files for each product.
- See attached PDF for current "**system requirements"** for each component being installed.

- Currently **"GTB Inspector"** network configuration is enabled in **"Bridge [Inline]"** mode. This diagram is within **"installation guide" GTB Inspector DLP, installation methods. Displayed is Bridge [Inline] mode which monitors.**



Hyper-V Install Configuration

- Create two virtual machines **(See below for current specification of our environment)**
  - GTB Inspector
    - VHDX -- D:\Hyper-V\GTB InspectorVirtual Hard Disks\GTB Inspector.vhdx
    - Memory – 16GB (16384MB)
    - Processor – 4 CPU
    - Network Adapter
      - **"vswitch_TestBed_LAN"** Management Port
        - Management port IP is (10.100.0.175)
      - **"Eth2 for GTB Inspector"** Connects to Monitor Port 1 on Tap Device
      - **"Eth3 for GTB Inspector"** Connects to Monitor Port 2 on Tap Device
  - GTB Central Console
    - VHDX -- D:\Hyper-V\GTB Central Console\Virtual Hard Disks\GTB Central Console.vhdx

- Memory – 16GB (16384MB)
- Processor – 4 CPU
- Network Adapter
  - **"vswitch_TestBed_LAN"** Management Port / Connection
    - Management Port / Connection IP is (10.100.0.176)

Install Instructions for Each Virtual Machine and any additional configuration

- **Inspector**
  - See install guide for most updated instructions, or attachment below. **Changes made within our environment are included below.**
  - Each network connection was installed and rebooted to ensure they were assigned correct name / location, and if not, this command can be used to rename the network to reflect and needed changes. */usr/local/gtb/libexec/manage_nics -i ethX –o ethX* **(This syntax is included within installation guide)**
  - **IP Address (10.100.0.175)**
  - **Hostname = gtbinspector / gtpinspector.lan.lab**
  - Created DNS A record for **"gtbinspector"** along with reverse lookup
  - **Configured LDAP integration with Active Directory (10.100.0.17)**
  - **UPN is required for username**
  - **Configured email**
    - SMTP Server Hostname **(postmark.nist.gov)**
    - Send email from **(**GTBInspector@nist.gov**)**
    - SMTP Server Port **(25)**
  - Check and ensure LAN and WAN interfaces are configured for eth2 **(WAN)** eth3 **(LAN)**
    - Configuration tab, Network, #-3 and #-4
  - 
    GTB Inspector Installation Guide.pdf
- **Central Control**
  - See install guide for most updated instructions or attachment below. **Changes made within our environment are included below.**
  - **IP Address (10.100.0.176)**
  - **Hostname = gtbcc / gtbcc.lan.lab**
  - Created DNS A record for **"gtbcc"** along with reverse lookup
  - **Configured LDAP integration with Active Directory (10.100.0.17)**
  - **UPN is required for username**
  - **Configured email**
    - SMTP Server Hostname **(postmark.nist.gov)**
    - Send email from **(**GTBInspector@nist.gov**)**
    - SMTP Server Port **(25)**


GTB Central Console Installation Guide.pdf

- **Install information for VMware**
  - **Install**
    - Installed a separate physical machine with vSphere (10.100.0.180) for testing since problems were observed with Hyper-V ability to block rule violations with HTTP/HTTPS traffic.
    - Configured two network cards in vSphere for pass thru access. This was completed to give the virtual machine access to physical network cards to eliminating possible configuration issues being observed in Hyper-V. (Will try to confirm if possible still exist with Hyper-V since new release from GTB has been released)
    - GTB's Inspector (10.100.0.181) is currently at release 15.4 and contains an options under **"Configuration → Network "labeled** (Failover Mode). In our environment this option is set to **"NO"** since we don't have a bypass card installed. This setting allows all web traffic to be filter via scanning engine.

14	Failover mode	No	Select "Yes" to enable failover mode of the Bypass Network Card in Bridge and TPROXY. Select "No" to enable fail closed mode.

    - Email filtering is designed to use **"MTA"** from Inspector and then forward along to intended recipient after been scanning for any rule violations.
    - Added GTTB Certificate to **"Default Domain Policy"** so any machine within the domain will update with the required Trusted Certificate Authority so as not to get a warning message. **(Confirmed working)**

    - **Lesson learned:**
      - Microsoft Hyper-V solution detects and logs traffic, however even when configured for blocking, only detection occurs. Support has indicated that this is since we're not using a bypass network card stated earlier with a physical box.

    - **Performance Impact:**
      - This tool has not been configured and ran against ICS enclaves currently, so there has been no performance impact that were aware of.

Specific configuration steps for GTB's Inspector and Central Console

within Testbed environment

*This document contains information for configuration within our environment. If scanning email for content violation, you'll need to configure email clients to point **SMTP** to **10.100.0.175** (Inspector - MTA) for email scanning. For additional configuration information please see vendors Administrator Guides which are included in download package from vendor.*

Inspector

Generating and applying License:

- **Generating**
  - Click on middle top web page once logged into Inspector
    - 

    - You will now be directed to a page that allows you to download, email, or upload a license file.
    - License files should be emailed to support@gttb.com . Support will reply with an updated file to be uploaded.
- **When to generate a new license file**
  - Anytime a network change effects the **MAC (Media Access Control)** address for Inspector you'll need to generate a new license key an email support@gttb.com. Before emailing change the extension from **".dat"** to **".txt"**. Example: **Inspector** – "***7-31-2018-sysinfo_inspector.dat to 7-31-2018-sysinfo_inspector.txt***". This change may be required if your email provider blocks **".dat"** file extension
  -
- **Configuration Setting**
  - Login into GTB Inspector web page and click **"Configuration"** tab.
    - 

  - All setting are accessible via **"Groups"** located on left side of webpage.
  - Central Console = **"gtbcc.lan.lab"**

4405 ○ **Network = Screenshot below**

Network

1	Inspector location	GTBInspector.lan.lab	The location or hostname the Inspector appliance.
2	Deployment mode	TPROXY	Deployment mode of the Inspector: "OOL" for Out-of-Line, "BRIDGE" for Inline, "TAP" for a Tap connection, "TPROXY" for Transparent Proxy.
3	LAN interface	eth2	LAN interface (ie. eth0, eth1, eth2, or eth3) where the network traffic is coming from. It is being used in all Inspector modes.
4	WAN interface	eth3	WAN interface (ie. eth0, eth1, eth2, or eth3) where the network traffic is coming to. It is being used in TAP, BRIDGE, and TPROXY modes.
5	OOL LAN	10.100.0.0/24, 172.16.3.0/24	List of source IP addresses, subnets or MAC addresses separated by commas which are inspected in the OOL mode.
6	OOL WAN		List of destination IP addresses, subnets or MAC addresses separated by commas which are inspected in the OOL mode. An empty entry accepts all WAN packets.
7	TPROXY LAN	10.100.0.0/20,192.168.0.0 /20,172.16.0.0/20	List of source IP addresses or subnets separated by commas which HTTP/HTTPS traffic is being inspected in the TPROXY mode.
8	TPROXY source exceptions	10.100.0.14, 10.100.0.11	List of source IP addresses or subnets which are not inspected in the TPROXY mode. Each object is delimited by comma or new line.
9	TPROXY destined exceptions		List of destination IP addresses or subnets which are not inspected in the TPROXY mode. Each object is delimited by comma or new line.
10	TPROXY IP address	10.100.0.175	IP address of TPROXY NIC device.
11	TPROXY netmask	255.255.255.0	Subnet mask of TPROXY NIC device.
12	TPROXY gateway	10.100.0.1	Default gateway of TPROXY NIC device.
13	TPROXY routing	10.100.0.0/24 via 10.100.0.1 dev eth0 192.168.0.0/20 via 10.100.0.1 dev eth0 172.16.0.0/20 via 10.100.0.1 dev eth0	Static routing rules each on a separate line. Example: 192.168.0.0/24 via 191.168.0.1 dev eth0. Where 192.168.0.0/24 is destination host/subnet, 191.168.0.1 is a gateway, eth0 is a NIC device of the Inspector.
14	Failover mode	No	Select "Yes" to enable failover mode of the Bypass Network Card in Bridge and TPROXY. Select "No" to enable fail closed mode.
15	OOL/TAP blocking	Yes	Select "Yes" to enable blocking in OOL/TAP modes.
16	Blocking interface	eth2	Network interface name for sending TCP Reset or FIN packets in "TAP" mode (ie. eth0, eth1, eth2, or eth3).
17	DNS servers	10.100.0.17, 10.100.0.13	DNS servers IP addresses separated by commas.
18	Network Overload Protection	No	Enable skipping stream inspection (BRIDGE mode only) due to excessive network traffic.
19	Network MTU	9000	The maximum transmission unit size for inspection ports (LAN and WAN), this can be up to 16110.
20	CRC checking	No	Select "Yes" to perform a CRC check of every network packet. Normally, should be set to "No".

4406

4407 ○ **Emails Alerts = Screenshot below**

Email Alerts

1	Security Respondents	wesley.downard@nist.gov,neeraj.shah@nist.gov	Default Security Respondents - list of email addresses separated by commas.
2	Special Case Security Respondents		Format: [Policy: list of email addresses separated by commas]. Example: PCI: demo@gttb.com
3	MD5 Recipients		Email address receiving MD5 of triggered events.
4	System Administrator Email	wesley.downard@nist.gov,neeraj.shah@nist.gov	System Administrator email address(es) separated by commas.
5	Notify about system errors by email	Yes	Select "Yes" to notify System Administrator about system errors by email.
6	Send Emails From	GTBInspector-ICSLab-220-A230@nist.gov	Email address, appears as the source of the email notification.
7	SMTP Server Hostname	postmark.nist.gov	The IP address or domain name (FQDN) of the SMTP server. This address is required in order for the Inspector to send email notifications.
8	SMTP Server Port	25	The SMTP server port number. Typically, it is port 25.
9	Use SSL/TLS	No	Select "Yes" to use SSL/TLS encrypted connection.
10	Email Username		Authenticated Email Username.
11	Email Password		Authenticated Email Password.
12	Time between Alerts	60	Minimum interval in seconds, between alert emails.
13	Enable HTTP Block Response	Yes	Select "Yes" to return an alert page to a web browser when HTTP request is blocked.
14	HTTP Response Message	http://testpage.gtbtechnologies.com:	Response message in HTML or redirect URL returned when the HTTP session is blocked.

4408

4409 ○ **LDAP Intergration = Screenshot below**

LDAP Integration

1	LDAP Server Hostname	10.100.0.17	IP address or hostname of the corporate LDAP server.
2	LDAP Server Port	389	LDAP server port.
3	LDAP Username (bind DN)	gttbldap@lan.lab	Example: Domain\Username (for MS Active Directory), cn=Admin,o=MyOrganization (for Novell eDirectory or OpenLDAP).
4	LDAP Password	******	LDAP password.
5	LDAP SSL	No	Select "Yes" to use SSL connection to the LDAP server.
6	LDAP Cache Refresh Period	1800	Period in seconds used for LDAP objects cache periodic refreshes. Zero means no periodic refreshes.
7	Hostnames Cache Refresh Period	3600	Period in seconds used for hostnames cache periodic refreshes. Zero means no periodic refreshes.
8	NRH UDP Port	2222	UDP port for receiving reports from Name Resolution Helpers (the device acts as server).
9	Cache Persistence Timeout	450	User names cache persistence timeout in seconds. If the system is stopped for more than timeout specified, cache becomes obsolete and is dropped. Zero means "never obsoleted".

4410

4411 ○ **Mail Transfer Agent = Screenshot below**

Mail Transfer Agent

1	List Of Allowed Hosts	*	Allowed hosts for email processing. Insert hostnames or IP addresses in separate rows. Insert * to accept emails from any host. A blank field means emails are rejected from any host.
2	Route Emails	Yes	Select "Yes" to have MTA route all emails to the next email hops listed in the "Domain Routing Rules" field.
3	Email Username		Authenticated next email hop Username. Example: demo@gttb.com.
4	Email Password		Authenticated next email hop User Password.
5	Domain Routing Rules	* 129.6.16.94	This entry contains routing rules per email domain on separate lines. Each rule consists of a domain pattern and a list of hostnames to which MTA will attempt to relay emails for this pattern. Use a colon to separate hostnames. Use double colon to specify a port number. Example: *.com 192.168.0.1:192.168.0.100, *.net 192.168.1.1::2525
6	Excluded domains		Emails destined to these domains will be passed without inspection. Domains should be colon delimited and without spaces. Example: gmail.com:gttb.com
7	Bcc domain inspection		List of email domains for inspection only (without routing). Domains should be colon delimited and without spaces. Example: gmail.com:gttb.com
8	MTA Listening Ports		List of listening TCP port numbers separated with colons. Default is 25. Example: 25:465
9	Email Size Limit	20	Maximum allowed email size in MBytes which is accepted for delivery and inspection. Value "0" means unlimited size.
10	Alert on Queue Above	4	System will alert Administrator hourly, when the number of email messages in the MTA queue is above this value. Set 0 to disable it.
11	Backup Emails	None	Enable email backup system.
12	Reject Email on fail	No	Select "Yes" to enable email rejection when inspection fails.

4412

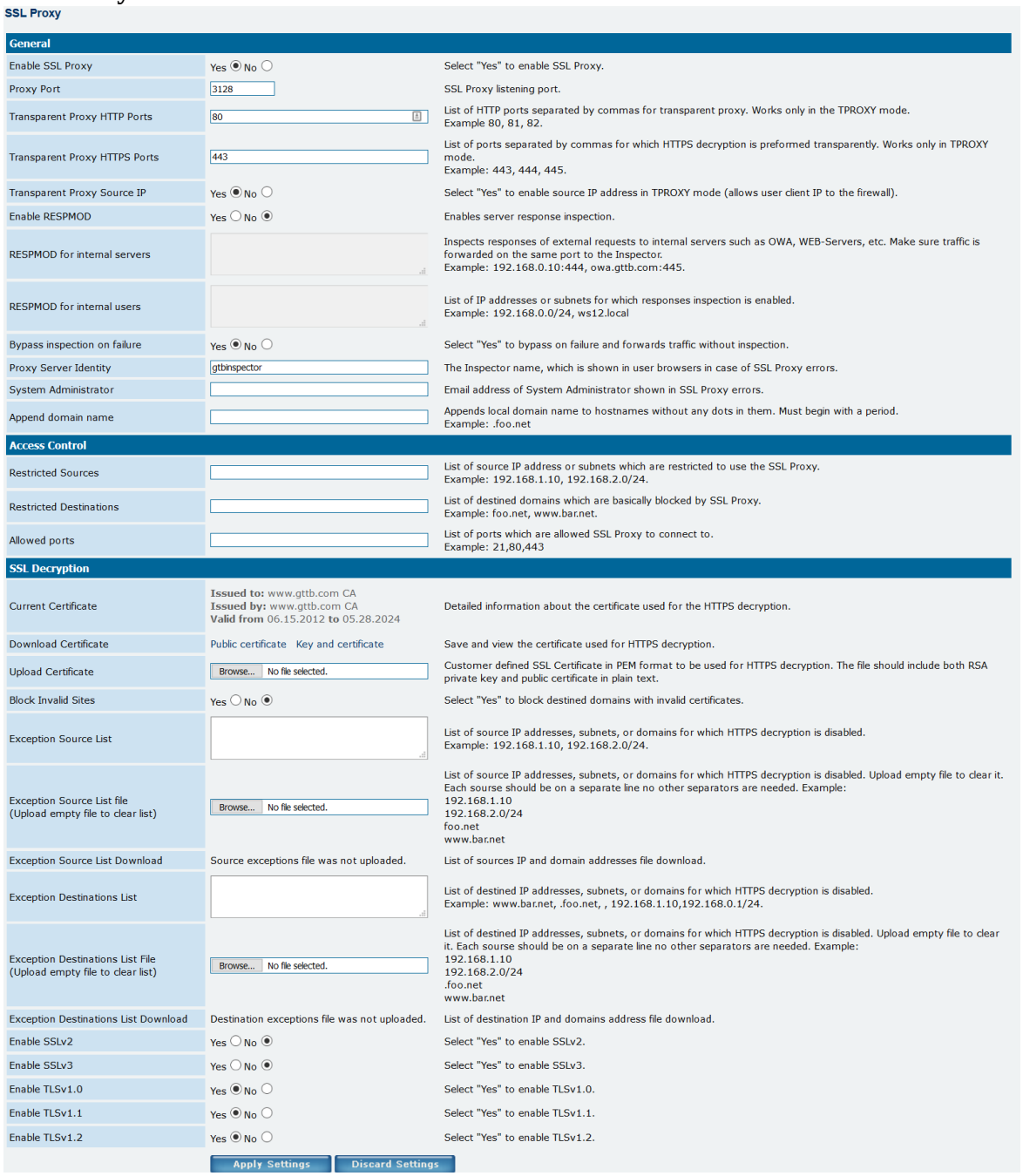
4413 ○ **SIEM = Screenshot below**

SIEM

1	SIEM Receiver Hostname	10.100.0.27	IP address or hostname of the corporate SIEM receivers separated by commas.
2	Log Content	Yes	Select "Yes" to include security events triggers into the SIEM message.
3	Arcsight CEF	Yes	Select "Yes" to use Arcsight Common Event Format in the SIEM messages.

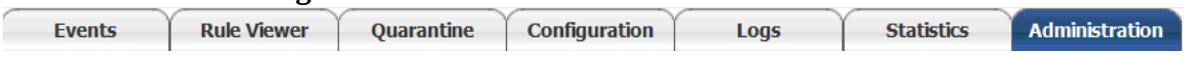
4414

4415 ○ **SSL Proxy = Screeshot below**



4416

4417 • **Administration setting**



4418

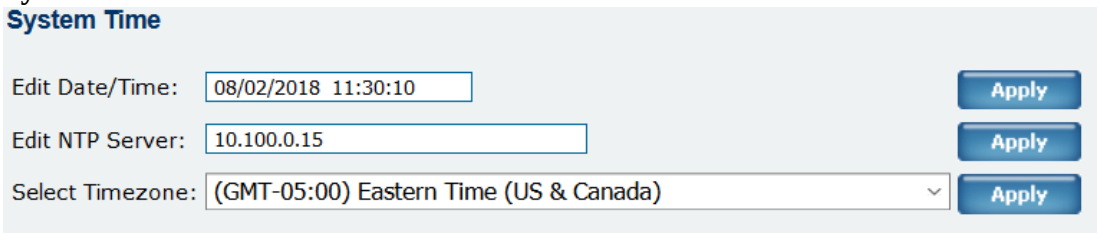
4419 ○ Licensing = Used for downloading and uploading license information.

4420 ○ Health Check = Ability to perform **"Self-Test"** to check Inspector install health.

4421 ○ Account Manager = Used to add new personal who will be administrating

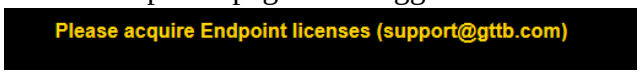
4422 Inspector or responding to alerts for further investigation.

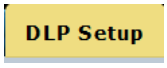
- **System Time = Screenshot below**



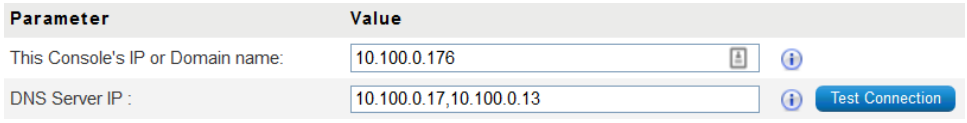
Central Console

Generating and applying License:

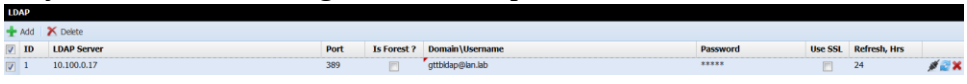
- **Generating**
  - Click on middle top web page once logged into Central Console
    - 

    - You will now be directed to a page that will allow you to download, email, or upload a license file.
    - License files should be emailed to support@gttb.com . Support will reply with an updated file to be uploaded.
- **When to generate a new license file**
  - Anytime a network change effects the **MAC (Media Access Control)** address for Central Console you'll need to generate a new license key and email it to support@gttb.com. Before emailing change the extension from **".dat" to ".txt"**. Example: **Central Console - 7-31-2018-sysinfo_cc.dat to 7-31-2018-sysinfo_cc.txt**. This change may be required if your email provider blocks **".dat"** file extension
  -
- **System settings**
  - Click on **"DLP Setup"** tab 

  - **Network (Located under Categories)**
    - Enter required information. See below for screenshot



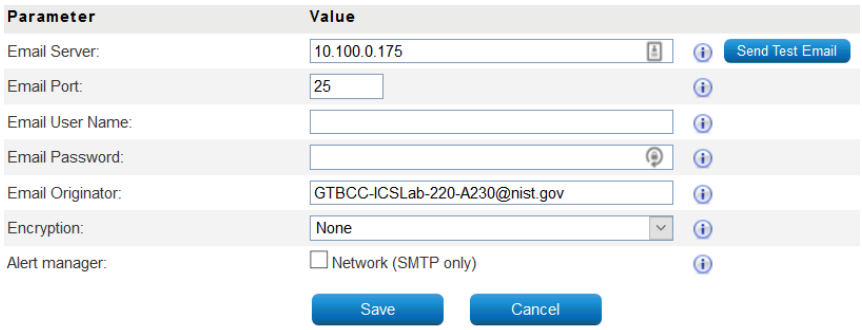
    - Click save to continue.
  - **LDAP**
    - Enter information for screenshot below. This user has been created and only has Domain User right. Check for password in database.



    - User name = gttblab@lan.lab

- Password = check database
- LDAP Server = 10.100.0.17

- **Email and alerts**
  - Enter information from screenshot below



  - Email Server = 10.100.0.175
  - Email Originator = GTBCC-ICSLab-220-A230@nist.gov
  - Click save
- **Data and Time**
  - NTP Server = 10.100.0.15 (Click set time to sync)
  - Time Zone = Eastern Time (US and Canada) (Click Apply to save)
  - Click Save

Other settings under **DLP Setup → System** aren't currently configured. These setting will be updated an included when these features are enabled.

Lesson learned: If integrating with Active Directory using LDAP it's recommended to use Secure LDAP to ensure user name and password are not sent in plaintext.

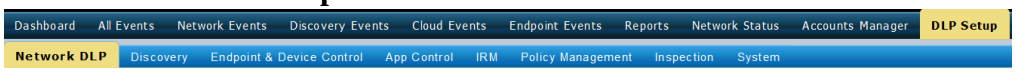
How ACL rules are created for use with GTB DLP Inspector.

GTB DLP Inspector views data as it passes thru the device and responds based on configured rules.

GTB Central Console is the portal were all policy rules and other settings are configured.

ACL Rules:

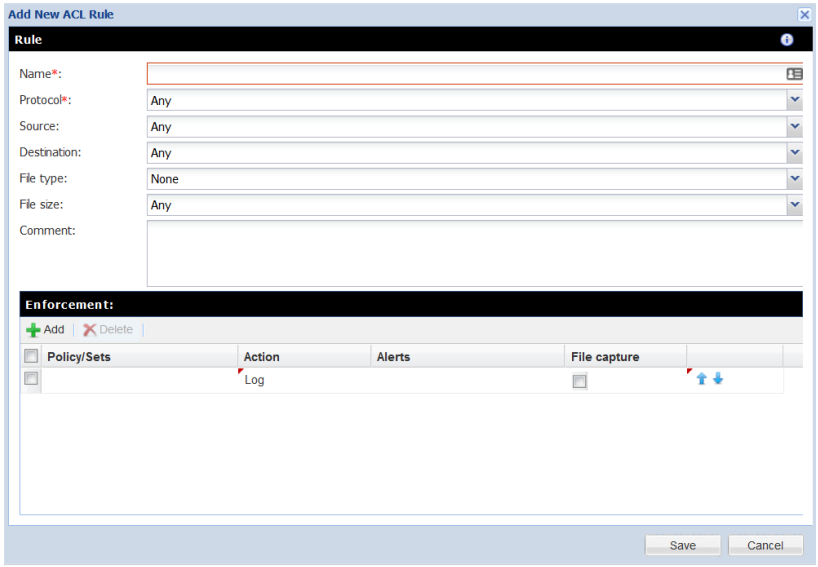
- Login into to Central Console via web browser (E.g. 10.100.0.176).
- Now click on **DLP-Setup→Network DLP** to access rules.



- Now, look to the left of window under categories and select your Inspector installation.

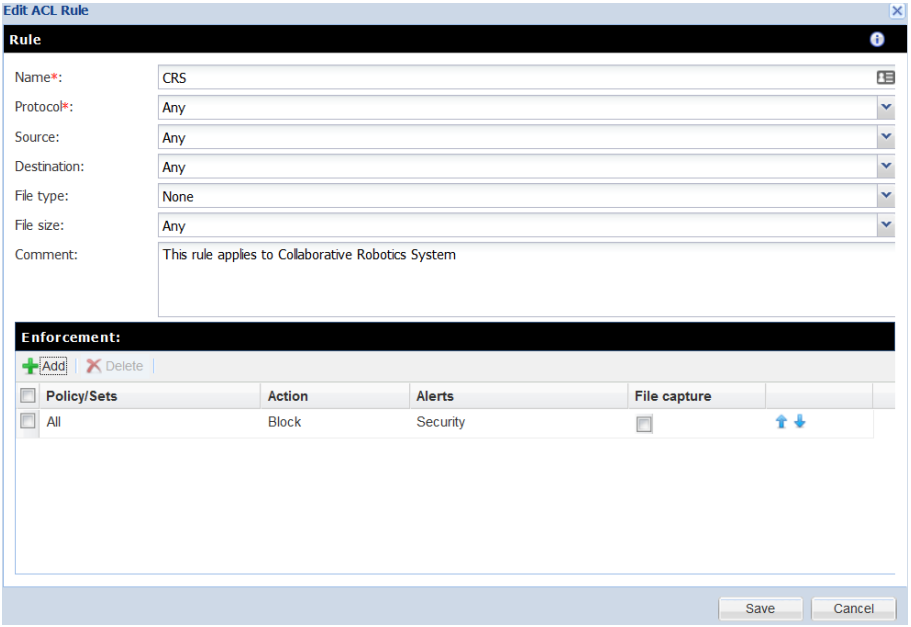
- Once selected you will see on the right current **ACL** Rules being applied.
- Click Add button. 

- A new window will appear titled **"Add New ACL Rule"**

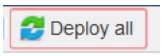


- Now type in a name for the new rule being created.
- Change Protocol to desire setting. This can be left to **"ANY"** which will look at all protocols passes thru the Inspector (*This may cause a performance impact on you Inspector installation depending on the number of clients within your organization*).
- **Source:** Choices are → **Any, IP Address, Hostname, Hostname (Custom), and Group (User/Computer)**.
- **Destination:** Choices are → **Any, IP Address, Hostname, Hostname (Custom), and Group (User/Computer)**.
- **File type:** Choices are → **None, All Files, Encrypted, and Extension**.
- **File Size:** Choices are → **Any,** and **Not more than**.

- **Comments:** Give a description of the rule being applied then click **Add** button.



- Once Add has been clicked you'll have an option to select a **"Policy/Sets"** to enforce. Default policies that are enforce are (Credit Card Number **CCN** and Social Security Numbers **SSN)**.
- Next, select the action to be taken. There are four choices, **Log**, **Block**, **S-Block**, and **Pass**.
- Now select if you would like additional personal to be notification upon rule violations.
- Finally, place a check in **File Capture** if you want to retain a copy of the offending data.
- Click **Save** to complete.
- Last step is to click on **Deploy all** button. This sends newly created policy to Inspector. This button will have a red blinking box around it is indicating required action.



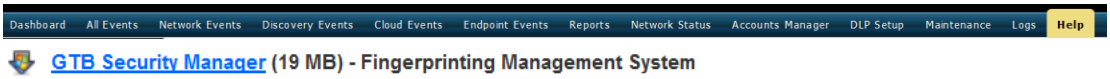
Useful Information:

- Once a new rule has been created double click on that rule to adjust the ordering from top to bottom by click the **UP** or **Down** arrows towards the right.
- Remember rules work from **Top → Down**, so think about ordering process. If unsure move the rule all the way to the top and then click **Deploy all** again.

How to Fingerprint Files using GTB Security Manager for DLP Protection

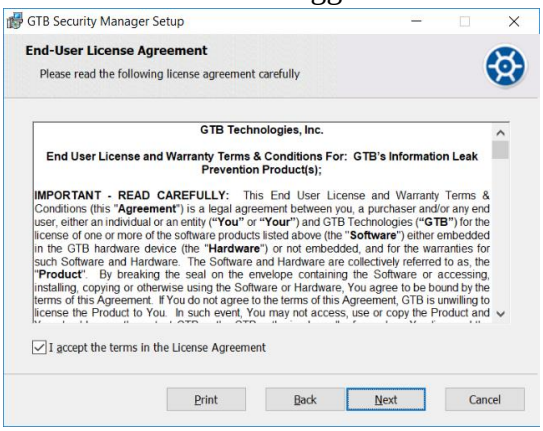
Download:

- First download "**GTB Security Manager"** by clicking on **Help** tab within Central Console server web portal then select "**GTB Security Manager"** link to start download.

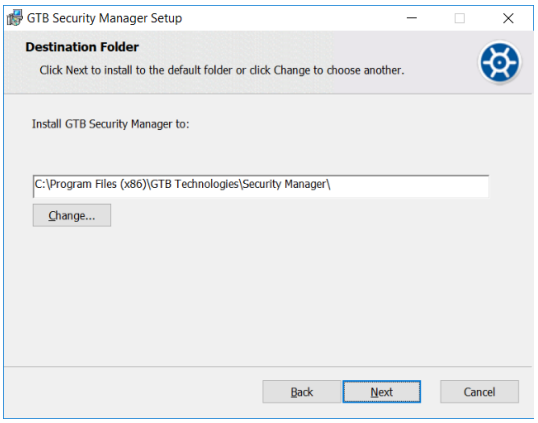


- Select location to save file being downloaded.
- Double click to start install for **"GTBSecurityManager_15.3.0.msi"** from location where file was saved to (version number might be different than one listed above).
- Once first screen appears click on **"Next"** to continue.

- Select Yes to License Aggreement and click **"Next"** to continue.

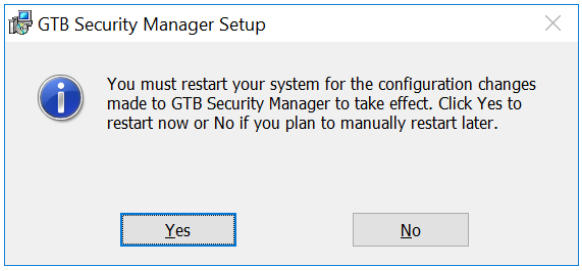


- Leave Destination Folder as default and Click **"Next"**



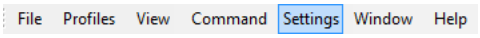
- Click **"Install"** to continue.

- When prompted by **User Access Control (UAC)** enter administrator password to continue install.
- If prompted to close Open Applications, select either option. Reboot is required if second option is selected.
- Click **"OK"** to continue.
- Once install has completed click **"Finish"** to complete install.
- If prompted to reboot, select **"Yes"**. MAKE SURE TO SAVE ALL OPEN FILES BEFORE SELECTING **"YES"**

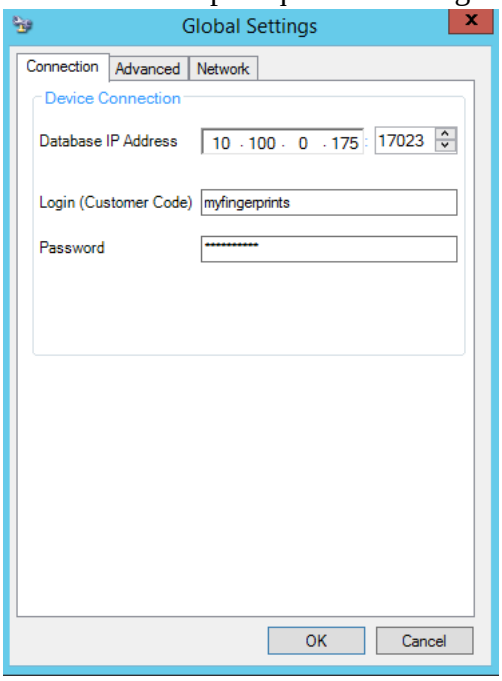


- Once machine has completed rebooting open **"GTB Security Manager"** by right click and selecting **"Run as administrator"**
- When prompted enter administrator password for application to start.

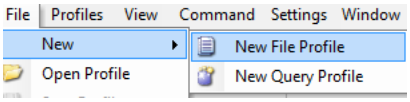
- Once "**GTB Security Manager"** has opened, click on setting button on menu bar.



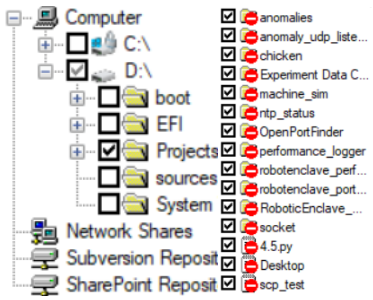
- Now enter the IP Address of where **"Central Console"** is installed. Login and password are already populated with default credentials from vendor. Both can be changed. See foot notes for additonal steps required to change Fingerprint Inspections login an password.



- Once IP Address has been enter click **"OK"** to save changes.
- Now, click on **File** from menu bar and select **New → New File Profile**

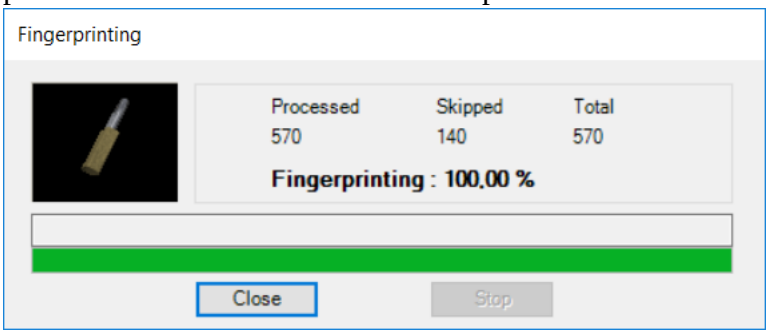


- A new window will appear allowing the ability to select files to be added. Files can be copied to **Local Machine**, or accessed from a **Network Share**, **Subversion Repositories,** or **SharePoint Respositories.**
- Select the folder, or files that need fingerprinting. Once a folder is selected all files within selected folder will recive a check mark indicating which files will be fingerprinted.

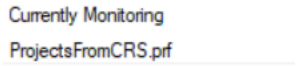


- Now click on floppy disk icon to save.
- Select location to save newly created profile.

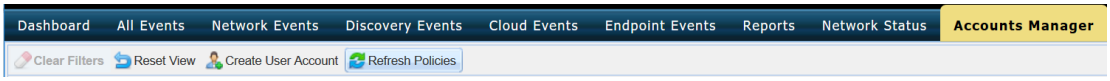
- Now the profile has been saved click the **padlock** icon to start fingerprinting process (Depending on the number of files being fingerprinted this can take a few minutes).
- To view the process see the Output screen that will display what files have been processed and there status. Once completed click **Close**



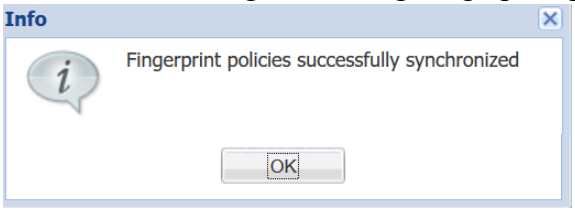
- Now look to the right side window for a tab labeled **"Profiles"** if this is missing click on **"View"** from menu bar and select **"Profiles Window"**. Click on Profile tab and a slide out appears show all the Profiles that can be monitored.
- Now select the Profile that was created earlier and right click, then select **Start Monitoring**.
- Once monitoring is enabled it'll appears under **"Currently Monitoring"** under help.



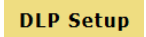
- Files that were included in fingerprinting profile will now have **ACL rules applied from Network DLP section from Central Console**.
- Login to **Central Console** and navigate to **Account Manager** Tab and click Refesh Polices.

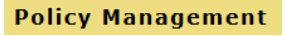


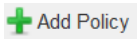
You'll see a message indicating Fingerprint polices successfully synchronized.



How to add policy to GTB Central Console for detecting fingerprinted files

- Login to Central Console
- Click on DLP Setup tab. 

- Now select Policy Management tab. 

- Now double click on Default to launch a new window.
- Click Add Policy. 

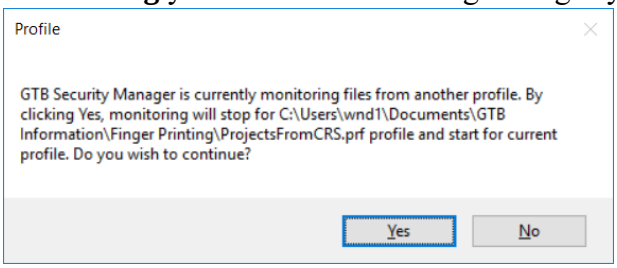
- Click drop down and select File. 

- Now click save button for setting to be applied.

All fingerprinted files from above steps will automatically be added to default Network DLP policy applied ACL. New Default values are **"SSN, CCN, and File"**

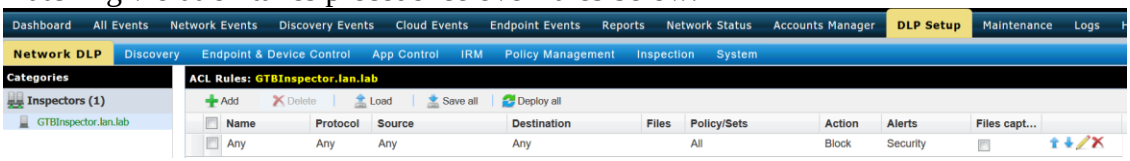
Additional Information for Fingerprinting:

- Recommended to configured **GTB Security Manager** to connect to IP address of DLP Inspector.
- Fingerprint only allows for one active Profile at a time. If another profile is set to **Start Monitoring** you'll receive a warning asking if you'd like to disable the active profile.



  - Recommendation would be to install **GTB Security Manager** on a machine that can be the central repositoiry for all fingerprinted files. Creating a large folder were the files can placed into for fingerprinting. Files don't have to remain in saved location once the profile has been fingerprinted and uploaded to **Central Console**. Access to fingerprinted files is only required when changes are made to profile containing said files.
- Although only one profile is able to monitored at a time you are able to define multiple Polices within that profile. This is useful since when a fingerprint violation is triggered it will be tagged with the Defined Policy name, which allows for easier usability.

Fingerprinted files follow **ACL Rules:** created within **Central Console** under **DLP Setup → Network DLP**. Rules are processed in order from top to bottom. This means the first rule with a matching violation takes precedence over rules below.



4.12.6 Highlighted Performance Impacts

No performance measurement experiments were performed for the installation of GTB into the CRS due to its location within the network topology. No workcell components involved with controlling the manufacturing process communicate across the boundary on a regular basis while the system is operational.

4.12.7 Link to Entire Performance Measurement Data Set

N/A

4.13 Graylog

4.13.1 Technical Solution Overview

Graylog is an open source log management tool. It can collect, parse and enrich logs, wire data, and event data from any data source. Graylog also provides centralized configuration management for 3rd party collectors such as beats, fluentd and nxlog. The processing pipelines allow for greater flexibility in routing, blacklisting, modifying and enriching messages in real-time as they enter Graylog. It has a powerful search syntax to help query exactly what we are looking for. With Graylog one can even create dashboards to visualize metrics and observe trends in one central location.[21]

Points to consider

- Open source product with good community support
- Easy to setup and customize. Support log collection from any OS platform.
- It is packaged for major Linux distributions, has a VM ready for use and Docker images are also available.
- The dashboard part, even if though well integrated and useful, lacks many features and visualizations contained in other elastic search tools such as Kibana (like aggregations).

4.13.2 Technical Capabilities Provided by Solution

Graylog provides components of the following Technical Capabilities described in Section 6 of Volume 1:

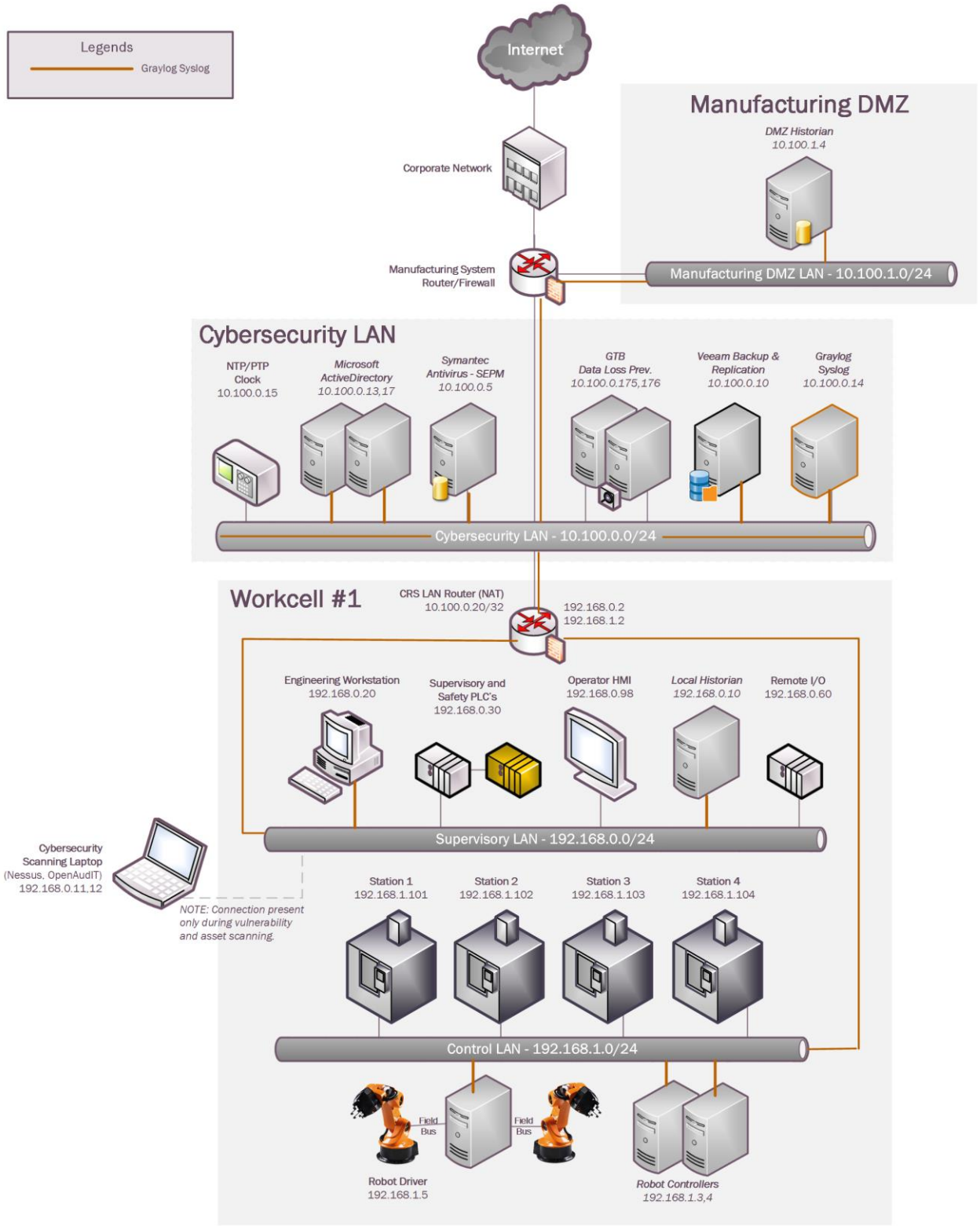
- Network Monitoring
- Event Logging
- Forensics

4.13.3 Subcategories Addressed by Implementing Solution

PR.DS-4, PR.PT-1, DE.AE-2, DE.AE-3, DE.CM-1, DE.CM-6, DE.DP-3, RS.AN-3

[21] Graylog Documentation http://docs.graylog.org/en/3.0/

4.13.4 Architecture Map of Where Solution was Implemented



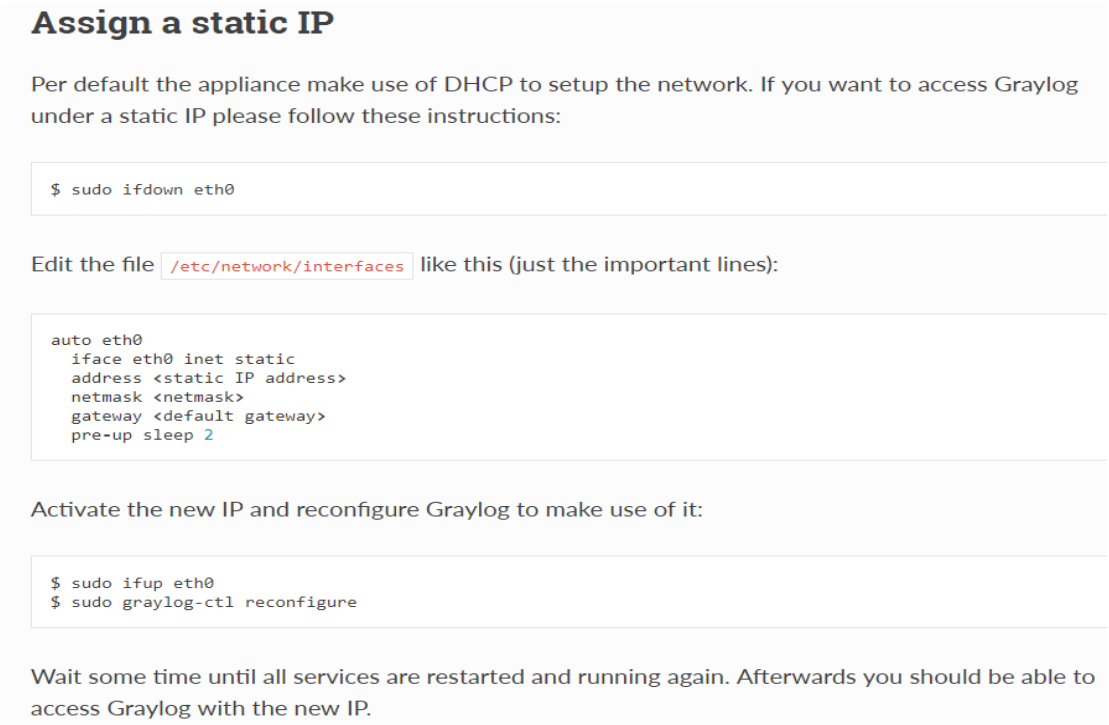
4.13.5 Installation Instructions and Configurations

Details of the solutions implemented:

Name	Version	Daily volume of logs	Server
Graylog Enterprise	2.4.6	< 5GB per day	Ubuntu 14

Setup:

- Download the installation package from the Graylog website (https://www.graylog.org/). Graylog can be installed on any flavor of Linux. In addition, Graylog also provides a preconfigured virtual machine for **non-production** environments. This virtual machine template (OVA) file was used in our environment.
- The OVA file was deployed on a Microsoft Hyper-V host server in our Cybersecurity LAN network.
- The Graylog server receives all syslog traffic by default on UDP port 514, accordingly UDP 514 was permitted in the firewall rules. Additional ports are required to be allowed if utilizing other features of Graylog as described in the documentation.
- Upon deploying the OVA file, the virtual machine will default to a DHCP IP address. Login to the system to assign it a static IP address as per below shown instructions.



Assign a static IP

Per default the appliance make use of DHCP to setup the network. If you want to access Graylog under a static IP please follow these instructions:

```
$ sudo ifdown eth0
```

Edit the file `/etc/network/interfaces` like this (just the important lines):

```
auto eth0
  iface eth0 inet static
  address <static IP address>
  netmask <netmask>
  gateway <default gateway>
  pre-up sleep 2
```

Activate the new IP and reconfigure Graylog to make use of it:

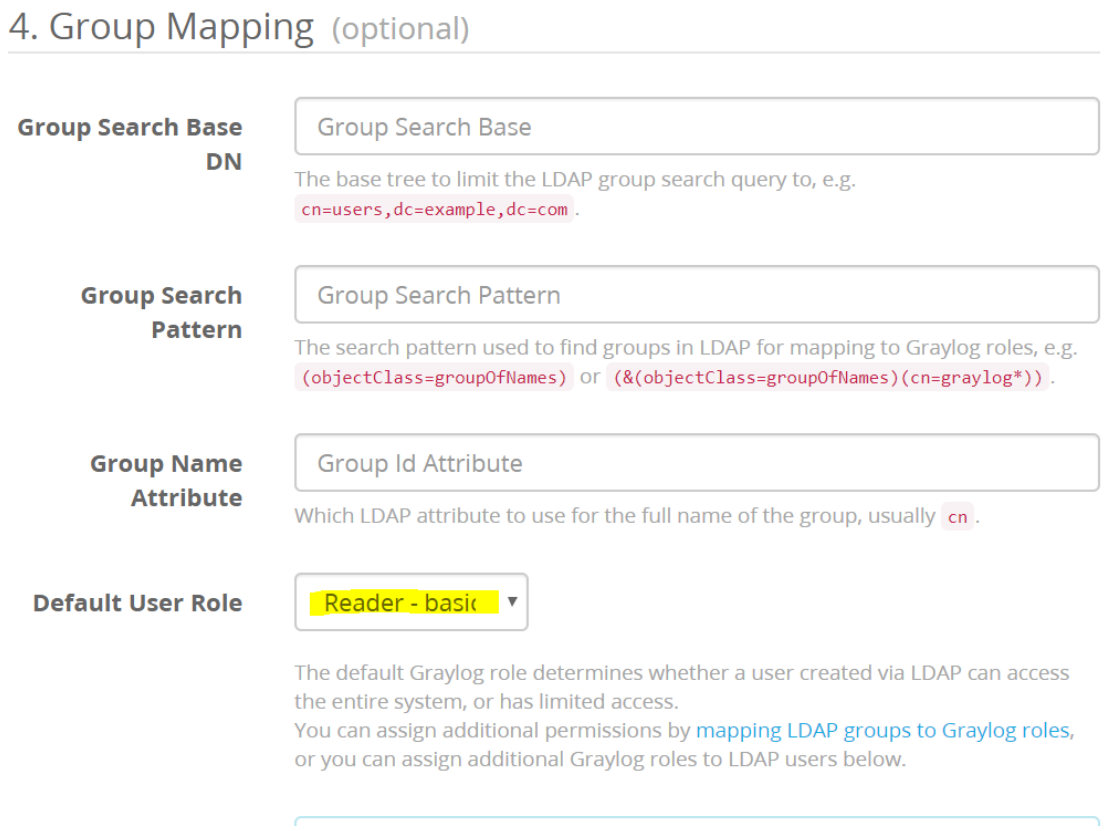
```
$ sudo ifup eth0
$ sudo graylog-ctl reconfigure
```

Wait some time until all services are restarted and running again. Afterwards you should be able to access Graylog with the new IP.

- Login to the Web Interface using the default credentials and change the admin password.

- Active Directory (AD)-integration is supported in Graylog. To configure, on the Top Menu Bar Click on **System** >> **Authentication**. On the Authentication Management page, click on **LDAP / Active Directory** and fill out the AD server details**.** Detailed instructions can be found in product documentation.[22]

    - Note: Any AD domain user that's added is assigned "**Reader**" access by default. This can be changed by configuring **Group Mapping** options in the same page. Change the Default User Role depending on your requirement. Adding permissions can be assigning by clicking on **LDAP Group Mapping** button on the same page



Configuration:

Syslog on Linux servers:

[22] Configuring External Authentication in Graylog
http://docs.graylog.org/en/2.3/pages/users_and_roles/external_auth.html?highlight=ldap

- The "**rsyslog**" package on Linux was leveraged to forward logs out of all Linux hosts in the Robotics system to the Graylog server. Rsyslog is by default present in all Linux distributions. Configure the **/etc/rsyslog.conf** file to enable forwarding the logs to the IP address of the Graylog server. Detailed instructions can be found here: https://marketplace.graylog.org/addons/a47beb3b-0bd9-4792-a56a-33b27b567856

- Below is a snippet of a **/etc/rsyslog.conf file** from one of the Linux servers. Restart the rsyslog service once the rsyslog.conf file is modified.

```
# Graylog configuration
*.* @10.100.0.14:514;RSYSLOG_SyslogProtocol23Format
root@gitlab:/home/icssec#
```

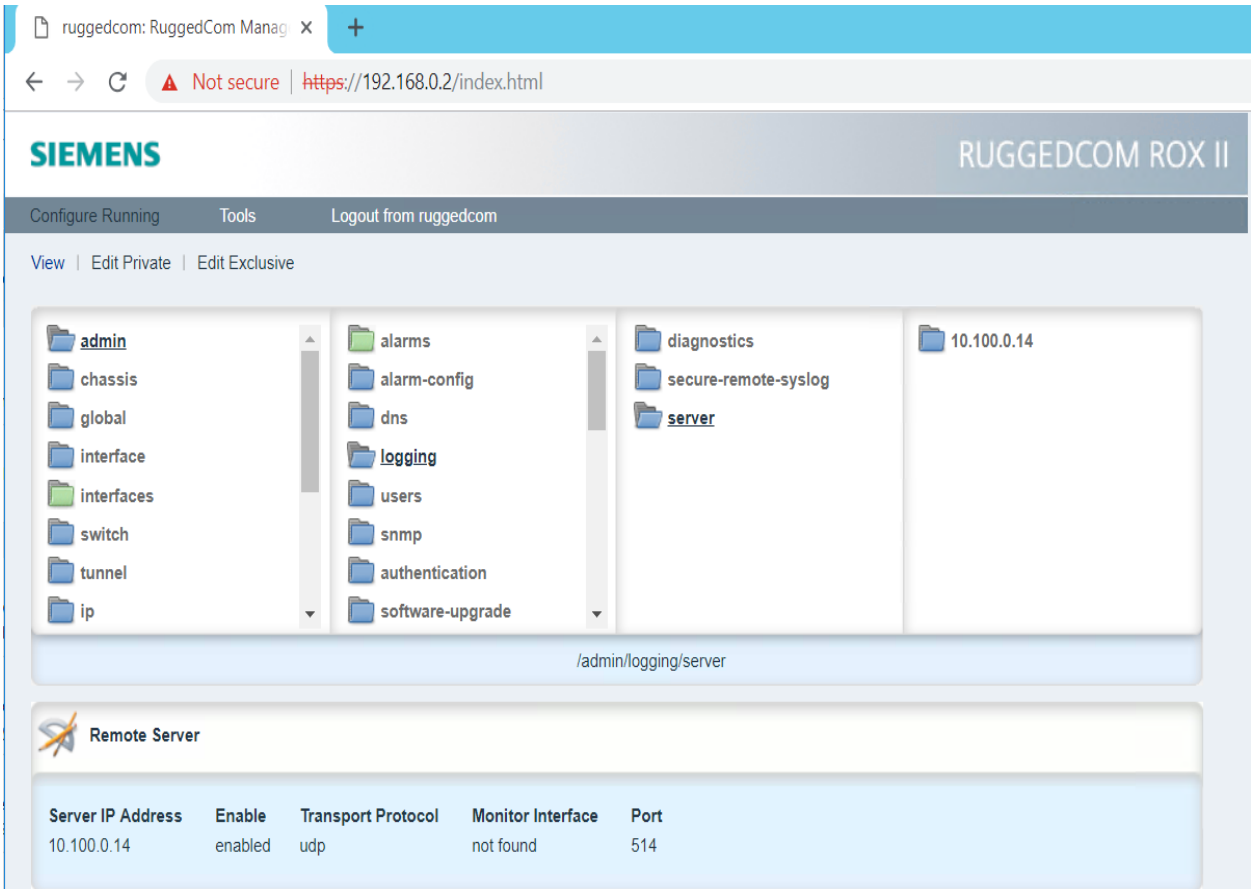
You should now begin to receive syslog data in Graylog from this client. Login to the Graylog Web UI and search for the asset / server name in the dashboard to view these logs. The corresponding Linux device will also be listed under "**Sources**" page when its actively forwarding the data.

Syslog on the Boundary Firewall (RuggedCom):

- Most of the firewall devices available today support syslog capabilities. This can be configured by either by setting it up from command line via SSH or from the Web Interface of the Firewall device. Ensure **UDP 514** is allowed between the firewall and Graylog server.

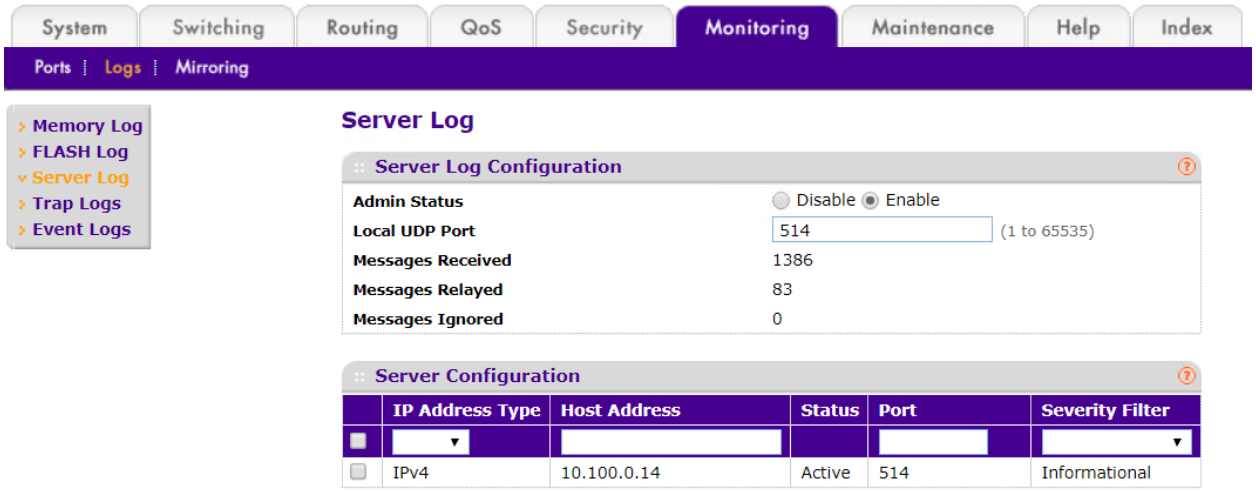
- Similarly, the RuggedCom boundary router/firewall device in Robotics system was configured to send syslog traffic to Graylog. Below screenshots reference the syslog setting on the RX1510 appliance where **10.100.0.14** is the IP address of our Graylog server. The log level was set to "**Informational and above**".
  Detailed instructions can be found in the product manual.[23]

[23] http://www.plcsystems.ru/catalog/ruggedcom/doc/ROXII_RX1500_User-Guide_WebUI_EN.pdf



Syslog on the Network Switches:

- Both the network switches (Netgear and Siemens i800) were configured to log to the Graylog server. The below image shows Syslog server configuration on the Netgear SW pointing to the IP address of the Graylog server.

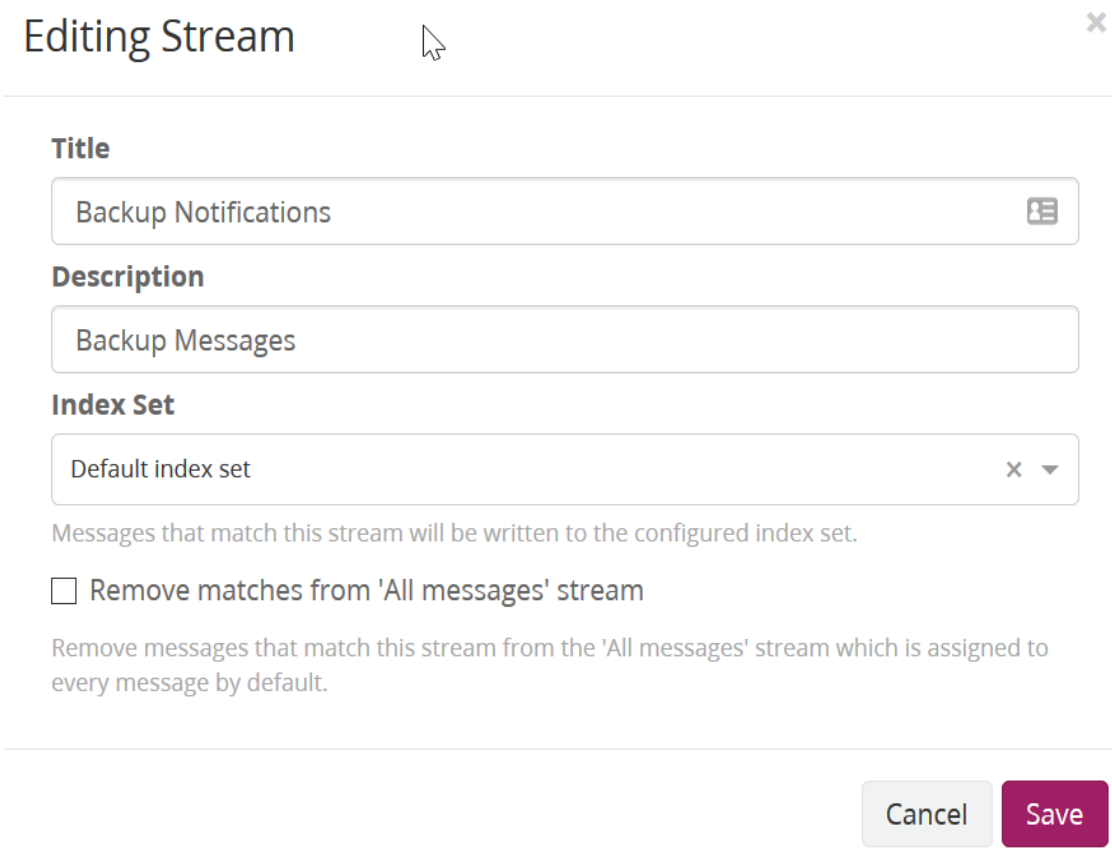


4711

4712

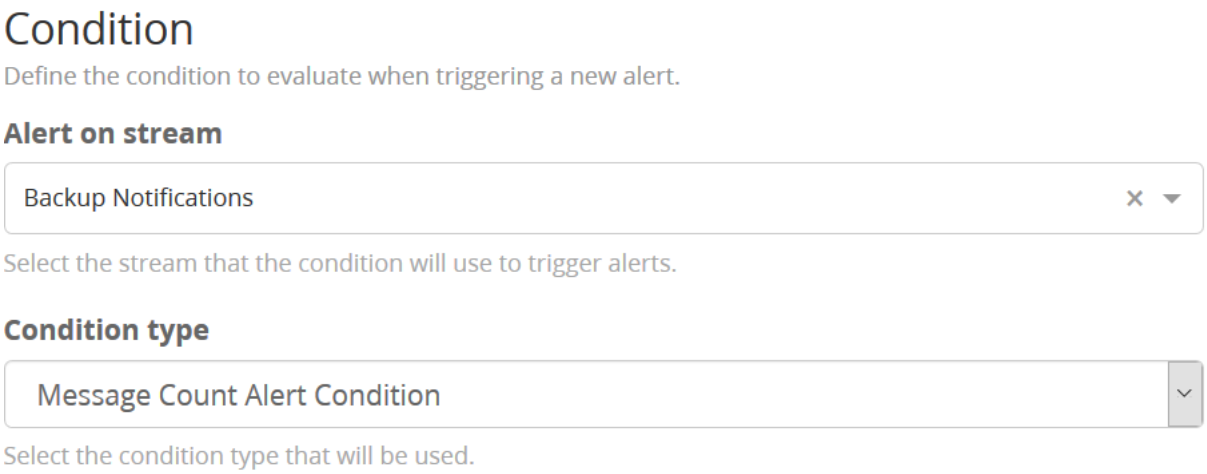
4713 Configuring Email Notifications for Alert conditions:

4714 • You can create email alerts for any custom events, alert condition as per your requirement.
4715 Below process show how our Graylog was configured to send out email notifications, for any
4716 Veeam backup events that it received from the Linux machines. Follow this process to
4717 define your custom alert conditions
4718 • There are multiple configuration settings required for email notification to work – Creating a
4719 **stream**, adding an **alert condition** and creating a **notification**.
4720 • To create a stream, click on **Streams** on the Top-Menu >> **Create a Stream >>** Enter Title,
4721 Description, and Index Set which should default to "**Default index set**"
4722 • Click **Save** to save the changes
4723



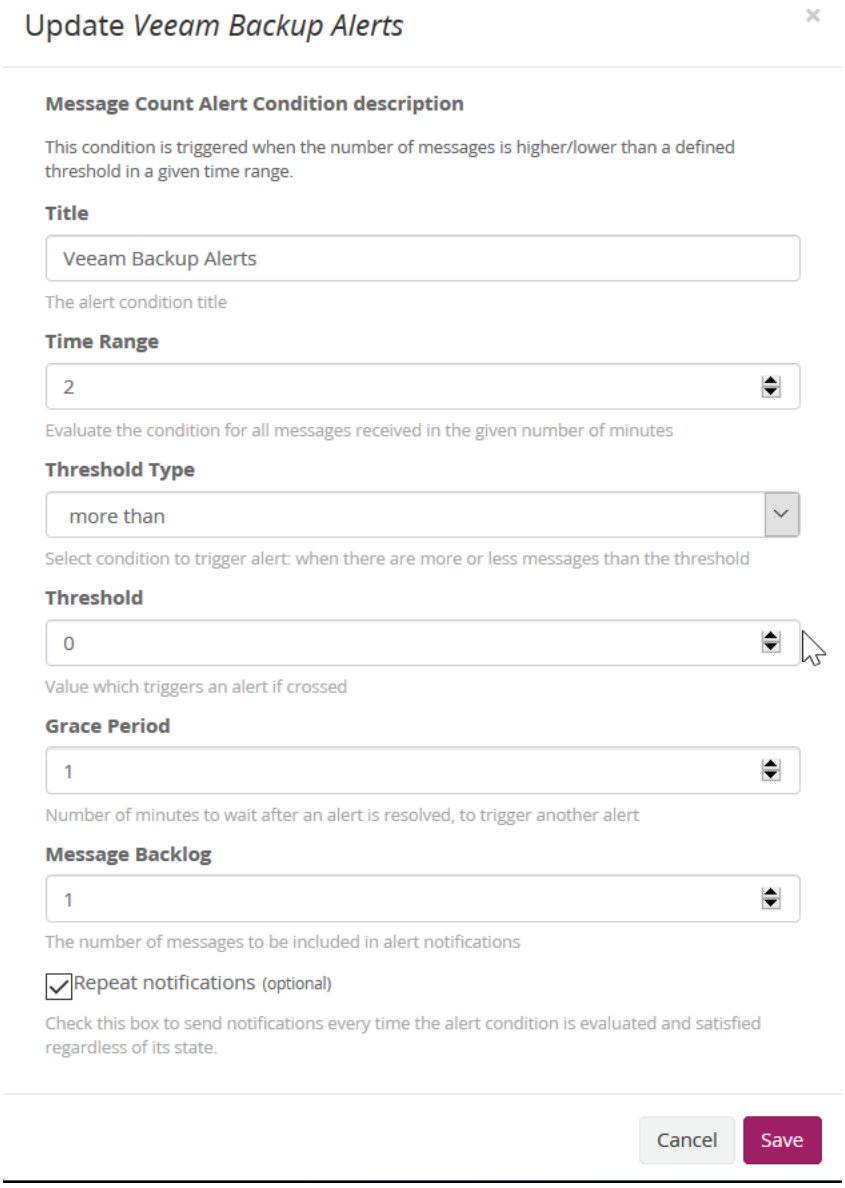
- Next, click on "**Alerts**" options on the top menu >> Click on **Manage conditions** >> Click on  to define a condition.

- Click drop menu under "**Alert on Stream**" and select the stream created earlier. Click on "**Condition Type**" menu drop down and select "**Message Count Alert Condition"**



- Click "**Add Alert Condition"**. Once window appears fill out the required information.

- Click **Save** to complete (See below for example of current Message Count Alert Condition).



- Now create a **notification**.
  - Click on "**Manage notifications**" blue button in upper right-hand corner.
  - Click green button for "**Add new notification**"
  - Under "**Notify on Stream"** select notification created earlier from drop down menu.
  - Under "Notification type" select "Email Alert Callback" from drop down menu.
  - Click "Add alert notification" button
  - Title: "Veeam Backup Alerts"

- Email Subject: “Successful Veeam Backup source: ${foreach backlog message}${message.source}${end}” without the quotes, see below for screen shot of current callback wording.
- Sender: < sender address >
- E-mail Body: “This can be adjusted as required”

Alert Description: ${check_result.resultDescription}
Date: ${check_result.triggeredAt}
Stream ID: ${stream.id}
Stream title: ${stream.title}
Stream description: ${stream.description}
Alert Condition Title: ${alertCondition.title}

${if backlog}Last messages accounting for this alert:
${foreach backlog message}${message}

${end}${else}<No backlog>
${end}

- User Receivers: “Select a Graylog user if desired”
- Email Receivers: “Enter email address for individuals receiving these alerts”
- Click **Save**

- Test new Streams / Alerts / Notifications to ensure they are configured correctly.

4.13.6 Highlighted Performance Impacts

Two performance measurement experiments were performed for the Graylog tool while the manufacturing system was operational:

1. CL003.1 - Syslog service was installed and running on CRS network hosts, and all generated syslog messages were forwarded from CRS hosts to Graylog server.
2. CL003.2 - Syslog forwarding to Graylog was configured on CRS networking devices.

4.13.6.1 Experiment CL003.1

The rsyslog service was installed and configured on CRS hosts to forward all syslog messages to the Graylog server. A total of 13 syslog packets were transmitted during the experiment by the rsyslog service on all CRS hosts (see Figure 4-48).

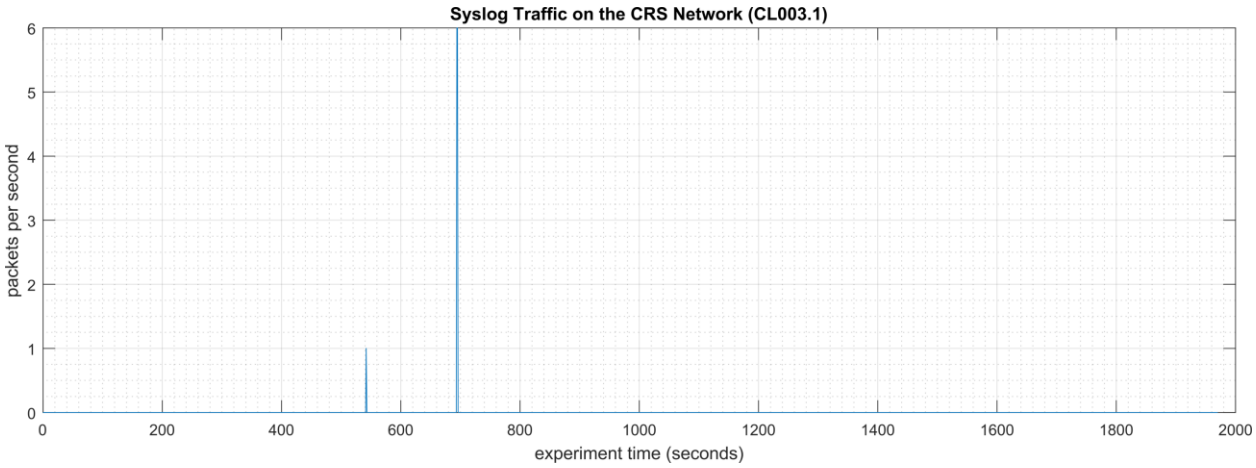


Figure 4-48 - Time series plot showing the rate of syslog network traffic (in packets per second) transmitted during the CL003.1 experiment.

No performance impact to the manufacturing process was measured during the experiment.

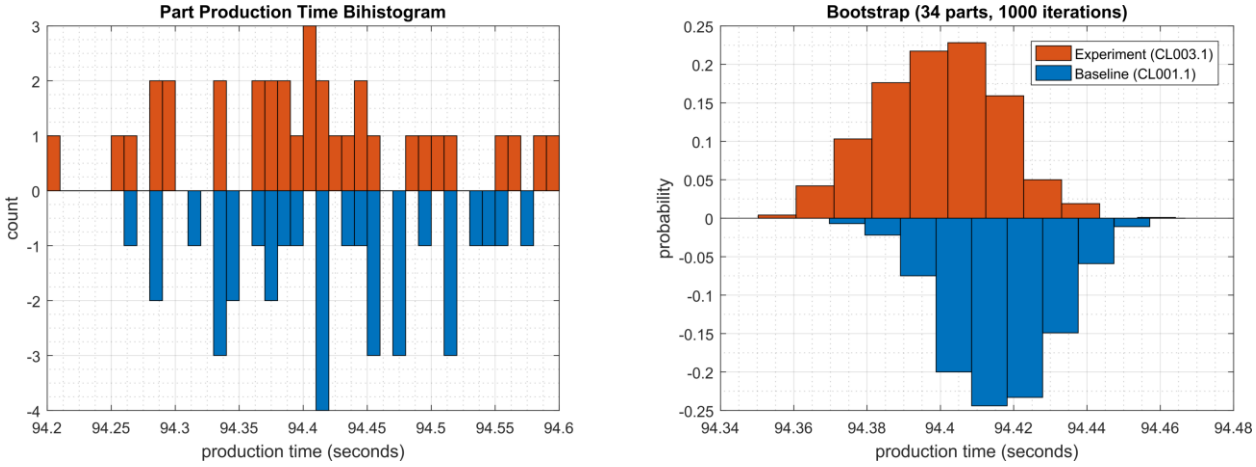


Figure 4-49 - Bihistograms showing the part production time (left) and estimated mean production time using the bootstrap method (right) using the measurements from baseline CL001.1 and experiment CL003.1.

4.13.6.2 Experiment CL003.2

The rsyslog service was installed and configured on CRS networking devices to forward all syslog messages to the Graylog server. A total of 28 syslog packets were transmitted during the experiment by the rsyslog service from CRS hosts and networking devices (see Figure 4-50).

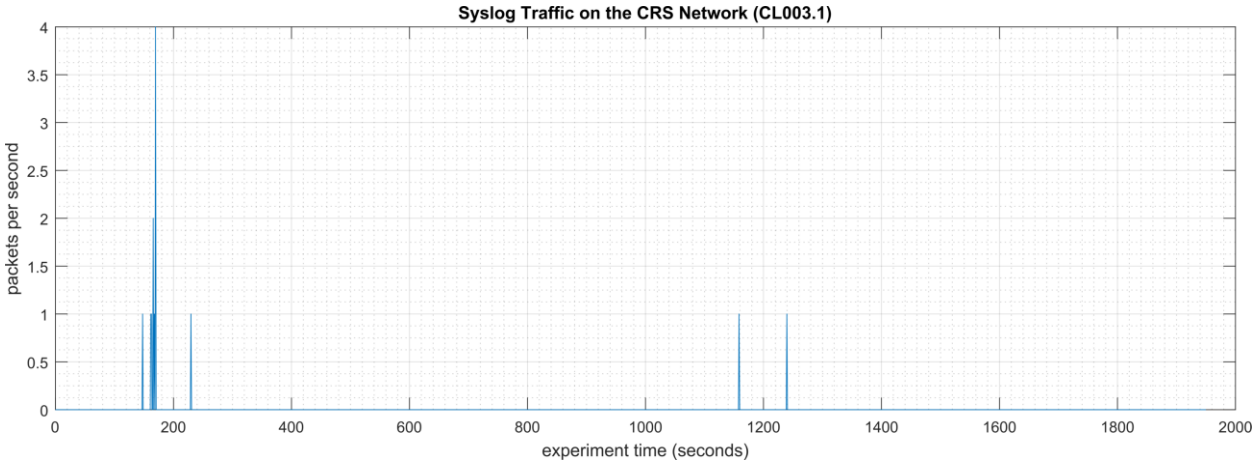


Figure 4-50 - Time series plot showing the rate of syslog network traffic (in packets per second) transmitted during the CL003.2 experiment.

No performance impact to the manufacturing process was measured during the experiment.

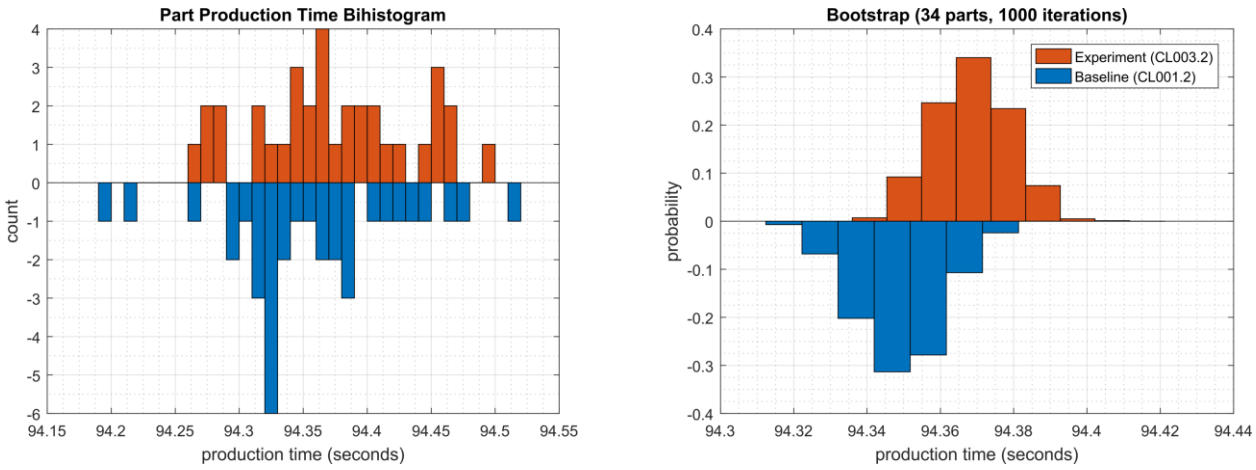


Figure 4-51 - Bihistograms showing the part production time (left) and estimated mean production time using the bootstrap method (right) using the measurements from baseline CL001.1 and experiment CL003.2.

4.13.7 Link to Entire Performance Measurement Data Set

- **CL003.1-Syslog.zip**
- **CL003.2-Syslog.zip**

4.14 DBAN

4.14.1 Technical Solution Overview

DBAN is a free open source data wiping utility allowing the ability to sanitize hard drives to ensure data is not left behind when drives are beginning decommissioned and prepared for removal from on premise. DBAN and other hard drive sanitization tools only work with spinning hard drives, SSD hard drives and other flash media refer to vendors for specific directions for sanitizing media before removing from company control.

4.14.2 Technical Capabilities Provided by Solution

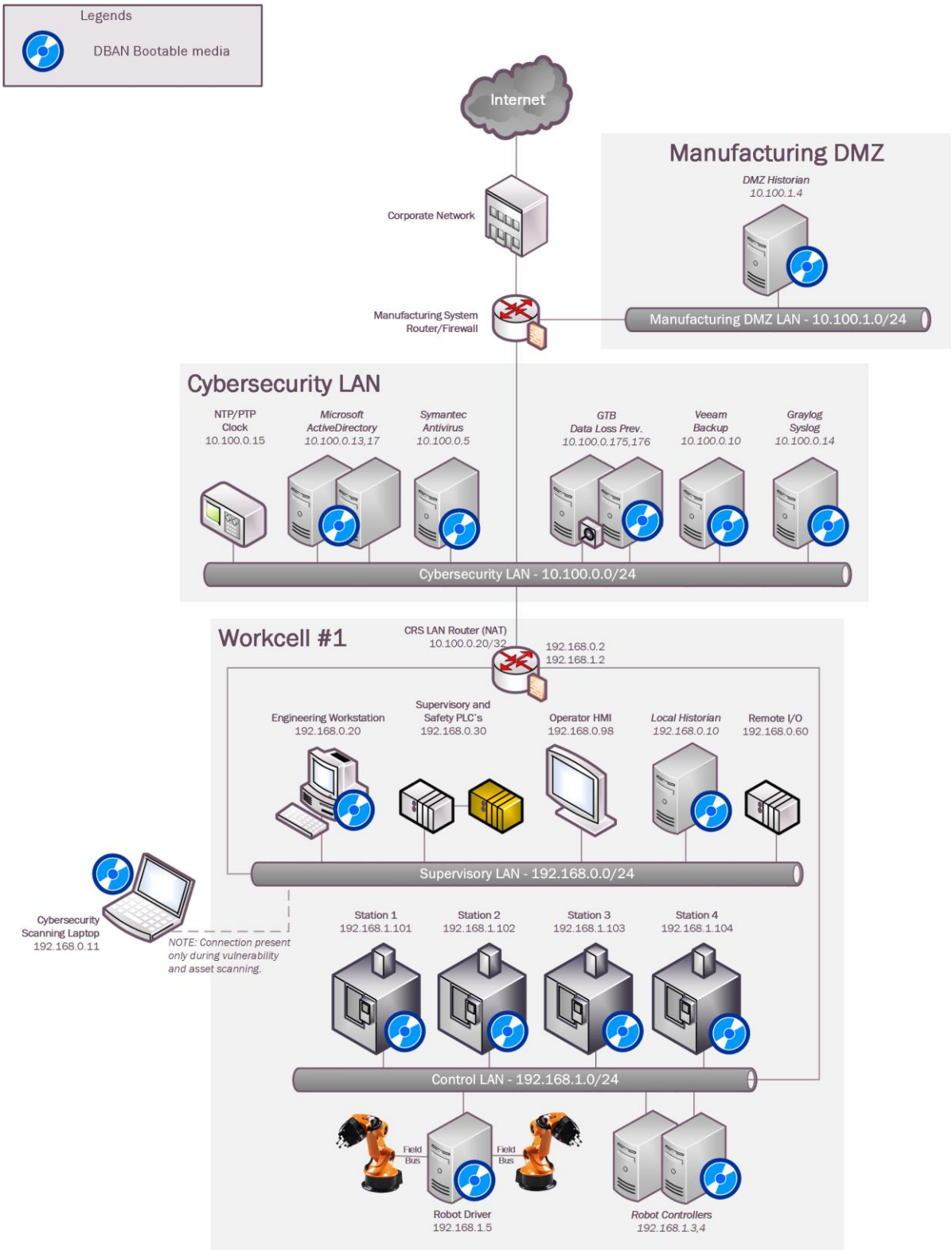
DBAN provides components of the following Technical Capabilities described in Section 6 of Volume 1:

- Media Sanitization

4.14.3 Subcategories Addressed by Implementing Solution

PR.DS-3, PR.IP-6

4.14.4 Architecture Map of Where Solution was Implemented



4.14.5 Installation Instructions and Configurations

Instructions for installing DBAN and use

Download:

DBAN can be downloaded from https://dban.org

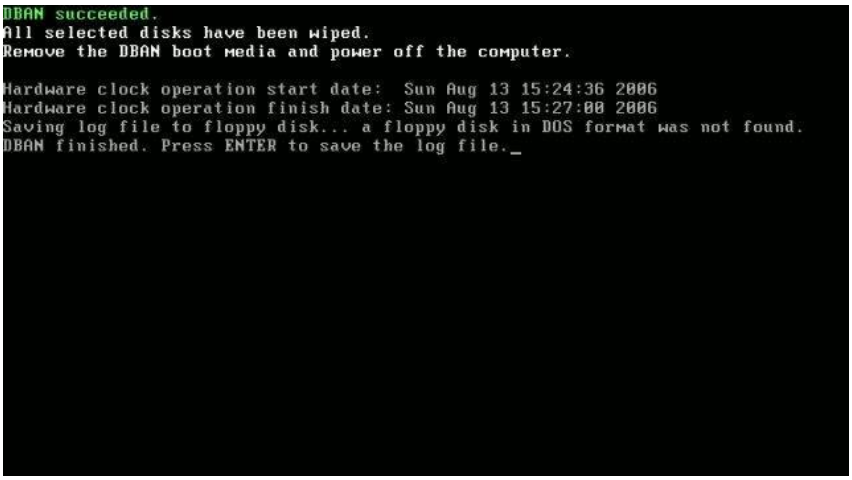
Click download link which redirects the page and a pop will appear to start download process for ISO image file **"dban-2.3.0_i586.iso".**

Download ISO file and burn to CD/DVD, or USB drive using widely available ISO bootable utilities.

Instructions:

1. Once ISO has been burned to bootable media go to device requiring sanitization.
2. Power on machine and boot from USB or CD/DVD depending on the install option from earlier steps above. **(Change Boot order in BIOS if no option for Boot Menu is available during machine power-up)**
3. Once machine has booted from media select desire option for media sanitization.

4. Select option to continue. Default sanitization mode is "**short DoD 5520.22-M**", but this can be changed depending on the level your security program indicates.
5. Follow menu options to start wiping process.
6. Once wipe had completed you will see a screen like the image below.



7. Once sanitization has completed, remove hard drive from device and label wiped ready for disposal.

Lesson Learned and thing to know:

Not all hard drives are able to be wiped clean using this sanitization method. Media that is either SSD or flash memory is written differently than spinning drives, so follow SSD/Flash media vendors' recommendations for proper media sanitization for all non-spinning hard drives.

4.14.6 Highlighted Performance Impacts

No performance measurement experiments were performed for the use of DBAN due to its typical installation and usage location.

4.14.7 Link to Entire Performance Measurement Data Set

N/A

4.15 Network Segmentation and Segregation

4.15.1 Technical Solution Overview

Network segmentation and segregation solutions enable a manufacturer to separate the manufacturing system network from other networks (e.g., corporate networks, guest networks), segment the internal manufacturing system network into smaller networks, and control the communication between specific hosts and services.

Each Router's native capabilities were leveraged to implemented network segmentation.

4.15.2 Technical Capabilities Provided by Solution

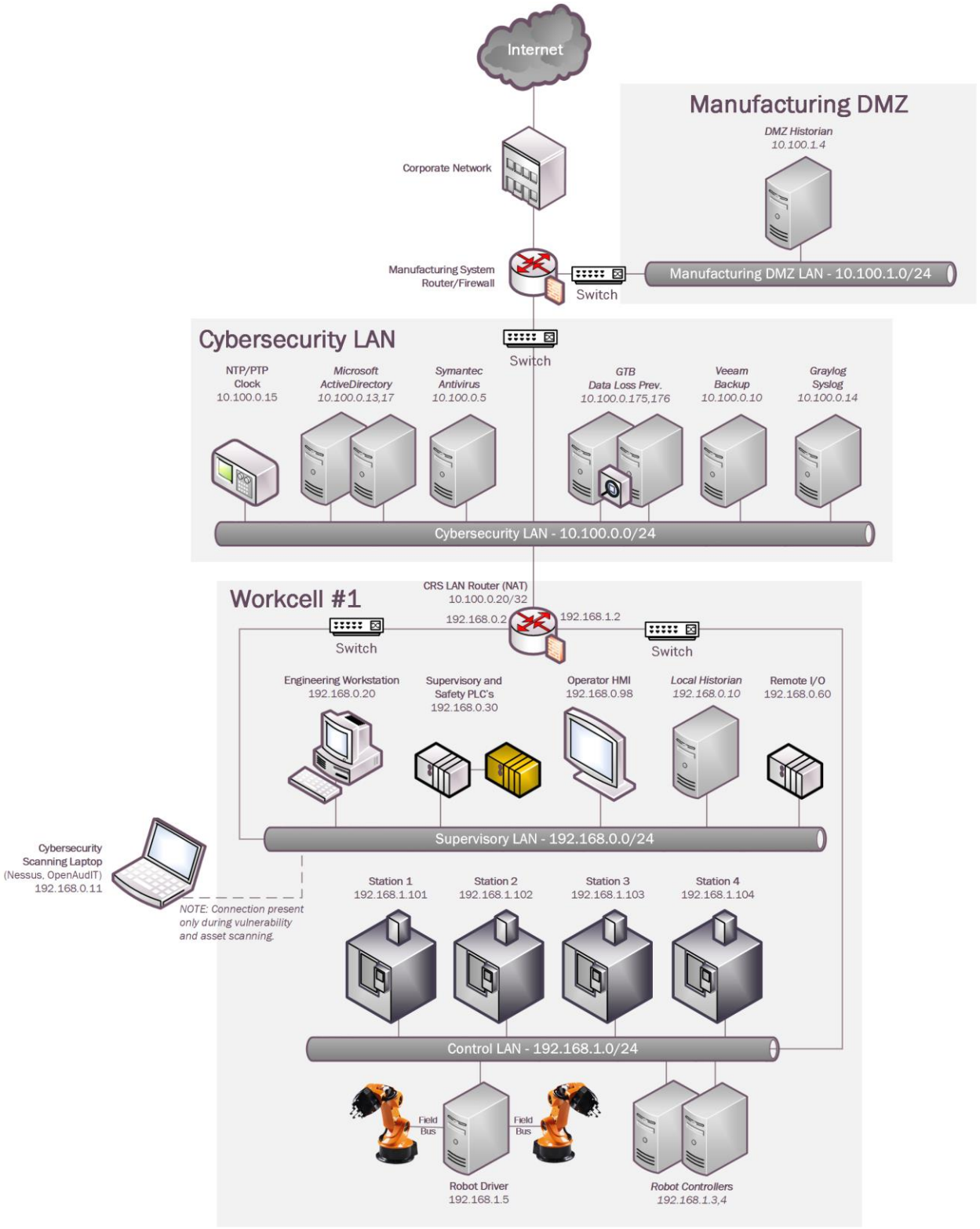
Network Segmentation and Segregation provides components of the following Technical Capabilities described in Section 6 of Volume 1:

- Network Segmentation and Segregation

4.15.3 Subcategories Addressed by Implementing Solution

PR.AC-5

4.15.4 Architecture Map of Where Solution was Implemented



4.15.5 Installation Instructions and Configurations

The following devices were involved in implementing Network Segmentation

Device	Details	Location
Cisco-ASA 5512	NGFW, running Firepower Services FTD 6.2.3	Manufacturing System
RuggedCom RX1510	Firewall, Router	Work cell

- **Segmentation in the Cybersecurity LAN:**

Following is a list of interfaces created on the Boundary Router/Firewall – Cisco ASA of the Cybersecurity LAN network

Interface	IP address of Interface	Subnet	Description
GE 0/0	129.6.66.x	129.x.x.x/x	Uplink to Corporate
GE 0/1	10.100.0.1	10.100.1.0/24	Cybersecurity LAN
GE 0/2	129.6.1.x	129.x.x.x/x	VPN users
GE 0/3	10.100.2.1	10.100.2.0/24	Management LAN
GE 0/4	10.100.1.1	10.100.0.0/24	Manufacturing DMZ LAN

- **Segmentation in the Work Cell:**

- The Work Cell consists of the following network devices.

Type	Description
RuggedCom RX Firewall	Boundary protection firewall, router
Siemens i800 Switch	Layer-2 Switch for the Control Network
Netgear GS724T Switch	Layer-2 Switch for the Supervisory Network

- Network segmentation was implemented using the RuggedCom firewall. The firewall has the following interfaces defined. There were two subnets created as listed in the below table.

Interface	IP address of Interface	Subnet	Description
Ge-2-1	192.168.1.2	192.168.1.0/24	Control LAN Network
Ge-2-2	N/A	N/A	Mirror Port
Ge-3-1	192.168.0.2	192.168.0.0/24	Supervisory LAN Network
Ge-3-2	10.100.0.20	N/A	Uplink to Cybersecurity LAN

- The Siemens i800 switch is connected to the Ge-2-1 interface of the RX1510 and used for the Control LAN network. Devices connected to this i800 switch such as the 4 Machining stations, Robot Driver server were assigned an IP address from the Control LAN subnet (192.168.1.0/24).

- The Netgear switch is connected to the Ge-3-1 interface of RX1510 and used for the Supervisory LAN network. Devices connected to this switch such as the PLC, HMI, Engineering workstation were accordingly assigned an IP address from this Supervisory LAN subnet (192.168.0.0/24)

4.15.6 Highlighted Performance Impacts

No performance measurement experiments were performed for network segmentation due to it being implemented on the CRS before the Manufacturing Profile implementation was initiated.

4.15.7 Link to Entire Performance Measurement Data Set

N/A

4.16 Network Boundary Protection

4.16.1 Technical Solution Overview

Boundary Protection devices are implemented to monitor and control connections and communications at the external boundary and key internal boundaries within the organization. Boundary protection mechanisms include for example, Routers, Firewalls, Gateways, Data diodes separating system components into logically separate networks and sub networks.

4.16.2 Technical Capabilities Provided by Solution

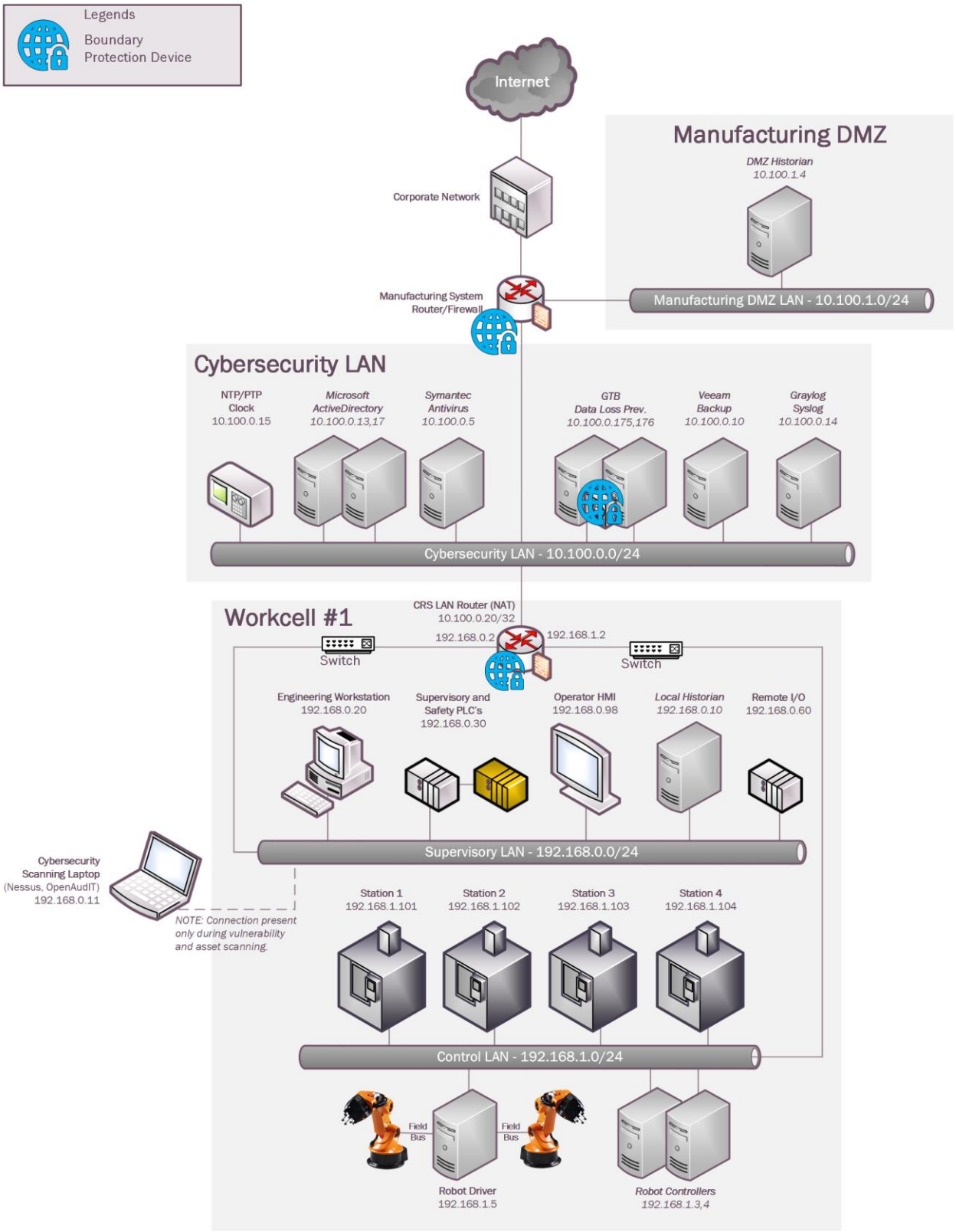
Network Boundary Protection provides components of the following Technical Capabilities described in Section 6 of Volume 1:

- Network Boundary Protection

4.16.3 Subcategories Addressed by Implementing Solution

PR.AC-5, PR.PT-4, DE.CM-1

4.16.4 Architecture Map of Where Solution was Implemented



4.16.5 Installation Instructions and Configurations

Setup:

The following devices were implemented for Boundary protection in the CRS System

Device	Details	Location
Cisco-ASA 5512	NGFW, running Firepower Services FTD 6.2.3	Manufacturing System
RuggedCom RX1510	Firewall + Router running ROS 2.12.2	Work cell
GTB Inspector	Data Loss Prevention (DLP) virtual appliance	Cybersecurity LAN

- **Configuration on Cisco-ASA**:

The following features, settings were enabled on the ASA firewall

- Network Segmentation
- ACL Rules
- NAT policy for Internet access
- Snort Inspection
- DMZ network

Network Segmentation

Separate network interfaces were configured for the different network segments as listed below

- Inside Interface (Network: 10.100.0.0/24)
- DMZ Interface (Network: 10.100.1.0/24)
- Outside Interface (Uplink to NIST Corporate for Internet)
- Management interface (out of scope)

Access Control List (ACL) rules

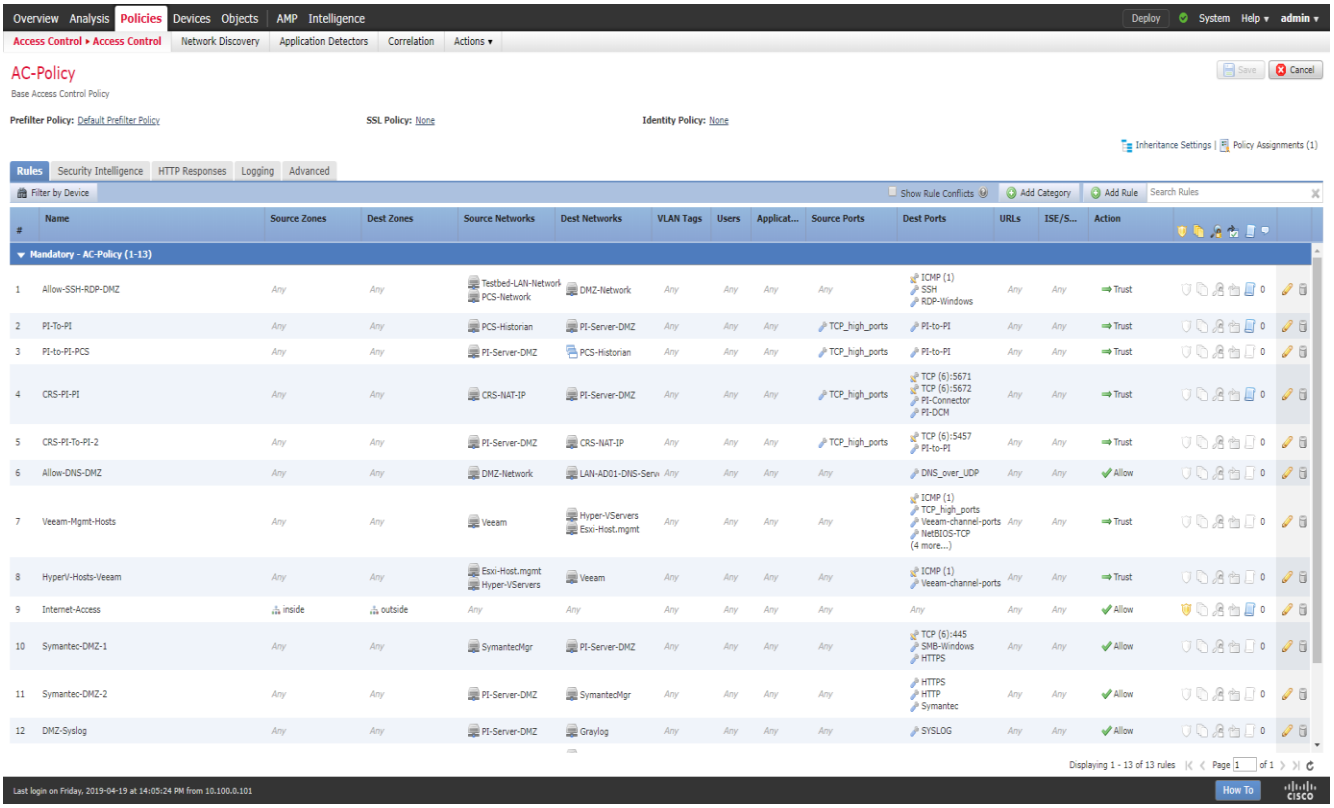
The following ACL rules were put in place on the ASA with a default Action to **Block all traffic**.

4939

Source	Source Port	Destination	Dest Ports	Protocol	Action
10.100.0.0/24,	Any	DMZ network	SSH,RDP,ICMP	TCP	Trust
DMZ Historian	TCP_High _Ports	PCS-Historian	5450	TCP	Trust
CRS-NAT (10.100.0.20)	TCP_High _Ports	DMZ-Historian	5450, 5460, 5671, 5672	TCP	Trust
DMZ Historian	TCP_High _Ports	CRS-NAT (10.100.0.20)	5457, 5450	TCP	Trust
DMZ Historian	Any	Active Directory (10.100.0.17)	53	UDP	Allow
Veeam Server	Any	Hyper-V Host servers, Esxi Host Server	NETBIOS, ICMP, HTTPS, 445, TCP_High_port, 2500-5000, 6160-6163	TCP	Trust
Hyper-V Host Servers, Esxi Host Server	Any	Veeam Server	ICMP, 2500-5000	TCP	Trust
inside_interface	Any	outside_interface	Any	Any	Allow
DMZ Historian	Any	Symantec Server	SMB (445), HTTPS	TCP	Trust
Symantec Server	Any	DMZ Historian	HTTP, HTTPS, 8014	TCP	Trust
DMZ Historian	Any	Graylog Server	514	UDP	Trust

4940

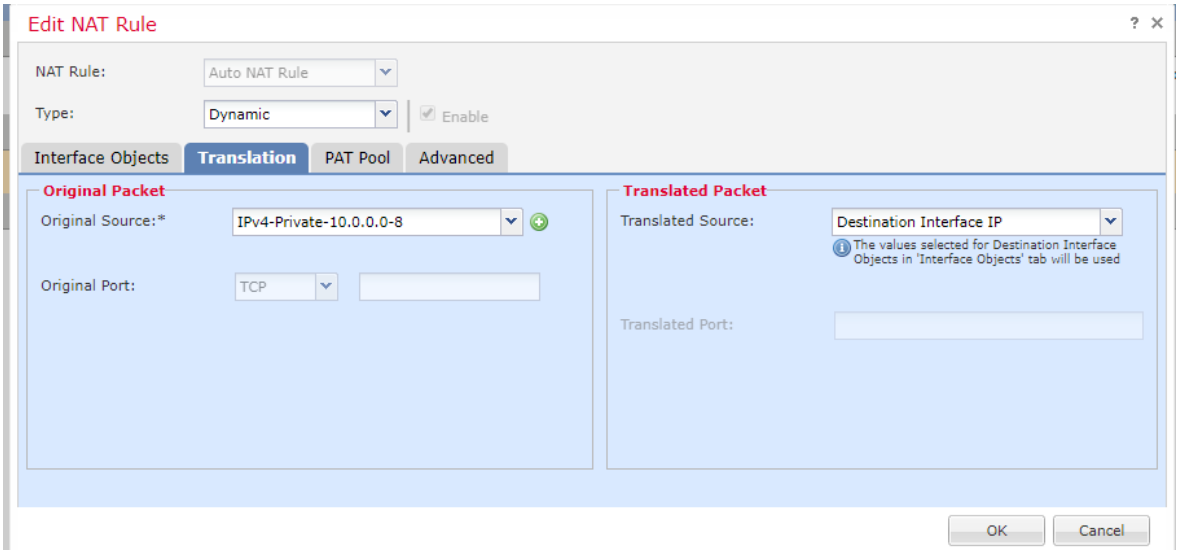
4941



NAT Policy

- A Dynamic NAT policy was configured to allow internet access.

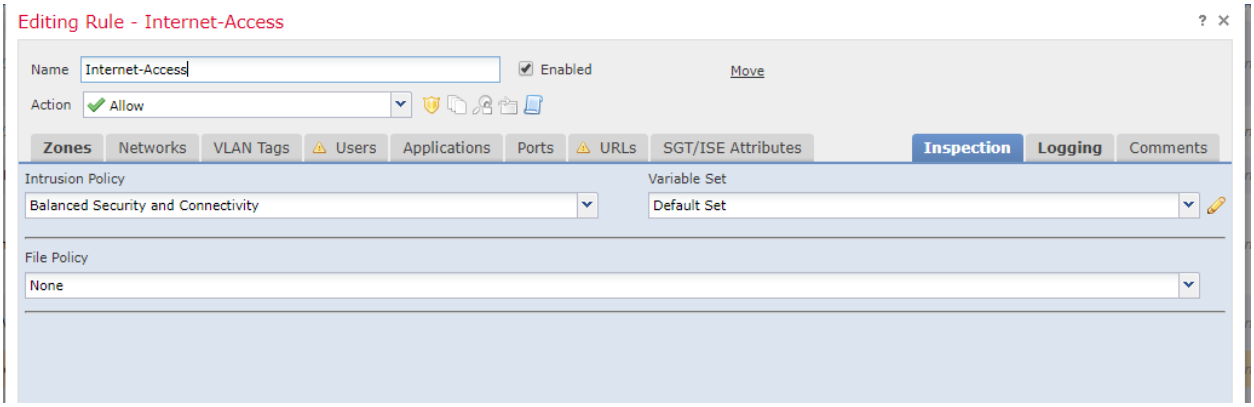
Type of NAT rule	Auto NAT [1]
Source Interface	inside
Destination Interface	outside
Original sources	10.100.0.0/8
Translated Source	Destination Interface IP
Options	Translate DNS Replies that match this Rule: False



Snort Inspection

- Snort Inspection was enabled on the following ACL rules

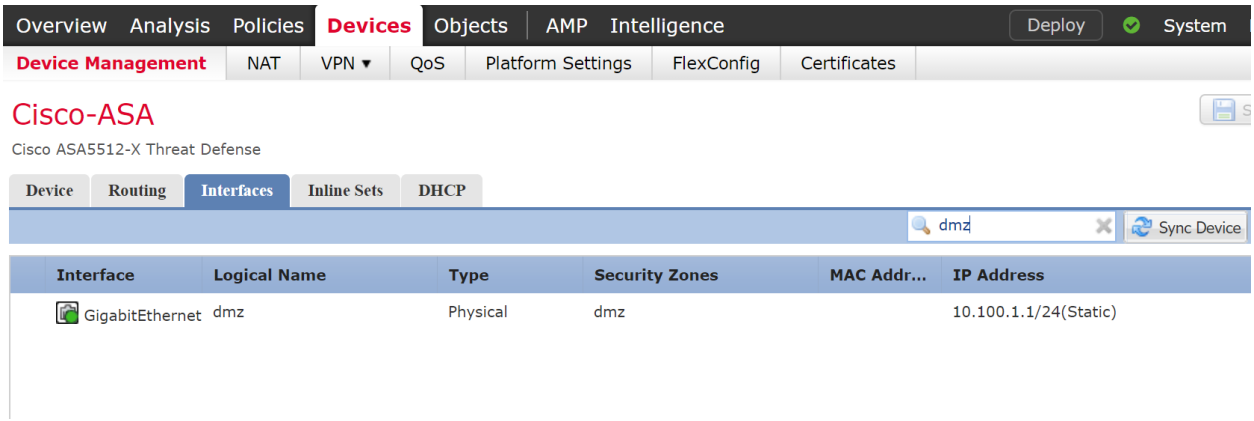
Name of the ACL	Intrusion Policy
Internet-Access rule	Balanced connectivity and security



4954

4955 **DMZ Network**

4956 A Separate interface was setup for the Manufacturing DMZ LAN Network for hosting the **DMZ**
4957 **Historian** server.



4958

4959 **2. Configuration on RuggedCom Firewall**:

4960 The following features, settings were enabled on this firewall

4961 • Network Segmentation
4962 • ACL Rules
4963 • Masquerading (NAT) rules

4964 **Network Segmentation**

4965 Separate network interfaces were configured for the different network segments as listed below

4966 • Supervisory LAN Interface (Network: 192.168.0.0/24)
4967 • Control LAN Interface (Network: 192.168.1.1/24)
4968 • LAN Interface (IP: 10.100.0.20, Uplink to Cybersecurity LAN)

4969 **Access Control List (ACL) rules**

4970 The following zones were created:

4971 • WAN - Zone for internet-bound / uplink connections to Cybersecurity LAN.
4972 • CTRL - Zone for the 192.168.1.0/24 subnet.
4973 • SUPERVISORY - Zone for the 192.168.0.0/24 subnet.
4974 • MGMT - Zone for the management interface traffic (out of scope)
4975
4976 The following firewall policies were created:
4977 • Allow traffic between firewall and WAN.

- Allow traffic between firewall and MGMT.
- Allow traffic between firewall and CTRL.
- Allow traffic between firewall and Supervisory.
- All other traffic is DROPPED.

The following firewall rules were created

1) ALLOW: POLARIS:ANY -> 192.168.1.0/24,10.100.0.0/24:22 (TCP)
2) ALLOW: vCONTROLLER1,vCONTROLLER2:ANY -> PLC:502 (TCP)
3) ALLOW: STATION1,STATION2,STATION3,STATION4:ANY -> PLC,HMI:502 (TCP)
4) ALLOW: STATION4:ANY -> PLC:502 (TCP)
5) ALLOW: HISTORIAN:ANY -> STATION1,STATION2,STATION3,STATION4,PLC:502 (TCP)
6) ALLOW: MINTAKA,vCONTROLLER1,vCONTROLLER2:ANY -> POLARIS:11311 (TCP)
7) ALLOW: vCONTROLLER1,vCONTROLLER2:ANY -> POLARIS:115,2049 (TCP)
8) ALLOW: vCONTROLLER1,vCONTROLLER2:ANY -> POLARIS:115,2049 (UDP)
9) ALLOW: ANY:ANY -> ANY:ANY (ICMP)
10) ALLOW: PLC,HMI:ANY -> STATION1,STATION2,STATION3,STATION4:502 (TCP)
11) ALLOW: PLC:ANY -> vCONTROLLER1,vCONTROLLER2:502 (TCP)
12) ALLOW: POLARIS:32678-65535 -> MINTAKA,vCONTROLLER1,vCONTROLLER2:32768-65535 (TCP)
13) ALLOW: POLARIS:ANY -> I800Switch-Management-UI:80,443 (TCP)
14) ALLOW: NESSUS/OPEN-AUDIT:ANY -> 192.168.1.0/24:22 (TCP)
15) ALLOW: VCONTROLLER1,VCONTROLLER2:32768-65535 -> POLARIS:32768:65535 (UDP)

Rules

Rule Name	IP Type	Action	Source Zone Hosts	Destination Zone Hosts	Log Level	Protocol	Source Port
PolarisSSH	ipv4	accept	192.168.0.20	192.168.1.0/24,10.100.0.0/24	none	tcp	none
ModbusRule1	ipv4	accept	192.168.1.3,192.168.1.4	192.168.0.30	none	tcp	none
ModbusRule2	ipv4	accept	192.168.1.101,192.168.1.102,192.168.1.10...	192.168.0.98,192.168.0.30	debug	tcp	none
ModbusRule3	ipv4	accept	192.168.0.21	192.168.1.101,192.168.1.102,192.168.1.10...	none	tcp	none
ModbusRule4	ipv4	accept	192.168.0.30,192.168.0.98	192.168.1.101,192.168.1.102,192.168.1.10...	debug	tcp	none
ModbusRule5	ipv4	accept	192.168.0.30	192.168.1.3,192.168.1.4	none	tcp	none
AllowFTPtoPLC	ipv4	accept	192.168.1.104	192.168.0.30	none	tcp	none
ROS	ipv4	accept	192.168.1.3,192.168.1.4,192.168.1.5	192.168.0.20	none	all	none
NFS1	ipv4	accept	192.168.1.3,192.168.1.4	192.168.0.20	none	tcp	
NFSudp	ipv4	accept	192.168.1.3,192.168.1.4	192.168.0.20	none	udp	none
AllowICMP	ipv4	accept	not found	not found	none	icmp	none
PolarisHighRange	ipv4	accept	192.168.0.20	192.168.1.3,192.168.1.4,192.168.1.5	none	tcp	32678:65535
i800MgmtUI	ipv4	accept	192.168.0.20	192.168.1.10	none	tcp	none
NessusSSH	ipv4	accept	192.168.0.11,192.168.0.12	192.168.1.0/24	none	tcp	none
Mountd	ipv4	accept	192.168.1.3,192.168.1.4	192.168.0.20	none	udp	32768:65535

5004

5005

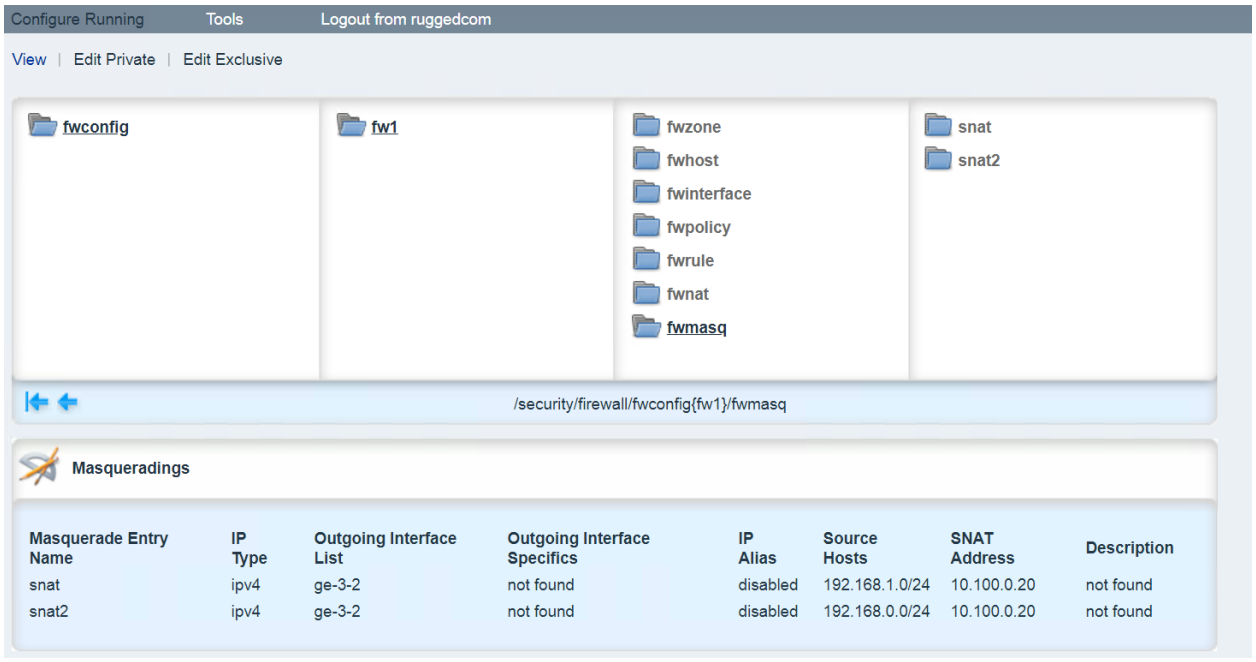
5006

5007 **NAT Policy**:

5008 • Two Masquerading rules were created (one for each LAN segment) to NAT all traffic going
5009 outbound from the Work Cell to the Cybersecurity LAN network. Masquerading is a form of
5010 Dynamic NAT. Both hide a single subnetwork behind a single IP address
5011

Rule #	Outgoing Interface	Source Network	NAT IP address
1	Ge-3-2 (Uplink interface to Cybersecurity LAN)	192.168.1.0/20	10.100.0.20
2	Ge-3-2 (Uplink interface to Cybersecurity LAN)	192.168.0.0/20	10.100.0.20

5012



5013

5014 **3. Configuration on GTB Inspector**:

5015 Refer to section 4.12.5

4.16.6 Highlighted Performance Impacts

Two performance measurement experiments were performed for network boundary protection while the manufacturing system was operational:

3. CL009.1 - Firewall rules and Access control list (ACL) rules are implemented at the CRS boundary router.
4. CL012.1 - Firewall and ACL rules are implemented on an upgraded boundary router.

These two experiments were performed chronologically after the experiment CL011.2 where the activities performed caused permanent performance impacts to the CRS (see Section 4.11.6.2). The performance impacts first observed during CL011.2 (and again measured as part of CL009.1 and CL012.1) are not included in those sections.

4.16.6.1 Experiment CL009.1

Firewall rules and access control list (ACL) rules were implemented at the CRS boundary router. All authorized connections were verified to be allowed by the firewall before the manufacturing process was operational.

A small increase in the average robot job actuation time was observed on Robot 2 for Job 203 (see Figure 4-52). No other increases were observed for any of the other jobs.

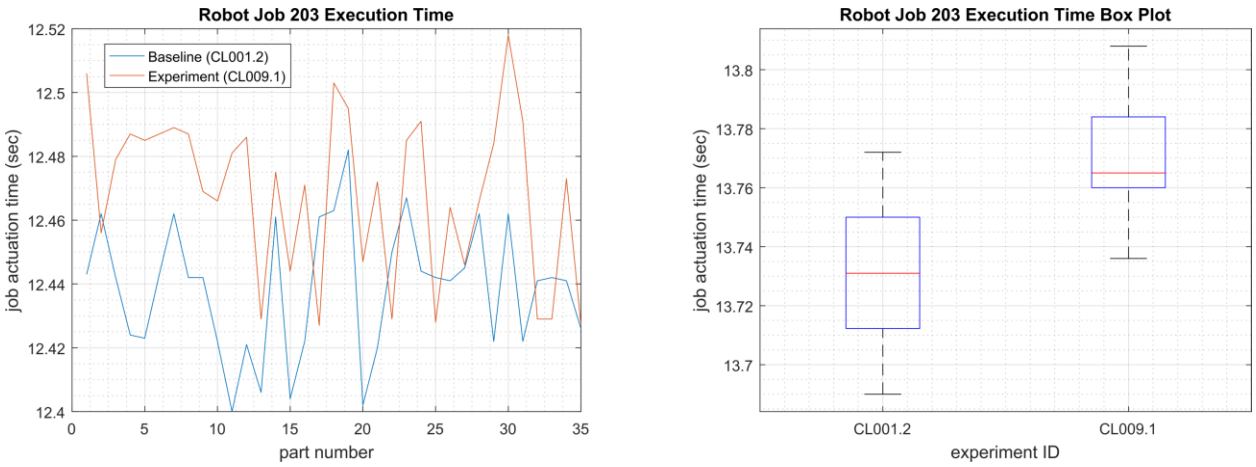


Figure 4-52 - Time-series (left) and boxplot (right) showing the job actuation times for Job 203 during the CL001.2 baseline and CL009.1 experiment.

A slight increase of the part production time mean was observed during this experiment but is not statistically significant.

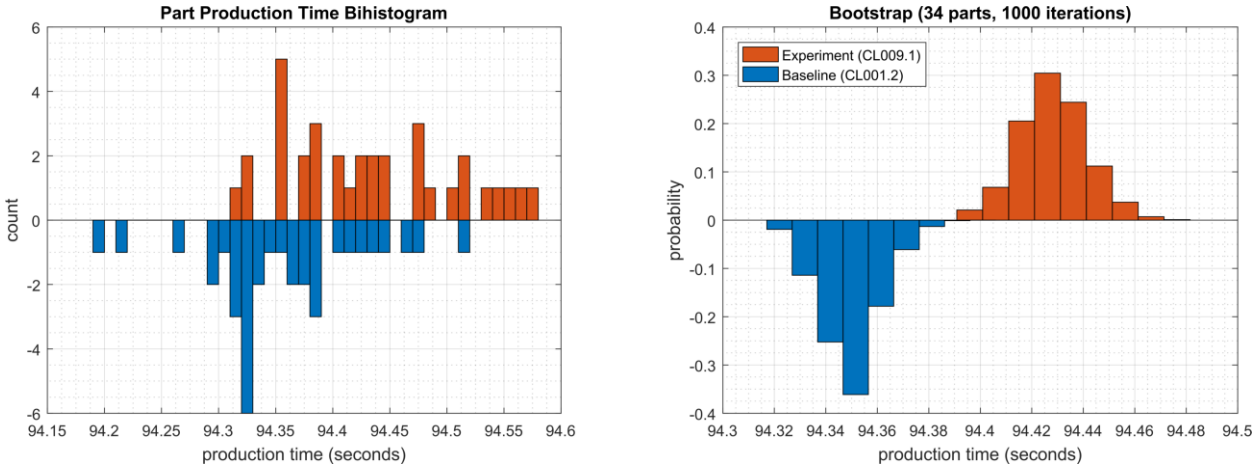


Figure 4-53 - Bihistograms showing the part production time (left) and estimated mean production time using the bootstrap method (right) using the measurements from baseline CL001.2 and experiment CL009.1.

4.16.6.2 Experiment CL012.1

The CRS boundary router was replaced with a Cisco ASA-5506, and the same firewall rules and access control list (ACL) rules were implemented. All authorized connections were verified to be allowed by the firewall before the manufacturing process was operational.

A slight increase of the part production time mean was observed during this experiment but is not statistically significant.

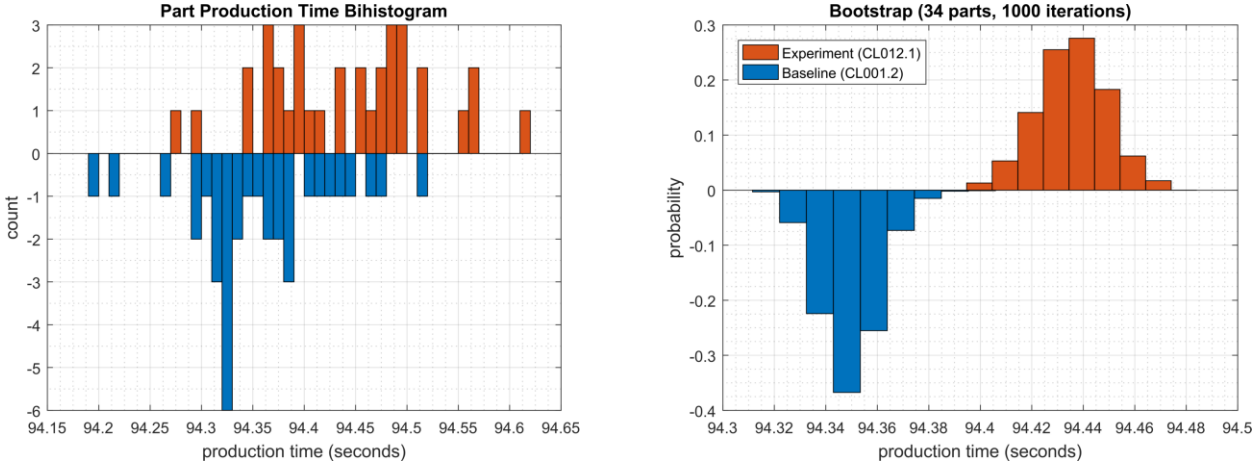


Figure 4-54 - Bihistograms showing the part production time (left) and estimated mean production time using the bootstrap method (right) using the measurements from baseline CL001.2 and experiment CL012.1.

4.16.7 Link to Entire Performance Measurement Data Set

- **CL009.1-BoundaryFirewall.zip**
- **CL012.1-CiscoASA5506.zip**

4.17 Managed Network Interfaces

4.17.1 Technical Solution Overview

Managing network interfaces controls what network devices are plugged into switches within manufacturing system, along with physical labeling connections to help with system identification and classification. Required actions will be performed directly on the exterior of the switch. Switch port in use will be labeled logically within switch console itself, along with the corresponding network cable for easy identification. All cable should be labeled/identified at the switch and at the opposite end of the network cable. Switch Port Security should be configured to restrict access to only allowed preconfigured Media Access Control (MAC) addresses devices.

Minimal cost for labeling. Effort of implement is high, but not difficult. The effort will be spent taking the required time to accurately identify cabling connections.

Most switches have built in Port security. Since this technical control is built into switches there is no additional cost for implementation. Configuration for Port security is well documented and easily configured.

4.17.2 Technical Capabilities Provided by Solution

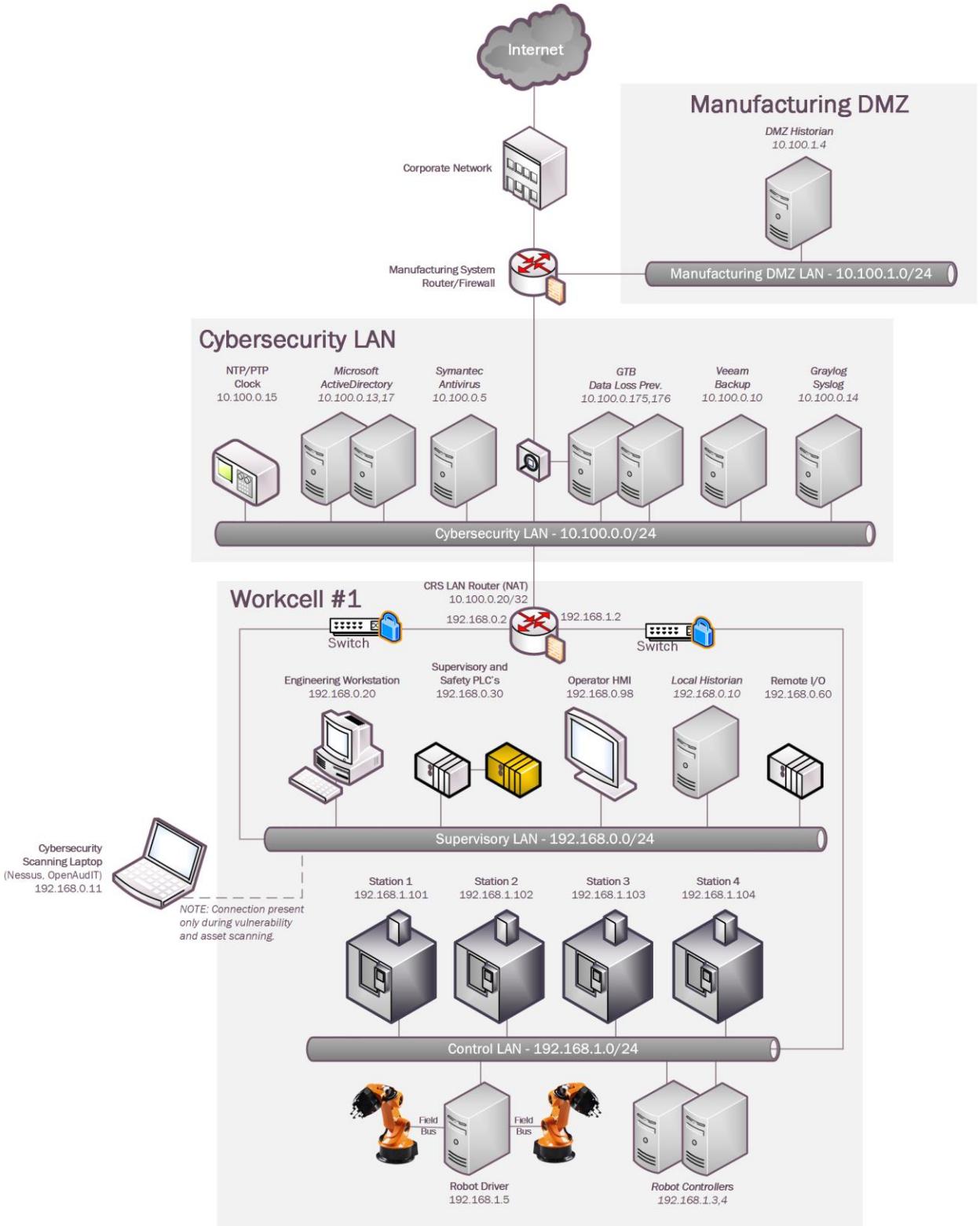
Managed Network Interfaces provides components of the following Technical Capabilities described in Section 6 of Volume 1:

- Managed Network Interfaces

4.17.3 Subcategories Addressed by Implementing Solution

PR.AC-5

4.17.4 Architecture Map of Where Solution was Implemented



4.17.5 Installation Instructions and Configurations

Managing Network Interface Instructions

Overview:

Port labeling provides ability for others to understand and know what network devices belong where. Managing your switches with correct labeling and classification makes troubleshooting simpler along with improving cybersecurity.

Labeling ports within switch:

Switches within CRS:

Siemens RuggedCom RX1510 (Router) 192.168.0.2

Siemens RuggedCom i800 (Switch) 192.168.1.10

Netgear GS724T (Switch) 192.168.0.239

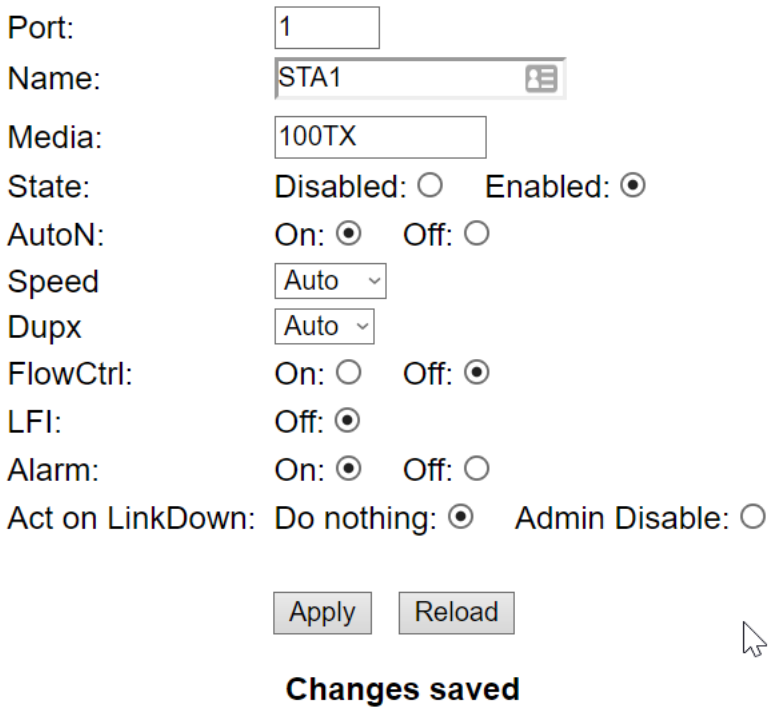
Siemens RuggedCom RX1510

- Interface labels can't be changed from defaults.

Siemens RuggedCom i800

- Login to switch via web browser. https://192.168.1.10
- Click on **Ethernet →Ports-Configure Port Parameters**.
- Click desired port number for renaming.

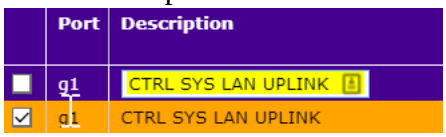
- Type in Name to identify port and click apply.



Netgear

- Login to switch via web browser. https://192.168.0.239
- Click on Tab labeled **"Switching"**

- Select port that will be labeled.
- Enter Description.



- Finally click apply button in lower right-hand corner.

Overview:

Port security prevents unauthorized devices from being plugged into a network switch while trying to obtaining sensitive information, which could be used for mapping out network connections for possible data exfiltration. When an unauthorized device is plugged into a protected port a warning message is logged and sent to a syslog server if supported by switch vendor.

Collaborative Robotics Enclave:

- This enclave contains three different switches/routers.
  - Siemens RuggedCom RX1510 (Can function as Router/Firewall/Switch)
  - Siemens RuggedCom i800 (Switch)
  - NETGEAR GS724Tv4 (Switch)

RuggedCom RX 1510: Has multiple ports which are individual configurable depending on desired network topology.

- Ports LM1/1 and LM1/2 = disabled
- Ports LM2/1 (Switchport = False, port is configured for routing), LM2/2 (Switchport = True, port is configured for mirroring)
- Ports LM3/1 and LM3/2 (Switchport = False, ports are configured for routing)
- Ports LM4/1 and LM4/2 = disabled
- Only port security being applied to RuggedCom RX 1510 is LM1/1, LM4/1, LM4/2 which are disabled.

RuggedCom i800: Layer 2 switch that allows for all ports for switching or mirroring.

- Ports **1 to 7** are all configured for switching.
- Port **8** is configured for mirroring.

NETGEAR GS724Tv4: Layer 2, Layer 2+ along with Layer 3 Lite features. All ports on this switch in our environment are configured for switching only.

- Ports **2, 4, 6, 8, 9, 10, 12, 14, 16, 17, 18, 20, 21, 22, 25, 26** are disabled **(If any device is plugged into any of these ports there will be no link light)**.
- Ports **1, 3, 5, 7, 11, 13, 15, 19** are all enabled and labeled **(Each port has Port Security enabled)**.
- Port **23** is used for management with no Port Security enabled **(Used for accessing switch with any network device)**.
- Port **24** is mirror port connect to **RA3**. This port is configured for Probe.

Port Security Configuration for NETGEAR and i800:

NETGEAR:

Port-Security
interface g1
dot1x port-control mac-based
description 'CTRL SYS LAN UPLINK'
Port Security
port-security max-dynamic 0
port-security max-static 3

```
port-security mac-address
00:0C:29:CE:7F:94 1
port-security mac-address
94:B8:C5:0E:E1:01 1
port-security mac-address
94:B8:C5:0E:E1:9F 1
interface g3
dot1x port-control mac-based
description 'Beckhoff Automation GmbH'
port-security
port-security max-dynamic 0
port-security max-static 1
port-security mac-address
00:01:05:17:DB:08 1
interface g5
dot1x port-control mac-based
description 'Polaris (DELL)'
port-security
port-security max-dynamic 0
port-security max-static 1
port-security mac-address
F8:B1:56:BA:09:A8 1
interface g7
dot1x port-control mac-based
description 'PROBE1-A'
port-security
port-security max-dynamic 0
port-security max-static 1
port-security mac-address
00:05:E4:03:7C:3B 1
dot1x port-control mac-based
description 'Wago Kontakttechnik Gmbh'
port-security
port-security max-dynamic 0
port-security max-static 1
port-security mac-address
00:30:DE:00:C4:3C 1
interface g13
dot1x port-control mac-based
description 'Robotics Hyper-V / Open
AudIT'
port-security
port-security max-dynamic 0
port-security max-static 3
```

```
port-security mac-address
00:15:5D:02:0A:07 1
port-security mac-address
00:15:5D:02:0A:0E 1
port-security mac-address
00:15:5D:02:0A:43 1
interface g15
dot1x port-control mac-based
description 'Laptop on CRS Desk'
port-security
port-security max-dynamic 0
port-security max-static 1
port-security mac-address
34:E6:D7:22:C3:ED 1
interface g19
dot1x port-control mac-based
description 'HyperV'
port-security
port-security max-dynamic 0
port-security max-static 3
port-security mac-address
00:10:18:B8:19:10 1
port-security mac-address
00:10:18:B8:19:11 1
port-security mac-address
00:15:5D:16:AC:07 1
```

i800:

MAC Address	Attached Machine	VID	Port	Type	CoS
00-15-5D-16-AC-02	vController1	1	6	Static	N/A
00-15-5D-16-AC-03	vController2	1	6	Static	N/A
94-B8-C5-0E-E1-9F	Uplink	1	5	Static	N/A
A0-CE-C8-1F-BD-99	MINTAKA	1	7	Static	N/A
B0-D5-CC-F4-26-EC	Station 4	1	4	Static	N/A

B0-D5-CC-FA-70-C9	Station 1	1	1	Static	N/A
B0-D5-CC-FA-7A-43	Station 3	1	3	Static	N/A
B0-D5-CC-FE-6E-B1	Station 2	1	2	Static	N/A
C8-1F-66-C8-6A-ED	MINTAKA	1	7	Static	N/A
C8-1F-66-CA-26-C0	Robotics VH	1	6	Static	N/A
C8-1F-66-CA-26-C2	Robotics VH	1	6	Static	N/A

4.17.6 Highlighted Performance Impacts

Two performance measurement experiments were performed for the Managed Network Interfaces technology implementation while the manufacturing system was operational:

1. CL010.1 - Alerts are generated on new physical network connections (via syslog).
2. CL010.2 - MAC address filtering is enabled and configured on CRS network devices, and unused physical network ports are disabled on CRS network devices.

4.17.6.1 Experiment CL010.1

No performance impact to the manufacturing process was measured during the experiment.

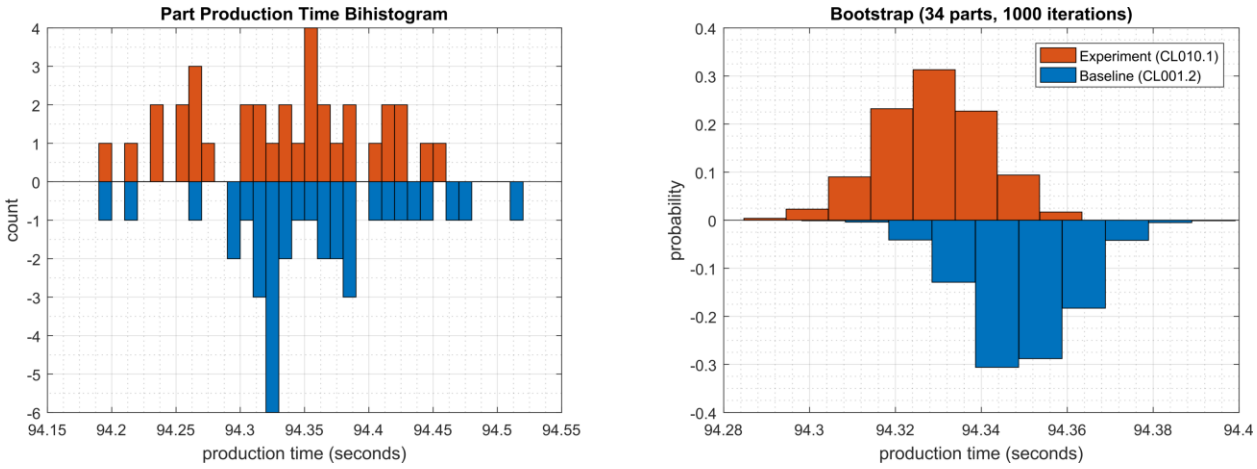


Figure 4-55 - Bihistograms showing the part production time (left) and estimated mean production time using the bootstrap method (right) using the measurements from baseline CL001.1 and experiment CL010.1.

4.17.6.2 Experiment CL010.2

An increase in the robot job execution time was observed on Robot 1 for Job 103 (see Figure 4-56), with two relatively large increases for parts 3 and 24. No other increases were observed for any of the other jobs.

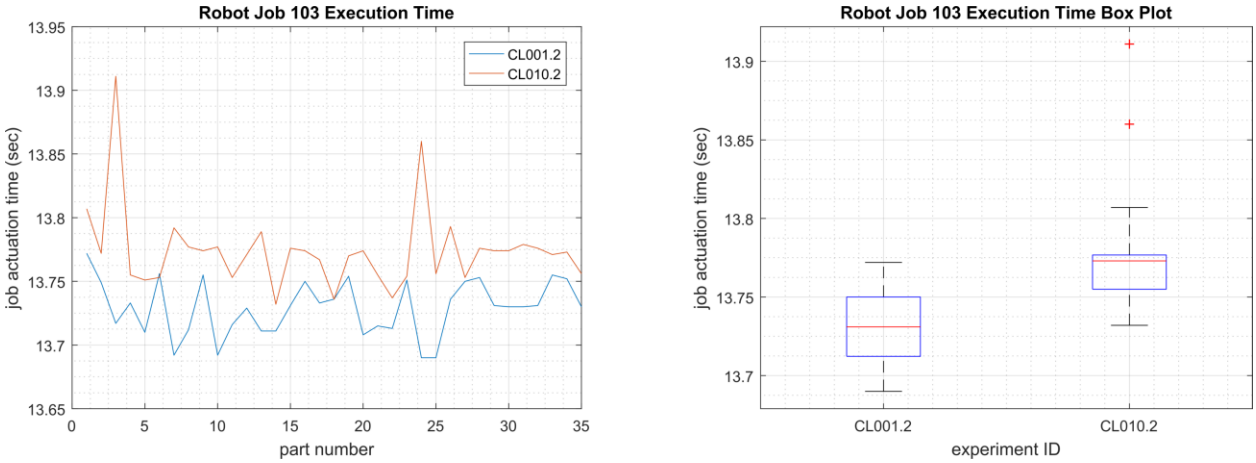


Figure 4-56 - Time-series (left) and boxplot (right) showing the job execution times for Job 103 during the CL0010.2 experiment and CL001.2 baseline.

A slight increase of the part production time mean was observed during this experiment but is not statistically significant.

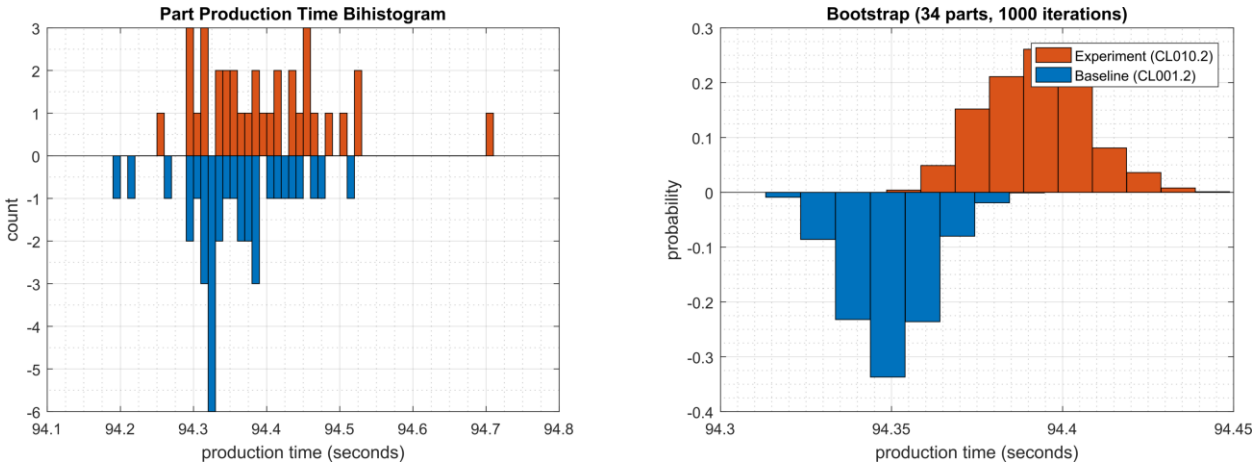


Figure 4-57 - Bihistograms showing the part production time (left) and estimated mean production time using the bootstrap method (right) using the measurements from baseline CL001.1 and experiment CL010.2.

4.17.7 Link to Entire Performance Measurement Data Set

- **CL010.1-NetworkPhysicalConnections.zip**
- **CL010.2-NetworkMACFiltering.zip**

4.18 Time Synchronization

4.18.1 Technical Solution Overview

Ability to have all devices sync from a reliable time source. Time synchronization is vital for system logins, event tracking and all other time sensitive events occurring with a manufacturing system.

No additional cost since services are included.

Ease of use simple

Effort and time required = minimal

4.18.2 Technical Capabilities Provided by Solution

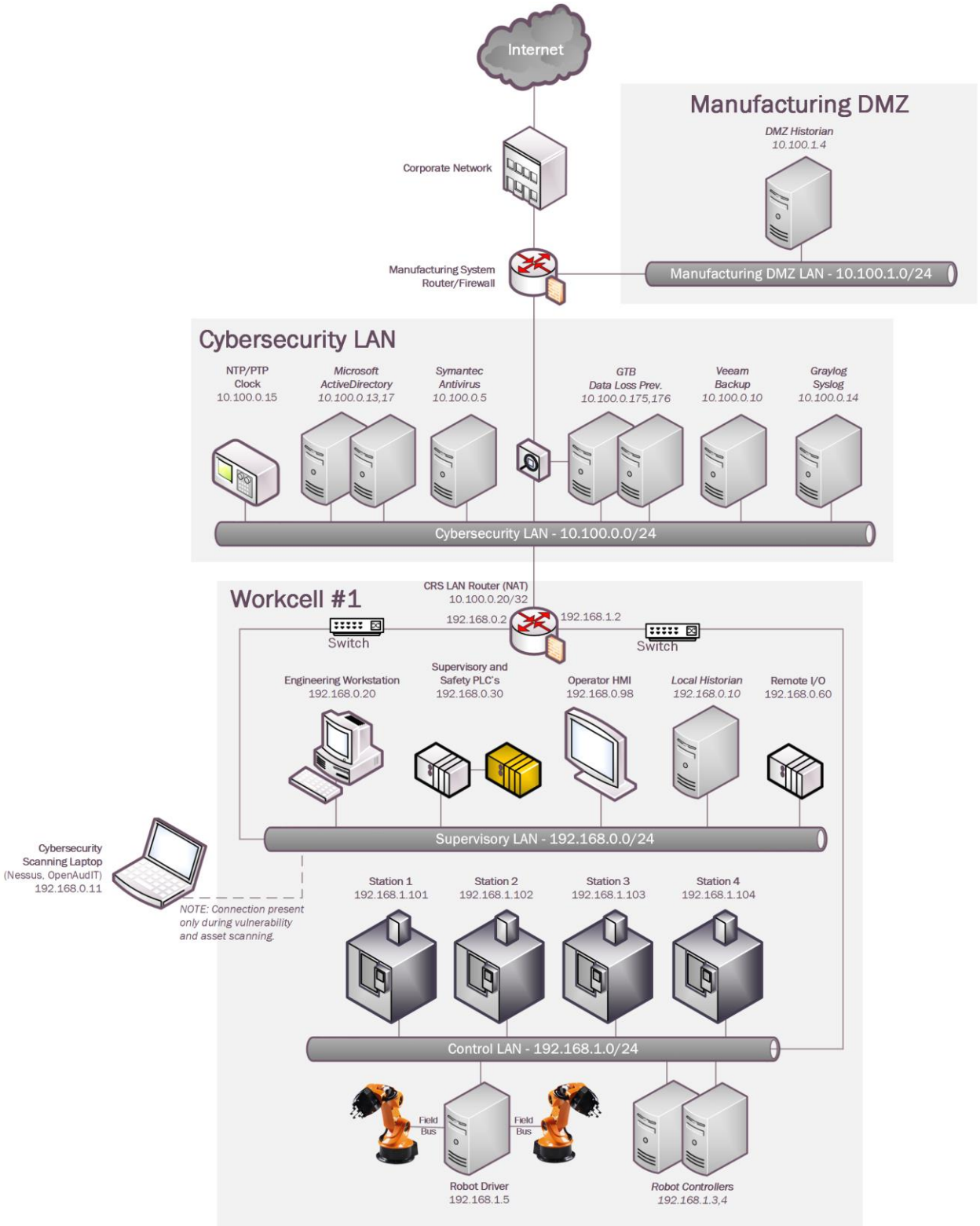
Time Synchronization provides components of the following Technical Capabilities described in Section 6 of Volume 1:

- Time Synchronization

4.18.3 Subcategories Addressed by Implementing Solution

PR.PT-1

4.18.4 Architecture Map of Where Solution was Implemented



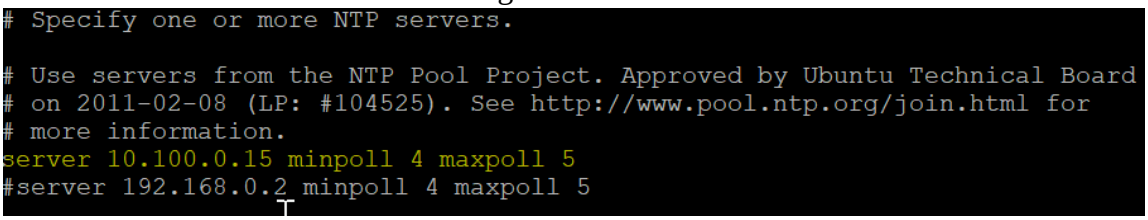
4.18.5 Installation Instructions and Configurations

Collaborative Robotics System Time Synchronization

Computers:

Linux Machines: Directions below work for all Linux machine within manufacturing system environment.

- Login to desired system using SSH client.
- Once logged on open a terminal window.
- Navigate to /etc
- open **"ntp.conf"** using text editor. **(Make sure to type "sudo" before command for required write permissions)**
- Edit the location for NTP Server setting. Save the file and exit.



- Now type this command to restart NTP **"sudo service ntp restart "**
- Provide password for **sudo** when prompted.
- Type **"ntpq -p"** to verify ntp is getting time from correct source.

Domain Controller: Is not providing time for this environment.

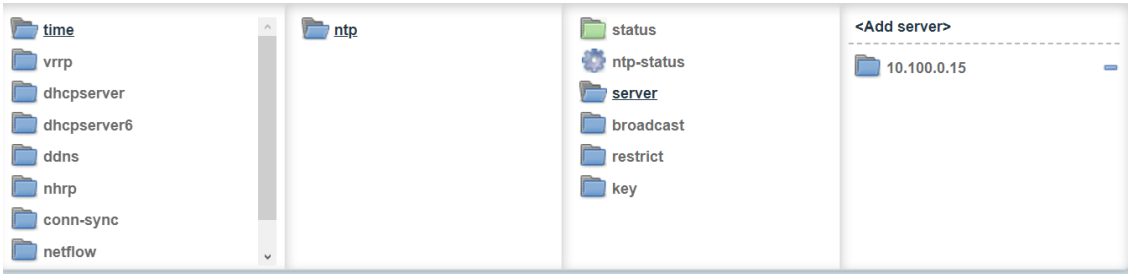
Other Devices:

Router:

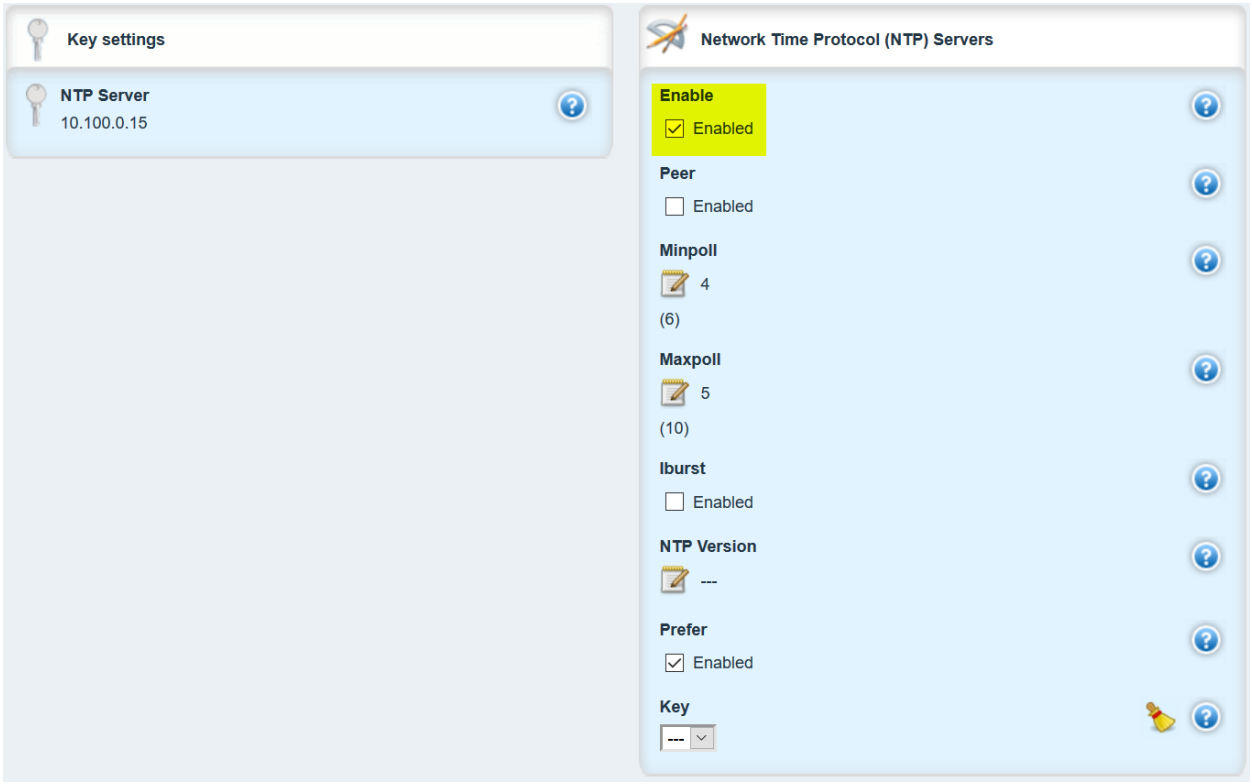
Siemens RuggedCom RX 1510: Device connects to Meinberg at 10.100.0.15 for time.

- Login into RuggedCom RX 1510 via web browser. https://192.168.1.2
- Click on **"Edit Private"** to put into configuration mode.

- Click on **Services → time → ntp → server.**



- Click on **Add** server or select existing to edit.
- Enter server IP address for device providing time service and click Add button.



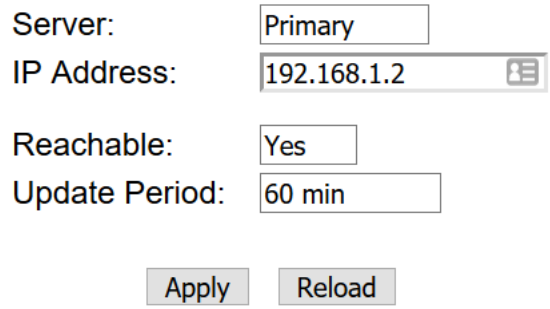
- Make sure to enable newly created entry. See screen shot to right side above.

Switches:

Siemens i800:

- Login via web browser. http://192.168.1.10
- Once logged in click on **"Administration → System Time Manager → Configure NTP → Configure NTP Servers"**

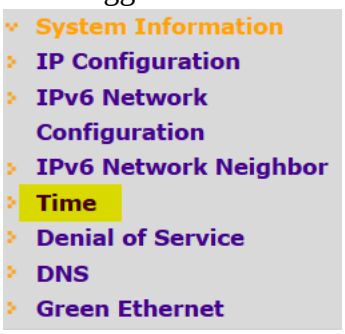
- Now Select primary or back and make the required changes.



- Click **Apply** to save changes.
- Log out

Netgear GS724T:

- Login via web browser portal. https://192.168.0.239
- Once logged in click on → **Time** button.



- Enter required information to configure NTP time on this switch.

Lesson Learned: The master time reference selected should be as close to your physical location as possible. This should reduce the Off Set.

4.18.6 Highlighted Performance Impacts

No performance measurement experiments were performed for time synchronization due to its installation in the system before the Manufacturing Profile implementation was initiated.

4.18.7 Link to Entire Performance Measurement Data Set

N/A

4.19 System Use Monitoring

4.19.1 Technical Solution Overview

System use monitor is accomplished by multiple tools to protect manufacturing system environment from harmful actives using data loss protection, system hardening and syslog server for monitoring, store and auditing. Each tool provides a different level required to protect the manufacturing system.

Implementation effort is moderate requiring understand of Linux systems, along with virtual machine experience. Time required to install and configure all components 20 to 30 hours depending on skill level.

4.19.2 Technical Capabilities Provided by Solution

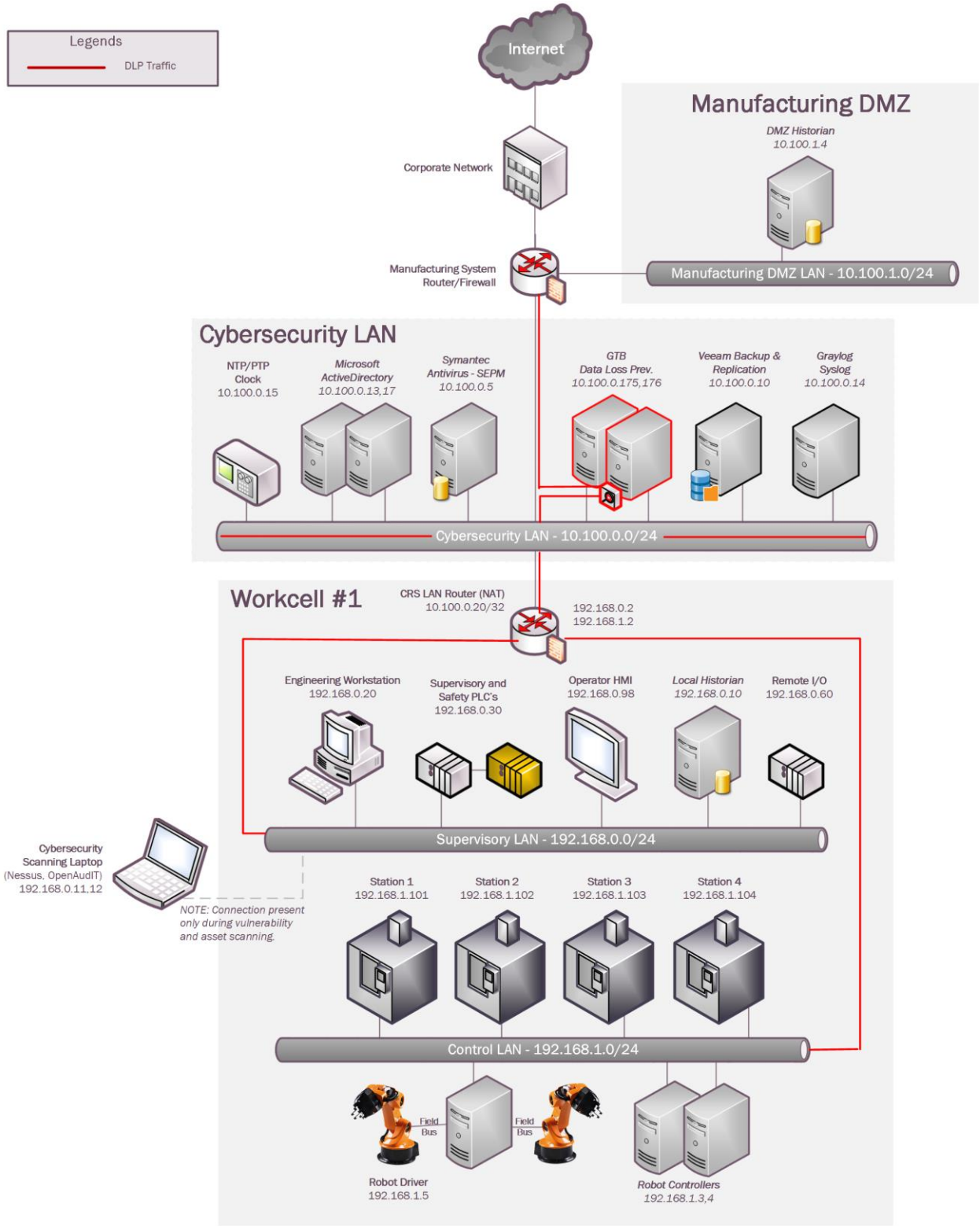
System Use Monitoring was provided by GTB Inspector, Ports and Services Lockdown, and Graylog.

4.19.3 Subcategories Addressed by Implementing Solution

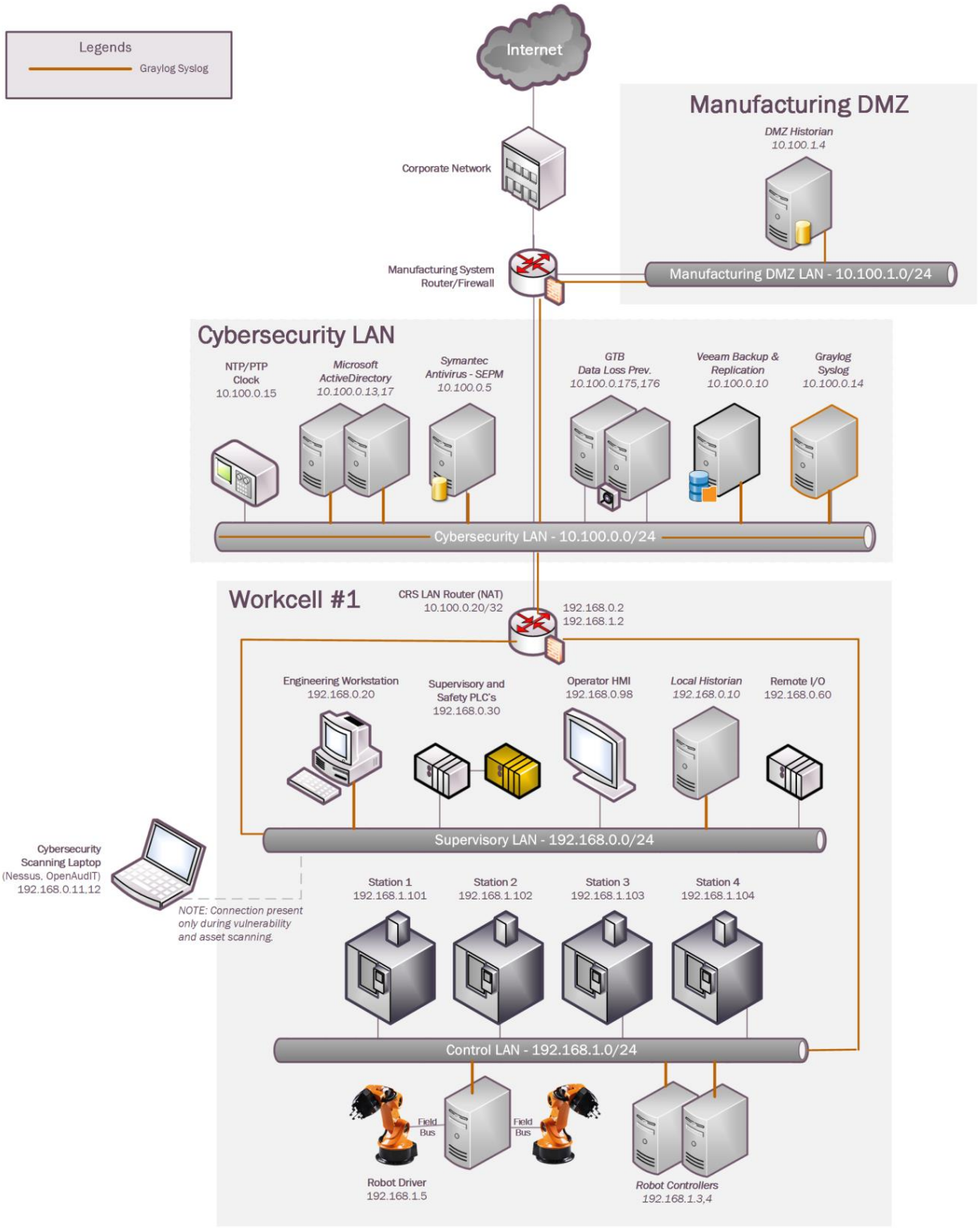
PR.AC-1, PR.DS-5, PR.MA-2, DE.CM-3

4.19.4 Architecture Map of Where Solution was Implemented

DLP Solution:



Graylog Solution:



4.19.5 Installation Instructions and Configurations

System use monitoring was implemented using a combination of tools such as GTB Inspector, Graylog and native Linux OS capabilities such as enabling rsyslog, hardening of permissions.

GTB Inspector: See Section 4.12.5 for instructions.

Graylog: See Section 4.13.5 for instructions.

Permissions on user home directories changed from 755 to 700 to protect data from authorized access using chmod.

4.19.6 Highlighted Performance Impacts

Due to the specific implementation of "System Use Monitoring" performed in the CRS, the performance impacts relating to this technical capability can be found in the following sections:

GTB Inspector - Section 4.12.6

Graylog - Section 4.13.6

4.19.7 Link to Entire Performance Measurement Data Set

N/A

4.20 Ports and Services Lockdown

4.20.1 Technical Solution Overview

Ports and services lockdown solutions enable a manufacturer to discover and disable nonessential logical network ports and services. A logical port is a number assigned to a "logical" connection. Port numbers are assigned to a service, which is helpful to TCP/IP in identifying what ports it must send traffic to. Hackers use port scanners and vulnerability scanners to identify open ports on servers. By revealing which ports are open, the hacker can identify what kind of services are running and the type of system. Closing down unnecessary ports by uninstalling un-necessary programs considerably reduces the attack surface. These actions need to be performed manually.

Native OS capabilities, Open-AudIT and Nessus scanner were leveraged to inventory list of ports and applications currently running on each device of the plant.

4.20.2 Technical Capabilities Provided by Solution

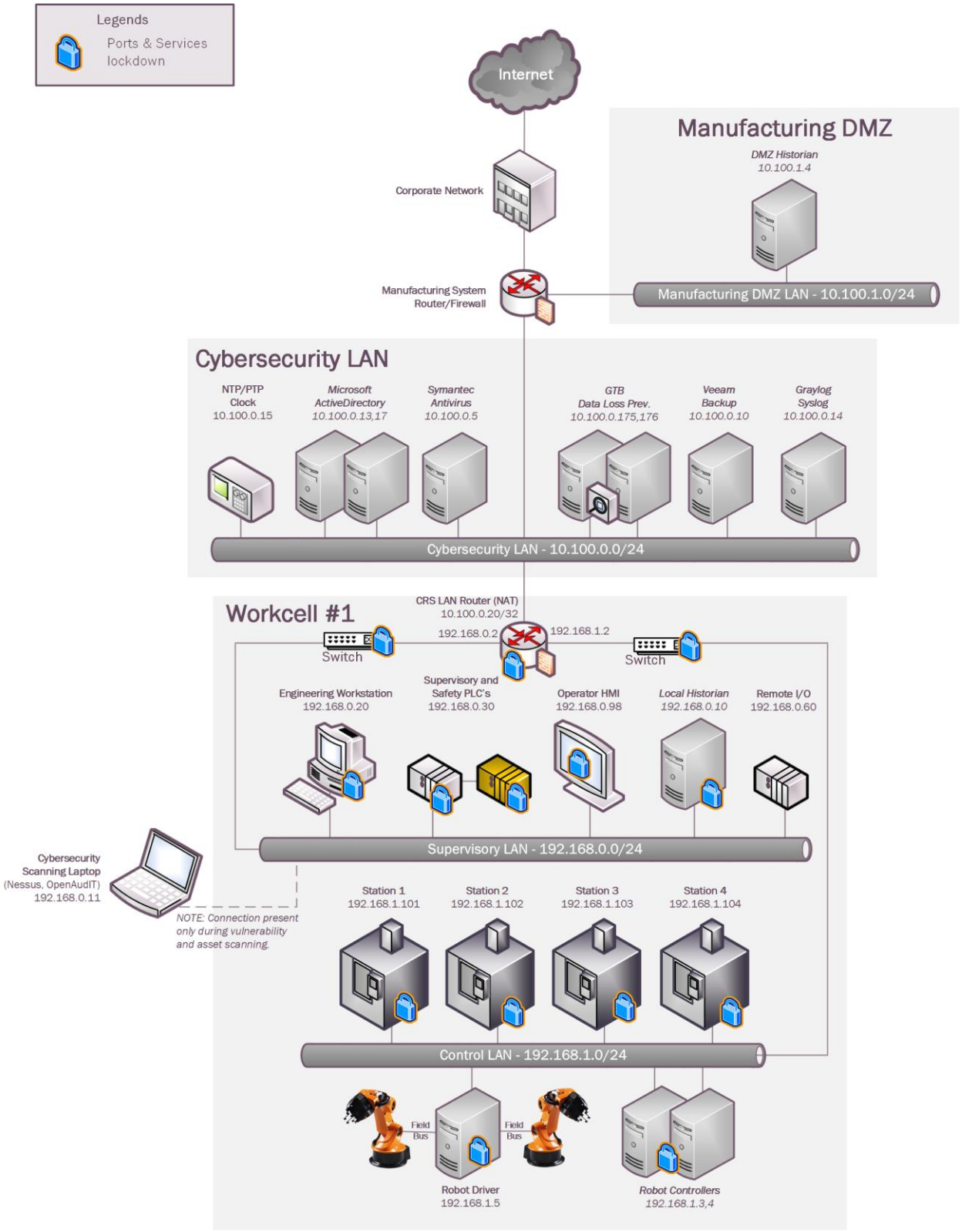
Ports and Services Lockdown provides components of the following Technical Capabilities described in Section 6 of Volume 1:

- Ports and Services Lockdown

4.20.3 Subcategories Addressed by Implementing Solution

PR.IP-1, PR.PT-3

4.20.4 Architecture Map of Where Solution was Implemented



4.20.5 Installation Instructions and Configurations

The following steps were performed

On the Linux hosts:

- A software inventory of each Linux system was performed using Open-AudIT. The inventory reports were reviewed, and a list of unwanted packages were identified. This includes software that comes with the OS by default such as Remina, vino, Thunderbird etc. These programs were then uninstalled.
- Hardened **/etc/exports** file on the NFS-server to export nfs-shares to specific client IP addresses with Read only permissions
- Disabled the **dnsmasq** service and socket on machining stations, as they are not required for normal operations
- Disabled services such as **mongodb**, **modem-manager** from Robot Driver server and Engineering Workstation.
- Restricted SSH access to select users in the /**etc/ssh/sshd_config** file.

- On the HMI:

- Ports 21 161 which were detected as open by Open-AudIT were disabled.
- Modified the HMI program to disable the option to "restart" a machining station and to "clear the part counter" of a station if the station is NOT in the STOP mode.

1. On the PLC:

- Ports 23, 80, 139, 443, 445, 5120, and 8080 were closed by disabling services.
- Services disabled: HTTP server, Telnet, web proxy, SMB, SNMP. This was performed by modifying Windows CE registry entries, as described on p.40 in the "Document about IPC Security" from Beckhoff. These actions required the PLC to be rebooted.
- Remaining open TCP ports: 21, 987. FTP is used by current work cell operations
- SMB and SNMP services were disabled. The SNMP service was disabled by modifying Windows CE registry entries.

2. On the Network devices:

- Changed the SNMP community string from the default **public** to something private.

4.20.6 Highlighted Performance Impacts

One performance measurement experiment was performed for the Ports and Services Lockdown technology implementation while the manufacturing system was operational:

1. CL008.1 - The concept of least privilege is implemented on CRS hosts.

4.20.6.1 Experiment CL008.1

A slight increase of the part production time variance was observed during this experiment, but it is not statistically significant.

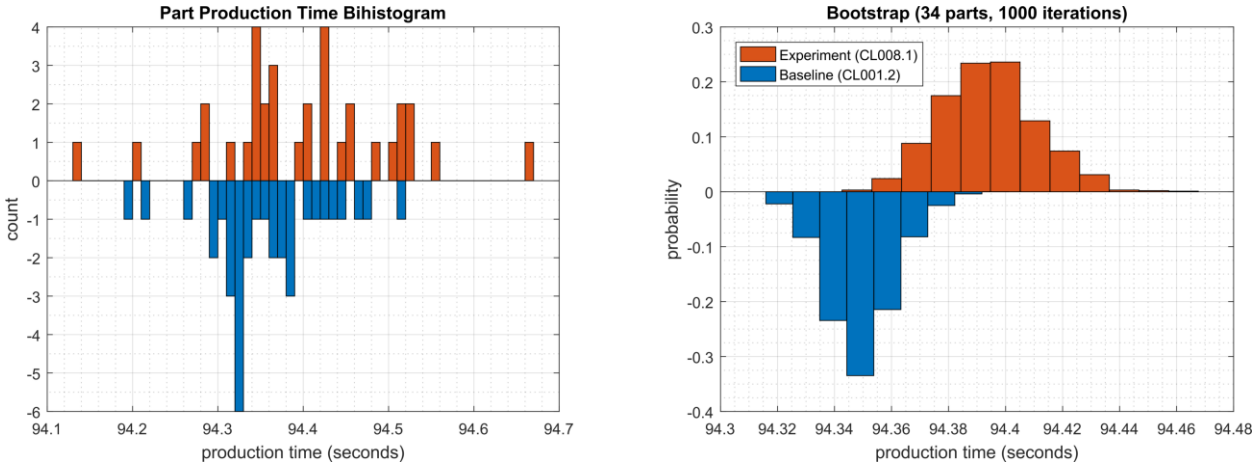


Figure 4-58 - Bihistograms showing the part production time (left) and estimated mean production time using the bootstrap method (right) using the measurements from baseline CL001.1 and experiment CL008.1

4.20.7 Link to Entire Performance Measurement Data Set

CL008.1-LeastPrivilege.zip

4.21 VeraCrypt

4.21.1 Technical Solution Overview

VeraCrypt is a free open source disk encryption software for Windows, Mac OSX and Linux[24]. VeraCrypt main features:

- Creates a **virtual encrypted disk** within a file and mounts it as a real disk.
- Encrypts an **entire partition or storage device** such as USB flash drive or hard drive.
- Encrypts a **partition or drive where Windows is installed** (pre-boot authentication).
- Encryption is automatic, real-time(on-the-fly) and transparent.
- Parallelization and pipelining allow data to be read and written as fast as if the drive was not encrypted.
- Encryption can be hardware-accelerated on modern processors.

4.21.2 Technical Capabilities Provided by Solution

VeraCrypt provides components of the following Technical Capabilities described in Section 6 of Volume 1:

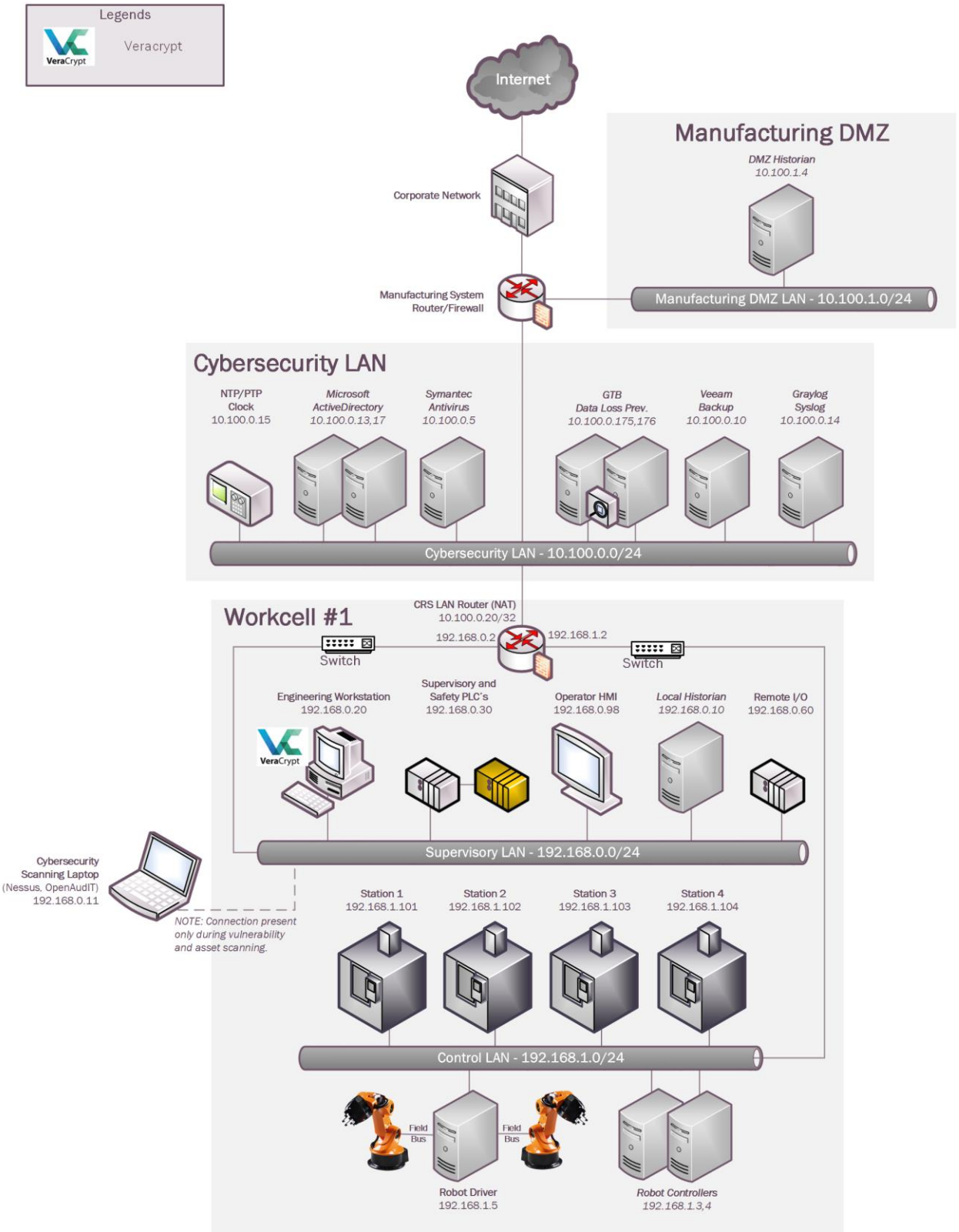
- Encryption

4.21.3 Subcategories Addressed by Implementation

PR.DS-5

[24] VeraCrypt: https://www.veracrypt.fr/en/Home.html

4.21.4 Architecture Map of Where Solution was Implemented



4.21.5 Installation Instructions and Configurations

Details of the Program used

Name	Version	Location
VeraCrypt	1.23	Work-Cell Supervisory LAN

Setup Overview:

VeraCrypt was installed on the Engineering Workstation (running Ubuntu Linux) to encrypt a directory containing confidential documents and code files.

Installation:

- VeraCrypt can be downloaded from https://www.veracrypt.fr . Download the version specific to the Operating System of the Computer you intend to encrypt data on.
- To install VeraCrypt on Ubuntu, download the .tar.bz2 bundle and extract it on the Linux system. Once done, run the setup script (x86 or x64 version) using the following command:

  `sudo ./veracrypt-1.23-setup-gui-x64` (File name varies depending on the version used)

- Once installed, launch it from the Unity Dash or your preferred application launcher. It is important to understand basics of volume-types that can be created using VeraCrypt. As per official documentation[25], there are two types of VeraCrypt volumes:

  - File-hosted (container)
  - Partition/device-hosted (non-system)

  A VeraCrypt file-hosted volume is a normal file, which can reside on any type of storage device. It contains (hosts) a completely independent encrypted virtual disk device.

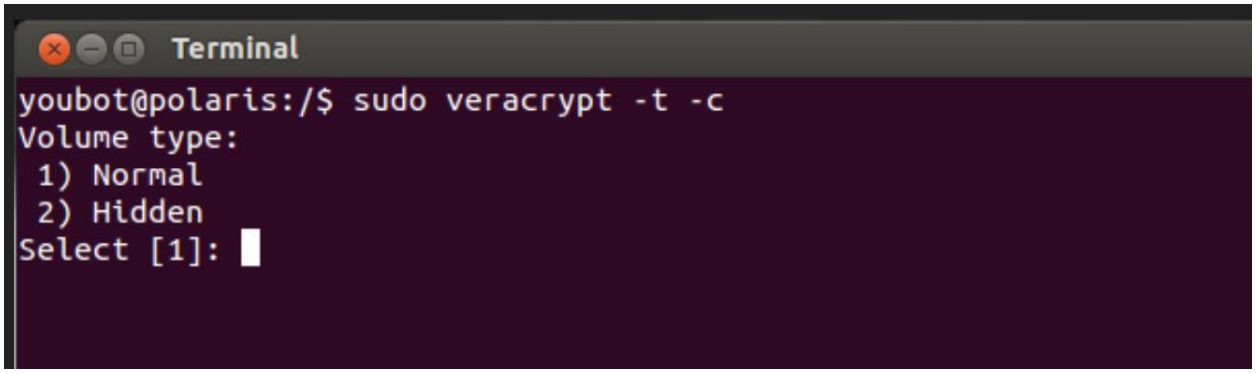
  A VeraCrypt partition is a hard disk partition encrypted using VeraCrypt. You can also encrypt entire hard disks, USB hard disks, USB memory sticks, and other types of storage devices.

  The following procedure shows how to configure encrypted volumes of **Container** type using **cli** (command line).

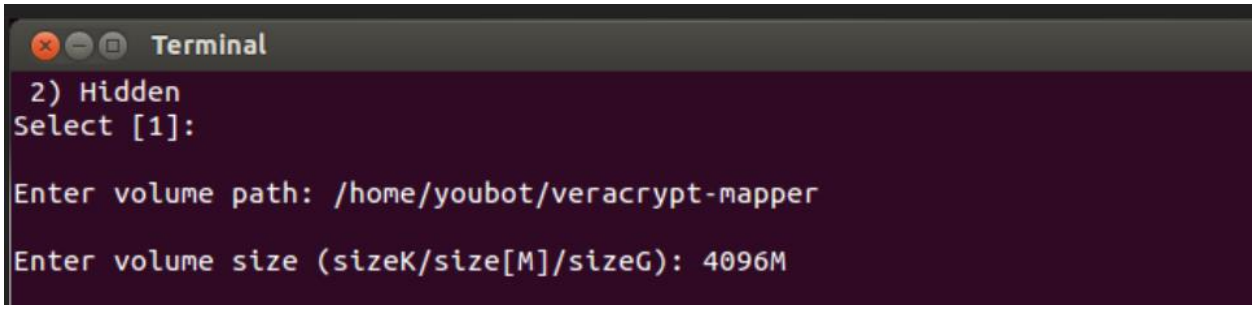
[25] https://www.veracrypt.fr/en/Documentation.html

- The first thing you need to do is create an encrypted volume where you will store all folders/files you'd like to protect. Run the following command(s) and follow the interactive menu

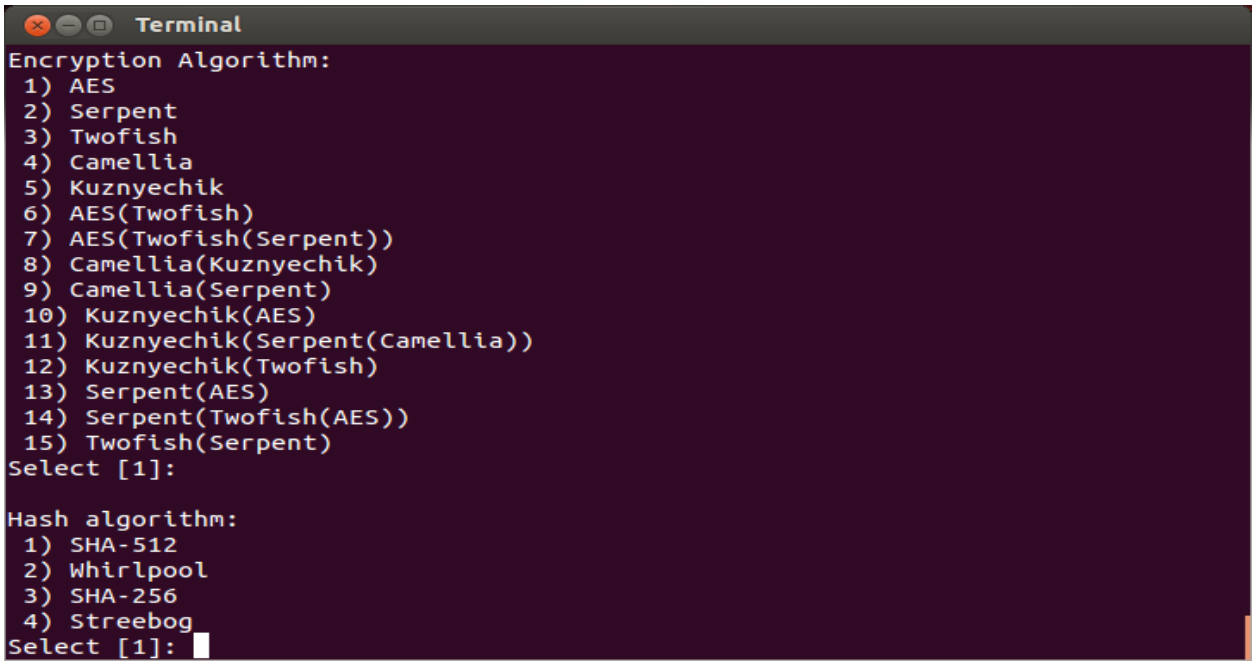
  sudo veracrypt -t -c



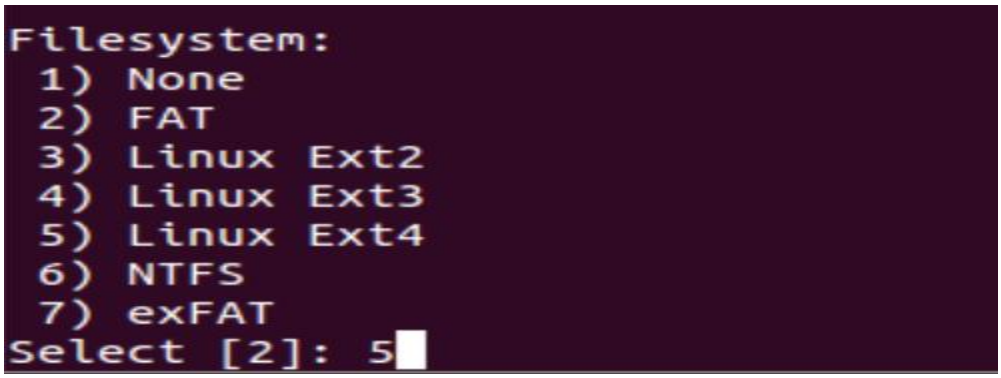
- Select **1** for Normal (Standard) Volume. Next, you need to create a file for your encrypted volume. Enter the complete path of the mapper file and select a size. This file will act as the virtual container of your encrypted data so, plan the path and volume size accordingly.



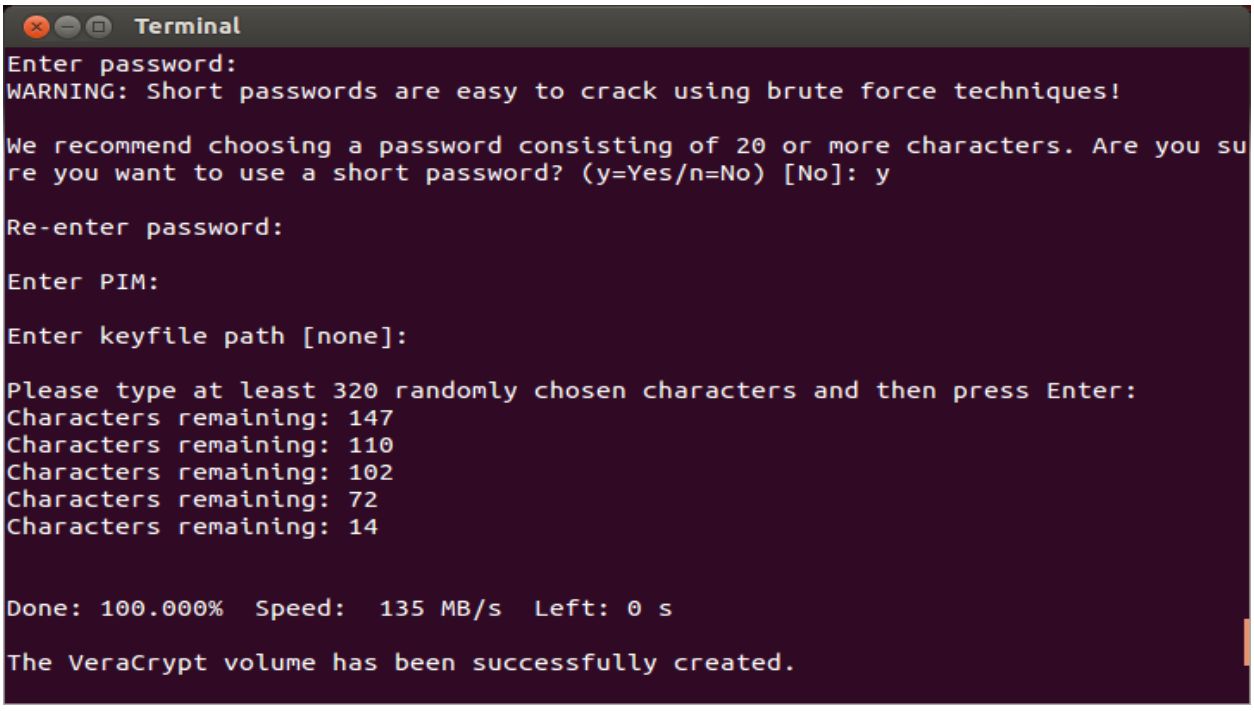
- Next, select an Encryption algorithm followed by Hashing algorithm from the list



- Select a Filesystem type depending on the OS of the computer. FAT works on all Operating systems.



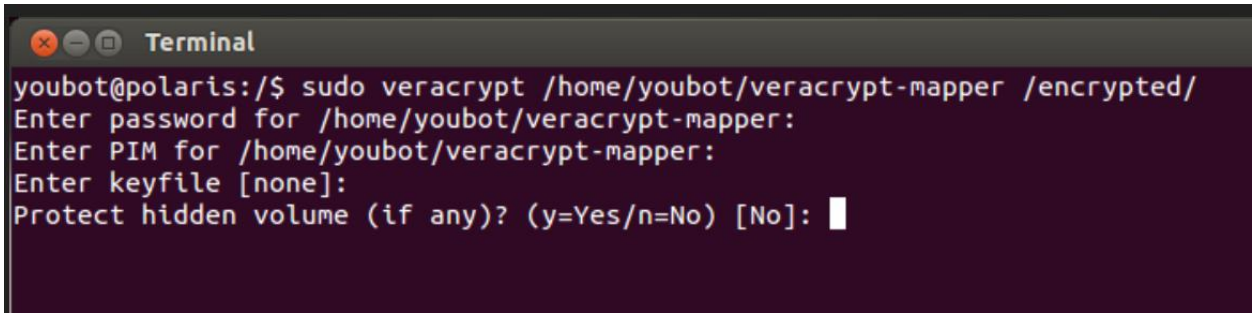
- Enter a password for the virtual container file. For the other options such as **Enter PIM** and **Enter Keyfile path**, hit Enter to leave them blank or configure one if required. Next the wizard will prompt you to type in 320 random characters. This helps to increase the cryptographic strength of the encryption keys. Punch in 320 characters randomly and the process should move forward. Next, the virtual container for our directory will be created and a success message will be shown once it's completed.



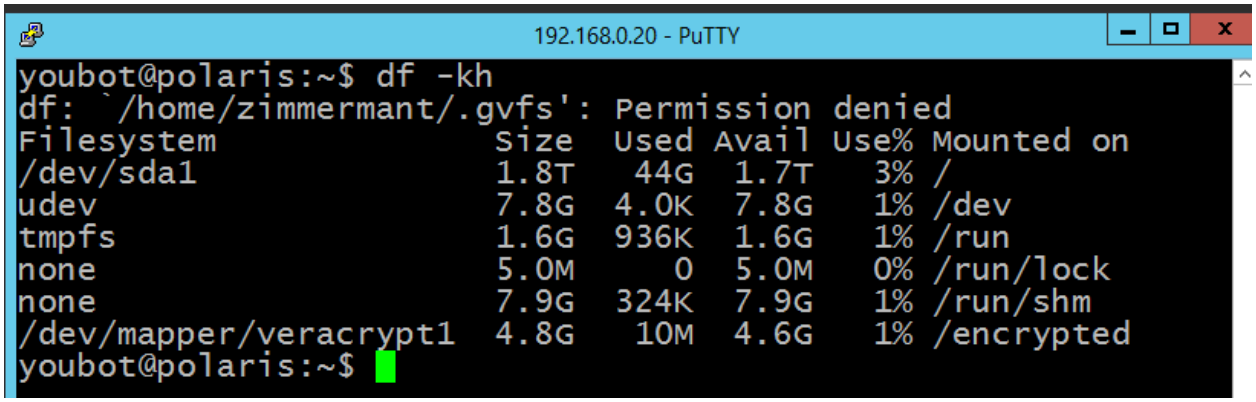
- Create a directory on which you would want to mount this virtual container on. In our example, a **/encrypted** directory was created to mount the container on. Next run the following command to mount

  sudo veracrypt <path of the container mapper file> <directory to mount on>

  Enter the password configured earlier and hit **Enter** for PIM and keyfile if left blank earlier. Choose **NO** for Protect hidden volume since there wasn't any created.



- If the above command completes successfully, you should have your directory mounted successfully. Run df **-kh** to verify the mount



- By default, other system users would only have **Read** access to this directory. To allow other users to write files, configure the permissions or owner as required. You can use this encrypted volume just like any other partition on your hard drive. Data saved in this directory is accessible only as long as the virtual container is mounted.
  An encrypted volume is just like a file and can be deleted. Ensure to take regular backups of the mapper file to avoid losing data incase if the volume gets deleted

- In case of a system reboot, the directory would have to be mounted again using the commands shown earlier. Configuring "Auto-mount" and "Favorite volumes" options is outside of the scope of this document.

4.21.6 Highlighted Performance Impacts

No performance measurement experiments were performed for VeraCrypt due to its implementation (i.e., it was used to encrypt data-at-rest; it does not encrypt data used to operate the manufacturing system).

4.21.7 Link to Entire Performance Measurement Data Set

N/A

4.22 Media Protection

4.22.1 Technical Solution Overview

Port locks provide a low-cost solution for protecting USB ports. Implementation and ease of use provide for quick install and easy removal. USB Port locks provide a simple yet effective solution to restrict USB use. Once USB Port lock has been inserted and engaged there is no way of removing lock device without damaging USB port unless key is used. Each USB Port lock can block up to two ports. These ports are the inserted port, and the port directly to either side depending on the blocking plate direction. USB Port Lock can be purchased with a collar that protects attached USB Mice and Keyboards from removal without prior approval.

4.22.2 Technical Capabilities Provided by Solution

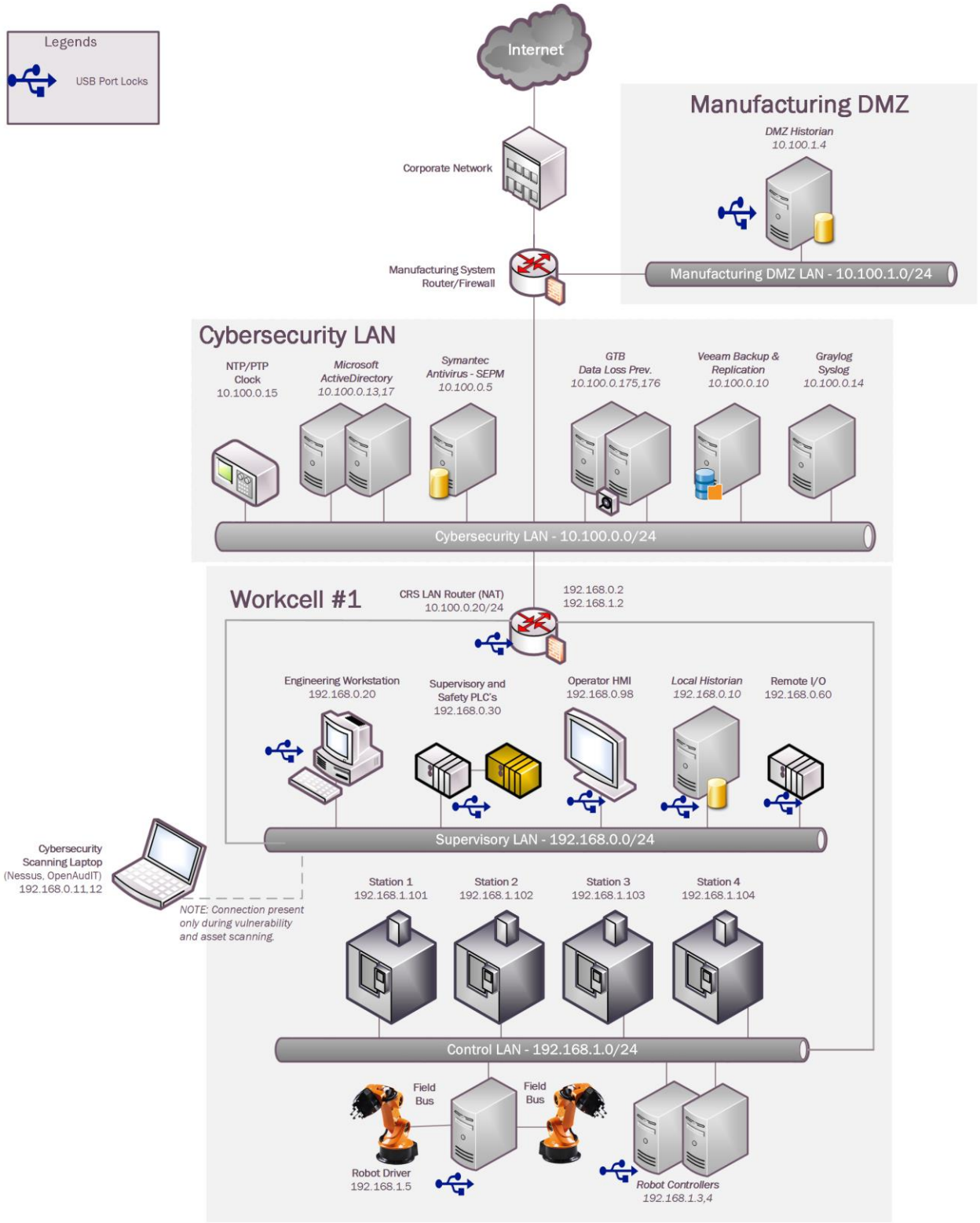
Media Protection provides components of the following Technical Capabilities described in Section 6 of Volume 1:

- Media Protection

4.22.3 Subcategories Addressed by Implementation

PR.PT-2

4.22.4 Architecture Map of Where Solution was Implemented



4.22.5 Installation Instructions and Configurations

- **Product / Tools selected to be implemented in testbed:**
  - Kensington USB Port Locks (Protects Linux Machines)
  - Symantec Endpoint Protection (USB Policy Enforcement - Protects Windows Machines)
  - Group Policy (GPO) Active Directory (Protects Windows Machines)
- **Products Overview:**
  - USB Port locks from Kensington provide an alternative for small manufactures that don't have the resources or primarily run Linux machines within their environment to have a solution that protections from rogue USB devices being used without approval.
    - **Pros:** Quick solution, Hardware only solution, inexpensive
    - **Cons:** Feels like having to force device into USB Port first few times

Insert USB Port lock then push locking button in to secure. Kensington provides inserts to block multiple ports including locks designed for securing USB Keyboards and Mice.

Lessons learned:

Patience is required when using this product so as not to inadvertently damage USB port

4.22.6 Highlighted Performance Impacts

No performance measurement experiments were performed for the USB port locks due to their implementation method (i.e., physically restricting access to USB ports).

4.22.7 Link to Entire Performance Measurement Data Set

N/A

Appendix A - Acronyms and Abbreviations

Selected acronyms and abbreviations used in this document are defined below.

CSF	Cybersecurity Framework
FIPS	Federal Information Processing Standards
HMI	Human Machine Interface
ICS	Industrial Control System
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
ISA	The International Society of Automation
IT	Information Technology
LAN	Local Area Network
NCCIC	National Cybersecurity and Communications Integration Center
NIST	National Institute of Standards and Technology
NVD	National Vulnerability Database
OT	Operational Technology
PLC	Programmable Logic Controller
US-CERT	United States Computer Emergency Readiness Team
VPN	Virtual Private Network

Appendix B - Glossary

Selected terms used in this document are defined below.

Business/Mission Objectives - Broad expression of business goals. Specified target outcome for business operations.

Capacity Planning - Systematic determination of resource requirements for the projected output, over a specific period. [businessdictionary.com]

Category - The subdivision of a Function into groups of cybersecurity outcomes closely tied to programmatic needs and particular activities.

Critical Infrastructure - Essential services and related assets that underpin American society and serve as the backbone of the nation's economy, security, and health. [DHS]

Criticality Reviews - A determination of the ranking and priority of manufacturing system components, services, processes, and inputs in order to establish operational thresholds and recovery objectives.

Critical Services - The subset of mission essential services required to conduct manufacturing operations. Function or capability that is required to maintain health, safety, the environment and availability for the equipment under control. [62443]

Cyber Risk - Risk of financial loss, operational disruption, or damage, from the failure of the digital technologies employed for informational and/or operational functions introduced to a manufacturing system via electronic means from the unauthorized access, use, disclosure, disruption, modification, or destruction of the manufacturing system.

Cybersecurity - The process of protecting information by preventing, detecting, and responding to attacks. [CSF]

Defense-in-depth - The application of multiple countermeasures in a layered or stepwise manner to achieve security objectives. The methodology involves layering heterogeneous security technologies in the common attack vectors to ensure that attacks missed by one technology are caught by another. [62443 1-1]

Event - Any observable occurrence on a manufacturing system. Events can include cybersecurity changes that may have an impact on manufacturing operations (including mission, capabilities, or reputation). [CSF]

Firmware - Software program or set of instructions programmed on the flash ROM of a hardware device. It provides the necessary instructions for how the device communicates with the other computer hardware. [Techterms.com]

Framework - The Cybersecurity Framework developed for defining protection of critical infrastructure. It provides a common language for understanding, managing, and expressing cybersecurity risk both internally and externally. Includes activities to achieve specific cybersecurity outcomes, and references examples of guidance to achieve those outcomes.

Function - Primary unit within the Cybersecurity Framework. Exhibits basic cybersecurity activities at their highest level.

Incident - An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. [CSF]

Integrator - A value-added engineering organization that focuses on industrial control and information systems, manufacturing execution systems, and plant automation, that has application knowledge and technical expertise, and provides an integrated solution to an engineering problem. This solution includes final project engineering, documentation, procurement of hardware, development of custom software, installation, testing, and commissioning. [CSIA.com]

Manufacturing Operations - Activities concerning the facility operation, system processes, materials input/output, maintenance, supply and distribution, health, and safety, emergency response, human resources, security, information technology and other contributing measures to the manufacturing enterprise.

Network Access - any access across a network connection in lieu of local access (i.e., user being physically present at the device).

Operational technology - Hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in the enterprise. [Gartner.com]

Programmable Logic Controller - A solid-state control system that has a user-programmable memory for storing instructions for the purpose of implementing specific functions such as I/O control, logic, timing, counting, three mode (PID) control, communication, arithmetic, and data and file processing. [800-82]

Profile - A representation of the outcomes that a particular system or organization has selected from the Framework Categories and Subcategories. [CSF]

- Target Profile - the desired outcome or 'to be' state of cybersecurity implementation
- Current Profile – the 'as is' state of system cybersecurity

Protocol - A set of rules (i.e., formats and procedures) to implement and control some type of association (e.g., communication) between systems. [800-82]

Remote Access - Access by users (or information systems) communicating external to an information system security perimeter. Network access is any access across a network connection in lieu of local access (i.e., user being physically present at the device). [800-53]

Resilience Requirements - The business-driven availability and reliability characteristics for the manufacturing system that specify recovery tolerances from disruptions and major incidents.

Risk Assessment - The process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact. Part of risk management, synonymous with risk analysis. Incorporates threat and vulnerability analyses. [800-82]

Risk Tolerance - The level of risk that the Manufacturer is willing to accept in pursuit of strategic goals and objectives. [800-53]

Router - A computer that is a gateway between two networks at OSI layer 3 and that relays and directs data packets through that inter-network. The most common form of router operates on IP packets. [800-82]

Security Control - The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for a system to protect the confidentiality, integrity, and availability of the system, its components, processes, and data. [800-82]

Subcategory - The subdivision of a Category into specific outcomes of technical and/or management activities. Examples of Subcategories include "External information systems are catalogued," "Data-at-rest is protected," and "Notifications from detection systems are investigated." [CSF]

Supporting Services - Providers of external system services to the manufacturer through a variety of consumer-producer relationships including but not limited to: joint ventures; business partnerships; outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements); licensing agreements; and/or supply chain exchanges. Supporting services include, for example, Telecommunications, engineering services, power, water, software, tech support, and security. [800-53]

Switch - A device that channels incoming data from any of multiple input ports to the specific output port that will take the data toward its intended destination. [Whatis.com]

System Categorization - The characterization of a manufacturing system, its components, and operations, based on an assessment of the potential impact that a loss of availability, integrity, or confidentiality would have on organizational operations, organizational assets, or individuals. [FIPS 199]

Third-Party Relationships - relationships with external entities. External entities may include, for example, service providers, vendors, supply-side partners, demand-side partners, alliances, consortiums, and investors, and may include both contractual and non-contractual parties. [DHS]

Third-party Providers - Service providers, integrators, vendors, telecommunications, and infrastructure support that are external to the organization that operates the manufacturing system.

Thresholds - Values used to establish concrete decision points and operational control limits to trigger management action and response escalation.

Appendix C - References

1. Executive Order no. 13636, Improving Critical Infrastructure Cybersecurity, DCPD-201300091, February 12, 2013. https://www.govinfo.gov/app/details/FR-2013-02-19/2013-03915

2. National Institute of Standards and Technology (2014) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0. (National Institute of Standards and Technology, Gaithersburg, MD), February 12, 2014. https://doi.org/10.6028/NIST.CSWP.02122014

3. Stouffer KA, Lightman S, Pillitteri VY, Abrams M, Hahn A (2015) Guide to Industrial Control Systems (ICS) Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-82, Rev. 2. https://doi.org/10.6028/NIST.SP.800-82r2

4. Stouffer K, Zimmerman T, Tang CY, Lubell J, Cichonski J, McCarthy J (2017) Cybersecurity Framework Manufacturing Profile. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Internal Report (NISTIR) 8183, Includes updates as of May 20, 2019. https://doi.org/10.6028/NIST.IR.8183

5. Federal Motor Vehicle Safety Standards, 49 C.F.R § 571, 2011.

6. Zimmerman T (2017) Metrics and Key Performance Indicators for Robotic Cybersecurity Performance Analysis. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Internal Report (NISTIR) 8177, Includes updates as of May 21, 2019. https://doi.org/10.6028/NIST.IR.8177

7. Zimmerman T (2019) Manufacturing Profile Implementation Methodology for a Robotic Workcell. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Internal Report (NISTIR) 8227. https://doi.org/10.6028/NIST.IR.8227