

NISTIR 8183A
Volume 3

Cybersecurity Framework Manufacturing Profile
Low Impact Level Example
Implementations Guide:
Volume 3 – Discrete-based Manufacturing System Use Case

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

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

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

NISTIR 8183A
Volume 3

Cybersecurity Framework Manufacturing Profile
Low Impact Level Example
Implementations Guide:
Volume 3 — Discrete-based Manufacturing System Use Case

Keith Stouffer
Timothy Zimmerman
CheeYee Tang
Michael Pease
Intelligent Systems Division
Engineering Laboratory

Jeffrey Cichonski
Applied Cybersecurity Division
Information Technology Laboratory

Neeraj Shah
Strativia, LLC
Largo, Maryland

Wesley Downard
G2, Inc.
Annapolis Junction, Maryland

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

September 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
296 pages (September 2019)

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

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at <https://csrc.nist.gov/publications>.

Comments on this publication may be submitted to:

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

All comments are subject to release under the Freedom of Information Act (FOIA).

Abstract

This guide provides example proof-of-concept solutions demonstrating how available open-source and commercial off-the-shelf (COTS) products could be implemented in discrete-based manufacturing environments to satisfy the requirements in the Cybersecurity Framework (CSF) Manufacturing Profile Low Impact Level. The example proof-of-concept solutions include measured network, device, and operational performance impacts observed during the implementation. Manufacturers should make their own determinations about the breadth of the proof-of-concept solutions they voluntarily implement. Some important factors to consider include: company size, cybersecurity expertise, risk tolerance, and the threat landscape. 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 complement 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:

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

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

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 Readers

This guide describes a proof-of-concept solution for securing manufacturing environments that has only been tested in a lab environment. Manufacturers should make their own determinations about the breadth of the proof-of-concept solutions they voluntarily implement. Some important factors to consider include: company size, cybersecurity expertise, risk tolerance, and the threat landscape. We welcome feedback on its contents and 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.

Revision to Include Updates in Cybersecurity Framework Version 1.1

The Cybersecurity Framework Manufacturing Profile, NISTIR 8183, was drafted and released when the Cybersecurity Framework was at Version 1.0. This guide provides implementation guidance and example proof-of-concept solutions with respect to the language in the original Cybersecurity Framework Manufacturing Profile.

The Cybersecurity Framework Manufacturing Profile, NISTIR 8183, is scheduled to be revised to include the updates in the Cybersecurity Framework Version 1.1, and will be published as NISTIR 8183, Revision 1.

Once NISTIR, 8183, Revision 1 has been released, this implementation guide will be revised to include the updates in the Cybersecurity Framework Version 1.1 as well, and will be published as NISTIR 8183A, Revision 1.

Table of Contents

| | |
|---|-----------|
| Executive Summary | vi |
| 1. Introduction | 1 |
| 1.1 Purpose and Scope | 1 |
| 1.2 Audience | 2 |
| 1.3 Document Structure | 3 |
| 2. Discrete-based Manufacturing System Low Impact Level Use Case | 4 |
| 2.1 Introduction | 4 |
| 2.2 Discrete-based Low Impact Level Use Case | 4 |
| 3. Policy and Procedure Implementations | 10 |
| 3.1 Security Program Document Example | 10 |
| 3.2 Cybersecurity Policy Document Example | 21 |
| 3.3 Cybersecurity Operations Document Example | 34 |
| 3.4 Risk Management Document Example | 52 |
| 3.5 Incident Response Plan Document Example | 60 |
| 3.6 System Recovery Plan Document Example | 74 |
| 3.7 Service Level Agreement | 94 |
| 4. Technical Solution Implementations | 98 |
| 4.1 Introduction | 98 |
| 4.2 Open-AudIT | 103 |
| 4.3 CSET | 114 |
| 4.4 GRASSMARLIN | 119 |
| 4.5 Wireshark | 128 |
| 4.6 Veeam Backup and Replication | 134 |
| 4.7 TeamViewer | 154 |
| 4.8 Microsoft Active Directory | 159 |
| 4.9 Symantec Endpoint Protection | 173 |
| 4.10 Tenable Nessus | 190 |
| 4.11 NamicSoft | 203 |
| 4.12 GTB Inspector | 218 |
| 4.13 Graylog | 226 |
| 4.14 DBAN | 236 |
| 4.15 Network Segmentation and Segregation | 240 |
| 4.16 Network Boundary Protection | 244 |
| 4.17 Managed Network Interfaces | 255 |
| 4.18 Time Synchronization | 260 |
| 4.19 System Use Monitoring | 264 |
| 4.20 Ports and Services Lockdown | 268 |
| 4.21 VeraCrypt | 272 |

4.22 Media Protection 278

Appendix A - Acronyms and Abbreviations 281

Appendix B - Glossary 284

Appendix C - References 288

Executive Summary

This guide provides example proof-of-concept solutions demonstrating how available open-source and commercial off-the-shelf (COTS) products could be implemented in discrete-based manufacturing environments to satisfy the requirements in the Cybersecurity Framework (CSF) Manufacturing Profile [4] Low Impact Level. A manufacturing system could be classified as Low potential impact if the loss of integrity, availability, or confidentiality could be expected to have a limited adverse effect on manufacturing operations, manufactured product, assets, brand image, finances, personnel, the general public, or the environment. A limited adverse effect means that, for example, the loss of integrity, availability, or confidentiality might:

- result in degradation in mission capability to an extent and duration that the system can perform its primary functions, but the effectiveness of the functions is noticeably reduced,
- result in minor damage to operational assets,
- result in minor financial loss, or
- result in minor harm to individuals.

The example proof-of-concept solutions include measured network, device, and operational performance impacts observed during the implementation. Manufacturers should make their own determinations about the breadth of the proof-of-concept solutions they voluntarily implement. Some important factors to consider include: company size, cybersecurity expertise, risk tolerance, and the threat landscape.

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 complement 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 manufacturers, 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 challenges in implementing a standards-based cybersecurity program. This guide provides example proof-of-concept solutions demonstrating how available open-source and commercial off-the-shelf (COTS) products could be implemented in manufacturing environments to satisfy the requirements in the Cybersecurity Framework (CSF) Manufacturing Profile Low Impact Level. A manufacturing system could be classified as Low potential impact if the loss of integrity, availability, or confidentiality could be expected to have a limited adverse effect on manufacturing operations, manufactured product, assets, brand image, finances, personnel, the general public, or the environment. A limited adverse effect means that, for example, the loss of integrity, availability, or confidentiality might:

- result in degradation in mission capability to an extent and duration that the system can perform its primary functions, but the effectiveness of the functions is noticeably reduced,
- result in minor damage to operational assets,
- result in minor financial loss, or
- result in minor harm to individuals.

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. Manufacturers should make their own determinations about the breadth of the proof-of-concept solutions they

voluntarily implement. Some important factors to consider include: company size, cybersecurity expertise, risk tolerance, and the threat landscape. 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's environment,
- the environment does not reflect the complexity of a production environment, and
- 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, and
- 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 Impact Level Use Case

2.1 Introduction

This use case is a proof-of-concept demonstrating how available open-source and commercial off-the-shelf (COTS) products could be implemented in a discrete-based manufacturing environment to satisfy the requirements in the Cybersecurity Framework (CSF) Manufacturing Profile Low Impact Level. Manufacturers should make their own determinations about the breadth of the proof-of-concept solutions they voluntarily implement. Some important factors to consider include: company size, cybersecurity expertise, risk tolerance, and the threat landscape.

2.2 Discrete-based Low Impact Level Use Case

The fictional company, Alpha Industries (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 procured from a manufacturing systems integrator. The workcell was purchased to evaluate and validate its operation, with the intent of purchasing more workcells to further increase productivity. 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 1500 m² in size.

2.2.2 Employees

Alpha has ten full-time employees, and six of those are machine operators. Alpha has no full-time control system engineers, or on-site IT or operational technology (OT) personnel. None of the employees have any formal cybersecurity training.

| Company Role | Count | Major Responsibilities |
|-------------------|-------|--|
| President | 1 | General oversight of the company. |
| HR Manager | 1 | Manager of human resource activities. |
| Bookkeeper | 1 | Documentation and tracking of business activities (e.g., finance, payroll, accounts receivable). |
| Supervisor | 1 | Oversight of manufacturing operations. |
| Machine Operators | 6 | Operation of the manufacturing system and its components. |

2.2.3 External Personnel

The following facility operations are outsourced to external entities.

| Role |
|--|
| Information Technology (IT) support services |
| Operational Technology (OT) support services |
| Machine tool support, service, and repair |
| General janitorial services |

2.2.4 Supply Chain

Raw material suppliers are utilized on-demand. No formal relationships or direct-order connections (i.e., network, online, or cloud-based ordering systems) with any suppliers currently exist. Alpha is considered a "tier two" supplier. Alpha sends completed parts to a tier one manufacturer. The tier one manufacturer integrates Alpha's parts into subassemblies that are subsequently installed into a vehicle by the original equipment manufacturer (OEM).

2.2.5 Supporting Services

The supporting services required by Alpha are electricity, water, and Internet. The broadband Internet connection is a business class service provided by a large national provider with business class service level agreement.

2.2.6 Legal and Regulatory Requirements

Alpha does not have knowledge of any legal or regulatory requirements regarding its cybersecurity program. However, as a tier two supplier, it is contractually obligated to follow all standards, procedures, and guidance provided by the tier one manufacturer 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.

2.2.7 Critical Infrastructure

The Department of Homeland Security (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 assumed 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 computer numerical control (CNC) machines (i.e., machining station) within a workcell. The CNC machines are tended to by two industrial robotic arms, which transfer parts to each station until all the machining processes are completed. Raw materials are loaded into a queue by an operator. A supervisory programmable logic controller (PLC) monitors the 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
- Human machine interface (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 Transmission control protocol (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 considered proprietary, trade secrets, or sensitive.

2.2.12 Network

The manufacturing system network is connected to the corporate network through a dedicated top-level router and firewall and is segmented into smaller networks organized into subnetworks and a demilitarized zone (DMZ). The network is managed by an external IT contractor. The workcell has a dedicated router and firewall utilizing network address translation (NAT) to help segment and isolate the workcell from the rest of the network. The workcell itself is divided into two subnets, the Supervisory local area network (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, regarding 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

This section provides example content that a Cybersecurity Program document may contain, including example policy and procedure statements that were developed for the fictional company Alpha. Certain commercial entities, equipment, or materials may be identified in this document in order to describe a concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, equipment, or materials are necessarily the best available for the purpose. Each organization’s information security experts should identify the content, and policy and procedure statements that will best integrate with their existing cybersecurity program and manufacturing system infrastructure.

Cybersecurity Program for Alpha

| | |
|------------------------|------------|
| Document Owner: | Supervisor |
|------------------------|------------|

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, approvers agree to all terms and conditions outlined in this document.)

| Approvers | Role | Signed | Approval Date |
|---------------|-----------|---------------------|---------------|
| S. Forthright | President | <digital signature> | 4-22-2018 |

3.1.1 Purpose

The Cybersecurity 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, or customers.

3.1.2 Audience

This document is intended to be used by the president, supervisor, or any other personnel, as deemed appropriate by the supervisor. It supports the company's responsibility for implementing a cybersecurity program.

3.1.3 Commitment from Management

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

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. No formal relationships or direct-order connections (i.e., network, online, or cloud-based ordering systems) with any suppliers currently exist. Alpha is considered a "tier two" supplier. Alpha sends completed parts to a tier one manufacturer. The tier one manufacturer integrates Alpha's parts 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 Programmable Logic Controller (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

- Not applicable - The manufacturing process does 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.
- Human Machine Interface (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 Workstation - 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 Workstation - 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 that 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 by in-stock availability. No formal relationships or direct-order connections (i.e., network, online, or cloud-based ordering systems) 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 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 and contractors depending on their role in the company.

Critical Manufacturing System Components

Critical manufacturing system components are defined as the following:

- Engineering workstation
- Supervisory PLC
- HMI
- Machining stations
- Robot arms
- Robot controllers
- Robot driver
- Network devices

Supporting Services

The supporting services required by Alpha are electricity, water, and Internet. The broadband Internet connection is a business class service provided by a large national provider with a business class service level agreement.

3.1.5 Cybersecurity Policy

The purpose of the Cybersecurity 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 Cybersecurity Program. The policy is developed and executed by the supervisor, and expectations are set for protecting Alpha's IT and Operational Technology (OT) assets.

3.1.6 Applicable Laws and Regulations

Alpha does not have knowledge of any legal or regulatory requirements regarding its cybersecurity responsibilities. 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, company 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 Cybersecurity Program and supporting policies, at least annually,
- assigning responsibility for company policies and procedures for the use of Alpha's IT/OT assets, implementation, documentation and for meeting its compliance obligations, and
- overseeing efforts to develop, implement, and maintain an effective cybersecurity program including regular review of reports from the supervisor.

The supervisor is responsible for:

- serving as the point of contact for any cybersecurity related incident,
- implementing and maintaining Cybersecurity Policy documents,
- overall security of all IT/OT assets, operations and remediating risks and vulnerabilities,
- acting as a liaison between workcell operators, vendors and management on matters relating to security, and
- reporting to the president about the status of the program, any security related risks, or cybersecurity 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 have no expectation of privacy on Alpha systems. All activity on Alpha systems and network is subject to monitoring. 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 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 a 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 must swipe their company-issued identification 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.

Additionally, personnel security is addressed through pre-employment screenings, adequate position descriptions, terms of employment, and cybersecurity education and training. Additional details regarding physical security requirements are mentioned in Section 3.2.6 Physical Security of the Cybersecurity Policy.

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 are required prior to granting access or operating any components of the manufacturing system. 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 components are controlled. Duties are separated to protect systems and data and access rights are audited at regular intervals.

3.1.10 Cybersecurity Awareness Training

Cybersecurity 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 cybersecurity incidents. Additionally, the supervisor will ensure the employee understands their role and responsibilities in Alpha's Cybersecurity 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. Below is an example list of training options. Trade organization subscriptions, newsletters, and magazines will offer more industry-specific training classes.

Example Training

- ICS-CERT VLP¹ (Virtual Learning Portal)
- SCADAhacker²
- SANS Industrial Control Systems Training³
- ISA Training⁴

Training for Privileged Users

Training for privileged users includes the assigned training for regular users. Advanced training will be provided from industry trade groups specializing in automation or other specialty training organization focusing on cybersecurity for ICS environments.

Example Training

- International Society of Automation (ISA)⁵
- SANS (Information Security Training)⁶

Training for Third Party contractors

Third party contractors must complete cybersecurity awareness training before they are allowed to access any IT/OT systems. Training can be completed in person at a training facility, or online in a virtual classroom environment.

Example Training

- SANS Industrial Control Systems Training⁷ (training with instructors – fee applies).
- ICS-CERT VLP⁸ (Virtual Learning Portal) (virtual classroom environment at no cost).

¹ <https://ics-cert-training.inl.gov>

² <https://scadahacker.com/training.html>

³ <https://ics.sans.org/training/courses>

⁴ <https://www.isa.org/training-and-certification/isa-training/security-cybersecurity-and-ansi-isa99-training-courses/>

⁵ <https://www.isa.org>

⁶ <https://www.sans.org>

⁷ <https://ics.sans.org/training/courses>

⁸ <https://ics-cert-training.inl.gov>

3.1.11 Third Party Responsibilities and Requirements

1. Third party contractors and vendors are required to comply with the Cybersecurity Policy to protect sensitive information and to ensure sensitive information is secured.
2. Third party contractors and vendors will be re-evaluated yearly from the date of completion of the first security compliance check. During this re-certification process, all objectives listed in the Security Awareness Training section above will be revisited to ensure compliance.
3. All remote connections from third party providers will be conducted using a desktop sharing program. These connections will be monitored and audited.
4. All software and hardware tools used on the network must be approved by the supervisor before they can be used or deployed.
5. Any data that will be shared requires a documented memorandum of understanding to be executed by both parties.
6. Network accounts will only be created and enabled as required. Accounts used by vendors for remote access require approval from the president. Refer to Remote Maintenance Approval in the Cybersecurity Policy document for additional details on the approval process.

3.1.12 Fire Protection, Safety, and Environmental Systems

All fire and safety systems for protecting the manufacturing system must comply with local, state, and federal laws. This is to include safety regulations for workers' safety from Occupational Safety and Health Administration (OSHA). Industry regulations for safety will be followed per guidance from the regulating industry. Any fire protection systems must be designed to protect human life as a first priority, and manufacturing equipment as a second priority. Fire protection for the manufacturing system must be safe to use around electrical equipment (e.g., PLCs, HMIs, robots, servers). Fire protection systems must be certified compliant by a licensed and accredited vendor.

All environmental systems (e.g., HVAC) used in the manufacturing system environment must be compliant with all local, state, and federal laws, and must be designed to protect human life as a first priority, and manufacturing equipment as a second priority.

3.1.13 Emergency Power

A short-term uninterruptible power supply (UPS) is used 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 Plan and System Recovery Plan describes the detection, analysis, containment, eradication, recovery and review of cybersecurity incidents. The process for responding to cybersecurity incident is designated in the Incident Response Plan, while the procedures for system recovery and resilience requirements are defined in the System Recovery Plan. Security incidents are managed by the supervisor who ensures that cybersecurity 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 System Recovery Plans are reviewed annually and updated as required.

Lessons learned from cybersecurity incidents will be used to revise and improve detection capabilities 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 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 (NDA) before data is transmitted; this would be considered sensitive information requiring approval from executive management before being sent.

Local Government

Relationships shall be established with local government with the primary purpose to share cybersecurity incident data.

State Government

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

Federal Government

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

- DHS (CISA)⁹ Agency for reporting incidents of Phishing, Malware, Vulnerabilities.
- DHS (NCCIC)¹⁰ Agency for reporting cybersecurity incidents relating to Industrial Control Systems.

3.1.16 Periodic Reevaluation of the Program

The Cybersecurity Program document will be continuously updated to reflect changes made to the 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 Alpha's operations, business or infrastructure components
- Any cybersecurity incident

3.1.17 Additional Resources

1. Implementing Effective Information Security Program by SANS Resources¹¹
2. InfoSec Program Plan by University of Tennessee Knoxville¹²
3. GCADA Sample Information Security Procedure¹³
4. IT Security Program by Old Dominion University¹⁴

⁹ <https://www.us-cert.gov/report>

¹⁰ <https://ics-cert.us-cert.gov/Report-Incident>

¹¹ <https://www.sans.org/reading-room/whitepapers/hsoffice/designing-implementing-effective-information-security-program-protecting-data-assets-of-1398>

¹² <https://oit.utk.edu/wp-content/uploads/2015-11-11-utk-sec-prog-plan.pdf>

¹³ [http://www.gcada.org/pdf/Sample%20Information%20Security%20Procedure%20\(safeguard%20policy\).pdf](http://www.gcada.org/pdf/Sample%20Information%20Security%20Procedure%20(safeguard%20policy).pdf)

¹⁴ <https://www.odu.edu/content/dam/odu/offices/occs/docs/odu-it-security-program.pdf>

3.2 Cybersecurity Policy Document Example

This section provides example content that a Cybersecurity Policy document may contain, including example policy and procedure statements that were developed for the fictional company Alpha. Certain commercial entities, equipment, or materials may be identified in this document in order to describe a concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, equipment, or materials are necessarily the best available for the purpose. Each organization’s information security experts should identify the content, and policy and procedure statements that will best integrate with their existing cybersecurity program and manufacturing system infrastructure.

Cybersecurity Policy for Alpha

| | |
|------------------------|------------|
| Document Owner: | Supervisor |
|------------------------|------------|

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, approvers agree to all terms and conditions outlined in this document.)

| Approvers | Role | Signed | Approval Date |
|---------------|-----------|---------------------|---------------|
| S. Forthright | President | <digital signature> | 4-22-2018 |

3.2.1 Purpose

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

3.2.2 Scope

This Cybersecurity Policy applies to any employee, contractor, or individual with access to the manufacturing system, or its 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.

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

3.2.4 Role-based Security Responsibilities

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

| Organizational Role | Security Responsibilities |
|---------------------|--|
| President | <ul style="list-style-type: none"> • Serve as Point of Escalation for any incidents. • Responsible for coordinating data breach response. |
| HR Manager | <ul style="list-style-type: none"> • Report any cybersecurity risks to the supervisor |
| Bookkeeper | <ul style="list-style-type: none"> • Report any cybersecurity risks to the supervisor |
| Supervisor | <ul style="list-style-type: none"> • Responsible for overall cybersecurity of all IT/OT assets. • Responsible for remediating detected events or vulnerabilities. • Implement and maintain Security Policy documents. • Serve as the point of contact for any cybersecurity related incident and keeping upper management in the loop. |
| Operators | <ul style="list-style-type: none"> • Help with the cybersecurity requirements for their specific area. • Often assume responsibility for intrusion detection. • Report any cybersecurity risks or events detected to the supervisor. • Assist in remediating vulnerabilities if asked by the supervisor. |

External Personnel

| Role | Security Responsibilities |
|---------------------------|--|
| IT / OT Contractor | <ul style="list-style-type: none"> • Implement/Setup Tools and Technologies as requested by the supervisor. • Report any cybersecurity risks to the supervisor • Assist in remediating vulnerabilities if required. • Comply with Alpha’s cybersecurity policy |
| Machine Vendor | <ul style="list-style-type: none"> • Assist in remediating vulnerabilities, upgrading software or hardware as required. • Comply with Alpha’s cybersecurity policy. |
| Visitor | <ul style="list-style-type: none"> • Comply with Alpha’s cybersecurity policy. |

3.2.5 Employee requirements

1. Employees must complete cybersecurity awareness training and agree to uphold the acceptable use policy.
2. Employees must immediately notify the supervisor if an unescorted or unauthorized individual is found in the facility.
3. Employees must always use a secure password on all systems as per the password policy. These credentials must be unique and must not be used on other external systems or services.
4. Terminated employees must return all company records, in any format.
5. Employees must verify with the supervisor that authorizations have been granted before allowing external personnel to connect to the IT or OT network.
6. Employees must report any physical or cybersecurity incidents to the supervisor.

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

3.2.6 Physical Security

1. Employees must always use and display company-provided physical identification (ID).
2. IDs must be designed to enable the immediate visual distinction between employees, external personnel, and visitors.
3. Sharing of IDs for any reason is strictly prohibited.
4. Employees must only access areas they are authorized.
5. A sign-in sheet will be maintained to record entry and exit of all visitors. These records must be reviewed periodically.
6. Any visitors, contractors, and maintenance personnel must always be escorted by an employee.
7. Unauthorized removal of any company documentation, equipment, or media from the facility is restricted, unless authorized by the supervisor.
8. All activities of visitors, contractors, and maintenance personnel will be subject to monitoring while onsite. The supervisor, or a designated employee, will be assigned to monitor all computer activities if the visitor, contractor, or maintenance personnel is connected to any company network.
9. The 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.
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 OT assets they have been assigned.
3. Physical access to OT assets is forbidden for non-authorized personnel.
4. All personnel interacting directly with OT assets must have proper training.
5. The supervisor is responsible for all OT devices. The supervisor is solely responsible for maintenance and configuration of the OT devices. 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 supervisor
7. All operators must be notified before security tools are used on the OT network.
8. Concept of least privilege must be followed when authorizing access to OT assets.
9. OT assets, such as PLCs, safety systems, etc., should have their keys in the “Run” position at all times unless being actively programmed.
10. Accessing IT devices or internet use from the OT network, or OT assets, unless authorized, is prohibited.
11. Use of personal devices to access OT resources is prohibited.

OT Asset Inventory

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

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 a desktop PC or laptop must be reimaged prior to assigning it to a different employee.

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

3.2.10 System Maintenance

1. Any maintenance tasks involving external personnel (e.g., contractors, vendors) must be approved by the supervisor.
2. External personnel with access to company resources must properly secure any resources that are used to access Alpha networks or systems.
3. All remote maintenance activities will be controlled and monitored to ensure no harmful or malicious activities occur. Detailed logging of the activity will be performed by an employee.
4. All systems and technical controls must be verified upon the completion of maintenance for any cybersecurity related impact.
5. The supervisor will log all maintenance activities in a Maintenance Tracker.

3.2.11 Data

1. Access to sensitive data must be authorized by the supervisor.
2. Data should not be shared informally. When access to sensitive information is required, personnel can request access from the supervisor and should take all necessary steps to prevent unauthorized access.
3. The supervisor must immediately be notified in the event a device is lost containing sensitive data (e.g. mobiles, laptops, USB devices).
4. Encrypted portable media or secure protocols must be used while transporting or transferring sensitive company data.
5. Extra precautions must be taken by remotely-operating employees to ensure sensitive data is appropriately protected.
6. Physical copies of data should be stored in a secure location when not in use.
7. Personnel should ensure physical copies of sensitive data are not left unattended (e.g., on a printer or a desk).
8. Physical copies of sensitive data should be shredded or disposed in a secure manner when no longer required.

Data types considered sensitive, proprietary, or containing trade secrets

| 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 | ✓ | | ✓ |

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 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 supervisor has privileged access to the manufacturing system. All other privileged user accounts are granted to individuals on a case-by-case basis by the supervisor.

Responsibilities:

1. Any privileged user within the 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 the same rights as a standard Westman user account (e.g., email access, Internet access).
 - Privileged accounts will have administrative privileges and must only be used when performing administrative functions within the manufacturing system (e.g., system updates of firmware or software, system reconfigurations, device restarts).
2. Privileged users will adhere to securely using Administrative accounts when performing duties within the manufacturing system. If a privileged 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 protection (e.g., workstations and servers) and be configured to limit resources consumed as not to impact manufacturing system production.

2. Installed antivirus will be configured to receive push updates from a central management server, or other antivirus clients if supported.

3.2.16 Internet

1. Only authorized Internet access from the manufacturing system network is permitted.
2. Internet access for individual devices must be approved by the supervisor.
3. Inbound and outbound traffic must be regulated using firewalls in the perimeter.
4. All internal and external communications must be monitored and logged. Logs must be reviewed regularly by the workcell operators and reported to the supervisor.

3.2.17 Continuous Monitoring

1. Comprehensive network monitoring using commercial or open-source tools to detect attacks, attack indicators, and unauthorized network connections must be implemented.
2. The manufacturing system must be monitored for any cybersecurity attack indicators.
3. All external boundary network communications will be monitored.
4. All cybersecurity incidents must be logged in the incident response management system for documentation and tracking purposes.
5. All local, state, federal, regulatory, and other mandated detection activities that apply to the manufacturing system must be followed in accordance with the law, regulations, or policies.
6. Monitoring activity levels will be increased during periods of increased risk or other factors.
7. All cybersecurity incidents must be communicated to the personnel defined below:

| 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 ICS-CERT¹⁵ to help secure the organization, including helping secure the industry. The Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) provides services for manufacturers to report cybersecurity events.

¹⁵ <https://ics-cert.us-cert.gov/>

3.2.18 User Access Agreement

Each employee provided with access to any IT or OT resources (e.g., the manufacturing system, email, HR system) will be required to review and accept the terms of a User Access Agreement.

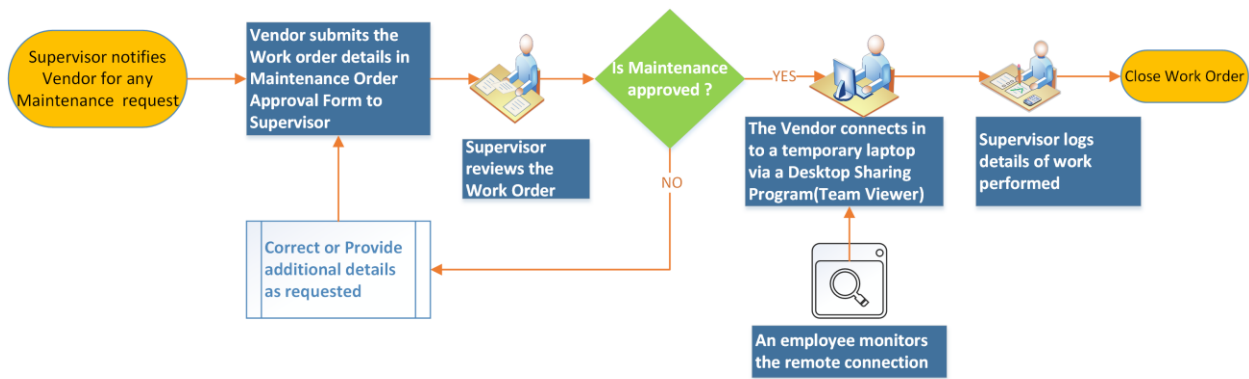
3.2.19 Remote Access

This policy applies to the users and devices that require access to manufacturing system resources from remote locations. The following rules are applicable for a one-time request.

1. All remote access requires approval by the supervisor.
2. Remote access to sensitive information is not permitted on unencrypted connections.
3. Installation and use of remote access software on authorized devices must be approved by the supervisor.
4. Any device used for remote access work must have anti-virus installed along with up-to-date antivirus signatures.

3.2.20 Remote Maintenance Approval Process

Shown below is the approval process and procedure for performing remote maintenance on IT/OT assets.



REMOTE MAINTENANCE APPROVAL PROCESS & WORKFLOW

3.2.21 Maintenance Approval Form

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

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

3.2.22 Acronyms

| Acronym | Definition |
|-----------------|--|
| AV | Anti-virus |
| CISA | Cybersecurity and Infrastructure Security Agency |
| DHS | Department of Homeland Security |
| HMI | Human Machine Interface |
| HR | Human Resources |
| ICS | Industrial Control System |
| ICS-CERT | Industrial Control Systems Cyber Emergency Response Team |
| ID | Physical or Logical identification (e.g., badge, login name, etc.) |
| INFOSEC | Information Security |
| ISA | International Society of Automation |
| IT | Information Technology |
| NCCIC | National Cybersecurity and Communications Integration Center |
| NDA | Non-Disclosure Agreement |
| OSHA | Occupational Safety and Health Administration |
| OT | Operational Technology |
| PLC | Programmable Logic Controller |
| PPD | Presidential Policy Directive |
| SCADA | Supervisory Control and Data Acquisition |
| UPS | Uninterruptible Power Supply |
| USB | Universal Serial Bus |
| VPN | Virtual Private Network |

3.2.23 Definitions

| Term | Definition |
|--|--|
| Access Management | The practices, policies, procedures, data, metadata, and technical and administrative mechanisms used to manage access to the resources of an organization |
| Asset | A device owned by the organization |
| AV scanning | The act of scanning a device for viruses |
| 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) |
| Industrial control system (ICS) | Typically, the hardware and software used to control processes, or operate machines and manufacturing processes |

| Term | Definition |
|------------------------------------|---|
| Information technology (IT) | Information Technology which includes devices such as servers, laptops, workstations, switches and routers. |
| 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) | Operational Technology which includes Industrial control system devices that are 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 |
| Security tools | |
| Sensitive Information | Data containing customer, personnel, proprietary, or trade secrets information pertaining to the operations of the organization; data that could cause damage to the organization if obtained by an attacker |
| Split tunneling | The process of allowing a remote user or device to establish a non-remote connection with a system and simultaneously communicate via some other connection to a resource in an external network. This method of network access enables a user to access remote devices (e.g., a networked printer) at the same time as accessing uncontrolled networks. [NIST SP 800-171 R1] |
| User | Individual using a device |
| Virus signature | Data used by antivirus software to identify viruses |
| Vulnerability | A weakness or a flaw in the system which an attacker can exploit to gain access. |
| Vulnerability scanning | Software used to detect common or known vulnerabilities on a device |

3.2.24 Additional Resources

1. Security Policies by SANS Resources¹⁶
2. Template for Security Policy by Project Management Docs¹⁷
5. Data Security Policy by Sophos labs¹⁸

¹⁶ <https://www.sans.org/security-resources/policies>

¹⁷ <http://www.projectmanagementdocs.com/template/Security-Policy.doc>

¹⁸ <https://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-example-data-security-policies-na.pdf?la=en>

3.3 Cybersecurity Operations Document Example

This section provides example content that a Standard Operating Procedure document may contain, including example policy and procedure statements that were developed for the fictional company Alpha. Certain commercial entities, equipment, or materials may be identified in this document in order to describe a concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, equipment, or materials are necessarily the best available for the purpose. Each organization’s information security experts should identify the content, and policy and procedure statements that will best integrate with their existing cybersecurity program and manufacturing system infrastructure.

Cybersecurity Operations for Alpha

| | |
|------------------------|------------|
| Document Owner: | Supervisor |
|------------------------|------------|

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, approvers agree to all terms and conditions outlined in this document.)

| Approvers | Role | Signed | Approval Date |
|---------------|-----------|---------------------|---------------|
| S. Forthright | President | <digital signature> | 4-22-2018 |

3.3.1 Introduction

This document defines the operational steps management and employees will follow ensuring consistence with response to events occurring within the manufacturing system for Alpha. This document contains content which should be referred to often to help ensure all employees and individuals performing work within the manufacturing system are familiar with cybersecurity operations.

3.3.2 Purpose

To provide a consistent cybersecurity operational environment for supporting the manufacturing system.

3.3.3 Scope

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

3.3.4 Asset Inventory

Identifying assets within the manufacturing system is a vital first step in protecting the company from malicious activities that could result in disruption to production. Additionally, knowing what devices are authorized to connect to the network enables the detection of unapproved devices which could be an indication of malicious activity. Similarly, tracking software installed on networked devices provides the necessary information to support software update and patching processes to eliminate vulnerabilities. Alpha uses both manual and automated asset inventory tools to support asset inventory management. Specifically, two types of asset inventories are performed on the manufacturing system:

- Manual Inventory - Devices that cannot be automatically scanned (e.g., PLC, machining stations). These devices are manually entered into an excel spreadsheet and updated at least quarterly.
- Automated Inventory - Devices that can be automatically scanned will be configured in the asset inventory tool for auditing (i.e., Open-AudIT). Access to Open-AudIT is granted only to authorized personnel.

All inventory processes are conducted during manufacturing system down time and must include both hardware and software. Periodic hardware and software scans are performed on devices within the manufacturing system to detect any unauthorized hardware or software changes. Examples of changes that might occur within the manufacturing system include updating software, license, system patches, firmware updates, and adding new devices like PLCs' or HMIs' or other ICS components required for operations. To detect these changes within the manufacturing system, scans are conducted at least quarterly to record current device information, configuration, and installed software (e.g., license information, software version, and configuration). These scan results are used to identify any unauthorized hardware and non-essential software applications installed on devices within the manufacturing system.

Additionally, device configuration baselines are used to ensure inadvertent changes are detected before system integrity impacts can affect the manufacturing process. Both manual and automated methods are used to capture current device configurations for validation against approved baselines. The manual method is used for ICS devices that do not support automated scanning tools. Specifically, devices lacking SSH, SNMP, WMI services are manually documented in the excel spreadsheet. Automated device configuration scans are implemented

using Open-AudIT which was selected for Alpha due to scalable configuration depending on required needs.

Once scanning has been performed, the information gathered is compared to approved baselines with any identified changes documented for review and investigation. Any hardware or software identified within the manufacturing system that is not authorized or required for operations is scheduled for removal at the earliest opportunity that does not impact the manufacturing process. Otherwise, for any identified changes, if the change is approved, the associated baseline is updated to reflect the approved change. If the change is not approved, the device is reverted to the approved configuration and an investigation into how the unauthorized change was deployed is performed to determine if a cybersecurity incident occurred.

Device configuration baselines must be reviewed at least quarterly and updated after any approved engineering change to the manufacturing system. During the period between baseline reviews, any new equipment added or configuration changes implemented will initiate a new baseline scan to be performed. Additionally, GRASSMARLIN¹⁹ and Wireshark²⁰ are used for updating the environment network diagrams, verifying information flows, and providing any additional information for supporting baseline updates after new equipment is added to the environment.

3.3.5 Networking

The Alpha network environment for supporting manufacturing must be secured from unauthorized access and tampering to ensure the availability, integrity, and confidentiality of the information used to support the manufacturing processes. This requires all network connection with manufacturing system components be documented and cables clearly labeled to indicate their designated purpose. Additionally, all network switches must be configured for supporting network segmentation and port security, to control network traffic and prevent unauthorized devices from accessing the manufacturing network. Any network connection with the manufacturing environment will be reviewed and authorized by the supervisor before being placed into production.

To assist with these efforts, Alpha creates and maintains a comprehensive network baseline that provides an accurate document of the network environment and supports the processes to detect anomalies within the manufacturing system networks. The network baseline documentation is reviewed and updated at least quarterly to identify all components and communications required for manufacturing production operations. Tools used for this process include Open-AudIT, GRASSMARLIN, and Wireshark. Additionally, using company provided network diagram tools, the network baseline documentation will include detailed network diagrams for all internal and external network connection including any cloud services. Specifically, network diagrams will include all relevant information for connection services provided including: assigned IP

¹⁹ <https://github.com/nsacyber/GRASSMARLIN>

²⁰ <https://www.wireshark.org>

address for devices, service provided, data flow directions, data types, support phone number, customer number, contact person, support level agreement, and hours of support.

The network baseline documentation will also include the configuration details for network segmentation and port security within the environment. The Alpha network for manufacturing systems is segmented to improve speed and cybersecurity within the environment. Network segmentation utilizes the RuggedCom firewall configured with the following interfaces to establish two (2) subnets for the environment. 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 include the 4 Machining stations and Robot Driver server were assigned an IP address from the Control LAN subnet (192.168.1.0/24). Finally, 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 include the PLC, HMI, and Engineering workstation with assigned IP address from this Supervisory LAN subnet (192.168.0.0/24)

| 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 |

Network traffic between network segments is controlled using firewall network devices. These devices are configured based on the approved network baseline to allow approved network traffic to enter or leave the manufacturing network segments while dropping all other traffic. The details associated with the network segmentation, firewalls, and firewall rules is included in the network baseline documentation. The following table provides a high-level summary of the connections maintained for the environment and device responsible for implementing approved communication connections.

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

The Alpha network for manufacturing systems also utilizes managed switches that are configured with port security enabled. Port security provides the ability to allow authorized devices based on their unique Media Access Control (MAC) addresses to utilize specific network switch ports. The port security documentation will include a reference to the asset information for the approved devices and list device MAC addresses with the assigned network switch and switch port.

Should Alpha require vendor or contractor remote maintenance support, these activities will be coordinated and approved before remote access is allowed. All remote maintenance activities will be controlled and monitored by a knowledgeable Alpha employee to ensure no harmful or malicious activities occur. Any vendors or contractors connecting to Alpha for remote maintenance will: require approval from the supervisor before connecting; utilize the approved secure remote access procedures; and have the remote access revoked after completing the approved task(s). All remote access maintenance activities will be documented to ensure a proper audit trail for activity conducted within the manufacturing systems.

All network devices will be configured to forward logs to the Alpha internal Syslog server. For the Alpha network for manufacturing systems, this includes the network switches, the Cisco Adaptive Security Appliance (ASA) firewall supporting the Cybersecurity LAN network, and the Stratix 8300 series firewall in the workcell.

At least monthly, authorized Alpha personnel will use the information collected from these devices and the GRASSMARLIN tool to perform comparisons of current network activity to the documented baseline. These efforts will help identify any unusual traffic which might indicate either system issues or potential malicious activity. Additionally, switch logs will be checked at least monthly to ensure no rogue devices have attempted to connect. Any observed network activity not already documented in the baseline must be reconciled and either incorporated into the baseline or investigated as a possible system or cybersecurity incident.

Additionally, authorized Alpha personnel will utilize a wireless enabled laptop or mobile device configured to use either the native capabilities of the operating system or approved wireless scanning software to perform weekly sweeps within the manufacturing areas to detect for unauthorized wireless devices or rogue access points. Any detected anomalies will be documented including location(s) of detection and submitted for additional investigation.

3.3.6 Manufacturing System Security

Adherence to the Cybersecurity Program by all personnel is critical to reduce the risk of cybersecurity incidents on the manufacturing system. The following sections describe policies and procedures relating to manufacturing system security.

3.3.6.1 Change Control

Any changes to the manufacturing system must be tracked by the change control process, ensuring that all personnel are notified of the proposed changes and are involved in the process. Changes will be formally reviewed and authorized before implementation.

A thorough review of the change must be performed to determine if:

- the change will impact manufacturing system performance, or
- the change will impact the security of the manufacturing system.

Change control reviewers will make a final determination before any changes are performed, along with justifications for accepted risks.

Approved changes will be scheduled during downtime or other maintenance activities to limit impact to production. Once changes have been completed, a security review will be conducted to determine if any unexpected changes to cybersecurity controls occurred as a result of the changes implemented. Any unexpected cybersecurity control changes are reviewed and processed in accordance with the Vulnerability and Remediation Management processes.

The manufacturing system will be evaluated at least quarterly to identify devices that are critical to its operation. This information will be used to provide a criticality report outlining the critical equipment and will be used to update other company cybersecurity documents and procedures.

Below is a table of devices that must be part of the change control process:

| 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 |

3.3.6.2 Personnel Actions

Actions performed on manufacturing system devices may require authentication. Those actions are defined in the following tables. The term *All Users* only applies to users that have been granted authorization to interact with the device. 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 |

| 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 |

| 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 |

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

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

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

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

| 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.

3.3.6.3 Monitoring the Manufacturing System

The manufacturing system environment will be monitored for unauthorized activity associated with personnel, software, network devices, and wireless access points. Alpha has established a central log server (Syslog Server) for supporting this capability and is configured to aggregate all system-generated logs and store the logs for archival and forensics purposes. Whenever supported, devices within the manufacturing system must be configured to send log data to the central syslog repository.

Logs will be checked periodically looking for abnormal alerts being generated from the manufacturing system. Specifically, logged events will be examined to determine if any impact the manufacturing process. At a minimum, detected cybersecurity event notification will be investigated to determine root cause and appropriate remediation steps will be taken to clear events and return the manufacturing system to a known good operating state. Events impacting

the manufacturing process will be reviewed to determine correlation with risk assessment outcomes and identify actions required to improve Alpha's cybersecurity posture.

All non-employees physically accessing the manufacturing system will be required to sign the visitor log, including the date, time of entry, and time of exit. Any unauthorized visitors will be escorted out of the facility. Visitors must be escorted by an employee of Alpha at all times.

3.3.6.4 Backups

The following backup procedures are defined for servers and hosts of the manufacturing system:

- Veeam directory backups are performed on select directories containing configuration and logic data for the manufacturing system are performed weekly during periods of low volume production (e.g., overnight).
- Veeam full system image backups are performed quarterly during periods of low volume production (e.g., overnight), and after any engineering change.

| Host | Veeam Directory Backups | Veeam Full System Image | Other Methods |
|-------------------------------------|-------------------------|-------------------------|---|
| Engineering Workstation | ✓ | ✓ | |
| Robot Driver | | ✓ | |
| Robotics Hypervisor | | ✓ | |
| Robot Controllers | | ✓ | |
| HMI Host Server | | ✓ | |
| Local Historian Host | | ✓ | OSIsoft PI historian data of the manufacturing process is duplicated in real-time to the DMZ Historian. |
| Hyper-V Host Server | | ✓ | |
| Active Directory Server | | ✓ | |
| Backup Active Directory Server | | ✓ | |
| DMZ Historian | | ✓ | The native OSIsoft PI application backup feature archives production data from the manufacturing process. These backups are stored on the local host; restore the host to obtain the most recent backup version. <u>NOTE:</u> Any recovered historical data will be limited to data present at the time of the backup. |
| Veeam Backup Server | | ✓ | |
| Symantec Antivirus Server | | ✓ | |
| Graylog Server | | ✓ | |
| GTB Inspector Server | | ✓ | |
| GTB Console Server | | ✓ | |
| Nessus Vulnerability Scanner Server | | ✓ | |
| Windows WSUS Server | | ✓ | |
| NTP Server | | ✓ | |

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

The following backup methods described are for hosts and devices that cannot be performed by the Veeam tool.

| Host | Backup Methods |
|---|---|
| Local Historian Database Virtual Machine | Backup of the VHD is handled by the Veeam full system image of the host server, Local Historian Host (FGS-61338LHH). |
| Supervisory PLC | <p>Backup of the PLC project files is handled by the Veeam full system image of the Engineering Workstation (FGS-47631EHH), as the files are stored locally on that host.</p> <p>Veeam full image backups of Engineering Workstation (FGS-47631EHH) must be manually performed after any engineering changes to the PLC project or its configuration.</p> <p>Backup of the SD card contents is performed annually during the workcell shutdown.</p> |
| Machine Stations | Perform a backup of all project files created by vendor-provided software after any engineering change. |
| Manufacturing System Router / Firewall | Perform a configuration backup via the CLI or web UI after any engineering change. |
| Boundary Router | Perform a configuration backup via the CLI or web UI after any engineering change. |
| Supervisory LAN Switch | Perform a configuration backup via the CLI or web UI after any engineering change. |
| Control LAN Switch | Perform a configuration backup via the CLI or web UI after any engineering change. |
| VMware Host | <p>Perform regular backups of each running Virtual Machine hosted on VMWare ESXi using Veeam.</p> <p>Perform a backup of the ESXi Host configuration after any configuration changes. (see VMWare KB²¹ for additional details).</p> |

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

²¹ <https://kb.vmware.com/s/article/2042141>

3.3.6.5 Media Sanitization

Storage media (e.g., flash memory, memory cards, hard drives) must be sanitized before disposal or removal from the facility. Sanitization procedures for manufacturing system devices are described below.

| Assets / Device type | Method used | Details |
|---|--------------|---|
| Hard Drives on servers, workstations | CLEAR | Tool: DBAN ²² , Category: Software, Type: Open-Source <u>Instructions:</u> (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 reimagining. (2) Remove the MicroSD and load it in a card reader. Perform a full reformat (not Quick Format) of the SD card before reuse. (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 ²³ (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 means the database has been cleared off the unit. |

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

²² <https://dban.org/>

²³ <http://www.redlion.net/sites/default/files/1299/6670/Crimson%203.0%20-%20System%20Menu%20Tech%20Note.pdf>

| Assets / Device type | Method used | Details |
|--|-------------------------------|---|
| <p>RuggedCom L3 switches (Router)</p> | <p>CLEAR and PURGE</p> | <p>The instructions below are found in Siemens RuggedCom Manual (ROX II v2.10 User Guide²⁴)</p> <p><u>Clear:</u></p> <ol style="list-style-type: none"> (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. <p><u>Purge:</u></p> <ol style="list-style-type: none"> (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: <code>rox-delete-bootpwd --force</code> (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. |
| <p>RuggedCom L2 switch</p> | <p>CLEAR</p> | <p>The instructions below are found in Siemens RuggedCom Manual (ROX v4.83 i8xx User Guide²⁵)</p> <p><u>Clear:</u></p> <ol style="list-style-type: none"> (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. |

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

²⁴ https://www.plcsystems.ru/catalog/ruggedcom/doc/ROXII_RX1500_User-Guide_WebUI_EN.pdf

²⁵ https://support.industry.siemens.com/cs/attachments/109737193/ROS_v4.3_i80x_User-Guide_EN.pdf?download=true

| Assets / Device type | Method used | Details |
|-------------------------------|--------------|---|
| Netgear L2 Switch | CLEAR | The instructions below are found in Netgear GS724T Manual ²⁶ 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 | |

3.3.6.6 Resources are Maintained

Resource performance can impact manufacturing process performance. Operators must perform daily checks on the manufacturing system components they operate or are responsible for. These checks must include physical observation of all components, and review of any warning messages or indicators, and any other areas of concern designated by the supervisor.

3.3.7 Personnel Training

Training is vital for keeping the company safe from cybersecurity threats. All employees, contractors and vendors must complete required annual cybersecurity training before being allowed to work or continue working within the manufacturing system environment. Individuals with privileged access are required to complete additional training identified by the president or the supervisor related to managing the cybersecurity controls and configurations for the devices they are granted privileged access rights.

²⁶ http://www.downloads.netgear.com/files/GDC/GS716TV2/GS716T_GS724T-SWA-October2012.pdf?_ga=2.154219964.507023277.1517932216-1121248166.1517932216

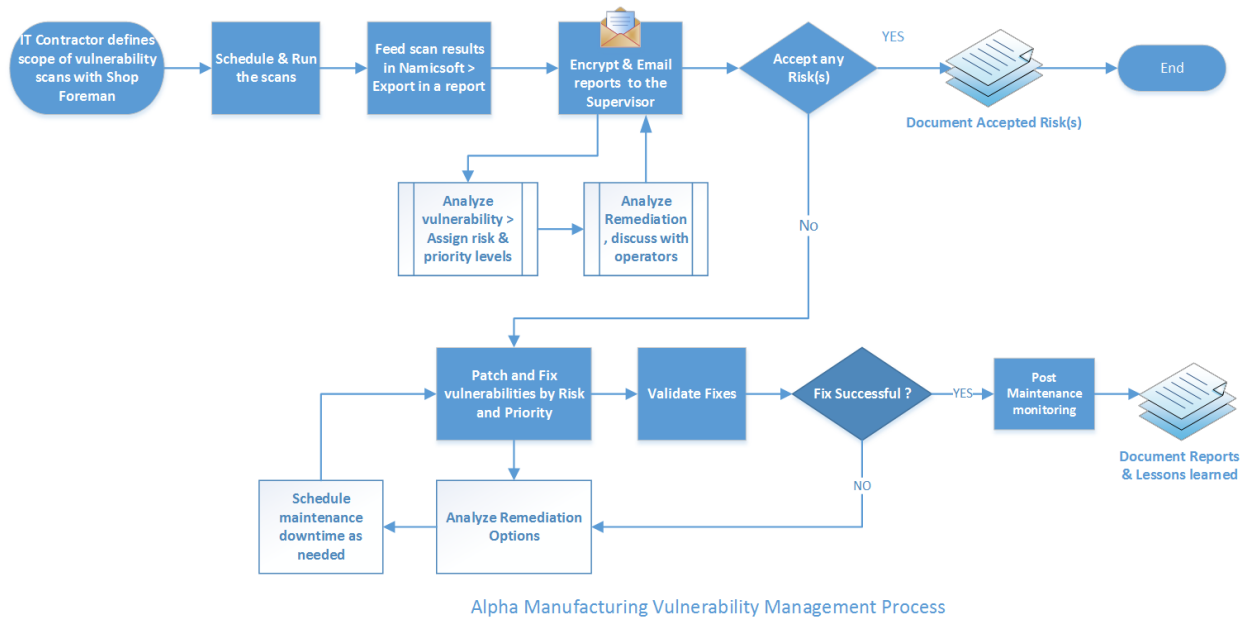
3.3.8 Vulnerability Management

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

The following general policies apply to vulnerability management:

- The Engineers or IT staff 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 Field LAN Network. Scans should be scheduled off hours and during periods of maintenance.
- It is recommended to run authenticated scans from the vulnerability scanner.

3.3.8.1 Vulnerability Management Process



3.3.8.2 Vulnerability Scanning and Management Tools

Tenable-Nessus is being used to perform vulnerability scans in Alpha. The results generated by Nessus at the completion of the scan are imported into NamicSoft, a vulnerability management, parsing and reporting tool. NamicSoft is used to create customized reports and logically group results for a consistent workflow within the organization. The reports are reviewed by the supervisor.

3.3.8.3 Vulnerability Scan Targets

All devices connected to the Workcell and Supervisory network segments are scanned. The IT support staff will configure a scan for all network segments of Alpha.

A new scan can be established, or a modification can be made to an existing scan, by submitting a request to the IT support staff.

Note: If an individual identifies that a scan is impacting the manufacturing process, they must report the situation immediately to the supervisor to request stopping the scan and report the situation to the president.

3.3.8.4 Vulnerability Scan Frequencies

Scans are performed by the IT support staff on an on-demand, per-request basis as needed. Due to the potential impact to manufacturing processes, scans are performed only during scheduled preventive maintenance periods.

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 reported, confirmed that the device is approved, and classified under its appropriate group.

3.3.8.5 Vulnerability Reporting

Upon completion of a vulnerability scan, the result is imported into NamicSoft for report generation. The generated reports are achieved and retained as proof that an assessment occurred and for supporting trend analysis.

All IT/OT devices are organized into groups in NamicSoft as per the system they reside in. A device may belong to one or more groups. Reports are generated for the entire system so that the devices and vulnerabilities can be easily presented to the supervisor. Below is a table of type of reports that are generated and disseminated.

| 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 |

3.3.9 Remediation Management and Priorities

All vulnerabilities discovered must be analyzed by the supervisor with assistance from control engineers and OT service contractor (if needed) to decide the next course of action.

All vulnerabilities discovered should be remediated within the remediation times defined in the following table.

| 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. | Within 15 days of discovery |
| High | High-severity vulnerabilities have a CVSS score between 7.0 and 8.9. | Within 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. | Within 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 | Within 180 days of discovery |
| Info | Info level do not present cybersecurity risk and are listed for informational purposes only. It is optional to remediate them. | Not required to remediate |

3.3.9.1 Exception Management

Exceptions are sometimes required as part of the organizational risk management process to ensure regulatory, cybersecurity, and manufacturing priorities are properly aligned to create a cost-effective cybersecurity environment for supporting the manufacturing systems. There are two primary use cases associated with exception requests: false positives – vulnerabilities identified incorrectly or that are not actually present within the identified system; and risk acceptance – risks that cannot be avoided, mitigated, or transferred.

False Positives exceptions must be documented and approved by the president. Approved false positives will be submitted to the IT support staff who will update scanning and reporting to exclude the false positive results from future reports.

Risk acceptances are necessary to address vulnerabilities that may exist in operating systems, applications, web applications or OT devices that cannot be remediated, or otherwise avoided. For example, 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. Exceptions may also be requested for vulnerabilities not identified as risks to the system and organization (e.g., if a patchable vulnerability is only exploitable by a user utilizing a web browser and accessing a compromised website, then a risk acceptance exception to the patch that has an identified impact on the manufacturing process could be considered given the mitigations of blocking internet access from the manufacturing network segments).

Risk acceptance exceptions must be requested through the IT support staff 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.

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

3.4 Risk Management Document Example

This section provides example content that a Risk Management document may contain, including example policy and procedure statements that were developed for the fictional company Alpha. Certain commercial entities, equipment, or materials may be identified in this document in order to describe a concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, equipment, or materials are necessarily the best available for the purpose. Each organization’s information security experts should identify the content, and policy and procedure statements that will best integrate with their existing cybersecurity program and manufacturing system infrastructure.

Risk Management Strategy for Alpha

| | |
|------------------------|------------|
| Document Owner: | Supervisor |
|------------------------|------------|

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, approvers agree to all terms and conditions outlined in this document.)

| Approvers | Role | Signed | Approval Date |
|---------------|-----------|---------------------|---------------|
| S. Forthright | President | <digital signature> | 4-22-2018 |

This Risk Management Plan defines how cybersecurity risks associated with the Alpha manufacturing systems will be identified, analyzed, and managed. This document can be used by the supervisor and senior management to foresee risks, estimate impacts, and define responses.

3.4.1 Scope

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

3.4.2 Risk Management Process

Risk Management 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. The overall process involves Identifying, Analysis, Categorizing, Remediating, and Reporting. A Risk Management Log is maintained to track known risks and remediation efforts.

3.4.3 Identification

Risks will be identified as early as possible in the project to minimize their impact. For the purposes of this process, risks are threats exploiting vulnerabilities or weaknesses in technology, processes, or policy that may cause an adverse impact or harm to the organizational operations, organizational assets, or individuals.

There are many different types of threats that can affect IT and OT infrastructure. Common threat sources (adapted from NIST SP 800-30²⁷) include:

- **Adversarial** — individuals, groups, organizations, or states that seek to exploit the organization's dependence on cyber resources.
- **Accidental** — Erroneous actions taken by individuals in the course of executing their everyday responsibility
- **Structural** — Failure of equipment, environmental controls, or software due to gaining, resource depletion, or other circumstances which exceed expected operating parameters.
- **Environmental** — Natural disasters and failures of critical infrastructures on which the organization depends, but which are outside the control of the organization.

The supervisor will coordinate the formal manufacturing system annual risk assessments in accordance with the latest version of the NIST SP 800-30²⁸ guidance. During this process, specific organizational threat events will be identified and defined for use in assessing vulnerabilities and weaknesses to determine if a risk exists.

For continuous monitoring and risk management, Alpha's employees or external contractors must report any potential risk following the risk notification process described below. Additionally, software tools including, but not limited to, Nessus and CSET²⁹ are used to support the risk assessment process by identifying vulnerabilities and weaknesses in the technology, processes, or policies for the organization.

²⁷ <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30.pdf>

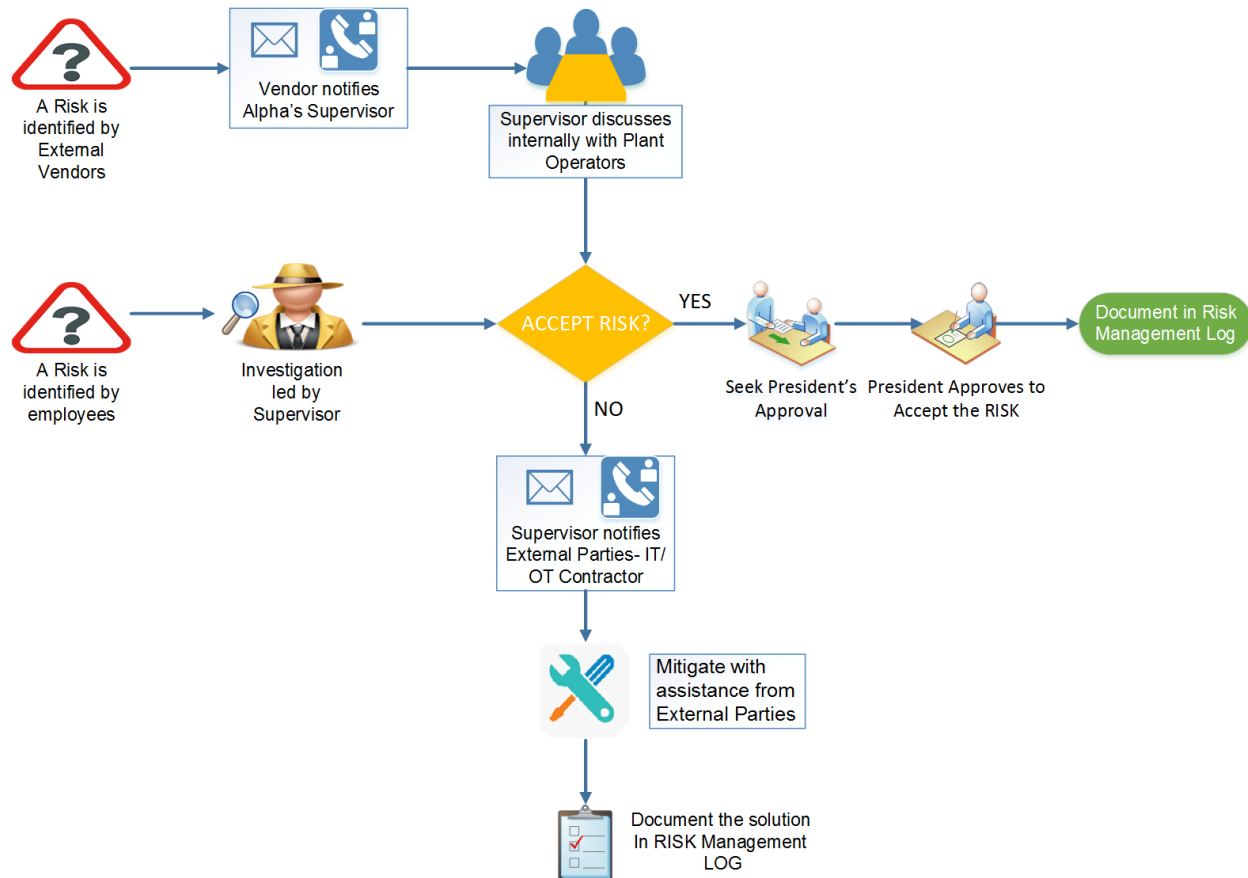
²⁸ <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30.pdf>

²⁹ <https://ics-cert.us-cert.gov/Assessments>

The supervisor will perform a CSET assessment at least annually. Due to the potential impact to manufacturing processes, scans are performed only during scheduled preventive maintenance periods. Nessus results will be imported into NamicSoft and reports generated and distributed to supervisor. Additionally, other types of risks, such as hardware based, physical, or environmental will be identified and documented manually.

Note: Any software-based vulnerabilities that cannot be remediated per the Vulnerability Management Plan will be included in the risk analysis process to determine the appropriate corrective action.

Risk Notification Process



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

3.4.4 Analysis

To begin the analysis process, each vulnerability must be assigned a vulnerability score from 1 to 10. Vulnerabilities identified by CSET will be manually assigned a score from 1 to 10 based on the severity of the finding by the assessor. For vulnerabilities identified through scanning tools such as Nessus, the CVSS associated with the vulnerability will be used as the vulnerability score.

At a minimum, vulnerabilities with a score in at the high (vulnerability score: 7.0 to 8.9) and critical (vulnerability score of 9.0 to 10) range will be analyzed to determine if an associated threat or threat event exists that has a probability of occurrence greater than zero. For each vulnerability, threat pairs, an impact on operations will be estimated. A qualitative risk analysis process will be used to determine the overall probability and impact levels using the guidance in the tables below. These factors are then combined to provide an estimated quantitative risk score for use in reporting and prioritization.

| Probability | Description | Quantitative Value |
|-------------|---|--------------------|
| High | Greater than <70 %> probability of occurrence in a year | 0.8 |
| Medium | Between <30 %> and <70 %> probability of occurrence in a year | 0.5 |
| Low | Below <30 %> probability of occurrence in a year | 0.3 |

Note: At the discretion of the assessor or the supervisor, the probability quantitative value may be adjusted to more accurately represent the probability of occurrence up to a maximum of 1 representing 100 % probability of occurrence and to a minimum of 0 representing 0 % probability due to no identified threat or threat event being identified for the vulnerability or weakness.

| Impact | Description | Quantitative Value |
|--------|--|--------------------|
| High | Risk that has the potential to seriously impact production cost, production schedule or performance | 1 |
| Medium | Risk that has the potential to moderately impact production cost, production schedule or performance | 0.5 |
| Low | Risk that has relatively minor impact on cost, schedule or performance | 0.1 |

Notes: Overall impact scores are the product of the qualitative level from the impact table and the asset criticality as defined below resulting in an impact range of 1-10. If an asset criticality has not been defined, then assume an asset criticality of 10 until the asset can be properly categorized.

Asset Criticality Matrix

Once a list of Alpha assets or systems 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.

Alpha will use the following scale to calculate Asset value.

| Criticality | Description | Asset Value |
|-------------|---|-------------|
| Critical | Loss or damage of this asset would have grave / serious impact to the operations of the Manufacturing system directly impacting production. This can result in total loss of primary services, core processes or functions. These assets are single point of failure. | 10 |
| High | Loss or damage of this asset would have serious impact to the operations of the Manufacturing system directly impacting production. This can result in major loss of primary services, core processes or functions. These assets can also be single point of failure. | 7 to 9 |
| Medium | Loss or damage of this asset would have moderate impact to the operations of the Manufacturing system or Production. This can result in some loss of primary services, core processes or functions. | 3 to 6 |
| Low | Loss or damage of this asset would have minor to no impact on the Operations of the Manufacturing system or Production. This can result in little or no loss of primary services, core processes or functions. | 1 to 2 |

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

| Asset | Value | Asset Value |
|--------------------------------------|----------|-------------|
| IT / Communication Systems | High | 8 |
| OT / Field Devices – PLC, HMI | Critical | 10 |
| Electrical Systems | Critical | 10 |
| Utility Systems | Medium | 6 |
| Site | High | 8 |

3.4.5 Categorization

Categorization of risks begins by computing the overall risk score. The overall risk score is computed using the following equation:

$$\text{Risk Score} = \text{Vulnerability Score} \times \text{Probability} \times \text{Impact} \times \text{Asset Criticality}$$

The resulting risk score (1 to 100) is then used for determining the overall risk level (adapted from NIST SP 800-30³⁰) which is utilize for prioritizing remediation efforts.

| Risk Level | Description | Risk Score |
|------------|---|------------|
| Very High | Very high risk means that the identified vulnerability could be expected to have multiple severe or catastrophic adverse effects on organizational operations, organizational assets, or individuals. | 96 to 100 |
| High | High risk means that the identified vulnerability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. | 80 to 95 |
| Medium | Moderate risk means that the identified vulnerability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. | 21 to 79 |
| Low | Low risk means that the identified vulnerability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. | 5 to 20 |
| Very Low | Very low risk means that the identified vulnerability could be expected to have a negligible adverse effect on organizational operations, organizational assets, or individuals. | 0 to 4 |

The resulting risk information is then entered into the risk management log for tracking and for coordinating remediation.

³⁰ <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30.pdf>

3.4.6 Remediation

For each risk rated moderate or higher, one of the following approaches will be selected for remediation:

- **Avoid** – eliminate the threat by eliminating the cause
- **Mitigate** – Identify ways to reduce the probability or the impact of the risk
- **Accept** – accept the risk
- **Transfer** – transfer the risk by having another party responsible for the risk (buy insurance, outsourcing, etc.)

Risk mitigations and transfer efforts may require additional research and time to implement. As necessary, the supervisor will reach out to IT/OT Vendor for any risks and request remediation assistance. For any corrective actions taken, including risk acceptance, the risk management log must be updated.

Each risk mitigation and transfer effort will be maintained on the Risk Management log and tracked by the supervisor until completed. Once completed, an assessment of the implemented mitigation will be performed to assess the new residual risk level for the vulnerability and determine if the residual risk is within an acceptable range for continued operations.

Any risk acceptances must follow the process established in the Remediation Management and Priorities and Exception Management sections of the Cybersecurity Operations Document.

3.4.7 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 | Yearly |
| CSET Report | A document describing Risk assessment results | Yearly |
| 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 president.

Sample Risk Management Log

The Risk Management Log will be maintained by the supervisor and reviewed in the monthly senior management meeting. This log captures the results of the latest risk analysis and the status of planned corrective actions.

| Risk | Category (Technical, Management, Contractual, External) | Probability | Impact | Risk Score | Risk Mitigation Strategy (e.g. Avoid, Transfer, Mitigate or Accept the risk) | Actions required | Status (Open, closed, In Progress) | Due Date |
|------|---|-------------|--------|------------|--|------------------|------------------------------------|----------|
| | | | | | | | | |
| | | | | | | | | |

3.4.8 Definition 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. |

3.4.9 Additional Resources

1. Risk Management plan – Maryland Department of Information Technology³¹
2. Sample Risk Management plan – State of North Dakota³²

³¹ doit.maryland.gov/SDLC/Documents/Project%20Risk%20Managment%20Plan.doc

³² <https://www.nd.gov/itd/sites/itd/files/legacy/services/pm/risk-management-plan-sample.pdf>

3.5 Incident Response Plan Document Example

This section provides example content that an Incident Response Plan document may contain, including example policy and procedure statements that were developed for the fictional company Alpha. Certain commercial entities, equipment, or materials may be identified in this document in order to describe a concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, equipment, or materials are necessarily the best available for the purpose. Each organization’s information security experts should identify the content, and policy and procedure statements that will best integrate with their existing cybersecurity program and manufacturing system infrastructure.

Incident Response Plan

for

Alpha

| | |
|------------------------|------------|
| Document Owner: | Supervisor |
|------------------------|------------|

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, approvers agree to all terms and conditions outlined in this document.)

| Approvers | Role | Signed | Approval Date |
|---------------|-----------|---------------------|---------------|
| S. Forthright | President | <digital signature> | 4-22-2018 |

3.5.1 Statement of Management commitment

Alpha’s is committed to appropriate incident response to accidental or deliberate cybersecurity incidents within the company. Alpha has created the Incident Response Plan to establish an actionable cybersecurity incident handling capability that includes planning, detection, analysis, containment, recovery, and reporting for information cybersecurity incidents.

3.5.2 Purpose and Scope

An incident can be defined as an occurrence that actually or potentially jeopardizes the availability, integrity, or confidentiality of the manufacturing system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of cybersecurity policies, cybersecurity procedures, or acceptable use policies. This document describes the plan for responding to cybersecurity incidents. It defines the roles and responsibilities of personnel, incident classification, the incident response workflow, and reporting requirements. The purpose of this plan is to determine the scope and risk of cybersecurity incidents, respond appropriately to the incident, communicate the incident with all stakeholders, and reduce the likelihood of future impact. This plan applies to all manufacturing system personnel, networks, systems, and data.

3.5.3 Roles and Responsibilities

The Alpha Incident Response Team is comprised of:

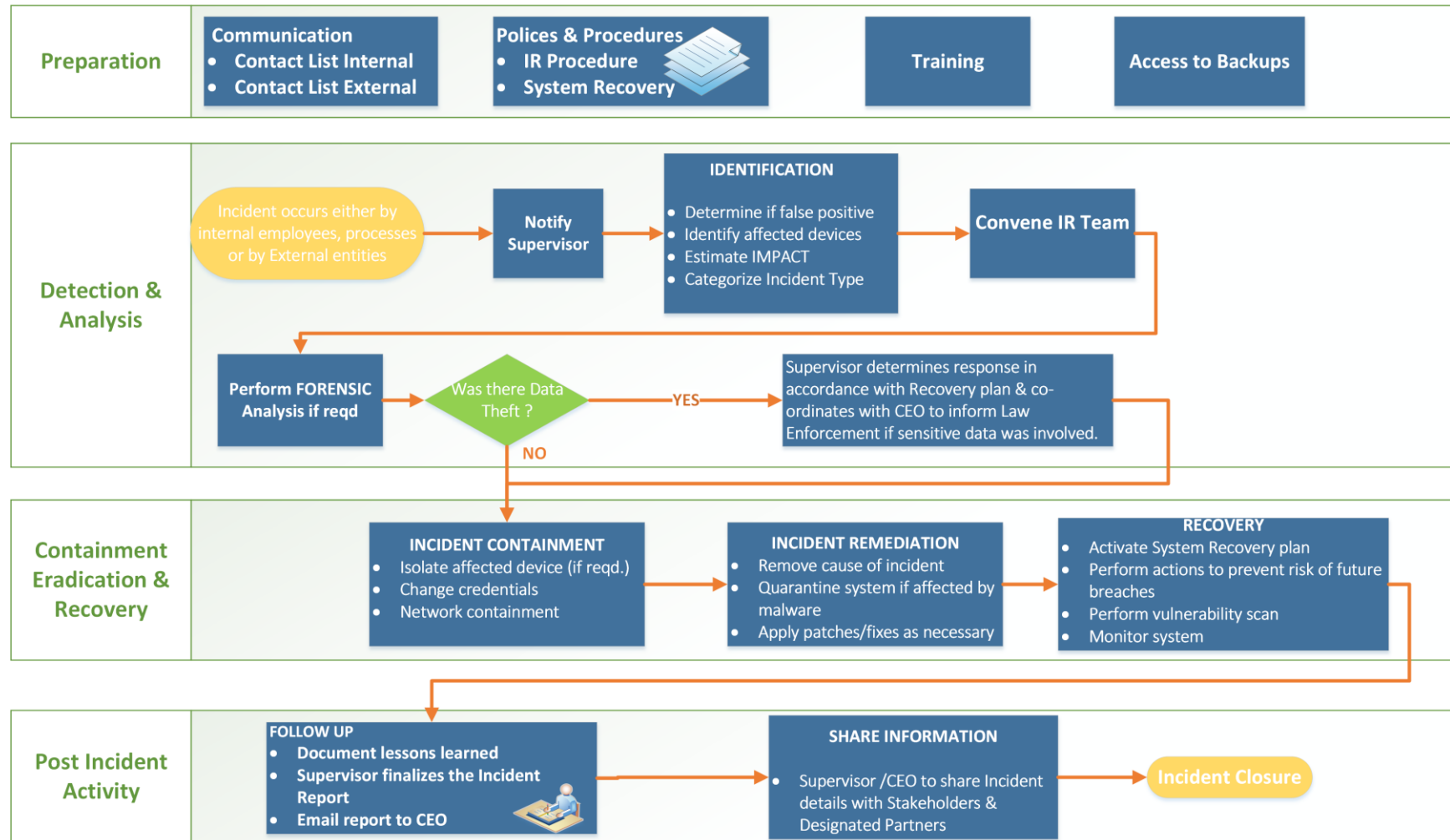
| Role | Incident Response Responsibilities |
|----------------------------|--|
| Supervisor | <ul style="list-style-type: none"> • Serves as a primary point of contact for any cybersecurity incident. • Ensure all employees understand how to identify and report a cybersecurity incident. • Leads the investigation for incidents, completing the Incident Report Form, and reporting to the president as required. • Documents all details of cybersecurity incidents. |
| HR Manager | <ul style="list-style-type: none"> • Handling of any personnel and disciplinary issues relating to a cybersecurity incident. • Inform the supervisor if a cybersecurity incident involves a data breach of sensitive information (e.g., PII). |
| Machine Operators | <ul style="list-style-type: none"> • Reporting cybersecurity incidents, operational issues or concerns to the supervisor. • Assisting with incident response when this plan is activated. |
| IT / OT Contractors | <ul style="list-style-type: none"> • Assist in investigation, troubleshooting, and mitigation of cybersecurity incidents as requested by the supervisor. • Advises the supervisor regarding procedures, policies and best practices for incident response. • Determine if a cybersecurity incident involves a data breach of sensitive information (e.g., PII). |

3.5.4 Policy

- Upon notification of a cybersecurity event, the supervisor must determine if the Incident Response Plan should be activated based on available information from the event.
- The supervisor must inform all personnel listed in Section 3.5.7 of this document when the response plan has been activated.
- Impact to the manufacturing system must be determined by thorough investigation, and an incident type and severity level assigned. The Incident Report Template form should be used for this purpose. The severity level will be assigned by the supervisor.
- Approval must be received from the president if additional resources (i.e., external entities) are to be contacted to assist with incident response (e.g., forensic investigators, IT consultants, cybersecurity consultants, law enforcement, etc.).
- The supervisor must coordinate the Incident Response Plan with stakeholders.
- User awareness, training, and testing procedures must be reviewed after every incident and updated as necessary.
- Legal counsel may be involved throughout the incident response due to the potential for legal action arising from the incident.

3.5.5 Incident Response Workflow

The Incident Response workflow must operate as follows.



3.5.6 Internal and External Communications

The following policies are applicable to internal and external communications that are performed during an incident response.

- The president must identify and promptly contact primary partners, stakeholders, and customers to inform them about response activities. This should be performed once the impact of the incident is understood, and a corporate response has been prepared.
- The supervisor must contact all personnel responsible for system recovery, listed below, once this plan has been executed.
- The supervisor must establish reporting requirements on the progress of incident response activities to stakeholders.
- Communications with any external entities must be initiated by personnel explicitly authorized by this plan, or as authorized by the supervisor during execution of this plan.
- Approval must be received from the president before collaborating with any outside entity during an incident response.

3.5.7 Personnel Contact Information

The following table contains the contact information for critical Alpha personnel who will likely be involved in the Incident Response process.

| Name | Title | Contact Type | Contact Information |
|----------------------|-------------------------|--------------|-----------------------------|
| S. Forthright | President | Work | 301-555-0141 ext. 102 |
| | | Mobile | 240-555-0159 |
| | | Alternate | 301-555-3554 |
| | | Email | s.forthright@nist-alpha.com |
| W. Lumbergh | Supervisor | Work | 301-555-0141 ext. 103 |
| | | Mobile | 240-555-0110 |
| | | Alternate | 301-555-3110 |
| | | Email | w.lumbergh@nist-alpha.com |
| E. Moriarty | Senior Machine Operator | Work | 301-555-0141 ext. 104 |
| | | Mobile | 240-555-0167 |
| | | Alternate | 301-555-3344 |
| | | Email | e.moriarty@nist-alpha.com |
| A. Martin | Senior Machine Operator | Work | 301-555-0141 ext. 105 |
| | | Mobile | 240-555-0171 |
| | | Alternate | 301-555-3171 |
| | | Email | a.martin@nist-alpha.com |
| A. Dufresne | Bookkeeper | Work | 301-555-0141 ext. 106 |
| | | Mobile | 240-555-0543 |
| | | Alternate | 301-555-3543 |
| | | Email | a.dufresne@nist-alpha.com |
| J. Smith | HR Manager | Work | 301-555-0141 ext. 106 |
| | | Mobile | 240-555-0543 |
| | | Alternate | 301-555-3543 |
| | | Email | j.smith@nist-alpha.com |

3.5.8 External Contact Information

The following table contains the contact information for external entities that may be contacted while execution of the Incident Response Plan is ongoing to support or provide relevant information to support the response process. External entities and organizations listed below must only be contacted by authorized personnel, as per the guidance described in this plan.

| Name | Title | Contact Type | Contact Information |
|--|--------------------|--------------|-------------------------------|
| IT Contractor Initech Account # 78795 | General Support | Work | 1-800-555-2388 Option 1 |
| | | Mobile | N/A |
| | | Alternate | N/A |
| | | Email | support@initech.com |
| OT Contractor Cyberdyne Systems Account # 88525462A | General Support | Work | 1-800-555-6543 Option 1, 3, 5 |
| | | Mobile | N/A |
| | | Alternate | N/A |
| | | Email | support@cyberdynesystems.com |
| Power Company Account # 5486548 | General Support | Work | 1-800-555-4343 Option 1,4,7,9 |
| | | Mobile | N/A |
| | | Alternate | N/A |
| | | Email | N/A |
| Network Provider Account # 43-5563 | General Support | Work | 1-800-555-3334 |
| | | Mobile | N/A |
| | | Alternate | N/A |
| | | Email | N/A |
| Telecom Carrier Account # 3340444 | General Support | Work | 1-800-555-8769 |
| | | Mobile | N/A |
| | | Alternate | N/A |
| | | Email | N/A |
| Insurance Provider Account # 8858444 | Agent (R. Parr) | Work | 1-800-555-7643 |
| | | Mobile | 240-555-5698 |
| | | Alternate | 240-555-5433 |
| | | Email | r.parr@insuricare.com |

3.5.9 Information Sharing Policy

1. The supervisor, in collaboration with the president, must promptly prepare a report detailing relevant information about the incident response, and may share the report with designated sharing partners.
2. All communications regarding information sharing about an incident or incident response to external parties must be made in consultation with the president.
3. The president and supervisor must determine the relevant information about the incident to be shared.

3.5.10 Public Communications

1. Any public response must be clear, consistent, and professional.
2. The president must approve all public communications regarding a cybersecurity incident.
3. If required, an outside public relations firm may be contracted to assist in development of a response and responding to any public inquiry.
4. All communications with the media must be approved by the president.
5. The president or supervisor may communicate the public response, depending on the severity of the cybersecurity incident.

3.5.11 Plan Maintenance

This plan must be reviewed and updated after:

- the plan is executed in response to a cybersecurity incident,
- the plan is executed during an incident response exercise,
- any organizational changes, or
- any modifications or maintenance to the manufacturing system or its components that may impact this plan.

The supervisor must update this plan in consultation with company personnel, as required, and must communicate any changes or updates made to this policy to personnel responsible for its execution.

3.5.12 Plan Testing

Incident Response team members must be convened at least once per calendar year to perform the following activities:

- review of the documented procedures,
- validation of plan effectiveness,
- identification of any gaps or weaknesses in the plan execution, and
- update the plan with any outdated or missing information.

3.5.13 Incident Type Classification

Alpha defines the following types of cybersecurity incidents for internal classification.

| Incident Type | Description |
|---|--|
| Intrusion | A security event, or a combination of multiple security events, that constitutes a security incident in which an intruder gains, or attempts to gain, access to a system or system resource without having authorization to do so. ³³ |
| Denial of Service (DoS) | The prevention of authorized access to a system resource or the delaying of system operations and functions. ³⁴ |
| Virus or malware | Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code. ³⁵ |
| Social engineering | An attempt to trick someone into revealing information (e.g., a password) that can be used to attack systems or networks. ³⁶ |
| Data loss | The exposure of proprietary, sensitive, or classified information through either data theft or data leakage. ³⁷ |
| Missing or stolen IT/OT hardware | Any manufacturing system hardware (in-use, backup, spare, or surplus) that cannot be accounted for. |
| User account compromise | The unauthorized disclosure, modification, or use of a user account on the manufacturing system. |
| System misuse | The unauthorized use of a manufacturing system component. |

³³ CNSSI 4009-2015 (IETF RFC 4949 Ver 2)

³⁴ NIST SP 800-82 Rev. 2 under Denial of Service (DoS) (RFC 4949)

³⁵ NIST SP 800-82 Rev. 2 under Malware (NIST SP 800-53)

³⁶ NIST SP 800-82 Rev. 2 under Social Engineering (NIST SP 800-61)

³⁷ CNSSI 4009-2015 (NIST SP 800-137)

3.5.14 Incident Severity Classification

The severity of a cybersecurity incident is determined based on the impact to manufacturing operations, the information impact, the potential for future operational or information impacts, and the recoverability. The table below describes the classification levels for incident severity, and their classifiers.

| Severity | Classifiers |
|-----------------|--|
| High | <ul style="list-style-type: none"> • All users of the company are impacted. • One or more of the mission objectives are severely impacted (e.g., production impact or stoppage). • Sensitive information loss (i.e., data breach). • There is no temporary operational procedure to maintain or restore manufacturing system production. • Recoverability is unpredictable, additional resources and outside help are required, or recovery is not possible.³⁸ |
| Moderate | <ul style="list-style-type: none"> • One or more of the mission objectives are impacted. • There are temporary operational procedures that can be implemented to maintain or restore manufacturing system production. • Service interruption potentially affects specific users and does not involve sensitive or personal data breach. • Non-sensitive information loss (i.e., data breach). • Recoverability is predictable with existing or additional resources.³⁸ |
| Low | <ul style="list-style-type: none"> • No impact to mission objectives. • Service interruption potentially affects only one user and does not involve sensitive information loss. • Recoverability is predictable with existing resources.³⁸ |

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

³⁸ NIST SP 800-61 Rev. 2

3.5.15 Incident Report Form Template

| Incident Reporting Form ^{39,40} | | |
|--|--|--|
| Contact Information | | |
| Date: | | Time: |
| Name: | Title: | Dept: |
| Office Phone: | | |
| Incident Details | | |
| Incident Date: | | Incident Time: |
| Type of Incident - Check all that apply | | |
| <input type="checkbox"/> Intrusion | <input type="checkbox"/> System Misuse | <input type="checkbox"/> Social Engineering |
| <input type="checkbox"/> Denial of Service | <input type="checkbox"/> Data Breach | <input type="checkbox"/> User Account Compromise |
| <input type="checkbox"/> Virus / Malware | <input type="checkbox"/> Hardware Stolen | <input type="checkbox"/> Other |
| Description of Incident: | | |
| | | |
| Impact or Potential Impact - Check All that Apply | | |
| <input type="checkbox"/> Loss or Compromise of Data | <input type="checkbox"/> Financial Loss | |
| <input type="checkbox"/> Damage to Systems | <input type="checkbox"/> Other Organizations Affected | |
| <input type="checkbox"/> Damage to Public | <input type="checkbox"/> Damage to Integrity or Production | |
| <input type="checkbox"/> System Downtime | <input type="checkbox"/> Unknown at this time | |
| Description of Impact: | | |
| | | |

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

³⁹ Pennsylvania Department of Human Services, http://www.dhs.pa.gov/cs/groups/webcontent/documents/form/p_031584.doc

⁴⁰ AHIMA BOK, <https://bok.ahima.org/doc?oid=76732>

| Incident Reporting Form (cont.) | | | |
|--|-------------------|--|-------------------------|
| Affected Systems | | | |
| Host | IP Address | Applications (if any) | Operating System |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| Scope of Data Loss (if any) | | | |
| <input type="checkbox"/> Public - Data previously approved for release or is publicly available. | | | |
| <input type="checkbox"/> Internal Use - Data intended for internal company use, other affiliated organizations, or business partners. Unauthorized disclosure may be against laws or regulations and may cause harm the company or its business partners or its customers. | | | |
| <input type="checkbox"/> Sensitive - Private, proprietary, customer, or trade secret data. Restricted to those with legitimate business need for access. Unauthorized disclosure is against laws or regulations, and will likely harm the company, its business partners, or customers (e.g., trade secrets, source code, personnel data, PII). | | | |
| Data Loss Details | | | |
| Description of Data Loss: | | | |
| | | | |
| Follow Up Actions Initiated | | | |
| <input type="checkbox"/> Law Enforcement Notified | | <input type="checkbox"/> System Removal from Network | |
| <input type="checkbox"/> Restored from Backups | | <input type="checkbox"/> Log Files Examined | |
| <input type="checkbox"/> AV Definitions Updated | | <input type="checkbox"/> No Actions | |
| <input type="checkbox"/> System Reimage or Quarantine | | <input type="checkbox"/> Other | |
| Description of Actions Initiated: | | | |
| | | | |
| Supervisor Sign-Off | | | |
| Name: | | Signature: | Date: |
| | | | |

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

3.5.16 Acronyms

| Acronym | Definition |
|----------------|--|
| CNSSI | Committee on National Security Systems Instruction |
| DMZ | Demilitarized Zone |
| DOS | Denial of Service |
| HR | Human Resources |
| IRP | Incident Response Plan |
| IT | Information Technology |
| LAN | Local Area Network |
| NIST SP | National Institute of Standards and Technology Special Publication |
| NTP | Network Time Protocol |
| OT | Operational Technology |
| PII | Personally Identifiable Information |
| PLC | Programmable Logic Controller |
| RFC | Request for Comment |
| SD | Secure Digital |
| VHD | Virtual Hard Drive |

3.5.17 Definitions

| Term | Definition |
|---------------------|---|
| Sensitive | Proprietary, customer, trades secret or other information with access restricted to those with legitimate business need. Unauthorized disclosure is against laws or regulations, and will likely harm the company, its business partners, or customers (e.g., trade secrets, source code, personnel data, PII). |
| Incident | An occurrence that actually or potentially jeopardizes the availability, integrity, or confidentiality of the manufacturing 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. |
| Internal Use | Data intended for internal company use, other affiliated organizations, or business partners. Unauthorized disclosure may be against laws or regulations and may cause harm the company or its business partners or its customers. |
| Personnel | All employees, contractors, vendors, and individuals authorized to perform work at the facility, physically or remotely. |
| Public | Data previously approved for release or is publicly available. |

| Term | Definition |
|----------------------|---|
| Stakeholder | Individual or organization having a right, share, claim, or interest in a system or in its possession of characteristics that meet their needs and expectations. (e.g., Business Owners, System Owners, Integrators, Vendors, Human Resources Offices, Physical and Personnel Security Offices, Legal Departments, Operations Personnel). |
| Vulnerability | Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. |

3.6 System Recovery Plan Document Example

This section provides example content that an Incident System Plan document may contain, including example policy and procedure statements that were developed for the fictional company Alpha. Certain commercial entities, equipment, or materials may be identified in this document in order to describe a concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, equipment, or materials are necessarily the best available for the purpose. Each organization’s information security experts should identify the content, and policy and procedure statements that will best integrate with their existing cybersecurity program and manufacturing system infrastructure.

System Recovery Plan for Alpha

| | |
|------------------------|------------|
| Document Owner: | Supervisor |
|------------------------|------------|

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, approvers agree to all terms and conditions outlined in this document.)

| Approvers | Role | Signed | Approval Date |
|---------------|-----------|---------------------|---------------|
| S. Forthright | President | <digital signature> | 4-22-2018 |

3.6.1 Purpose

The System Recovery Plan is designed to ensure the continuation of vital manufacturing/business processes in the event a cybersecurity incident occurs. Its purpose is to provide a structured approach for responding to cybersecurity incidents by leveraging the infrastructure inventory and configuration information relevant to the organization’s IT and OT environments to restore operational capabilities.

3.6.2 Objectives

This System Recovery Plan has been developed to accomplish the following objectives:

- limit the magnitude of any loss by minimizing the duration of a manufacturing interruption,
- assess damage, repair the damage, and restore manufacturing system operation,
- manage the recovery operation in an organized and effective manner, and
- prepare personnel to respond effectively in system recovery situations.

3.6.3 Plan Execution

This plan is executed during or after a cybersecurity incident, as directed by the supervisor.

3.6.4 Roles and Responsibilities

The Incident Response team will be repurposed as the System Recovery team while execution of the System Recovery Plan is ongoing. Team members will have the following roles and responsibilities:

| Role | Responsibilities |
|-----------------------|---|
| Supervisor | <ul style="list-style-type: none"> • Lead and oversee the entire system recovery process. • Contact any contractors or vendors for assistance, as needed. • Make sure all employees understand their roles and responsibilities. • Update this document as per the Maintenance Policy. • Update the president periodically on the progress of the system recovery process. |
| President | <ul style="list-style-type: none"> • Assist the supervisor their role as required. • Serve as point of escalation for any issues. |
| IT Contractors | <ul style="list-style-type: none"> • Recover, restore, troubleshoot, and resolve any recovery issues on manufacturing system hardware, software, or systems. • Escalate any issues related to recovery to the supervisor. • Comply with this plan. |
| OT Contractors | <ul style="list-style-type: none"> • Assist with the recovery of any manufacturing system hardware, software, or systems, as required. • Advise the supervisor of any recommended procedures, policies, and best practices to assist with the recovery process. • Comply with this plan. |

3.6.5 Internal and External Communications

All communications guidance provided in the Incident Response Plan also applies to the System Recovery Plan. The following recovery-specific guidance must also be followed:

- The president will contact primary partners and customers to inform them about recovery activities. This should be performed once the impact of the incident is understood, and a corporate response has been prepared.
- The supervisor will contact all personnel responsible for system recovery, listed below, once this plan is executed.
- Legal counsel should be involved throughout the system recovery process due to the potential for legal action arising from the cybersecurity incident.
- The supervisor will periodically update the president and other stakeholders on the progress of recovery activities. The president will define the required stakeholders and update period based on the impact of the incident.
- Communications with external entities must be initiated by personnel explicitly authorized by this plan, or as authorized by the supervisor during execution of this plan.

3.6.6 Restoring Trust

- The president or supervisor, with the advice of any contracted consultants and forensic experts, will notify all partners, vendors, and customers of the steps taken to restore the manufacturing system and strengthen cybersecurity controls.
- The supervisor will discuss with employees the cause for the plan to be executed and what actions are being taken to avoid similar incidents from occurring in the future.
- After the cybersecurity incident has been mitigated and all facts surrounding the incident are known, the supervisor will provide a full report available to the public. The report will contain content relevant to the cybersecurity incident, along with the steps being taken to safeguard the manufacturing system, and describe the actions being taken to avoid similar incidents from occurring in the future.

3.6.7 Personnel Contact Information

The following table contains the contact information for critical personnel who will likely be involved in the system recovery process.

| Name | Title | Contact Type | Contact Information |
|----------------------|-------------------------|--------------|-----------------------------|
| S. Forthright | President | Work | 301-555-0141 ext. 102 |
| | | Mobile | 240-555-0159 |
| | | Alternate | 301-555-3554 |
| | | Email | s.forthright@nist-alpha.com |
| W. Lumbergh | Supervisor | Work | 301-555-0141 ext. 103 |
| | | Mobile | 240-555-0110 |
| | | Alternate | 301-555-3110 |
| | | Email | w.lumbergh@nist-alpha.com |
| E. Moriarty | Senior Machine Operator | Work | 301-555-0141 ext. 104 |
| | | Mobile | 240-555-0167 |
| | | Alternate | 301-555-3344 |
| | | Email | e.moriarty@nist-alpha.com |
| A. Martin | Senior Machine Operator | Work | 301-555-0141 ext. 105 |
| | | Mobile | 240-555-0171 |
| | | Alternate | 301-555-3171 |
| | | Email | a.martin@nist-alpha.com |
| A. Dufresne | Bookkeeper | Work | 301-555-0141 ext. 106 |
| | | Mobile | 240-555-0543 |
| | | Alternate | 301-555-3543 |
| | | Email | a.dufresne@nist-alpha.com |
| J. Smith | HR Manager | Work | 301-555-0141 ext. 106 |
| | | Mobile | 240-555-0543 |
| | | Alternate | 301-555-3543 |
| | | Email | j.smith@nist-alpha.com |

3.6.8 External Contact Information

The following table contains the contact information for external entities and organizations that may be contacted while execution of the System Recovery Plan is ongoing to support or provide relevant information to support the recovery process. External entities and organizations listed below must only be contacted by authorized personnel, as per the guidance described in this System Recovery Plan.

| Name | Title | Contact Type | Contact Information |
|--|--------------------|--------------|-------------------------------|
| IT Contractor Initech Account # 78795 | General Support | Work | 1-800-555-2388 Option 1 |
| | | Mobile | N/A |
| | | Alternate | N/A |
| | | Email | support@initech.com |
| OT Contractor Cyberdyne Systems Account # 88525462A | General Support | Work | 1-800-555-6543 Option 1, 3, 5 |
| | | Mobile | N/A |
| | | Alternate | N/A |
| | | Email | support@cyberdynesystems.com |
| Power Company Account # 5486548 | General Support | Work | 1-800-555-4343 Option 1,4,7,9 |
| | | Mobile | N/A |
| | | Alternate | N/A |
| | | Email | N/A |
| Network Provider Account # 43-5563 | General Support | Work | 1-800-555-3334 |
| | | Mobile | N/A |
| | | Alternate | N/A |
| | | Email | N/A |
| Telecom Carrier Account # 3340444 | General Support | Work | 1-800-555-8769 |
| | | Mobile | N/A |
| | | Alternate | N/A |
| | | Email | N/A |
| Insurance Provider Account # 8858444 | Agent (R. Parr) | Work | 1-800-555-7643 |
| | | Mobile | 240-555-5698 |
| | | Alternate | 240-555-5433 |
| | | Email | r.parr@insuricare.com |

3.6.9 Plan Maintenance

The System Recovery Plan must be reviewed and updated after:

- the plan executed in response to a cybersecurity incident,
- the plan is executed during an incident response or recovery exercise,
- any organizational changes, or
- any modifications or maintenance to the manufacturing system or its components that may impact this plan.

The supervisor is responsible for updating the document in consultation with other personnel, IT and OT contractors and vendors, as required.

3.6.10 Plan Testing

The System Recovery Plan will be tested each calendar year. System Recovery team members will perform exercises to:

- review documented procedures,
- validate the effectiveness of the plan,
- identify any gaps or weaknesses in its execution, and
- update the plan with any outdated or missing information.

3.6.11 Hardware to be Recovered

The following tables document important information to support the recovery of manufacturing system devices. Each device is listed in its own table with relevant information (e.g., hostname, file systems, physical location, backup strategies). The restoration process for each device below is described in Section 3.6.12. For more detailed system information regarding each host, reference the Hardware Inventory.

3.6.11.1 Workcell Systems

| Engineering Workstation | |
|-------------------------|--|
| Hostname | POLARIS |
| Model | Dell Precision T5610 |
| IP Address | 192.168.0.20 |
| Network | Supervisory LAN |
| Location | Workcell 1 |
| Type | Physical |
| Operating System | Ubuntu 12.04 |
| File System(s) | 2 TB HDD |
| Backup Strategies | <p>Veeam directory backups are performed on select directories containing configuration and logic data for the manufacturing system: weekly, while the manufacturing system is shutdown.</p> <p>Veeam full system image backups are performed:</p> <ul style="list-style-type: none"> • monthly, while the manufacturing system is shutdown, and • after any engineering change. |
| Recovery Priority | High |
| Recovery Strategies | <p>Veeam Directory Recovery (Section 3.6.12.1)</p> <p>Veeam Full Image Recovery (Section 3.6.12.2)</p> |

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

| Robot Driver | |
|---------------------|--|
| Hostname | MINTAKA |
| Model | Dell R420 |
| IP Address | 192.168.1.5 |
| Network | Control LAN |
| Location | Workcell 1 |
| Type | Physical |
| Operating System | Ubuntu 12.04 |
| File System(s) | 500 GB HDD |
| Backup Strategies | Veeam full system image backups are performed: <ul style="list-style-type: none"> • monthly, while the manufacturing system is shutdown, and • after any engineering change. |
| Recovery Priority | High |
| Recovery Strategies | Veeam Full Image Recovery (Section 3.6.12.2) |

| Robotics Hypervisor | |
|---------------------|--|
| Hostname | Robotics-VH |
| Model | Dell R420 |
| Location | Workcell 1 |
| Type | Physical |
| Operating System | Windows Server 2012 R2 |
| File System(s) | 2 TB HDD |
| Backup Strategies | Veeam full system image backups are performed: <ul style="list-style-type: none"> • daily overnight, and • after any configuration change. |
| Recovery Priority | High |
| Recovery Strategies | Veeam Full Image Recovery (Section 3.6.12.2) |

| Robot Controller 1 | |
|---------------------|--|
| Hostname | vController1 |
| IP Address | 192.168.1.3 |
| Network | Control LAN |
| Location | Robotics Hypervisor (Robotics-VH) |
| Type | Virtual |
| Operating System | Ubuntu 14.04 |
| File System(s) | 50 GB HDD |
| Backup Strategies | Veeam full system image backups are performed: <ul style="list-style-type: none"> • daily overnight, and • after any configuration change. |
| Recovery Priority | High |
| Recovery Strategies | Veeam Full Image Recovery (Section 3.6.12.2) |

| Robot Controller 2 | |
|---------------------|--|
| Hostname | vController2 |
| IP Address | 192.168.1.4 |
| Network | Control LAN |
| Location | Robotics Hypervisor (Robotics-VH) |
| Type | Virtual |
| Operating System | Ubuntu 14.04 |
| File System(s) | 50 GB HDD |
| Backup Strategies | Veeam full system image backups are performed: <ul style="list-style-type: none"> • daily overnight, and • after any configuration change. |
| Recovery Priority | High |
| Recovery Strategies | Veeam Full Image Recovery (Section 3.6.12.2) |

| Local Historian | |
|---------------------|--|
| Hostname | PI-Robotics |
| IP Address | 192.168.0.10 |
| Network | Supervisory LAN |
| Location | Robotics Hypervisor (Robotics-VH) |
| Type | Virtual |
| Operating System | Windows Server 2008 R2 |
| File System(s) | 50 GB HDD |
| Backup Strategies | Veeam full system image backups are performed: <ul style="list-style-type: none"> • daily overnight, and • after any configuration change. |
| Recovery Priority | High |
| Recovery Strategies | Veeam Full Image Recovery (Section 3.6.12.2) |

| HMI | |
|---------------------|---|
| Hostname | HMI |
| Model | Red Lion G310R210 |
| IP Address | 192.168.0.98 |
| Network | Supervisory LAN |
| Location | Workcell 1 |
| Type | Physical |
| Operating System | Crimson 3.0 700.000 (Vendor Proprietary) |
| Backup Strategies | Backup of database created by Crimson software on engineering change. |
| Recovery Priority | High |
| Recovery Strategies | Red Lion G310R210 Recovery (Section 3.6.12.7) |

| Supervisory PLC | |
|---------------------|---|
| Hostname | PLC |
| Model | Beckhoff CX9020 |
| IP Address | 192.168.0.30 |
| Network | Supervisory LAN |
| Location | Workcell 1 |
| Type | Physical |
| Operating System | Windows CE |
| File System(s) | |
| Backup Strategies | Backup of project files created by vendor-provided software after any engineering change. |
| Recovery Priority | High |
| Recovery Strategies | PLC Logic Recovery (Section 3.6.12.4) PLC SD Card Recovery (Section 3.6.12.5) |

| Machining Station 1, 2, 3, 4 | |
|------------------------------|---|
| Hostname | None |
| IP Address | 192.168.1.101, .102, .103, .104 |
| Network | Control LAN |
| Location | Workcell 1 |
| Type | Machining Stations |
| Operating System | Vendor Proprietary |
| Backup Strategies | Backup of project files created by vendor-provided software after any engineering change. |
| Recovery Priority | High |
| Recovery Strategies | Restore configuration from archived configuration backups following vendor-provided instructions. |

3.6.11.2 Network Devices

| Manufacturing System Router / Firewall | |
|--|---|
| Hostname | CiscoASA |
| Model | Cisco ASA 5512 |
| IP Address(es) | Corporate Network: REDACTED Cybersecurity LAN: 10.100.0.1 DMZ LAN: 10.100.1.1 Management LAN: 10.100.2.4 |
| Location | Cabinet 102 |
| Type | Physical |
| Operating System | Firmware: FTD 6.2.3.7 Build 51 |
| Backup Strategies | Manual. Performed via the CLI or web UI. |
| Recovery Priority | High |
| Recovery Strategies | Cisco ASA Recovery (Section 3.6.12.8) |

| CRS LAN Router | |
|---------------------|---|
| Model | RUGGEDCOM RX1510 |
| IP Address | 10.100.0.20, 192.168.0.2, 192.168.1.2 |
| Location | Workcell 1 |
| Type | Physical |
| Operating System | Vendor Proprietary |
| Backup Strategies | Manual. Performed through CLI or web UI |
| Recovery Priority | High |
| Recovery Strategies | Siemens RX1510 Recovery (3.6.12.9) |

| Supervisory LAN Switch | |
|------------------------|---|
| Model | Netgear GS724 |
| IP Address | |
| Location | Workcell 1 |
| Type | Physical |
| Operating System | Vendor Proprietary |
| Backup Strategies | Manual. Performed through CLI or web UI |
| Recovery Priority | High |
| Recovery Strategies | Netgear GS724 Recovery (3.6.12.11) |

| Control LAN Switch | |
|---------------------|---|
| Model | Siemens i800 |
| IP Address | |
| Location | Workcell 1 |
| Type | Physical |
| Operating System | Vendor Proprietary |
| Backup Strategies | Manual. Performed through CLI or web UI |
| Recovery Priority | High |
| Recovery Strategies | Siemens i800 Recovery (3.6.12.10) |

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

3.6.11.3 Cybersecurity LAN Servers

| Hyper-V Host Server | |
|---------------------|---|
| Hostname | LANVH |
| Model | Dell PowerEdge R620 |
| IP Address | 10.100.2.10 |
| Network | Management LAN (Hosted VMs are on Cybersecurity LAN) |
| Location | Cabinet 102 |
| Type | Physical |
| Operating System | Windows Server 2012 R2 Datacenter x64 Edition |
| Hosted VMs | <ul style="list-style-type: none"> • LAN-AD • LAN-AD02 • SymantecMgrVM • Security Onion • Graylog • GTBInspector • GTBCC • The-Hive • NessusVM • WSUS |
| File System(s) | C: (1 TB) D: (3.5 TB) |
| Backup Strategies | Veeam full system image backups are performed: <ul style="list-style-type: none"> • daily overnight, and • after any configuration change. |
| Recovery Priority | High |
| Recovery Strategies | Veeam Full Image Recovery (Section 3.6.12.2) |

| Active Directory Server | |
|-------------------------|--|
| Hostname | LAN-AD |
| Model | N/A |
| IP Address | 10.100.0.13 |
| Network | Cybersecurity LAN |
| Location | Hyper-V Host Server (LANVH) |
| Type | Virtual |
| Operating System | Windows Server 2012 R2 |
| File System(s) | 45 GB (VHD) |
| Backup Strategies | Veeam full system image backups are performed: <ul style="list-style-type: none"> • daily overnight, and • after any configuration change. |
| Recovery Priority | High |
| Recovery Strategies | Veeam Full Image Recovery (Section 3.6.12.2) |

| Backup Active Directory Server | |
|--------------------------------|--|
| Hostname | LAN-AD02 |
| Model | N/A |
| IP Address | 10.100.0.17 |
| Network | Cybersecurity LAN |
| Location | Hyper-V Host Server (LANVH) |
| Type | Virtual |
| Operating System | Windows Server 2012 R2 |
| File System(s) | 250 GB (VHD) |
| Backup Strategies | Veeam full system image backups are performed: <ul style="list-style-type: none"> • daily overnight, and • after any configuration change. |
| Recovery Priority | High |
| Recovery Strategies | Veeam Full Image Recovery (Section 3.6.12.2) |

| DMZ Historian | |
|---------------------|--|
| Hostname | PI-DMZ |
| Model | N/A |
| IP Address | 10.100.1.4 |
| Network | Manufacturing DMZ |
| Location | Cabinet 102 |
| Type | Virtual |
| Operating System | Windows 2008 R2 Standard Edition |
| File System(s) | 250 GB (VHD) |
| Backup Strategies | Veeam full system image backups are performed: <ul style="list-style-type: none"> • daily overnight, and • after any configuration change. <p>The native OS/soft PI application backup feature archives production data from the manufacturing process. These backups are stored on the local host; restore the host to obtain the most recent backup version. NOTE: Any recovered historical data will be limited to data present at the time of the backup.</p> |
| Recovery Priority | Medium |
| Recovery Strategies | Veeam Full Image Recovery (Section 3.6.12.2) OS/soft PI production data recovery. |

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

| VMware Host | |
|---------------------|---|
| Hostname | ESXi-Host |
| Model | Dell R710 |
| IP Address | 10.100.2.9 |
| Network | Management LAN |
| Location | Cabinet 102 |
| Type | Physical |
| Operating System | VMWare vSphere ESXi 6.0.0 |
| Hosted VMs | <ul style="list-style-type: none"> • PI-DMZ • Veeam |
| File System(s) | 4.5 TB (DataStore1) |
| Backup Strategies | Manual. Performed through CLI or web UI |
| Recovery Priority | High |
| Recovery Strategies | VMWare ESXi Recovery (3.6.12.12) |

| Veeam Backup Server | |
|---------------------|--|
| Hostname | Veeam |
| Model | N/A |
| IP Address | 10.100.0.10 |
| Network | Cybersecurity LAN |
| Location | VMware Host (ESXi-Host) |
| Type | Virtual |
| Operating System | Windows Server 2012 R2 |
| File System(s) | C: (50 GB, VHD) E: (500 GB, VHD) F: (4 TB, VHD) Network Share (Host, F:\Backup\Network Devices) |
| Backup Strategies | Veeam full system image backups are performed: <ul style="list-style-type: none"> • daily overnight, and • after any configuration change. |
| Recovery Priority | High |
| Recovery Strategies | Veeam Instant Virtual Machine Recovery (3.6.12.3) |

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

| Symantec Antivirus Server | |
|---------------------------|--|
| Hostname | SymantecMgrVM |
| Model | N/A |
| IP Address | 10.100.0.5 |
| Network | Cybersecurity LAN |
| Location | Hyper-V Host Server (LANVH) |
| Type | Virtual |
| Operating System | Windows Server 2012 R2 |
| File System(s) | 70 GB (VHD) |
| Backup Strategies | Veeam full system image backups are performed: <ul style="list-style-type: none"> • daily overnight, and • after any configuration change. |
| Recovery Priority | Medium |
| Recovery Strategies | Veeam Full Image Recovery (Section 3.6.12.2) |

| Graylog Server | |
|---------------------|--|
| Hostname | Graylog |
| Model | N/A |
| IP Address | 10.100.0.14 |
| Network | Cybersecurity LAN |
| Location | Hyper-V Host Server (LANVH) |
| Type | Virtual |
| Operating System | Ubuntu 14.04 |
| File System(s) | Root File System (50 GB) Data File System (500 GB) |
| Backup Strategies | Veeam full system image backups are performed: <ul style="list-style-type: none"> • daily overnight, and • after any configuration change. |
| Recovery Priority | Low |
| Recovery Strategies | Veeam Full Image Recovery (Section 3.6.12.2) |

| GTB Inspector Server | |
|----------------------|--|
| Hostname | GTBInspector |
| Model | N/A |
| IP Address | 10.100.0.175 |
| Network | Cybersecurity LAN |
| Location | Hyper-V Host Server (LANVH) |
| Type | Virtual |
| Operating System | CentOS 7.4.1708 |
| File System(s) | 162 GB (Vendor configured) |
| Backup Strategies | Veeam full system image backups are performed: <ul style="list-style-type: none"> • daily overnight, and • after any configuration change. |
| Recovery Priority | Low |
| Recovery Strategies | Veeam Full Image Recovery (Section 3.6.12.2) |

| GTB Console Server | |
|---------------------|--|
| Hostname | GTBCC |
| Model | N/A |
| IP Address | 10.100.0.176 |
| Network | Cybersecurity LAN |
| Location | Hyper-V Host Server (LANVH) |
| Type | Virtual |
| Operating System | CentOS 7.4.1708 |
| File System(s) | 107 GB (vendor configured) |
| Backup Strategies | Veeam full system image backups are performed: <ul style="list-style-type: none"> • daily overnight, and • after any configuration change. |
| Recovery Priority | Low |
| Recovery Strategies | Veeam Full Image Recovery (Section 3.6.12.2) |

| Nessus Vulnerability Scanner Server | |
|-------------------------------------|--|
| Hostname | NessusVM |
| Model | N/A |
| IP Address | 10.100.0.25 |
| Network | Cybersecurity LAN |
| Location | Hyper-V Host Server (LANVH) |
| Type | Virtual |
| Operating System | Windows Server 2012 R2 |
| File System(s) | C: (65 GB, VHD) |
| Backup Strategies | Veeam full system image backups are performed: <ul style="list-style-type: none"> • daily overnight, and • after any configuration change. |
| Recovery Priority | Medium |
| Recovery Strategies | Veeam Full Image Recovery (Section 3.6.12.2) |

| Windows WSUS Server | |
|---------------------|--|
| Hostname | WSUS |
| Model | N/A |
| IP Address | 10.100.0.12 |
| Network | Cybersecurity LAN |
| Location | Hyper-V Host Server (LANVH) |
| Type | Virtual |
| Operating System | Windows Server 2012 R2 |
| File System(s) | C: (400 GB, VHD) |
| Backup Strategies | Veeam full system image backups are performed: <ul style="list-style-type: none"> • daily overnight, and • after any configuration change. |
| Recovery Priority | Low |
| Recovery Strategies | Veeam Full Image Recovery (Section 3.6.12.2) |

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

| NTP Server | |
|---------------------|---|
| Hostname | NTPSrv |
| Model | Meinberg LANTIME M900 |
| IP Address | 10.100.0.15 |
| Network | Cybersecurity LAN |
| Location | Cabinet 102 |
| Type | Physical |
| Operating System | Firmware: 6.20.023 |
| Backup Strategies | Configuration backups are performed manually via the device web interface: <ul style="list-style-type: none"> • after any configuration change. Configuration backup files are transferred manually (i.e., via flash drive or network share) and are stored in the Veeam server. |
| Recovery Priority | Medium |
| Recovery Strategies | Vendor-specified recovery procedures (Section 3.6.12.11) |

3.6.12 Recovery Procedures

The following table defines generalized recovery procedures manufacturing system devices.

3.6.12.1 Veeam Directory Level Recovery

Directory level (file-level) backups enable restoration and recovery of individual files and folders. Data required for this type of restoration are stored in the Veeam Server. Reference Veeam guidance⁴¹ to complete the restoration process.

Warning: The manufacturing system must be in a non-operational state when the recovery is performed if the host to be recovered is in the Operations LAN or Supervisory LAN.

3.6.12.2 Veeam Full Image Recovery

Full image (volume-level) backups enable restoration and recovery of a host, or specific volumes of the host file system. Data required for this type of restoration are stored in the Veeam Server. Reference Veeam guidance⁴² to complete the restoration process.

Warning: The manufacturing system must be in a non-operational state when the recovery is performed if the host to be recovered is in the Operations LAN or Supervisory LAN.

⁴¹ https://helpcenter.veeam.com/docs/backup/vsphere/restore_vead.html?ver=95u4

⁴² https://www.veeam.com/veeam_backup_9_5_u4_enterprise_manager_user_guide_pg.pdf

3.6.12.3 Veeam Instant Virtual Machine Recovery

Virtual Machine backups enable full system images to be created, similar to Veeam Full Image backups for physical hosts. These types of backups can be used for recovery of files, file systems, and complete restoration. Reference Veeam guidance for Hyper-V⁴³, VMWare⁴⁴, and Veeam⁴⁵ to complete the restoration process.

3.6.12.4 PLC SD Card Recovery

PLC SD card recovery can be performed to rapidly restore the PLC logic back to an operational state in case of compromise or corruption.

1. Power off the PLC and remove the SD card from the front of the device.
2. Insert the SD card into the Engineering Workstation.
3. Delete all existing contents from the SD card, or simply reformat the card.
4. Copy and paste the files from the most recent backup onto the SD card.
5. Safely remove the SD card from the Engineering Workstation.
6. Insert the SD card into the PLC and power on the device.

Notice: This recovery can only restore the logic; it will not restore any configuration of the PLC or other modules within the chassis.

Warning: Do not use this recovery method if the PLC or any of the other modules have been replaced as part of this recovery.

Warning: The manufacturing system must be in a non-operational state when this recovery is performed.

⁴³ https://helpcenter.veeam.com/docs/backup/hyperv/data_recovery.html?ver=95u4

⁴⁴ https://helpcenter.veeam.com/docs/backup/vsphere/data_recovery.html?ver=95u4

⁴⁵ https://helpcenter.veeam.com/docs/backup/vsphere/vbr_config_restore.html?ver=95u4

3.6.12.5 PLC Firmware Recovery

PLC firmware recovery⁴⁶ can be performed to restore the PLC operating system. This operation must be performed from the Engineering Workstation.

1. Download the most recent firmware image from the Beckhoff website.
2. Power off the PLC and remove the SD card from the front of the device.
3. Insert the SD card into the Engineering Workstation.
4. Delete all existing contents from the SD card, or simply reformat the card.
5. Copy and paste the new firmware files from the most recent backup onto the SD card.
6. Safely remove the SD card from the Engineering Workstation.
7. Insert the SD card into the PLC and power on the device.
8. Connect to the PLC from the Engineering Workstation TwinCAT software, open the PLC project, activate the configuration, and deploy the PLC project.
9. Disconnect from the PLC.

Warning: The manufacturing system must be in a non-operational state when this recovery is performed.

3.6.12.6 Red Lion HMI Recovery

HMI recovery⁴⁷ can be performed to restore the PLC logic back to a known state in case of compromise or corruption. This operation must be performed from the Engineering Workstation using the Crimson software.

1. Connect to the HMI from the Engineering Workstation Crimson software.
2. Open the HMI project, and upload the database to the HMI.

Warning: The manufacturing system must be in a non-operational state when this recovery is performed.

⁴⁶ <https://infosys.beckhoff.com>

⁴⁷ https://www.redlion.net/sites/default/files/1288/4198/Crimson%203%20Manual%20English%20%28Revision%203.4%29%205612KB_0.pdf

3.6.12.7 Cisco ASA 5512 Recovery

In most cases, restoring the Cisco ASA configuration may be enough, however, in certain situations, performing the vendor-specified factory reset procedure before restoring may be required. To perform the factor reset, use the following command:

```
hostname(config)# configure factory-default [IP address [mask]]
```

Note: IP address [mask] are the inside management interface address to configure after the reset.

Example: hostname(config)# configure factory-default 192.168.1.1 255.255.255.0

Restore the configuration from the archived configuration backups. For details on this process see the Cisco manual for ASAs⁴⁸.

3.6.12.8 Siemens RX1510 Recovery

Recovery procedures⁴⁹ can be performed to restore the RX1510 back to a known state in case of compromise or corruption. This operation must be performed from the Engineering Workstation or other device connected to the workcell network.

1. Access the web interface of the RX1510 from the Engineering Workstation.
2. From the admin section, restore the device to factory defaults.
3. Copy the most recent configuration file to a USB flash drive and insert into the RX1510.
4. From the admin section, navigate to the full-configuration-load page and complete the process.

3.6.12.9 Siemens i800 Recovery

Recovery procedures⁵⁰ can be performed to restore the i800 logic back to a known state in case of compromise or corruption. This operation must be performed from the Engineering Workstation or other device connected to the workcell network.

1. Power off the i800 and remove the SD card from the bottom of the device.
2. Insert the SD card into the Engineering Workstation.
3. Delete all existing contents from the SD card, or simply reformat the card.
4. Copy and paste the files from the most recent backup onto the SD card.
5. Safely remove the SD card from the Engineering Workstation.
6. Insert the SD card into the i800 and power on the device.

⁴⁸ https://www.cisco.com/c/en/us/td/docs/security/asa/asa72/configuration/guide/conf_gd/start.html

⁴⁹ https://support.industry.siemens.com/cs/attachments/109481700/ROXII_v2.13_RX1500_User-Guide_WebUI_EN.pdf

⁵⁰ <https://support.industry.siemens.com/cs/document/109737193/ruggedcom-ros-v4-3-user-guide-for-i800-i801-i802-i803?lc=en-WW&pnid=25022>

3.6.12.10 Netgear GS724 Recovery

Recovery procedures⁵¹ can be performed to restore the GS724 back to a known state in case of compromise or corruption. This operation must be performed from the Engineering Workstation or other device connected to the workcell network.

1. Access the web interface of the GS724 from the Engineering Workstation.
2. Navigate to **Maintenance > Download > HTTP File Download**.
3. Select the most recent configuration file or firmware image from the Engineering Workstation and click **Apply**.

3.6.12.11 NTP Server Recovery

NTP Server recovery can be performed through the device web interface⁵². If the device is not operational, attempt to perform the vendor-specified Factory Reset procedure via the display/keypad on the front of the device. Once the device is operational, restore configuration from archived configuration backups via the web interface.

3.6.12.12 VMWare ESXi Recovery

Reload the same version of ESXi from trusted media and restore the configuration from the backup archives (see VMWare KB⁵³ for additional details). One method utilizing the ESXi Console is detailed below.

From ESXi Console:

1. Put the host into maintenance mode by running the command:
`vim-cmd hostsvc/maintenance_mode_enter`
2. Copy the backup configuration file to the host's /tmp directory using SCP and name it configBundle.tgz.
3. Run the following command to restore the configuration:
`vim-cmd hostsvc/firmware/restore_config /tmp/configBundle.tgz`

Note: Executing this command will initiate an automatic reboot of the host after command completion.

4. Restore the individual virtual machines from Veeam backup archives following Veeam Instant Virtual Machine Recovery procedures (Section 3.6.12.3).

⁵¹http://www.downloads.netgear.com/files/GDC/GS716TV3/GS716Tv3_GS724Tv4_GS748Tv5_SWA_25Sept2013.pdf?_ga=2.205436368.1356352150.1566933456-1528595668.1566933456

⁵²https://www.meinbergglobal.com/download/docs/manuals/english/m900_gps.pdf

⁵³<https://kb.vmware.com/s/article/2042141>

3.7 Service Level Agreement

This section provides example content that a Vendor Service Level Agreement may contain, including example policy and procedure statements that were developed for the fictional company Alpha. Certain commercial entities, equipment, or materials may be identified in this document in order to describe a concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, equipment, or materials are necessarily the best available for the purpose. Each organization’s information security experts should identify the content, and policy and procedure statements that will best integrate with their existing cybersecurity program and manufacturing system infrastructure.

Service Level Agreement (SLA)
for Vendor
by
Alpha

Effective Date: 02-22-2019

| | |
|------------------------|-----------|
| Document Owner: | President |
|------------------------|-----------|

Version

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

Approval

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

| Approvers | Role | Signed | Approval Date |
|-----------|------------------|---------------------|---------------|
| Alpha | Customer | <digital signature> | 2-22-2019 |
| Vendor | Service Provider | <digital signature> | 2-22-2019 |

3.7.1 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.

3.7.2 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.

3.7.3 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

3.7.4 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

3.7.5 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

3.7.6 Alpha's Requirements

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

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

3.7.7 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 Alpha's for all scheduled maintenance.

3.7.8 Service Assumptions

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

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

3.7.9 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.

3.7.10 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

3.7.11 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 to 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 at the discretion of Alpha in-line with the above timescales and dependent on the priority of the support request. The service provider may not utilize remote access as an alternative for providing onsite support as described in section 3.7.10 of this agreement.

3.7.12 Personnel Changes

The Service Provider will notify Alpha within 24 hours when an individual supporting Alpha leaves the Service Provider or is transferred. Alpha will disable remote access, if granted, for the individual within 24 hours of notification. The Service Provider will revoke the individual's access to Alpha information and information systems within 24 hours. Additionally, any system account passwords the individual had will need to be changed to ensure user access into the network has been completely removed.

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 Impact 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 implementation. The process of sequentially implementing and measuring enabled the detection of performance-impacting interactions between the technical solutions.

- **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 requirements. Some technical solutions provided multiple modes of operation that met the security 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.
- **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 implementation impact measurements to determine the relative performance impact. The final technology implementation impact (if it not a multi-mode measurement) can also be used as the security implementation impact.

Before the 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 assess 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]

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose. Each organization's information security experts should identify the technical solutions that will best integrate with their existing cybersecurity program and manufacturing system infrastructure.

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).

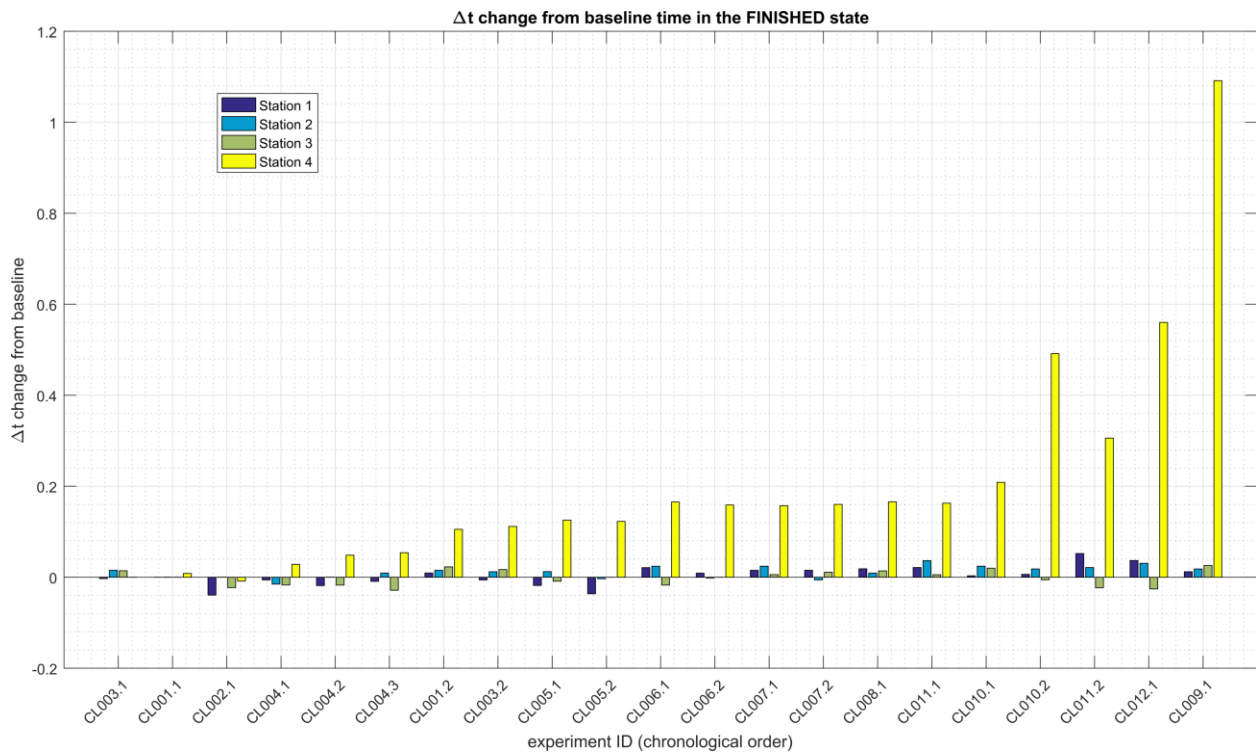


Figure 4-1 - Bar plot showing the increasing Station 4 “FINISHED” state deviation from the baseline. The data from Station 1, 2, and 3 are also shown. The plotted values are the mean for all 35 parts in the experiment. The largest discrete deviation measured was around 1.55 sec.

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.

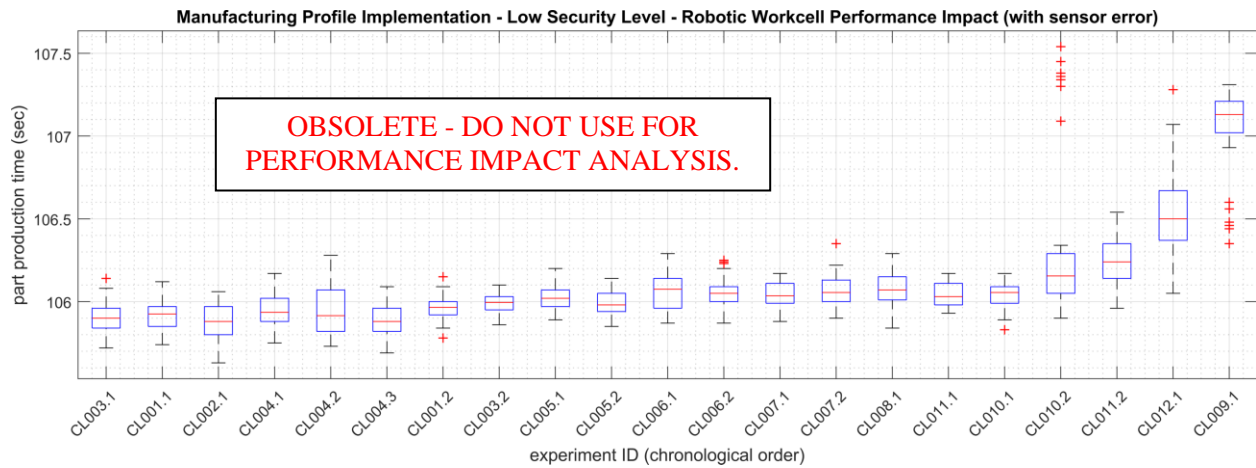


Figure 4-2 - Performance impact to the manufacturing process KPI “part production time” using the original definition, where the time is measured from the arrival of the part at Station 1 to the departure of the part from Station 4. Note the large increase and outliers for the last four experiments (CL010.2,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

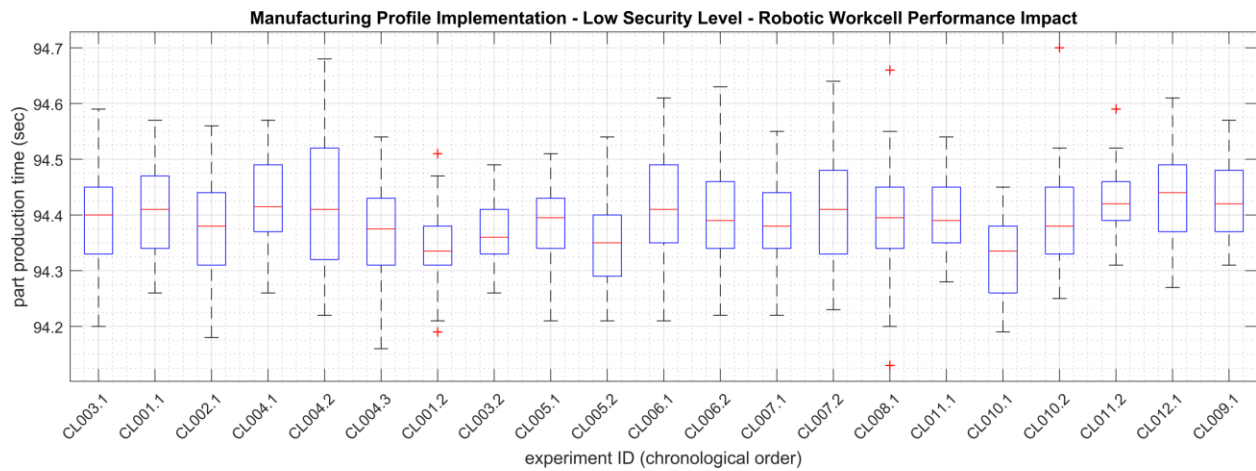


Figure 4-3 - Performance impact to the manufacturing process KPI “part production time” using the updated definition, where the time is measured from the arrival of the part at Station 1 to the arrival of the part at Station 4. Note the improvement in stability compared to the original definition shown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

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

4.1.3 Implementation Note - Availability of Measurement Data

All raw and processed measurement data captured from each experiment is freely available online at: <https://doi.org/10.18434/M32072>.

Links to each of the data files are provided below, and directly referenced at the end of each implementation.

- [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 scheduled scanning, dashboards, and baselining of equipment.

Open-AudIT is a downloadable Open Virtual Appliance (OVA) which is easy to install. OVA install allows installation in a hypervisor environment allowing for installation within an existing virtual environment without requiring purchasing additional hardware. Configuration for initial discovery scans is straightforward.

4.2.2 Technical Capabilities Provided by Solution

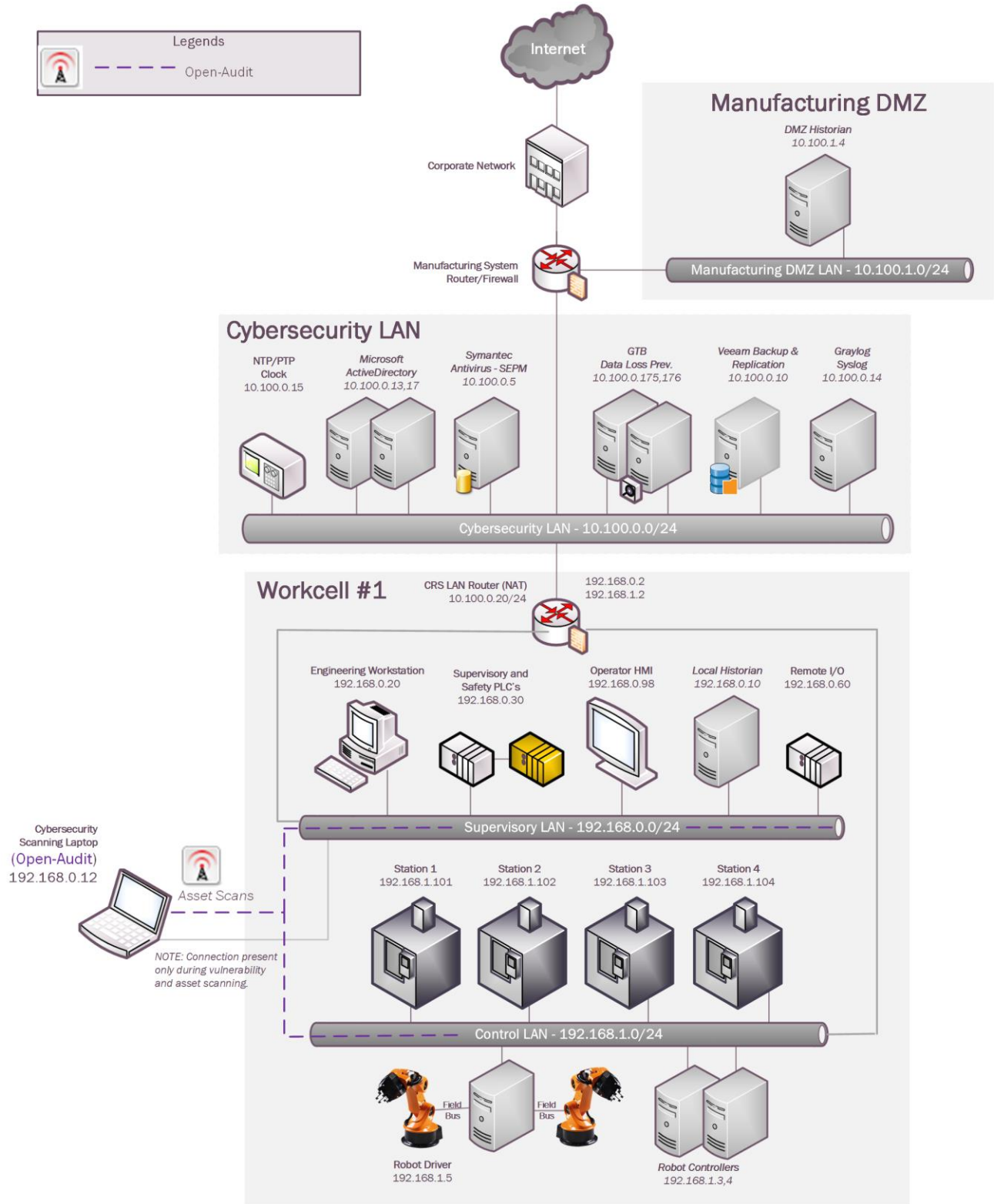
Open-AudIT provides components of the following Technical Capabilities described in Section 6 of Volume 1:

- Hardware Inventory
- Software Inventory
- Systems 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



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

4.2.5 Installation Instructions and Configurations

Details of the solution implemented:

| Name | Version | Hardware details |
|-------------------|---------|---|
| Open-Audit | 3.0.0 | Hyper-V Virtual Machine (Generation 1): <ul style="list-style-type: none"> Processors: 2 virtual cores Memory: 2 GB Disk space: Allocated by the Virtual Appliance files provided by the vendor. Network: 1 interface Operating System: CentOS 7 |

4.2.5.1 Open-Audit Environment setup

1. A virtual machine running CentOS Linux 7 as provided by the Vendor with hardware specifications as described in the table above.
2. The guest OS IP information was set as follows:

```
IP address: 10.100.0.177
Gateway: 10.100.0.1
Subnet Mask: 255.255.255.0
DNS:10.100.0.17
```

4.2.5.2 Setup Instructions

1. Download the Opmantek Virtual Appliance⁵⁴
2. If deploying on a Hyper-V host server⁵⁵, convert the downloaded **.ova** file to **.vhdx** format.
3. Login using the default credentials, set a hostname and assign the VM a static IP address. Edit */etc/sysconfig/network-scripts/ifcfg-eth0* to set the networking information.
4. Restart networking services using the command `service network restart`.

4.2.5.3 Additional Setup via Web browser

1. Navigate to the Open-Audit Web UI (Example <http://<ip-address-of-server>>)
2. Select **Yes**, if prompted to proceed to untrusted site. This error is produced since SSL has not been configured and Open-Audit redirects HTTP sessions over to HTTPS.
3. Click on **Open-Audit Enterprise**.

⁵⁴ <https://opmantek.com/>

⁵⁵ <https://blogs.msdn.microsoft.com/timomta/2015/06/11/how-to-convert-a-vmware-vmdk-to-hyper-v-vhdx/>

4. Login using the default **username / password** mentioned on the webpage.
5. Click on **Admin > LDAP Server > Create LDAP Servers for Active Directory** integration.

Screenshot of our Active directory connection provided for reference.

| | | |
|---------------------------|------------------------|---|
| Name | TestConnection | ? |
| Description | Documentation | ? |
| Organisation | Default Organisation | ? |
| Domain | LAN.LAB | ? |
| Host | 10.100.0.17 | ? |
| Port | 389 | ? |
| Use Secure (LDAPS) | No | ? |
| Version | 3 | ? |
| Use LDAP for Roles | Yes | ? |
| Type | Active Directory | ? |
| Base DN | CN=Users,DC=lan,DC=lab | ? |

6. Click **Submit** once all information has been entered.

4.2.5.4 Active Directory Groups for LDAP Integration

- Create the following **Security** Groups of **Global** Type in your Active Directory to integrate with Open-Audit.

```
open-audit_roles_admin
open-audit_roles_org_admin
open-audit_roles_reporter
open-audit_roles_user
open-audit_orgs_default_organisation
```

- Add the appropriate users to these groups. Test logging in with your Active Directory credentials.

4.2.5.5 Configuring Discover Credentials

1. Click on **Discover > Discoveries > Create Credentials.**
2. Enter the requested information:

Name – Name of the Credentials being used. Example (**SSH**)

Organization – Default Organization is selected. Pickup another if your configuring more the one organization.

Description – Description of item being added.

Type – Select which type of credentials will be used. (**SNMP (v1 / v2), SNMP v3, SSH, SSH Key, or Windows**)

Credentials – enter the appropriate credentials for the select type from above.

The image below shows Discover credentials created for scanning workcell network.

| | | |
|--------------|---|---|
| ID | <input type="text"/> | ? |
| Name | <input type="text" value="CRS Scans"/> | ? |
| Organisation | <input type="text" value="Default Organisation"/> | ? |
| Description | <input type="text" value="Perform Linux Scans"/> | ? |
| Type | <input type="text" value="SSH"/> | ? |
| Username | <input type="text" value="icsuser01"/> | |
| Password | <input type="password" value="....."/> | ? |
| Edited By | <input type="text" value="nmis"/> | ? |
| Edited Date | <input type="text" value="2018-09-26 13:56:53"/> | ? |

3. Click **Submit**

4.2.5.6 Organization Groups

1. Click on **Manage > Orgs > Create Orgs**
2. Enter **Name** and **Description**.
3. Click **Submit**.

The image below shows an Organization Group created as per our environment

The screenshot shows a form with four fields, each with a question mark icon to its right:

- Name:** CRS Machines
- Description:** Robotics Machines within Work Cell
- Parent ID:** Default Organisation
- Type:** Organisation

4.2.5.7 Discovery Scans

1. Click on **Discover > Discoveries > Create Discoveries**
2. Enter a name under **Name**.
3. Enter a network subnet to be scanned under **Subnet**.
4. Select the Open-Audit server under **Network Address**.
5. Click **Advanced** to setup additional options if desired. These options are **Org, Type, Devices Assigned to Org, and Devices Assigned to Location**.
6. Click **Submit**.

The image below shows Discovery scan created for scanning the work-cell

The screenshot shows a form titled "Discoveries" with three input fields and two buttons:

- Name:** CRS Work Cell
- Subnet:** 192.168.0.0/23
- Network Address:** http://127.0.0.1/open-audit/
- Submit:** A blue button.
- Advanced:** A button with a gear icon.

4.2.5.8 Additional Information

1. Change all default passwords before deploying in production.
2. 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)
3. Use SNMPv3 whenever using SNMP for scanning devices.
4. Software is Open Source. Professional Edition allows up to 20 machines after that there is a cost which is relatively inexpensive. Upgrade to Enterprise Edition to perform system baselines scans.
5. For more information and hardware requirements, visit the Community forums⁵⁶

⁵⁶ <https://community.opmantek.com>

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.

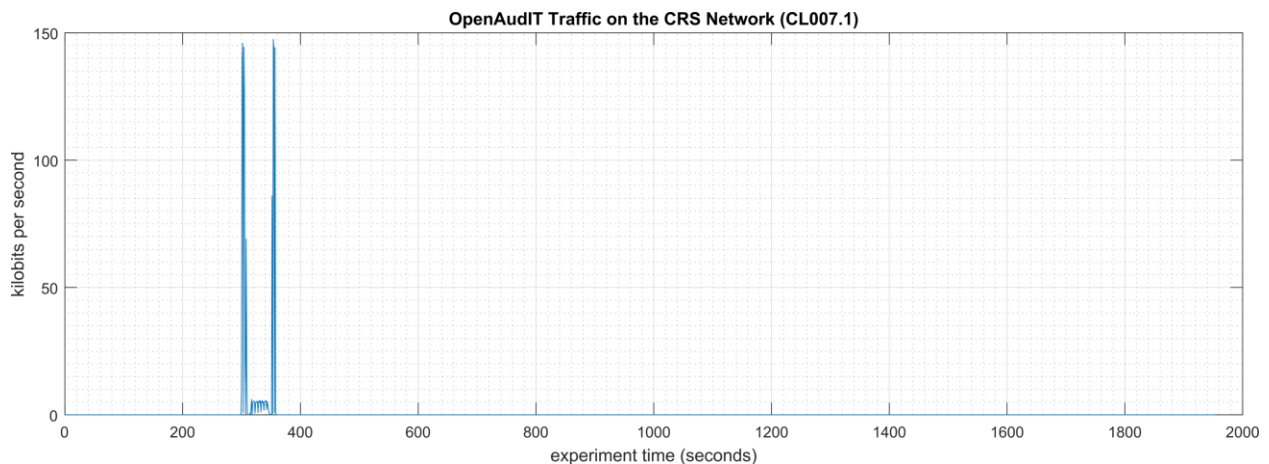


Figure 4-4 - Time series plot showing the rate of network traffic (in kilobits per second) transmitted and received by the Open-Audit tool during the experiment time period, with the most prominent activity between 300 to 358 seconds.

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

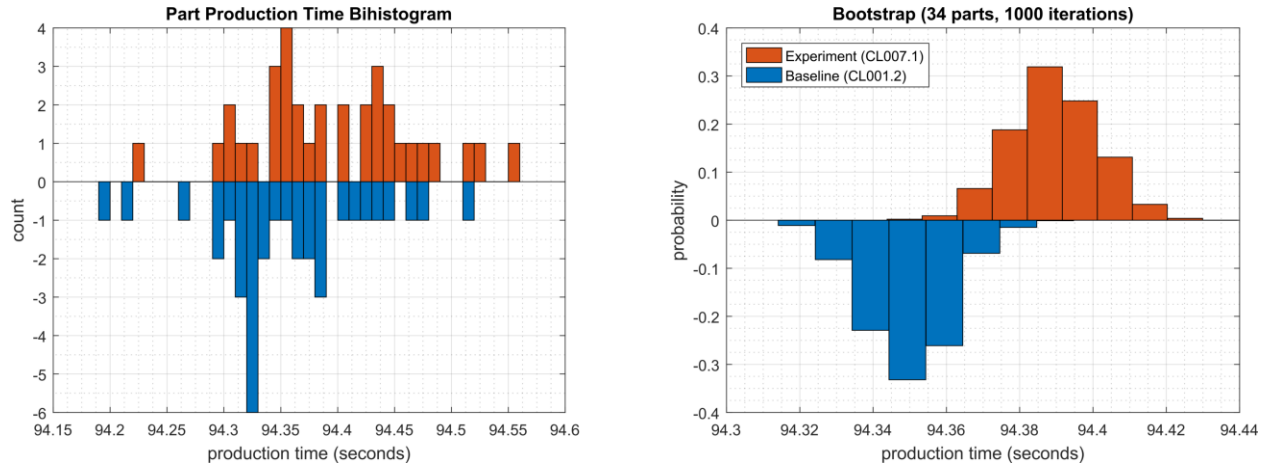


Figure 4-5 - Bihistograms showing the part production time (left) and estimated mean production time using the bootstrap method (right) using the measurements from baseline CL001.2 and experiment CL007.1.

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).

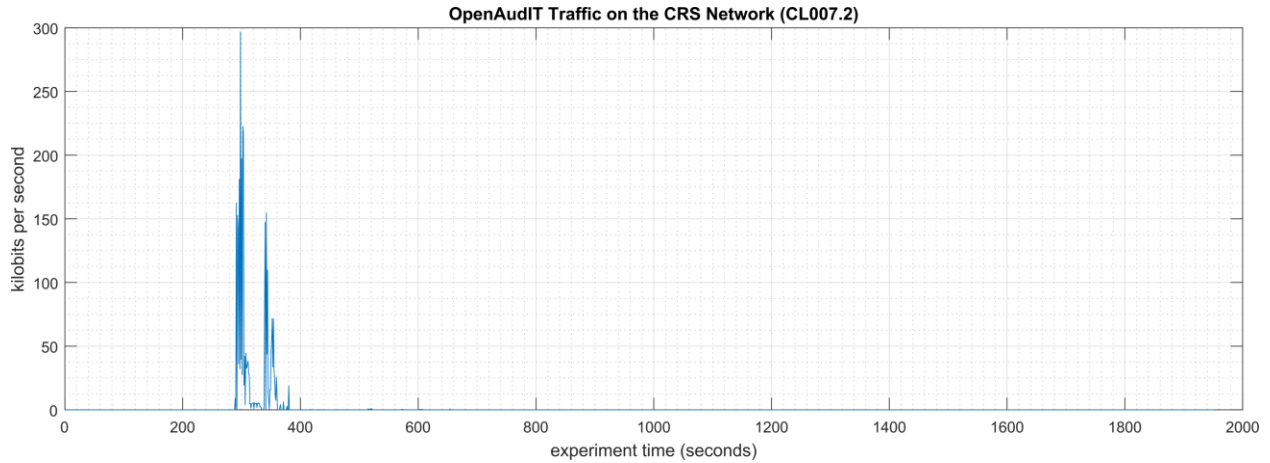


Figure 4-6 - Time series plot showing the rate of network traffic (in kilobits per second) transmitted and received by the Open-Audit tool during the experiment time period, with the most prominent activity between 290 to 380 seconds.

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).

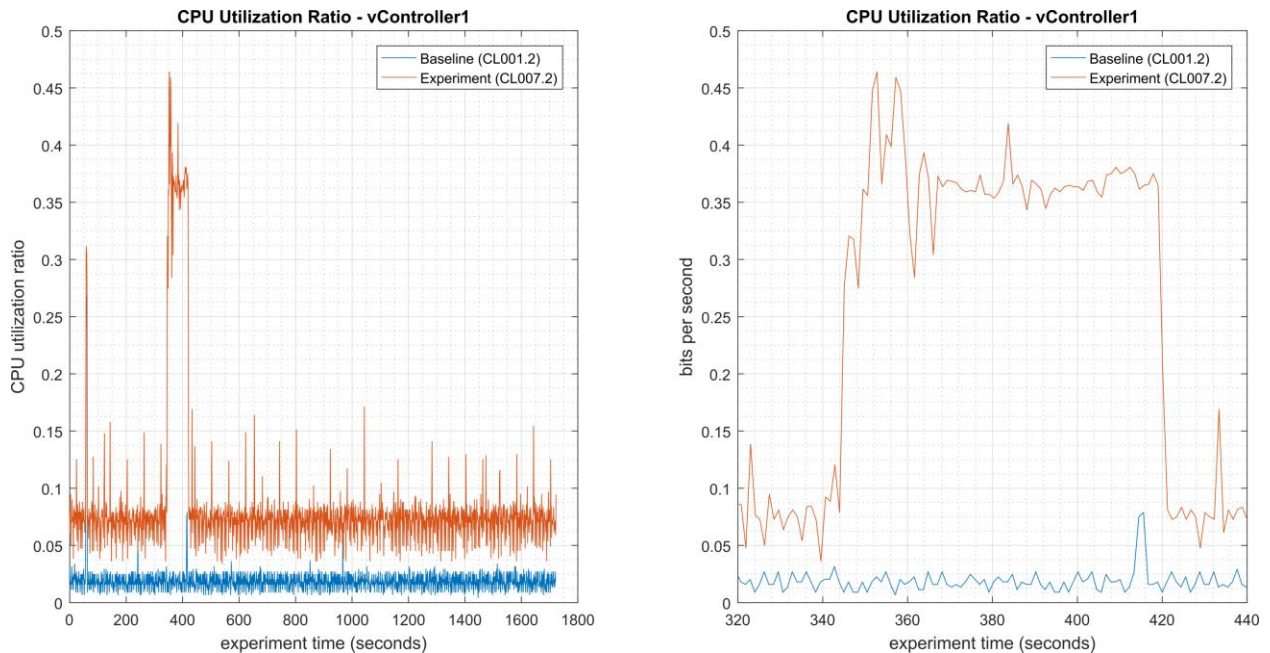


Figure 4-7 - Time series plots showing the CPU utilization ratio for vController1 during the experiment (left), and during the period of measured impact (right).

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

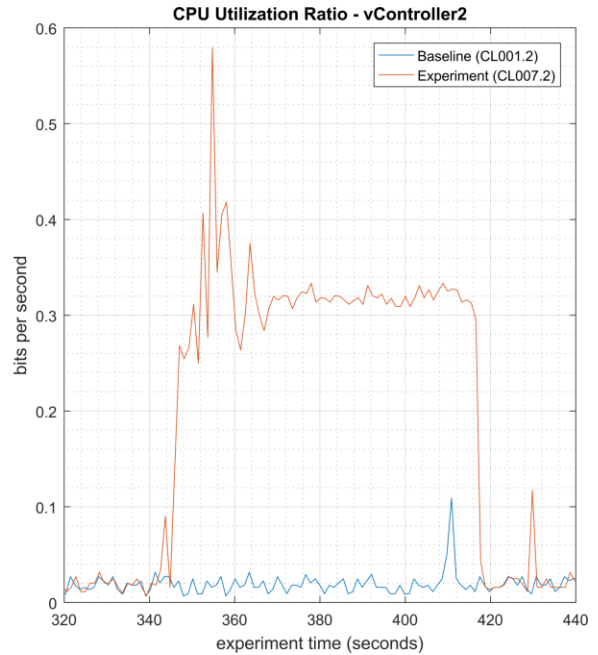
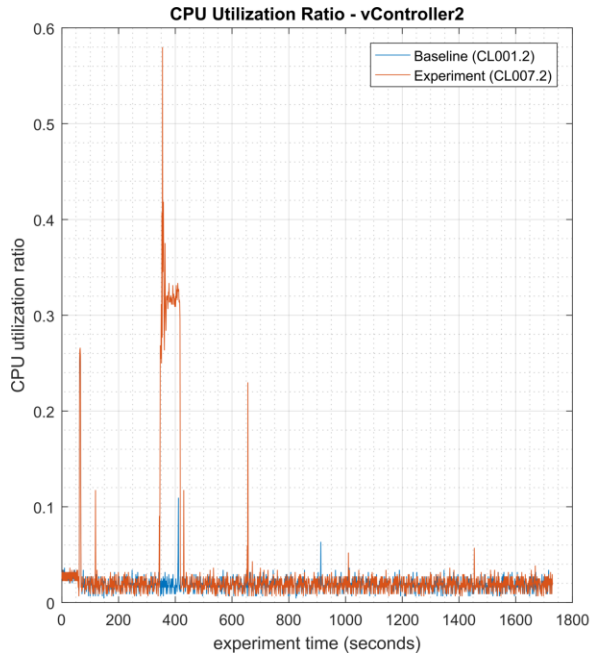


Figure 4-8 - Time series plots showing the CPU utilization ratio for vController2 during the experiment (left), and during the period of measured impact (right).

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

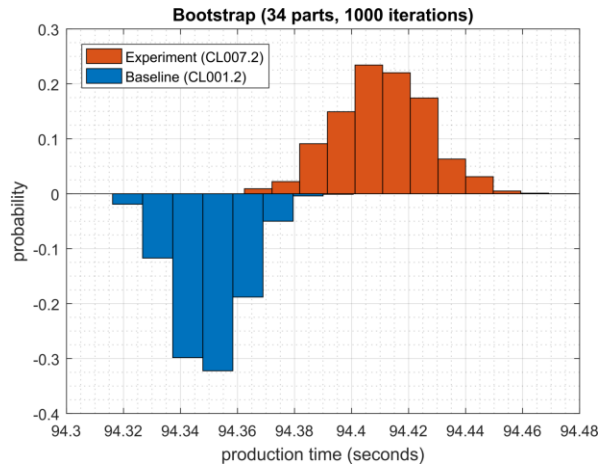
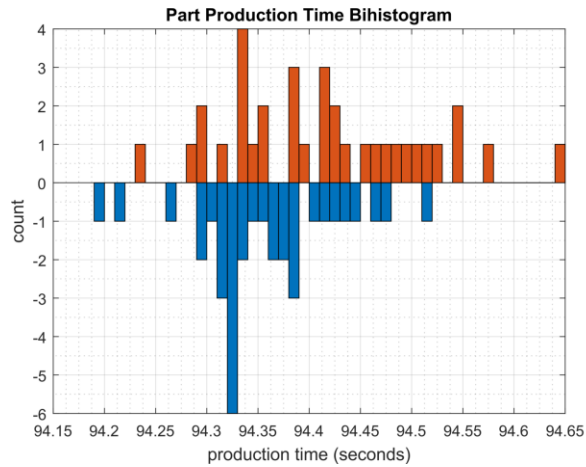


Figure 4-9 - Bihistograms showing the part production time (left) and estimated mean production time using the bootstrap method (right) using the measurements from baseline CL001.2 and experiment CL007.2.

4.2.7 Links to Entire Performance Measurement Data Set

- [CL007.1-OpenAudITNetworkScan.zip](#)
- [CL007.2-OpenAudITAuthenticatedNetworkScan.zip](#)

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

4.3 CSET

4.3.1 Technical Solution Overview

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

4.3.2 Technical Capabilities Provided by Solution

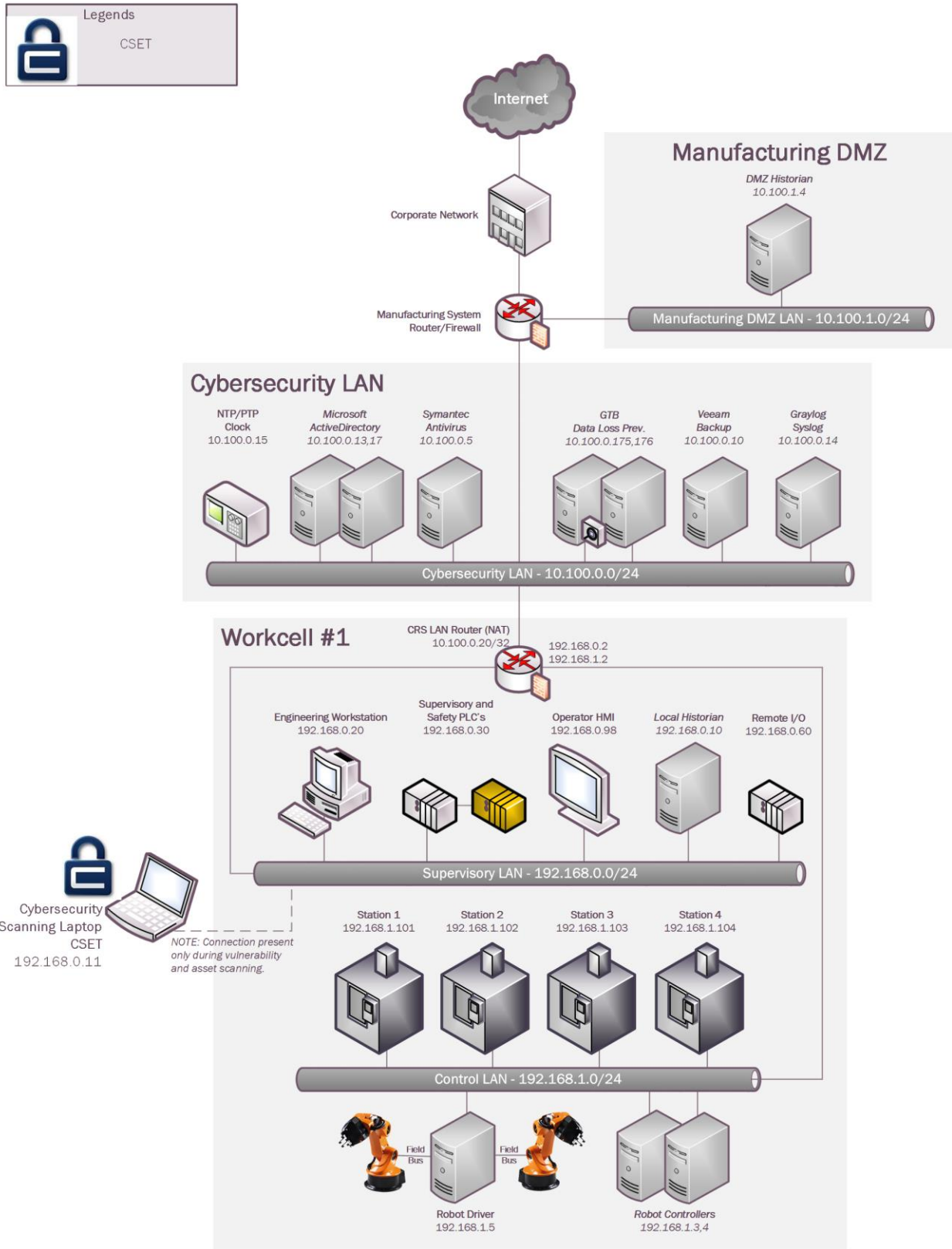
CSET provides components of the following Technical Capabilities described in Section 6 of Volume 1:

- Network Architecture Documentation
- Risk Assessment

4.3.3 Subcategories Addressed by Implementing Solution

ID.AM-3, ID.AM-4, ID.RA-1

4.3.4 Architecture Map of Where Solution was Implemented



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

4.3.5 Installation Instructions and Configurations

Details of the solution implemented:

| Name | Version | Hardware Details |
|------|---------|---|
| CSET | 8.1 | Laptop with the following specs: <ul style="list-style-type: none"> • Processor: i7 • Memory: 16 GB • Disk: 256 GB • OS: Windows 7 Professional |

4.3.5.1 Environment setup

1. CSET was installed on a temporary Windows laptop in the workcell network on an on-demand basis

4.3.5.2 Installation

1. Download CSET⁵⁷. 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).
2. Use any ISO-specific utility program that can mount the file.
3. Find and run the CSET_Setup.exe file in the folder, virtual drive, or CD.
4. Complete the instructions in the installation wizard to install the program.

4.3.5.3 Running CSET

1. Launch the program by double-clicking its desktop icon
2. Select **New Assetment** on the home screen.
3. Click **Start Here** button in the lower right corner of program.
4. Enter all required information

⁵⁷ <https://www.us-cert.gov/forms/csetiso>.

Assessment Name: Collaborative Robotics | Assessment Date: 4/23/2019

Facility Name: Alpha Manufacturing

City or Site Name: Gaithersburg

State, Province, or Region: Maryland

Assessor Name: John Doe | Assessor Email: | Assessor Telephone: |

5. Click **Continue** to proceed.
6. Click the drop down menus and select the appropriate choices.

Sector: Critical Manufacturing Sector

Industry: Machinery Manufacturing

What is the gross value of the assets you are trying to protect?: < \$1,000,000

What is the relative expected effort for this assessment?: Small (1-2 hours)

- Privacy is a significant concern for the assets I am trying to protect.
- My organization is concerned with the cybersecurity integrity of our procurement supply chain.
- My organization uses industrial control systems (ICS).

7. Click **Continue** to proceed.
8. (Optional) Click the **Create a network diagram** button to create one, otherwise click **Continue**.
9. Change Mode Selection to **Advanced** and **Cybersecurity Frame-based Approach**

- Basic** - Generate a basic assessment using the provided demographic information
- Advanced** - Let me choose which cybersecurity standard(s) the assessment will be based on:

Before selecting which cybersecurity standards your assessment is based on, please choose one of the following options.

- Questions-based Approach**
The questions-based approach uses simple questions and allows for partial credit.
- Requirements-based Approach**
The requirements-based approach uses the exact wording of the standard and is best for those industries that are regulated by a specific standard.
- Cybersecurity Framework-based Approach**
The cybersecurity framework-based approach uses allows you to define a custom profile based on the Cybersecurity Framework.

10. Click **Continue** to use default profile or create a new profile.
11. Click **Continue** again.
12. Answer all the questions as they appear.
13. Complete all questions and generate a final report.

4.3.5.4 Additional Information

Video tutorials⁵⁸ are available on the CSET YouTube Channel to help you better understand how to use this tool.

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 Links to Entire Performance Measurement Data Set

N/A

⁵⁸ <https://www.youtube.com/c/CSETCyberSecurityEvaluationTool>

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:⁵⁹

- 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:

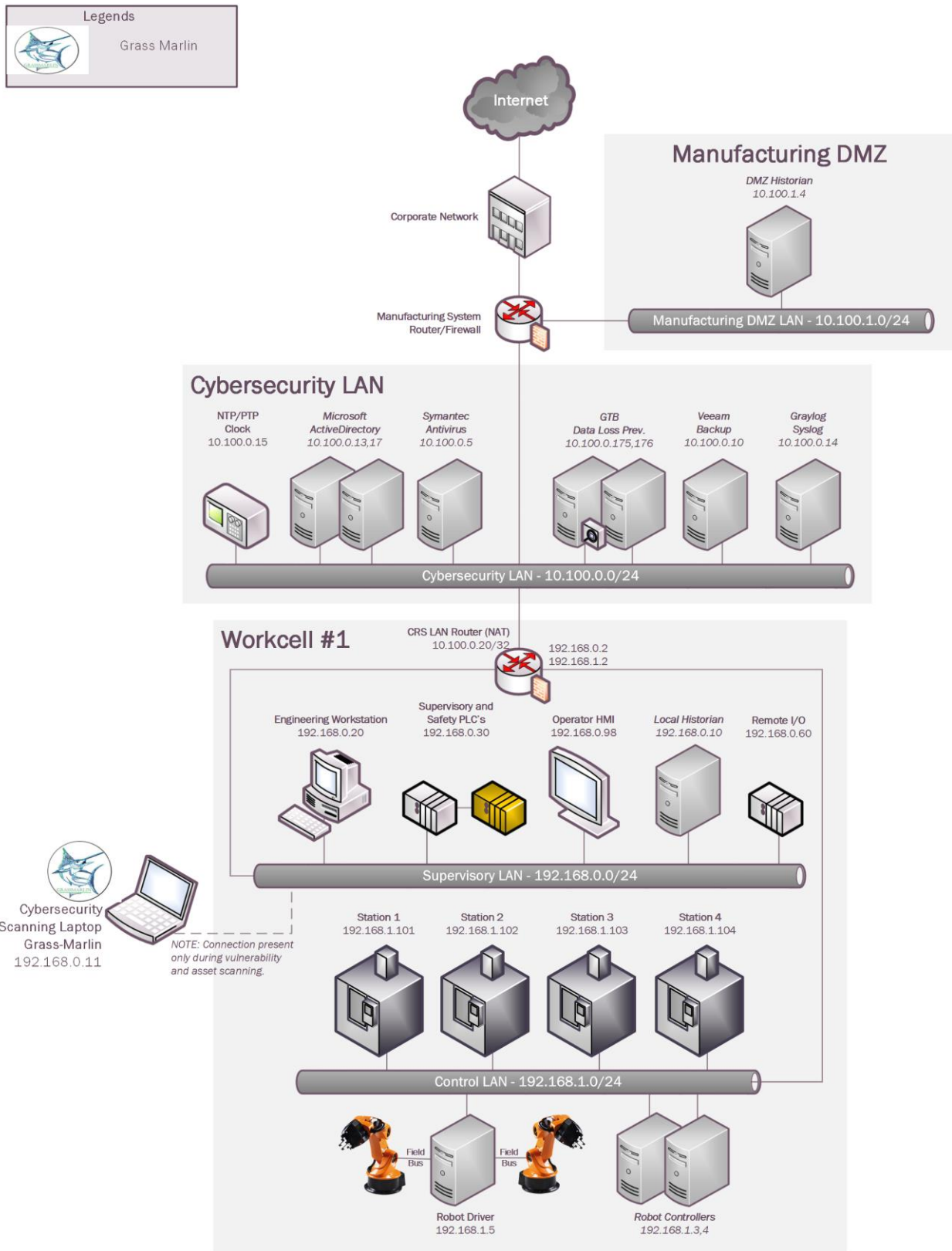
- Network Architecture Documentation
- Baseline Establishment
- Map Data Flows

4.4.3 Subcategories Addressed by Implementing Solution

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

⁵⁹ 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



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

4.4.5 Installation Instructions and Configurations

Details of the solution implemented:

| Name | Version | Hardware Details |
|-------------|---------|---|
| GRASSMARLIN | 3.2.1 | Laptop with the following specs: <ul style="list-style-type: none"> • Processor: i7 • Memory: 16 GB • Disk: 256 GB • OS: Windows 7 Professional |

4.4.5.1 Environment Setup

1. A temporary Windows laptop with GRASSMARLIN installed was setup in the workcell network on an on-demand basis.

4.4.5.2 Installation

1. Download GRASSMARLIN⁶⁰
2. Run the installer. The installer will install additional programs such as Java and Wireshark during the setup.

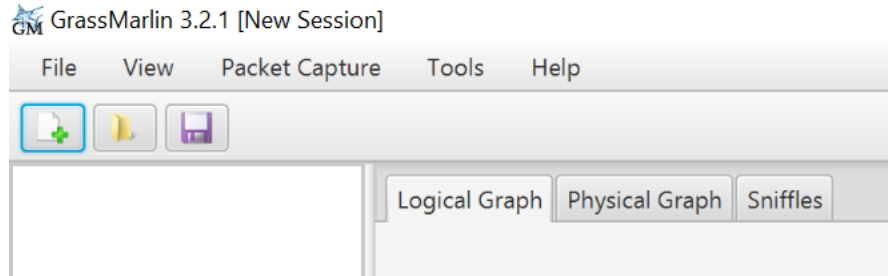
4.4.5.3 Using the Software

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.

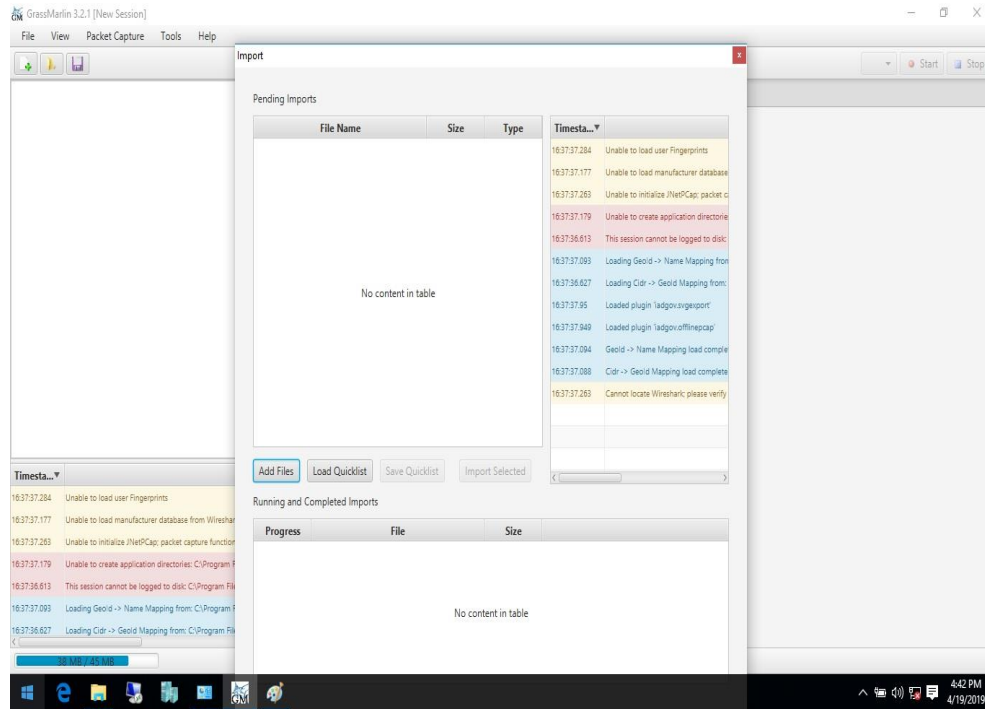
1. Use tcpdump to capture network packets & save to a pcap file on a Linux system
 - a. Install **tcpdump** package if not present already
 - b. Run, `tcpdump -i <mirror-port interface> -w mypcap.pcap`
For example: `tcpdump -i eth1 -w /home/icssec/pes.pcap`
Where `eth1` is the span / mirror port connection
2. Run GRASSMARLIN on a Windows system by double clicking the program icon from the Programs Menu. On a Linux system, run `sudo grassmarlin` to launch the installer.
3. Import a pcap in GRASSMARLIN as follows,

⁶⁰ <https://github.com/nsacyber/GRASSMARLIN/releases>

- Click on the **Import** icon in the toolbar (or select **Import files** from the File Menu)

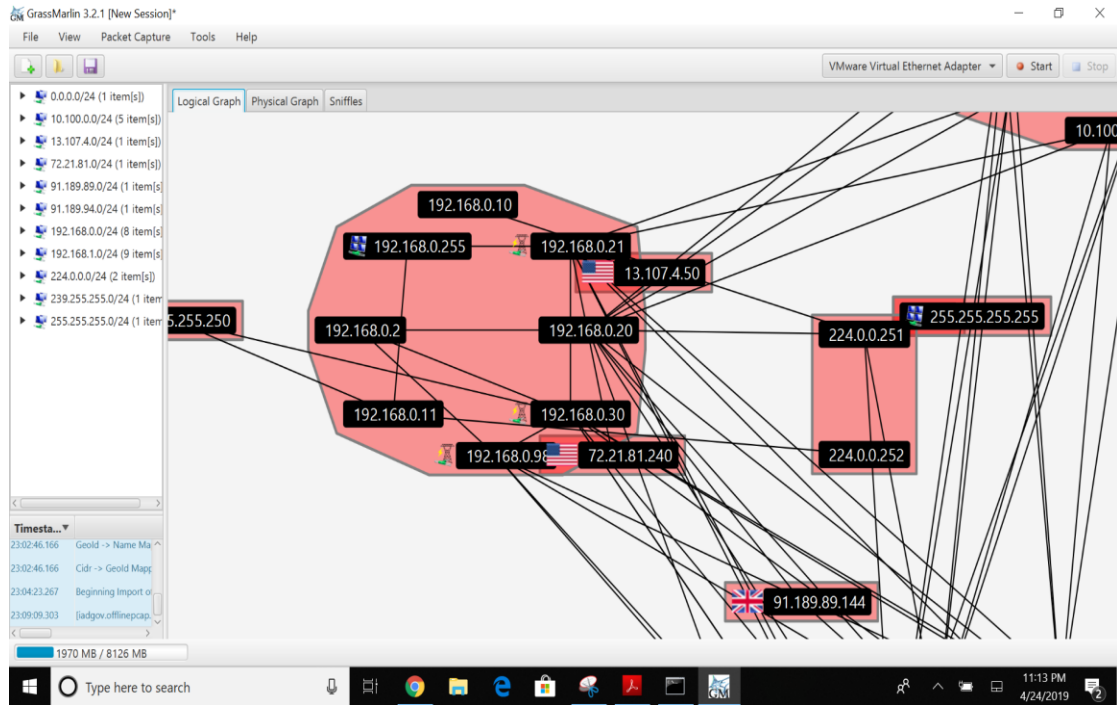


- Click on **Add Files**. Browse to the pcap file. Once done, the pcap will now show up under **Pending Imports**.

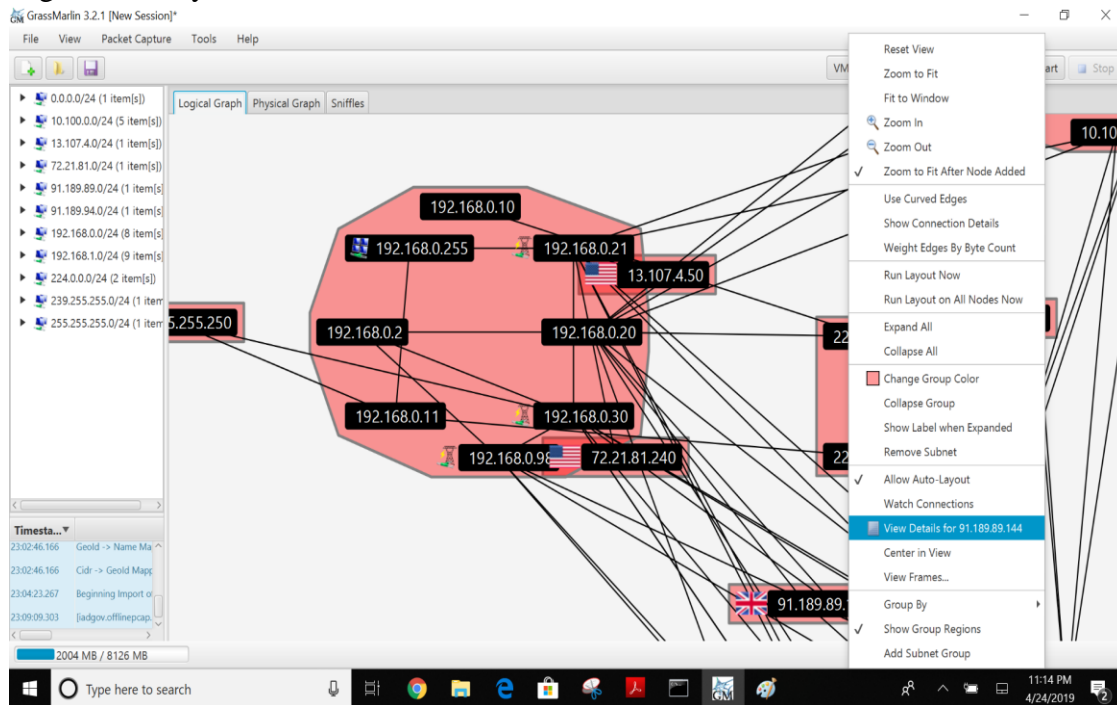


- Select the file and click on **Import Selected**. Hit the **Close** button upon completion to back to the Main interface. The Import process can take several minutes to **hours** depending on the size of the pcap file.

Upon the completion of **Import**, the main screen will display a Logical Graph of the network topology as shown below.



4. Review the logical graph. All public IP addresses will also be highlighted with their respective country’s flag. This can be useful in finding out information about any external IPs that your network is communicating with.
5. Right-click any external IP address > **View Details**.

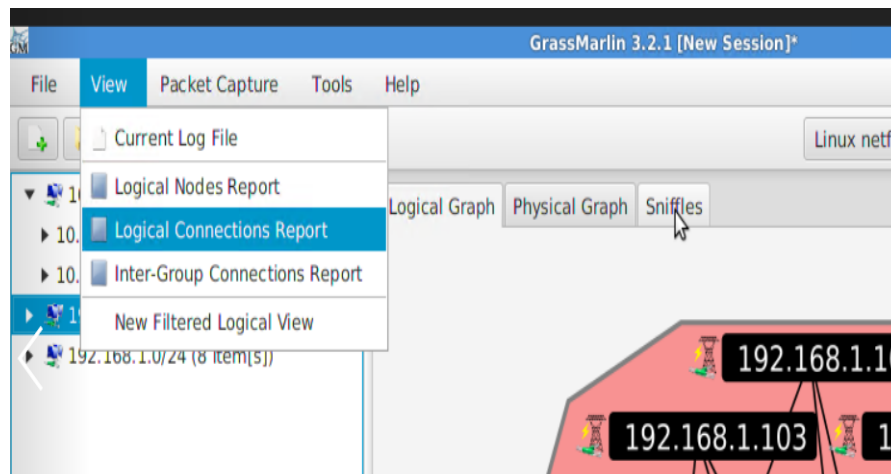


This publication is available free of charge from: <https://doi.org/10.6028/NIST.IR.8183A-3>

6. Generate a list of all nodes in the Graph as follows
 1. Click **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.
 2. Select any Property Name from the drop-down and click **Add** button to add new Columns in the Report.

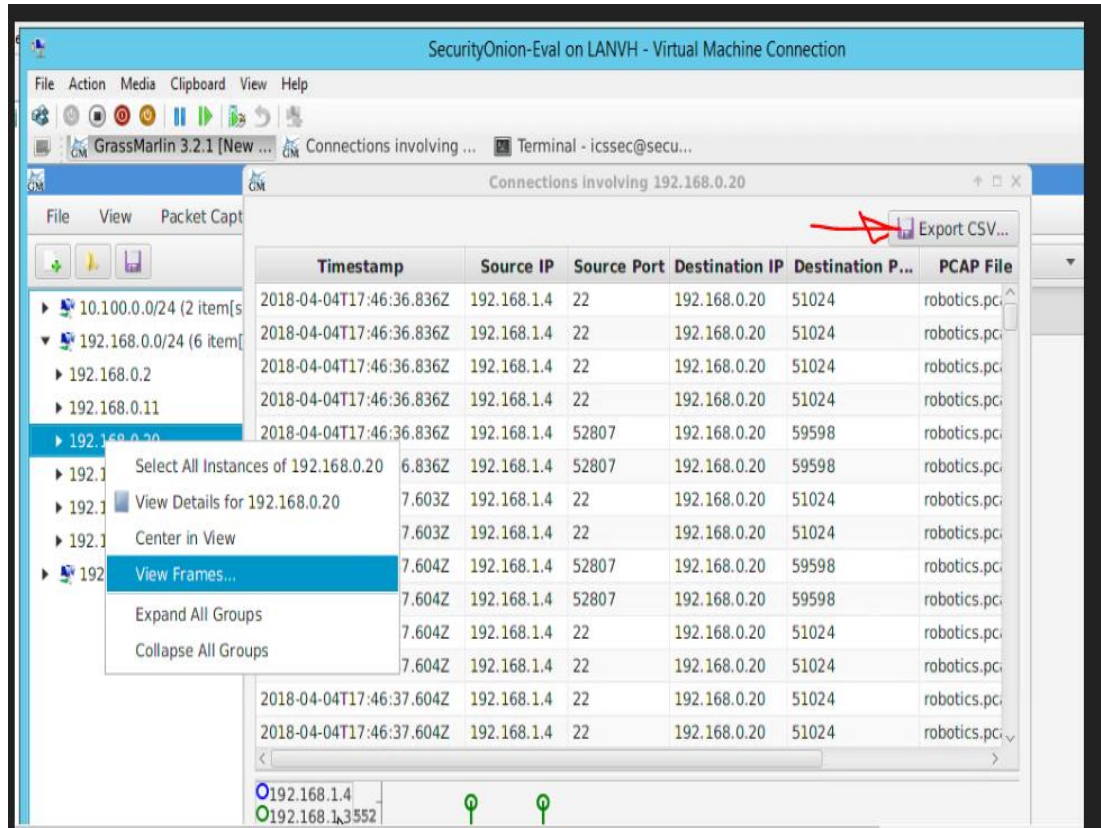
| IP | MODBUS.ICSPProtocol | MODBUS.Role |
|---------------|---------------------|-------------------------|
| 192.168.1.101 | MODBUS (4) | SLAVE (4) |
| 192.168.0.30 | MODBUS (4) | MASTER (4) SLAVE (4) |
| 192.168.1.5 | | |
| 192.168.1.4 | MODBUS (4) | MASTER (4) |
| 10.100.0.11 | | |
| 192.168.0.20 | | |
| 192.168.1.3 | MODBUS (4) | MASTER (4) |
| 192.168.1.104 | MODBUS (4) | SLAVE (4) |
| 192.168.1.102 | MODBUS (4) | SLAVE (4) |
| 192.168.0.98 | MODBUS (4) | MASTER (4) |
| 192.168.1.103 | MODBUS (4) | SLAVE (4) |
| 192.168.0.21 | MODBUS (4) | MASTER (4) |
| 192.168.0.2 | | |

7. Click on report of all connections in the pcap file as follows
 - Click **View (Top Menu)>> Logical Connections Report.**



- Click on **Export CSV** for further analysis of all the communications happening on your network.

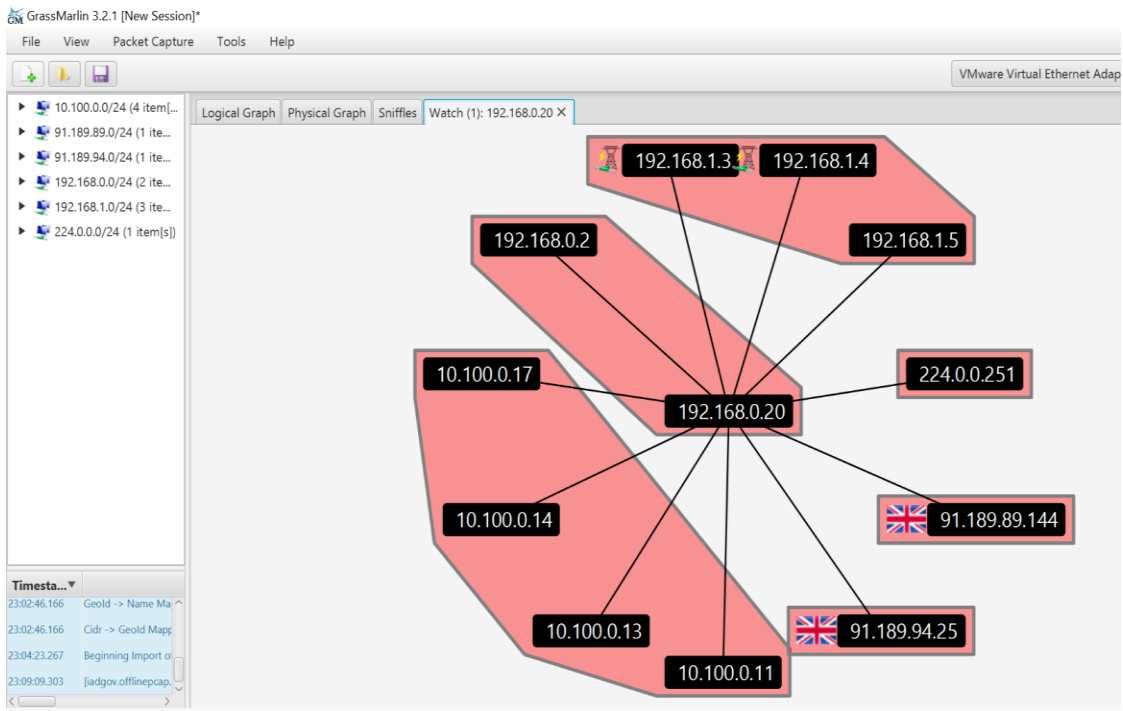
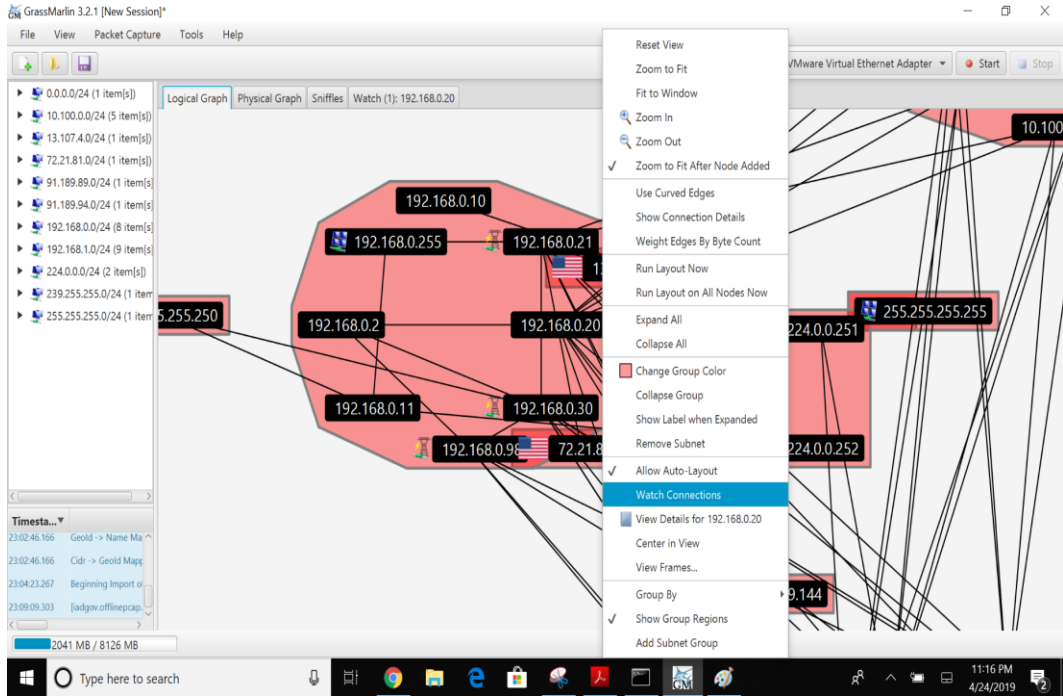
8. To view all the logical communications for a specific host for capturing a baseline,
 - a. Right-click on a **Node** > **View Frames**.
This opens a new screen as shown below displaying all the different IP addresses that particular host is communicating with including Port and Protocol information.
 - b. Click on **Export CSV** button to export this data to a csv file.
Note: This process needs to be repeated for every node.



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

9. Generate a Watch -Graph as follows,

- Right-click a **node** > Select **Watch Connections** from the **Watch- connections** menu. This will generate a graph in a new window **Watch <IP address>**



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

4.4.5.4 Additional Information

A User guide⁶¹ is available for GRASSMARLIN.

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 Links to Entire Performance Measurement Data Set

N/A

⁶¹ <https://github.com/nsacyber/GRASSMARLIN>

4.5 Wireshark

4.5.1 Technical Solution Overview

Wireshark is a free and open-source packet analyzer.

4.5.2 Technical Capabilities Provided by Solution

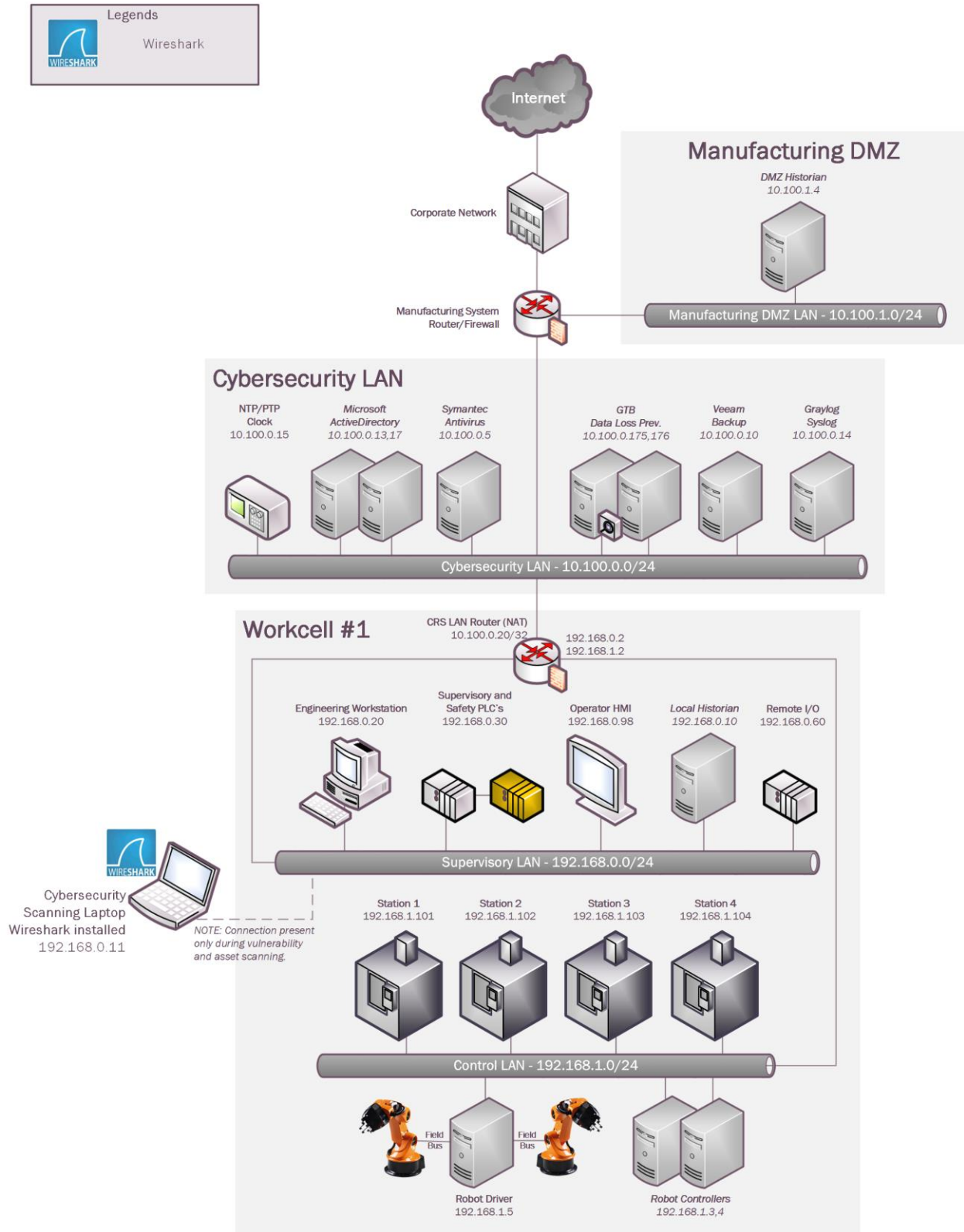
Wireshark provides components of the following Technical Capabilities described in Section 6 of Volume 1:

- 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, DE.AE-1, DE.AE-2, DE.CM-7, RS.AN-3

4.5.4 Architecture Map of Where Solution was Implemented



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

4.5.5 Installation Instructions and Configurations

Details of the solution implemented:

| Name | Version | Hardware Details |
|-----------|---------|---|
| Wireshark | 3.0.2 | Laptop with the following specs. <ul style="list-style-type: none"> • Processor: i7 • Memory: 16 GB • Disk: 256 GB • OS: Windows 7 Professional |

4.5.5.1 Environment Setup

A Windows laptop with Wireshark installed was setup on an on-demand basis.

4.5.5.2 Installation

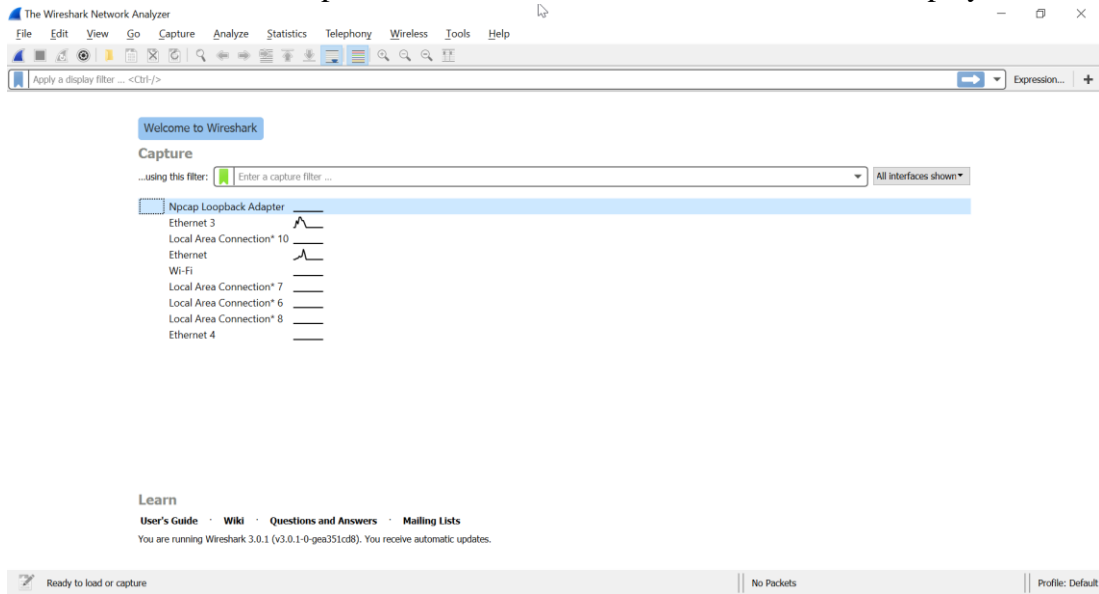
1. Download Wireshark⁶² (**Select 32bit or 64 bit**)
2. Run the exe to start install process. For instance, *Wireshark-win64-3.0.1.exe*
3. Click **Next**, leave the defaults selected and continue install.
4. Click **I Agree** to continue, when prompted for Npcap install
5. Now click **Next and Finish** to start process.
6. Select **Reboot Now** or **I want to manually reboot later**.
7. Click **Finish** to complete.

4.5.5.3 Running Wireshark

1. Launch Wireshark by doing a right-click on the Wireshark Desktop icon > **Run as Administrator (Windows 10)**. Wireshark requires administrative privileges to be fully functional, otherwise there will be undesired results.

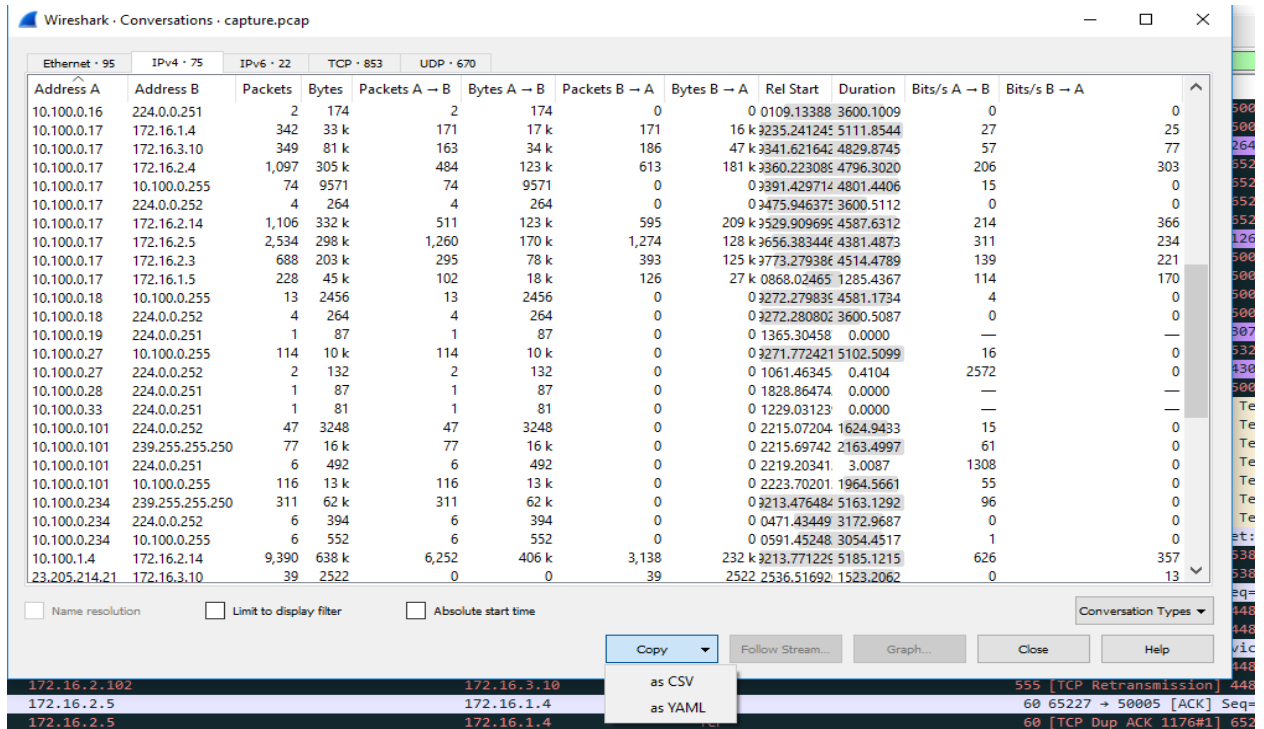
⁶² <https://www.wireshark.org>

2. Select the interface to capture traffic from, from the list of interfaces displayed



4.5.5.4 Capturing Network Baseline using Wireshark

1. Click **Open** to load a previously captured pcap file or run a **Start Capture**
2. Click on **Statistics > Conversations** upon loading the pcap or capturing live traffic.
3. Click **COPY > as Csv** to save this data as a Csv file for further analysis. Screenshot shown below for reference



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

- (Optional) Click on **Statistics > IPv4 Statistics > Destination and Ports** to get a list of all the 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.

| Topic / Item | Count | Average | Min val | Max val | Rate (ms) | Percent | Burst rate | Burst start |
|--------------|--------|---------|---------|---------|-----------|---------|------------|-------------|
| UDP | 244 | | | | 0.0000 | 100.00% | 0.0100 | 577.838 |
| 138 | 16 | | | | 0.0000 | 6.56% | 0.0100 | 577.838 |
| 137 | 228 | | | | 0.0000 | 93.44% | 0.0100 | 646.796 |
| 172.16.3.10 | 280703 | | | | 0.0195 | 17.75% | 0.4400 | 5542.363 |
| > UDP | 108 | | | | 0.0000 | 0.04% | 0.0200 | 655.814 |
| > TCP | 259177 | | | | 0.0180 | 92.33% | 0.4400 | 5542.363 |
| NONE | 21418 | | | | 0.0015 | 7.63% | 0.0600 | 718.162 |
| 0 | 21418 | | | | 0.0015 | 100.00% | 0.0600 | 718.162 |
| 172.16.2.5 | 420916 | | | | 0.0292 | 26.61% | 2.3600 | 8443.682 |
| 172.16.2.4 | 42194 | | | | 0.0029 | 2.67% | 0.7000 | 4838.174 |
| > UDP | 84 | | | | 0.0000 | 0.20% | 0.0600 | 4838.074 |
| > TCP | 6554 | | | | 0.0005 | 15.53% | 0.6700 | 4838.174 |
| 54702 | 27 | | | | 0.0000 | 0.41% | 0.2100 | 14141.953 |
| 54701 | 27 | | | | 0.0000 | 0.41% | 0.2100 | 13241.934 |
| 54700 | 42 | | | | 0.0000 | 0.64% | 0.2100 | 12821.873 |
| 54699 | 30 | | | | 0.0000 | 0.46% | 0.2100 | 12341.911 |
| 54698 | 30 | | | | 0.0000 | 0.46% | 0.2100 | 11441.890 |
| 54697 | 21 | | | | 0.0000 | 0.32% | 0.2100 | 11084.048 |
| 54696 | 21 | | | | 0.0000 | 0.32% | 0.1500 | 11084.039 |
| 54695 | 15 | | | | 0.0000 | 0.23% | 0.0900 | 11083.531 |

| Topic / Item | Count | Average | Min val | Max val | Rate (ms) | Percent | Burst rate | Burst start |
|--------------|--------|---------|---------|---------|-----------|---------|------------|-------------|
| UDP | 244 | | | | 0.0000 | 100.00% | 0.0100 | 577.838 |
| 138 | 16 | | | | 0.0000 | 6.56% | 0.0100 | 577.838 |
| 137 | 228 | | | | 0.0000 | 93.44% | 0.0100 | 646.796 |
| 172.16.3.10 | 280703 | | | | 0.0195 | 17.75% | 0.4400 | 5542.363 |
| > UDP | 108 | | | | 0.0000 | 0.04% | 0.0200 | 655.814 |
| > TCP | 259177 | | | | 0.0180 | 92.33% | 0.4400 | 5542.363 |
| NONE | 21418 | | | | 0.0015 | 7.63% | 0.0600 | 718.162 |
| 0 | 21418 | | | | 0.0015 | 100.00% | 0.0600 | 718.162 |
| 172.16.2.5 | 420916 | | | | 0.0292 | 26.61% | 2.3600 | 8443.682 |
| 172.16.2.4 | 42194 | | | | 0.0029 | 2.67% | 0.7000 | 4838.174 |
| > UDP | 84 | | | | 0.0000 | 0.20% | 0.0600 | 4838.074 |
| > TCP | 6554 | | | | 0.0005 | 15.53% | 0.6700 | 4838.174 |
| 54702 | 27 | | | | 0.0000 | 0.41% | 0.2100 | 14141.953 |
| 54701 | 27 | | | | 0.0000 | 0.41% | 0.2100 | 13241.934 |
| 54700 | 42 | | | | 0.0000 | 0.64% | 0.2100 | 12821.873 |
| 54699 | 30 | | | | 0.0000 | 0.46% | 0.2100 | 12341.911 |
| 54698 | 30 | | | | 0.0000 | 0.46% | 0.2100 | 11441.890 |
| 54697 | 21 | | | | 0.0000 | 0.32% | 0.2100 | 11084.048 |
| 54696 | 21 | | | | 0.0000 | 0.32% | 0.1500 | 11084.039 |
| 54695 | 15 | | | | 0.0000 | 0.23% | 0.0900 | 11083.531 |

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

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 Links to Entire Performance Measurement Data Set

N/A

4.6 Veeam Backup and Replication

4.6.1 Technical Solution Overview

Veeam Backup and Replication⁶³ is a proprietary backup and system 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. 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 manufacturing environments.
- Tech support available for Free edition users.
- Easy to setup and use.

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:

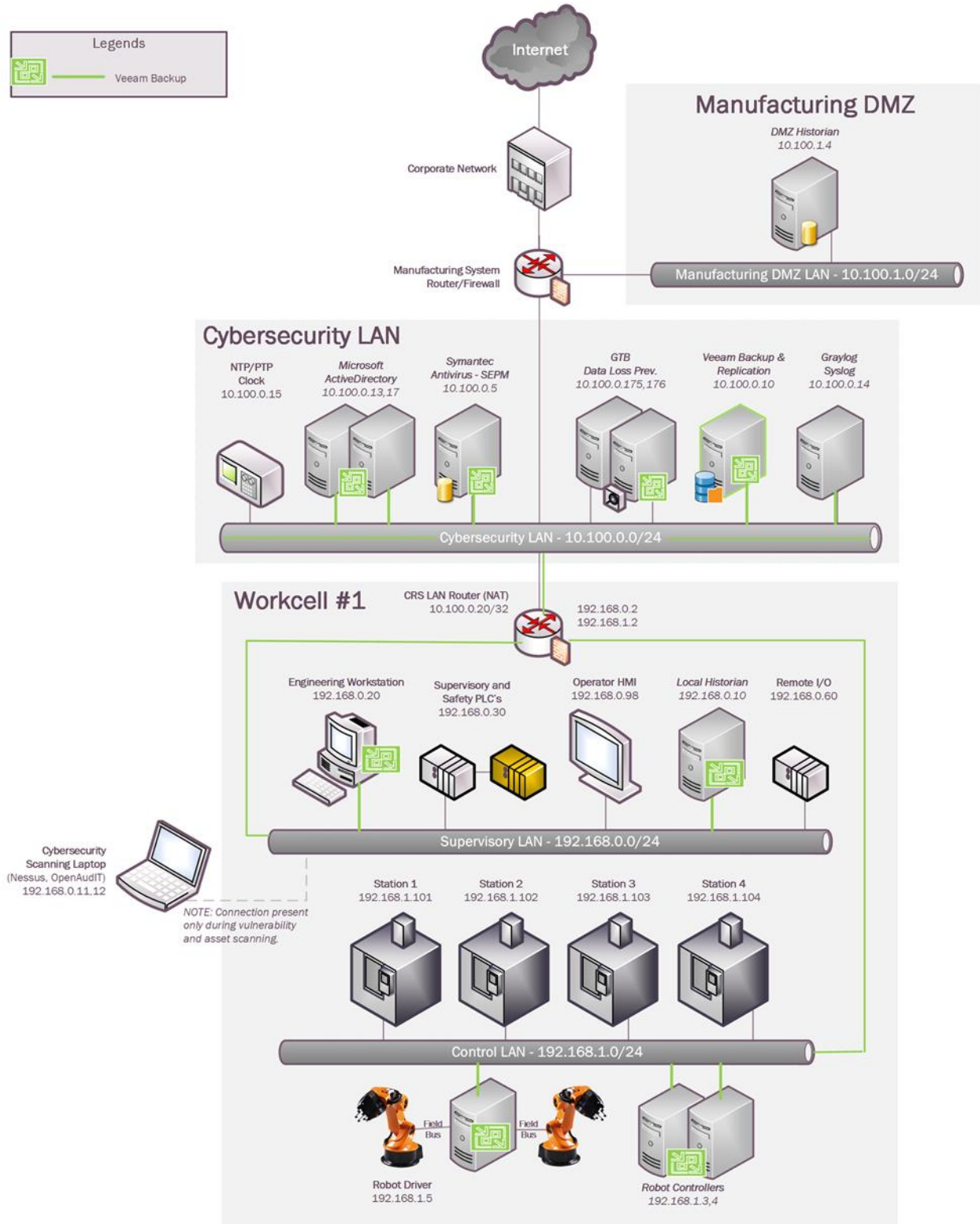
- Data Backup
- Data Replication

4.6.3 Subcategories Addressed by Implementing Solution

PR.IP-4

⁶³ <https://www.veeam.com/vm-backup-recovery-replication-software.html>

4.6.4 Architecture Map of Where Solution was Implemented



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

4.6.5 Installation Instructions and Configurations

Details of the solutions implemented:

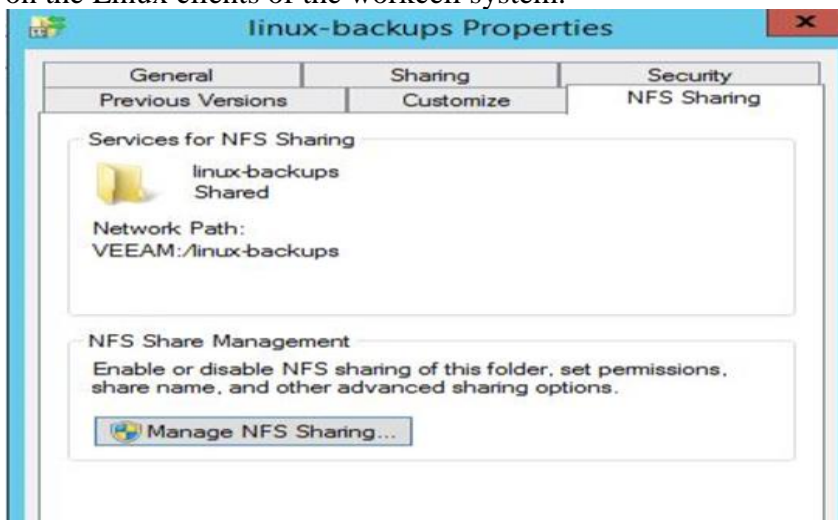
| Name | Version | Hardware Details |
|---|-----------|---|
| Veeam Backup and Replication | 9.5 | VMware Virtual Machine <ul style="list-style-type: none"> Processors: 2 virtual cores Memory: 8 GB Disk space: 4 TB. Network: 1 interface Operating System: Windows 2012R2 |
| Veeam Agent for Linux (Free version) | 3.0.0.748 | Installed on all physical Linux systems of the workcell |

4.6.5.1 Environment Setup

1. A virtual machine running Windows 2012 R2 was setup with hardware specifications as described in the table above.
2. The guest OS IP information was set as follows:

```
IP address: 10.100.0.10
Gateway: 10.100.0.1
Subnet Mask: 255.255.255.0
DNS:10.100.0.17
```

3. An NFS share folder (called **linux-backups**) as shown below was setup on the Veeam server for saving backups. Within this folder, different sub folders were created as per the hostnames of each system to be backed up. This NFS directory would then be mounted on the Linux clients of the workcell system.



4. Access to the NFS-share was regulated by allowing **read/write** access to the NAT IP address **10.100.0.20** of Work-cell network. For Security reasons, avoid selecting **Allow Root access**.

4.6.5.2 Initial Setup

1. Download **Veeam Backup & Replication**.⁶⁴
2. Install the prerequisites as mentioned in the product guide. Run the installer, follow the on-screen instructions to complete the install.⁶⁵
3. Create a network share folder on the Veeam server for storing all the backups.
4. Create a Service account in Active Directory with read/write permissions to this network share.

The Free Edition of Veeam Backup and Replication lets you manage virtual machine backups from the Central Veeam Backup and Replication Console. However, any physical servers using the Free version of Veeam agent for Linux cannot be managed from the Central console. These need to be managed locally from the client system itself.

4.6.5.3 Performing Backups

1. Download and install the Veeam agent for Linux⁶⁶ on the physical Linux systems as required. Use the **Offline Mode**⁶⁷ of agent installation for air-gapped environments (without internet access).
2. Run `sudo veeam` to launch the Veeam Control Panel utility.
The initial screen will look as shown below. Accept the **End User Agreement** and click on **Continue**.

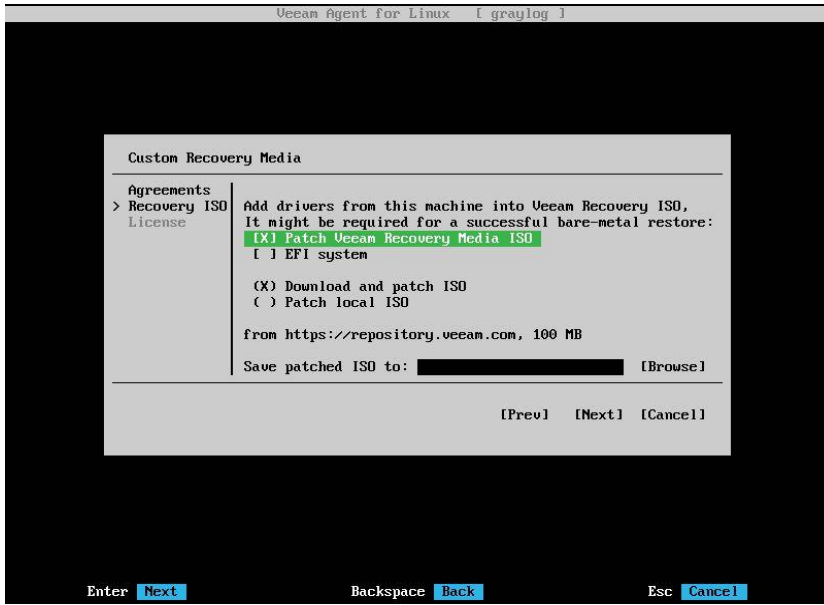
⁶⁴ <https://www.veeam.com>

⁶⁵ https://helpcenter.veeam.com/docs/backup/hyperv/install_vbr.html?ver=95u4

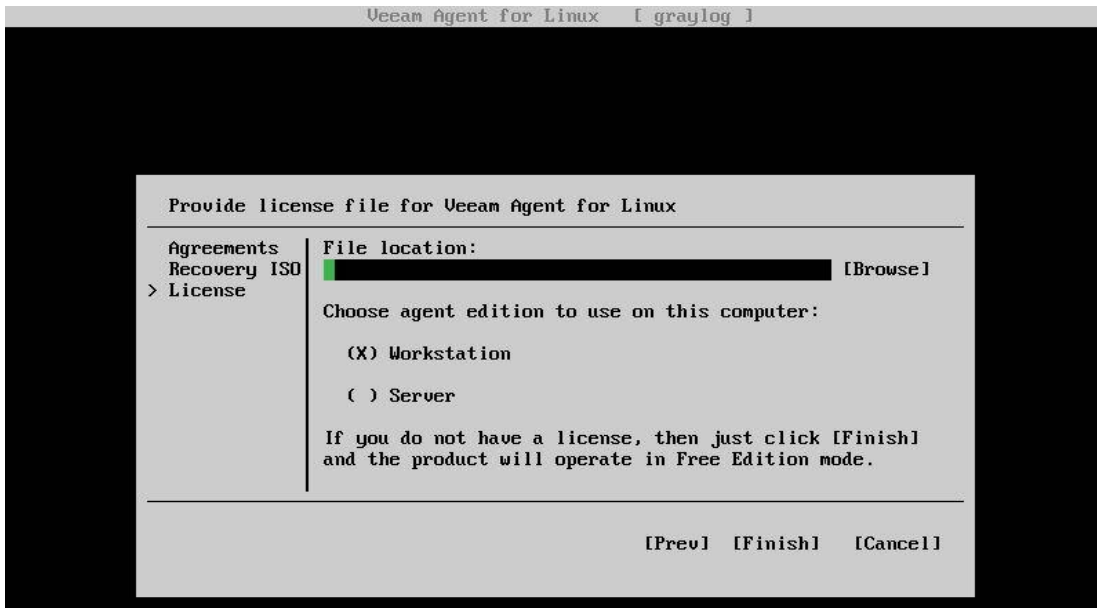
⁶⁶ <https://www.veeam.com/linux-backup-free.html>

⁶⁷ https://helpcenter.veeam.com/docs/agentforlinux/userguide/installation_offline.html?ver=30

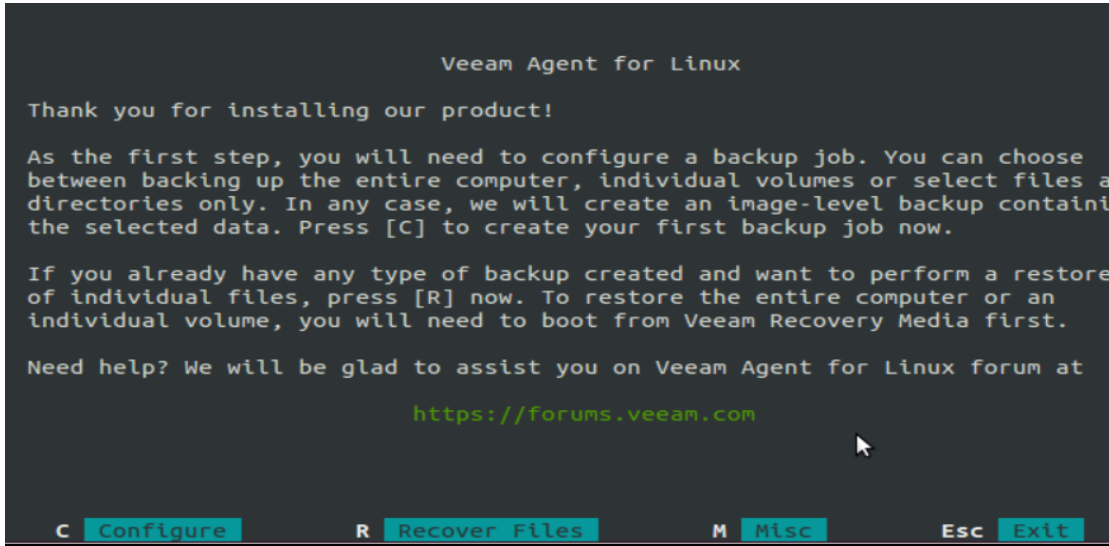
This publication is available free of charge from: <https://doi.org/10.6028/NIST.IR.8183A-3>



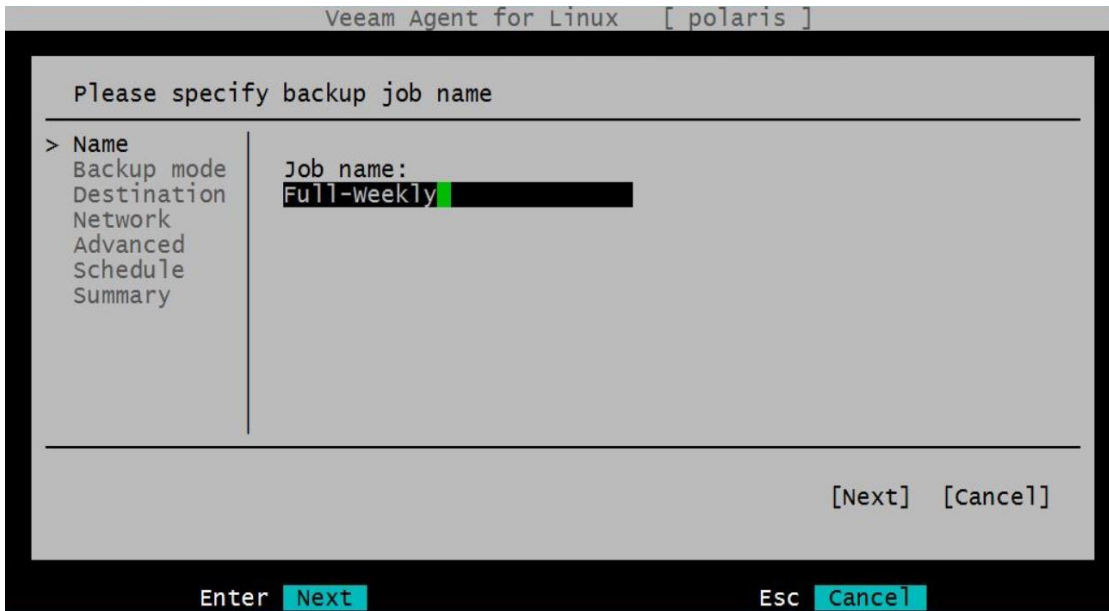
3. Select either **Patch Veeam Recovery media ISO** and/or **Download and patch ISO** if the Linux system has internet connectivity else uncheck both of these options to proceed. The Veeam Recovery Media for Linux can also be downloaded manually from the Veeam website.
4. Click **FINISH** Under License screen for Free Edition Mode



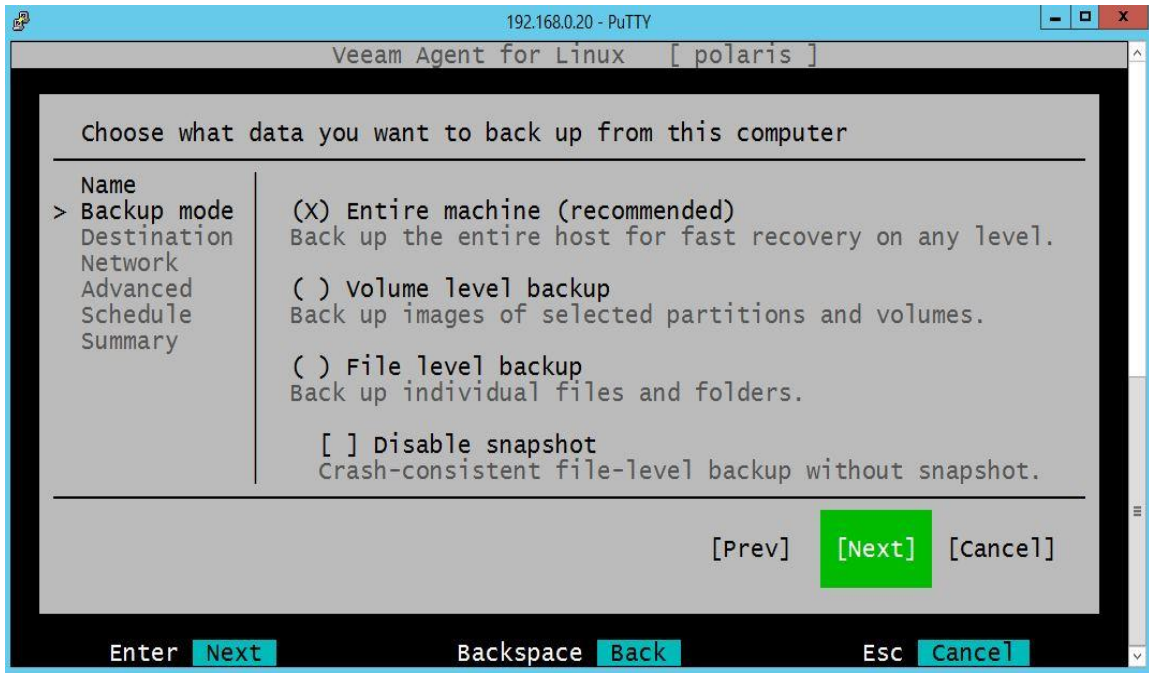
5. Press C to Configure a new backup job.



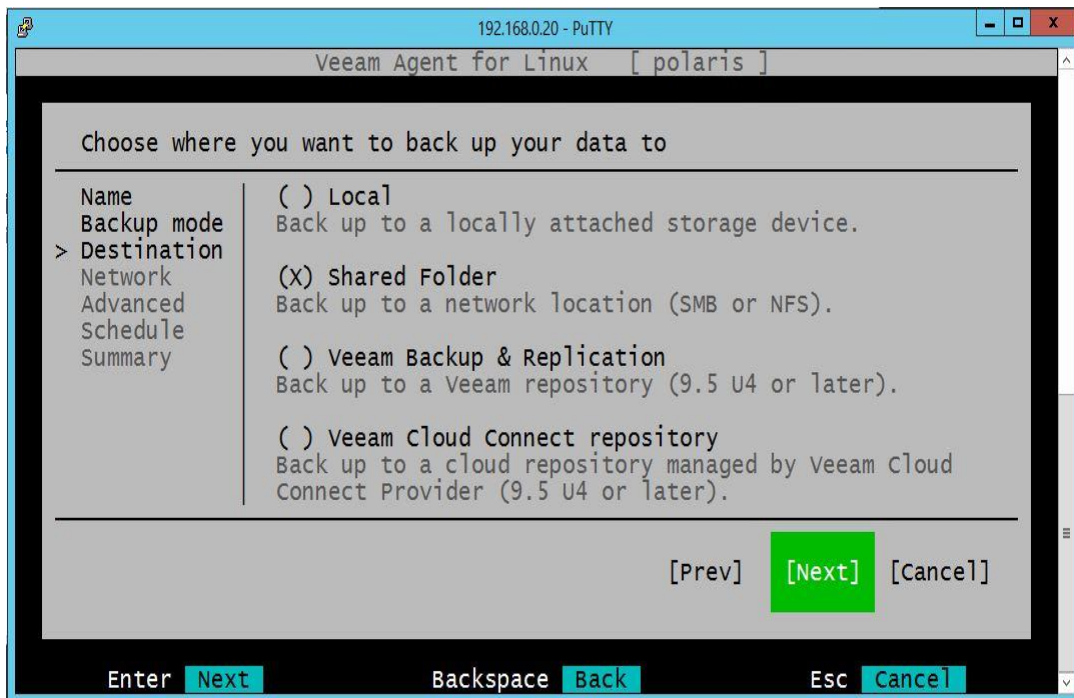
6. Enter a Job name. Click **Next**.



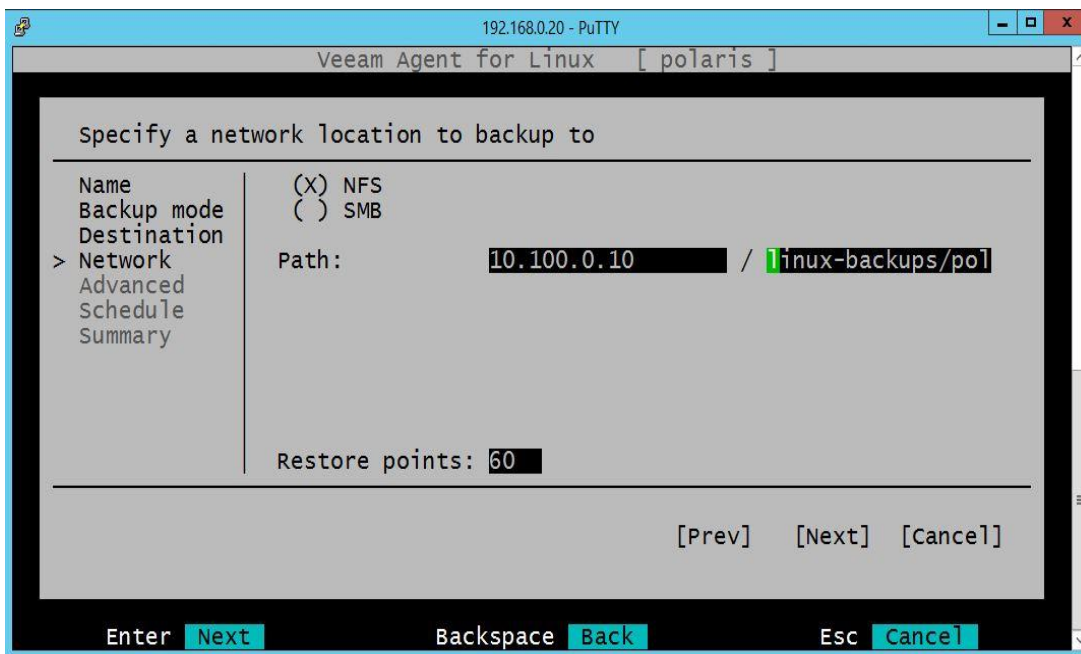
- Choose the type of backup to perform under **Backup Mode**. Click Enter.
For instance, to capture a full system image select **Entire Machine**.



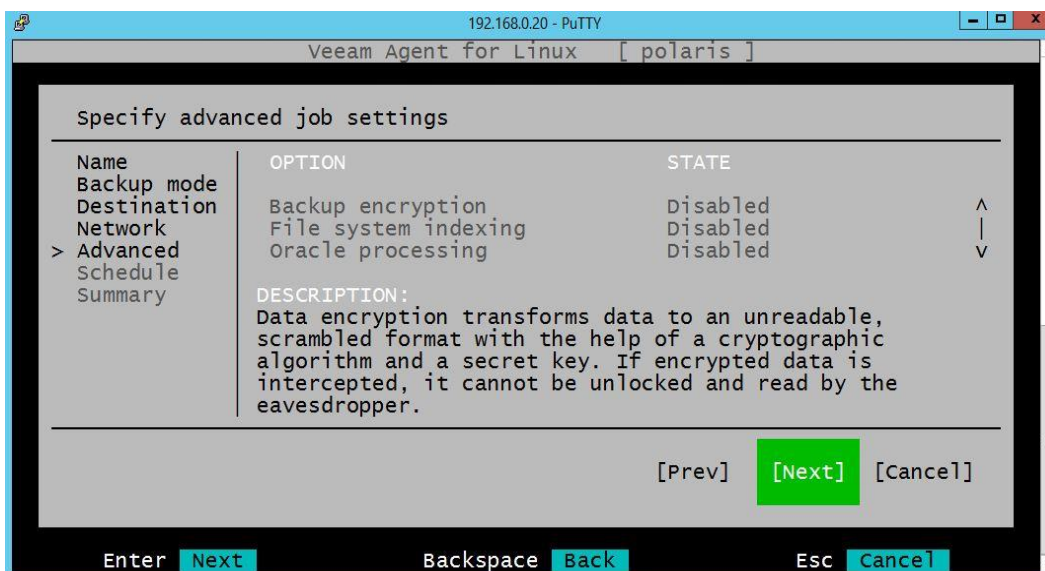
- Select **Shared Folder** under **Destination**, to enable saving backups to the NFS folder created earlier on the Veeam Storage server. The option **Local** can be used to save the backup to a directly connected external USB device.



9. Select **NFS** and enter the network path of the NFS mount setup earlier



10. Enable other options as required under **Advanced** screen. For security purposes, enable **Backup Encryption**



11. Configure a schedule under **Schedule screen** or select **Run the job automatically** option to run a onetime manual backup.
12. Verify the settings on the Summary Screen. Click Next to kick off the job. Click **FINISH** when done.

4.6.5.4 Performing Recovery

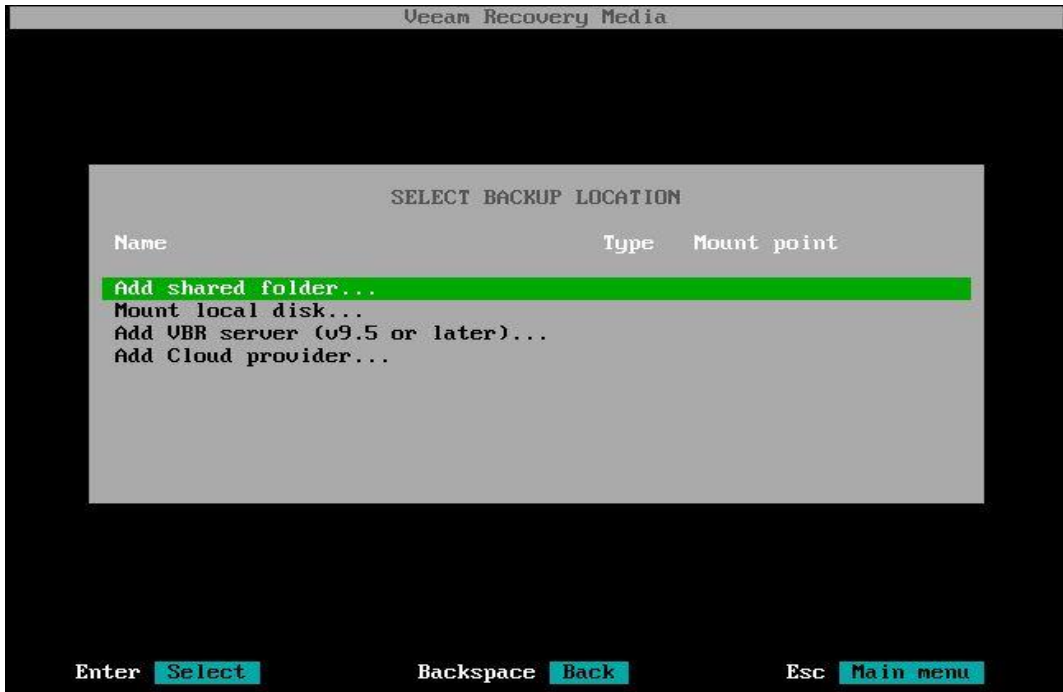
A Restore operation can only be initiated from the client (if using Free edition) and requires the Veeam Recovery Media.

1. Download the Veeam Recovery Media⁶⁸ (if not already) and burn it to a bootable USB. Boot the server off it.
2. Accept the License at the initial screen. Click **Continue**.
3. Click **Configure Network** (if performing a restore from a network drive). 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
4. Click **Restore Volumes** to restore backup type of **Entire Computer**.



⁶⁸ <https://www.veeam.com/linux-backup-free.html>

- 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**.

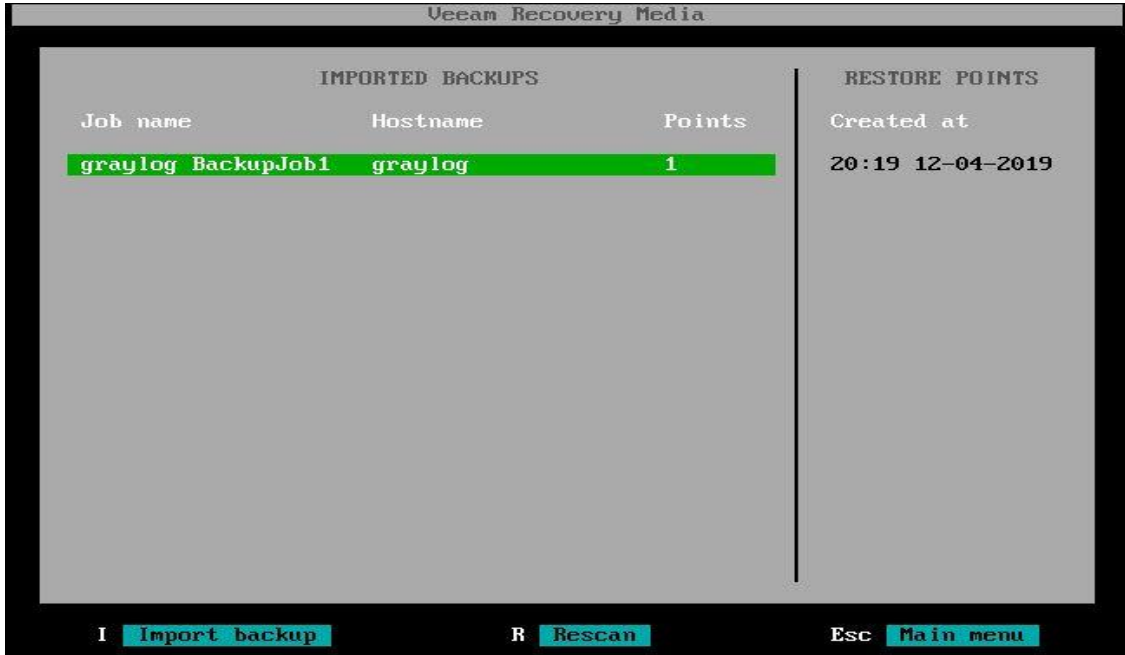


- Configure the Network Path of the backup target as required. Below image shows the Path set to connect to Veeam backup server using NFS.

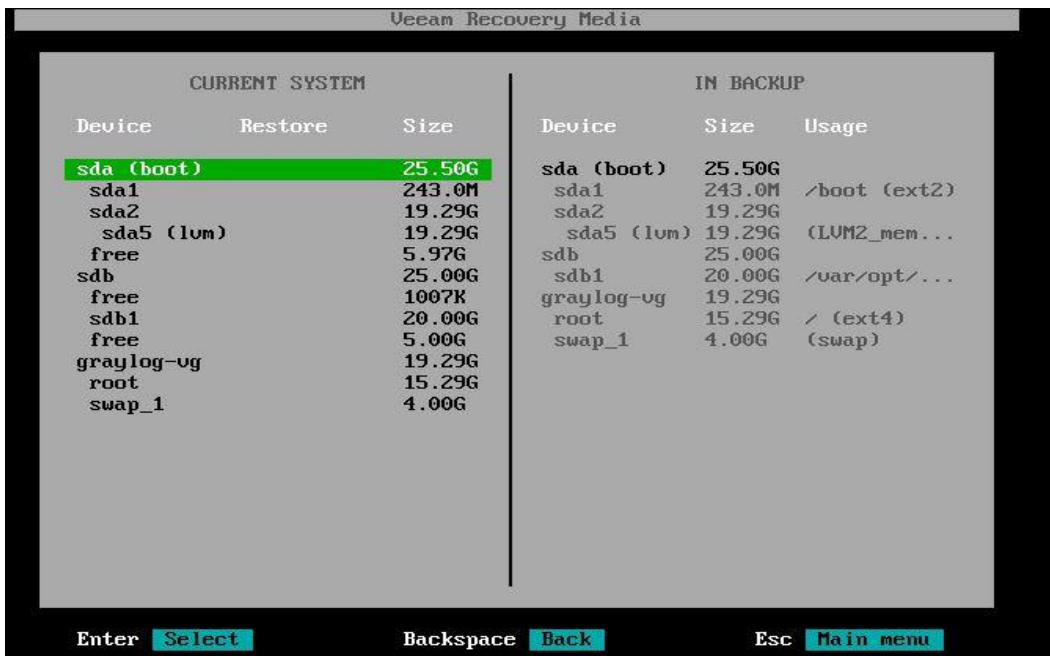


7. Select a **Restore Point** under **Imported Backups** screen from the Right. Click **I** for **Import Backup**

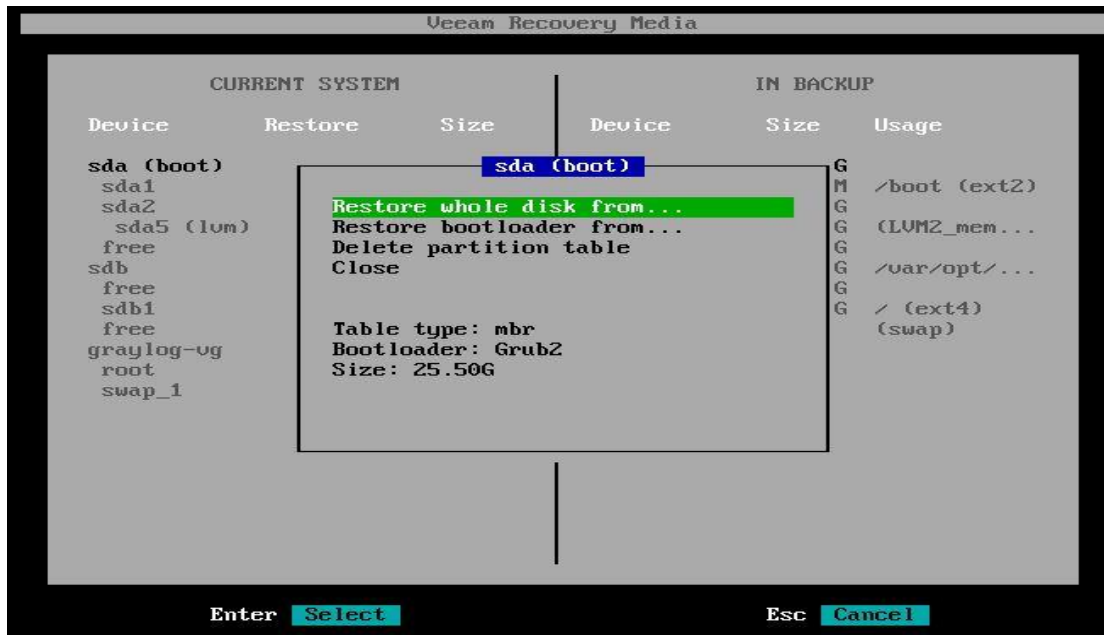
Note: The screen will auto populate Restore points based off the backup jobs saved previously.



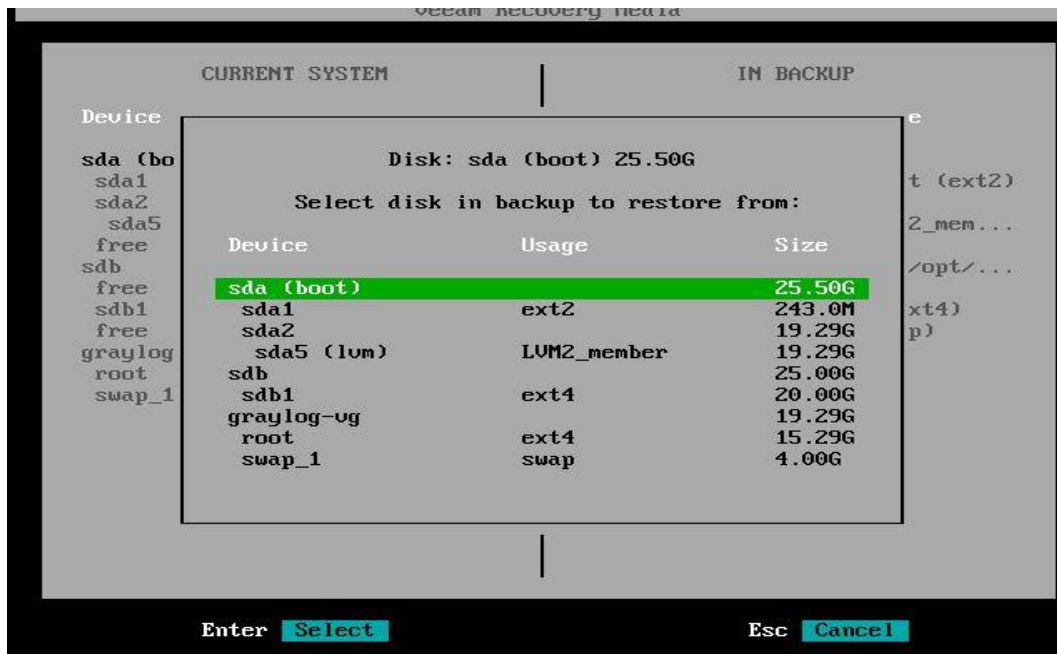
8. Select the Appropriate volume/disk to Restore and hit **Enter**. This will confirm your selection. This screen displays a comparison of the filesystem layout that's currently on the Linux server versus to what it currently has on that Backup Restore point.



9. Select the “Restore Whole Disk from” if restoring an Entire Volume / System Image or other options as shown in the list. Basically, this is telling the system to restore the image of /sda volume to the local /sda that’s currently only the system.



10. Choose the disk from backup to restore from. Select the appropriate disk and hit Enter.



11. Hit S to Start the restore.

| CURRENT SYSTEM | | | IN BACKUP | | |
|----------------|--------------|--------|------------|--------|--------------|
| Device | Restore | Size | Device | Size | Usage |
| sda (boot) | loader (sda) | 25.50G | sda (boot) | 25.50G | |
| sda1 | sda1 (/boot) | 243.0M | sda1 | 243.0M | /boot (ext2) |
| sda2 | | 19.29G | sda2 | 19.29G | |
| sda5 (lum) | | 19.29G | sda5 (lum) | 19.29G | (LUM2_mem... |
| free | | 5.97G | sdb | 25.00G | |
| sdb | | 25.00G | sdb1 | 20.00G | /var/opt/... |
| free | | 1007K | graylog-vg | 19.29G | |
| sdb1 | | 20.00G | root | 15.29G | / (ext4) |
| free | | 5.00G | swap_1 | 4.00G | (swap) |
| graylog-vg | | 19.29G | | | |
| root | root (/) | 15.29G | | | |
| swap_1 | swap_1 (s... | 4.00G | | | |

Enter **Select** S **Start restore** Backspace **Back** Esc **Main menu**

12. Review the Recovery Summary screen. Hit Enter to start the Recovery.

13. Eject the Veeam Recovery Media once restore completes and Reboot the server.

4.6.5.5 Changing Backup Job Type

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.

1. Run the commands below 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 >
```

2. Run `sudo veeam` to launch the Veeam Config Menu Once deleted. Hit **C for Configure** to create a new job.

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.

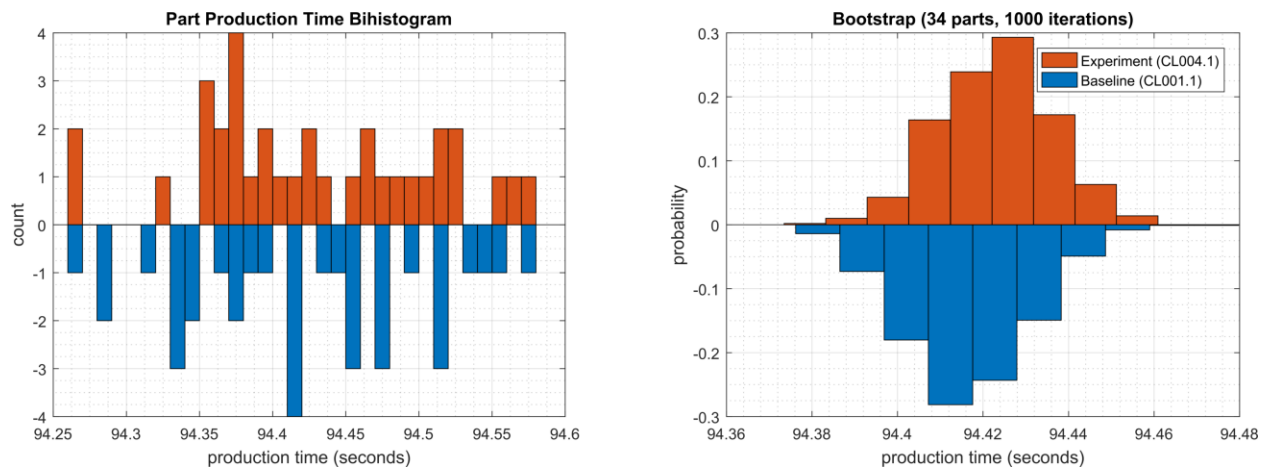


Figure 4-10 - Bihistograms showing the part production time (left) and estimated mean production time using the bootstrap method (right) using the measurements from baseline CL001.1 and experiment CL004.1.

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.

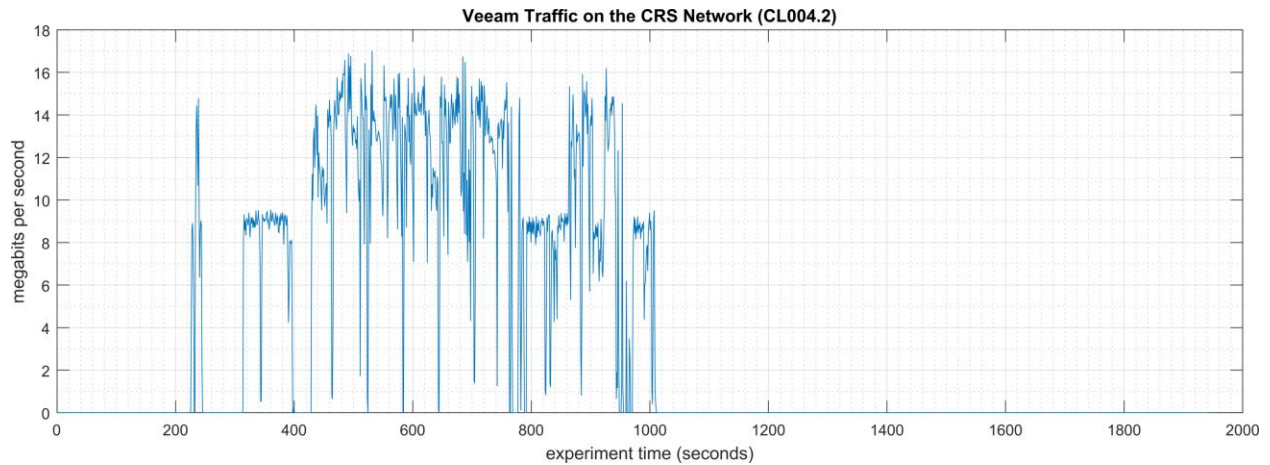


Figure 4-11 - Time series plot showing the rate of network traffic (in megabits per second) transmitted and received by the Veeam tool during the CL004.2 experiment. Network traffic transmitted and received by the vControllers are not shown in this plot.

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.

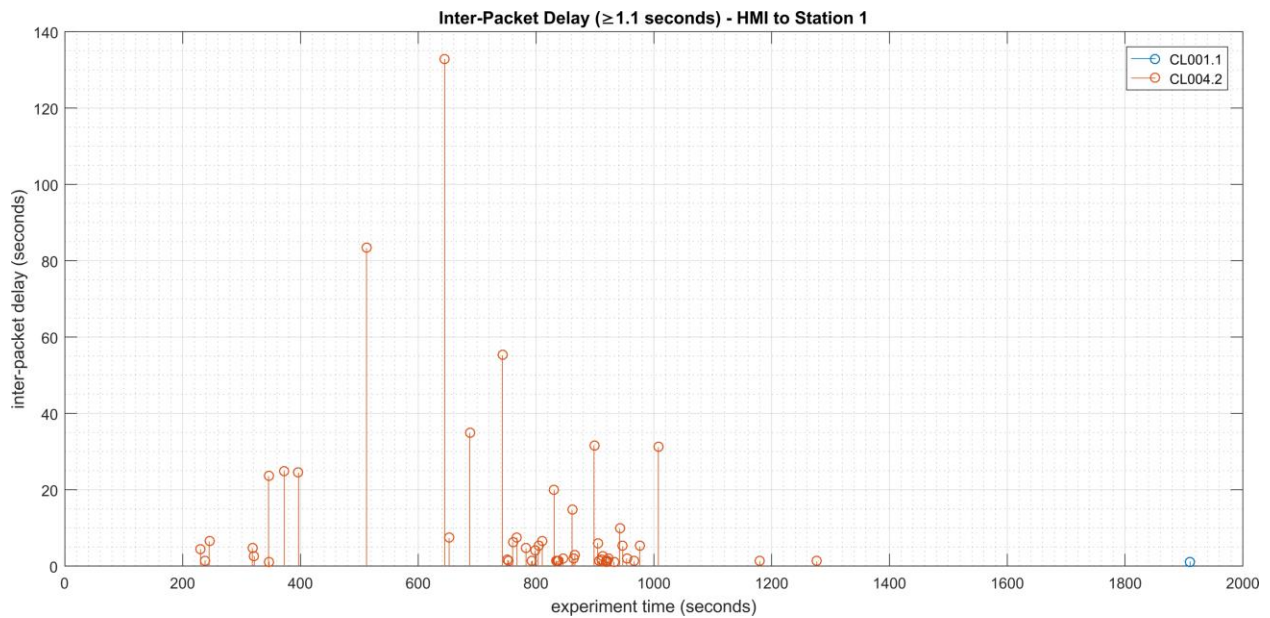


Figure 4-12 - Stem plot displaying the inter-packet delays (greater than or equal to 1.10 seconds) of Modbus TCP traffic between the HMI and Station 1, as measured during the baseline CL001.2 and experiment CL004.2. Note the large inter-packet delays measured between experiment time 400 to 1000 sec., 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.

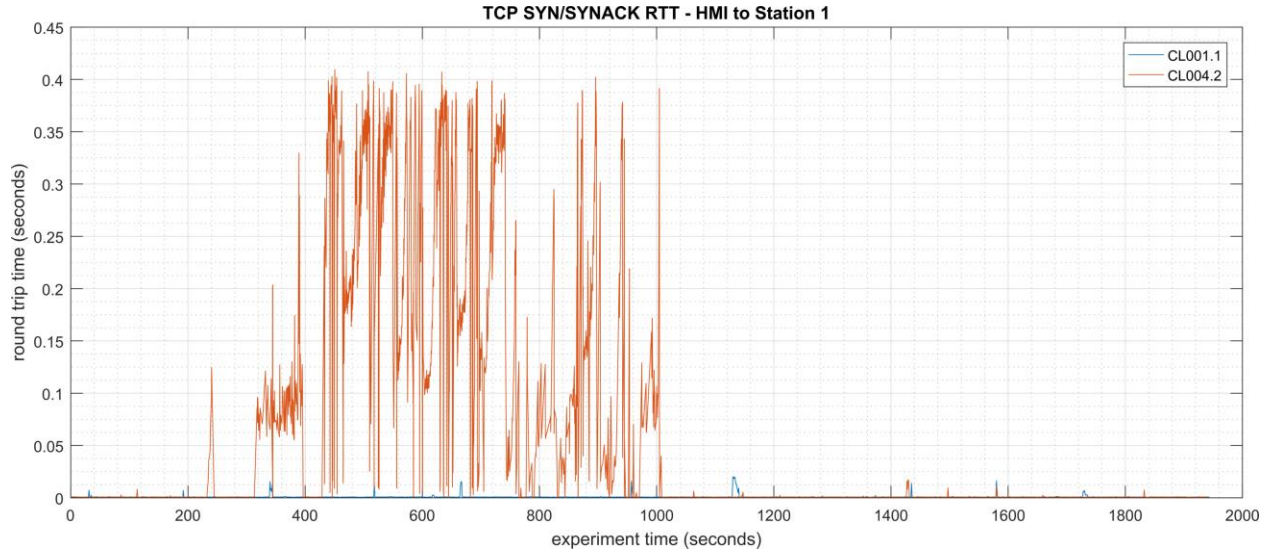


Figure 4-13 - Time-series plot showing the measured round-trip time of SYN and SYN-ACK packets sent between the HMI and Station 1 during the experiment. Large round-trip times (>350 msec.) occurred regularly from 400 seconds to 1000 seconds (experiment time).

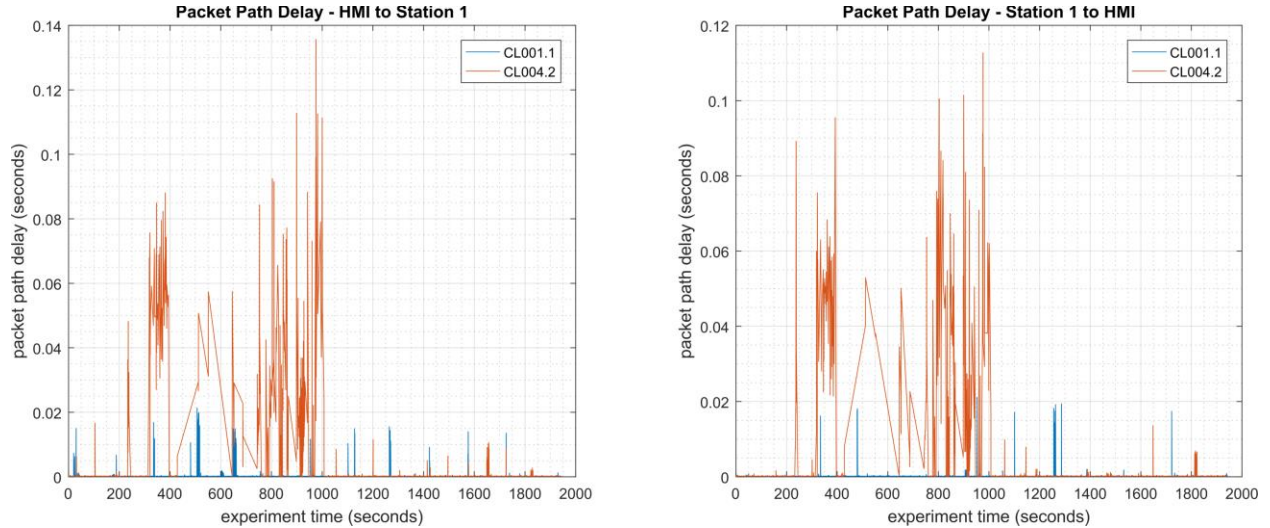


Figure 4-14 - Time-series plots showing the measured packet path delay Modbus TCP packets sent from the HMI to Station 1 (left) and sent from Station 1 to the HMI (right) during the experiment.

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.

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

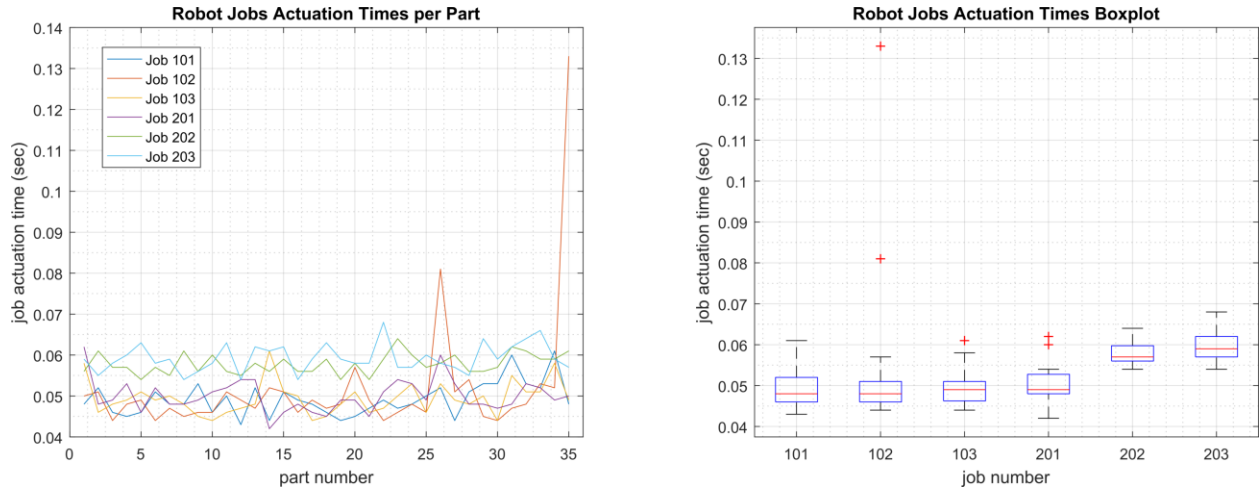


Figure 4-15 - Time-series (left) and boxplot (right) showing the job actuation times for each job during the CL004.2 experiment. Note the two increased actuation times for job 102, which occurred while the Veeam tool was imaging the vControllers.

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

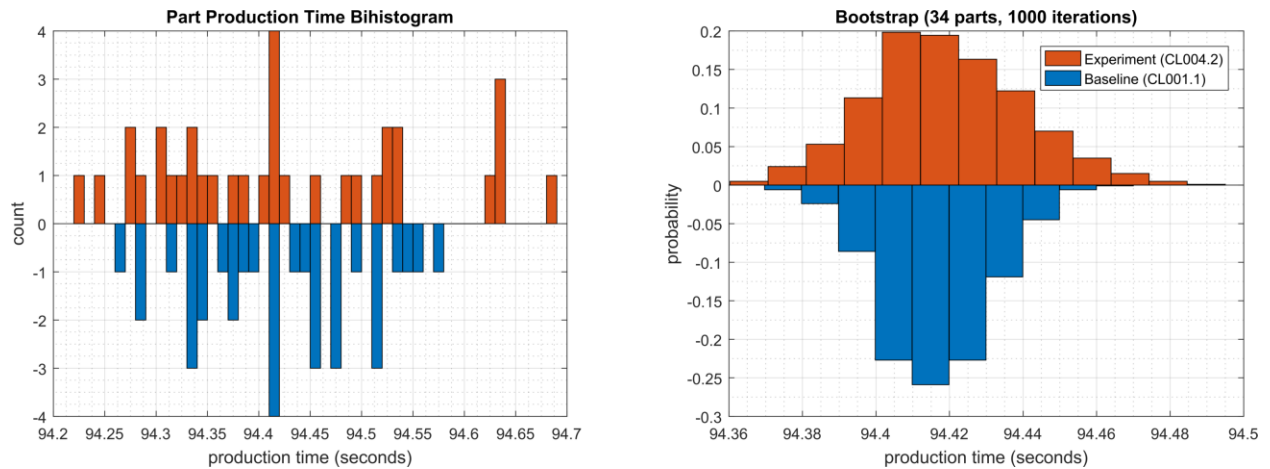


Figure 4-16 - Bihistograms showing the part production time (left) and estimated mean production time using the bootstrap method (right) using the measurements from baseline CL001.1 and experiment CL004.2.

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.

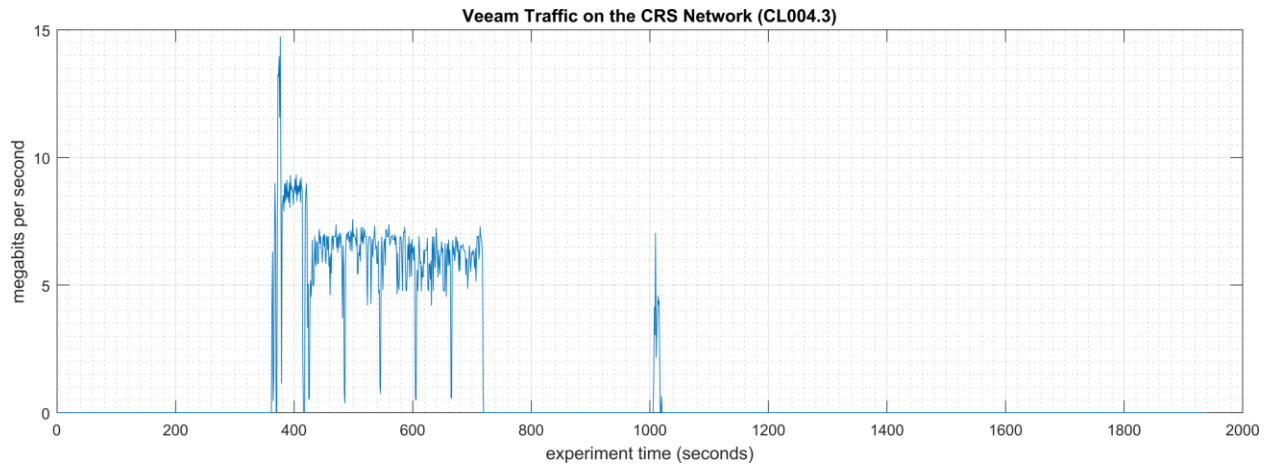


Figure 4-17 - Time series plot showing the rate of network traffic (in megabits per second) transmitted and received by the Veeam tool during the CL004.3 experiment.

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.

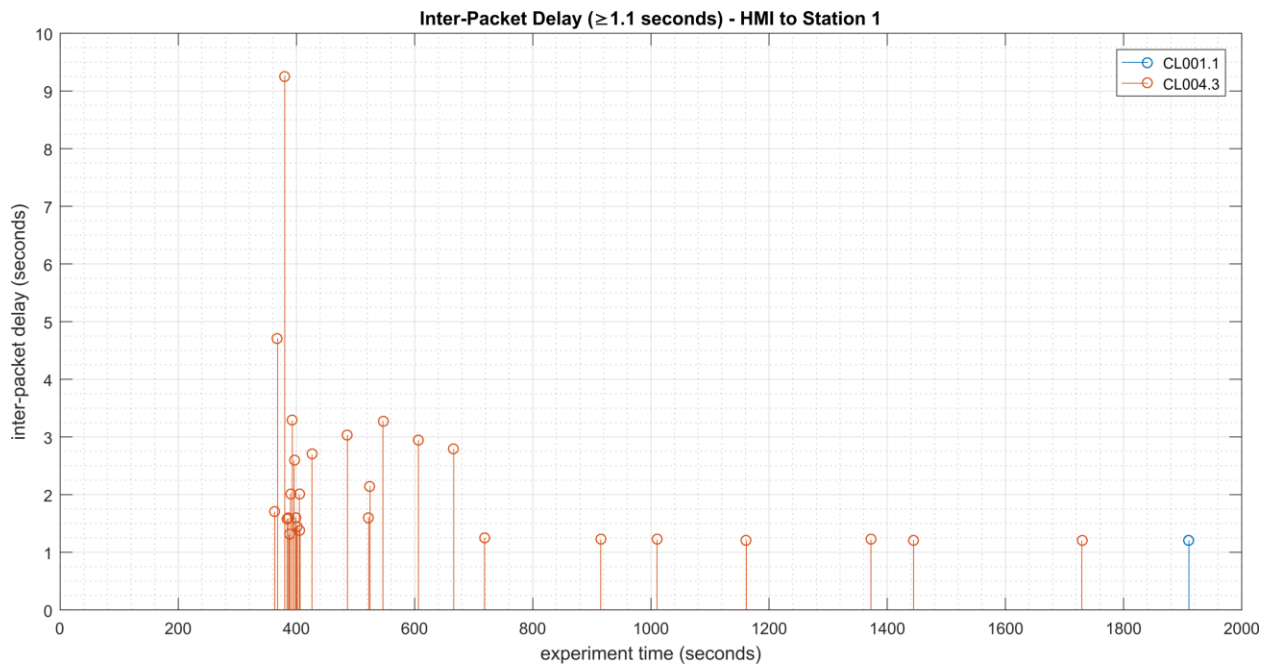


Figure 4-18 - Stem plot showing the inter-packet delays (greater than or equal to 1.10 seconds) of Modbus TCP traffic between the HMI and Station 1, as measured during the baseline CL001.2 and experiment CL004.3. Note the large inter-packet delays measured between experiment time 370 to 700 sec., resulting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

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

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.

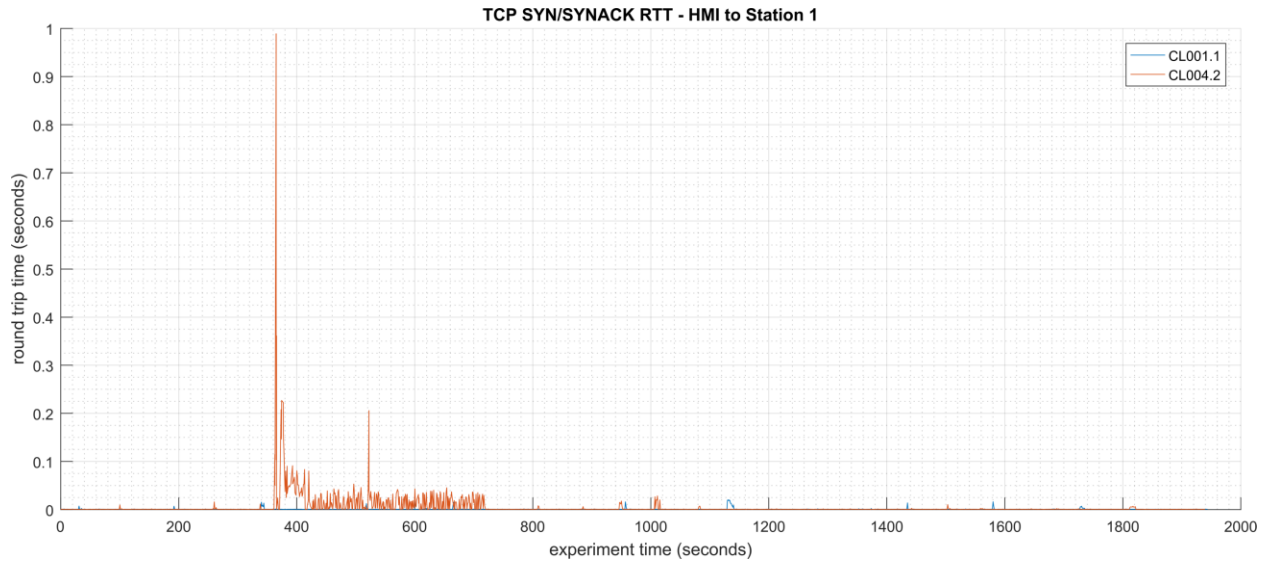


Figure 4-19 - Time-series plot showing the measured round-trip time of SYN and SYN-ACK packets sent between the HMI and Station 1 during the experiment.

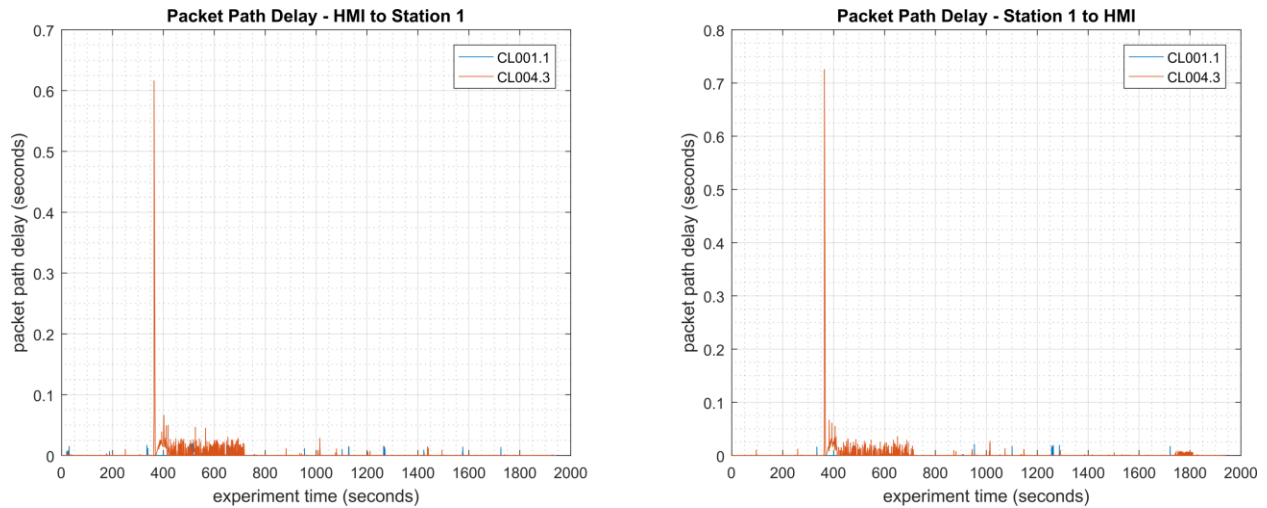


Figure 4-20 - Time-series plots showing the measured packet path delay Modbus TCP packets sent from the HMI to Station 1 (left) and sent from Station 1 to the HMI (right) during the experiment. Note the large path delay of over 600 msec. around 350 sec., followed by consistent delays of around 20 msec.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

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

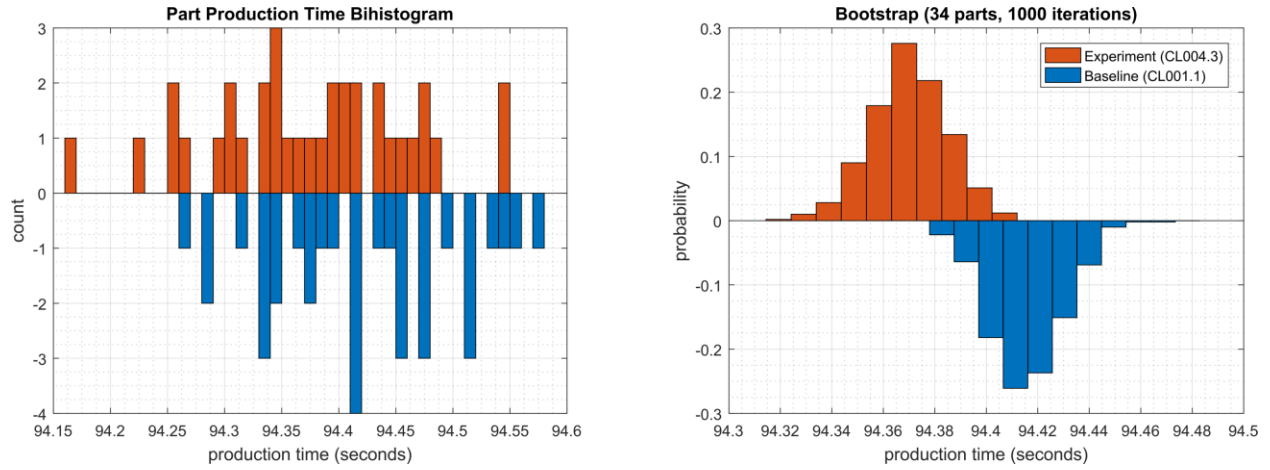


Figure 4-21 - Bihistograms showing the part production time (left) and estimated mean production time using the bootstrap method (right) using the measurements from baseline CL001.1 and experiment CL004.3.

4.6.7 Links 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

TeamViewer⁶⁹ is a remote desktop sharing tool that provides secure remote access.

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

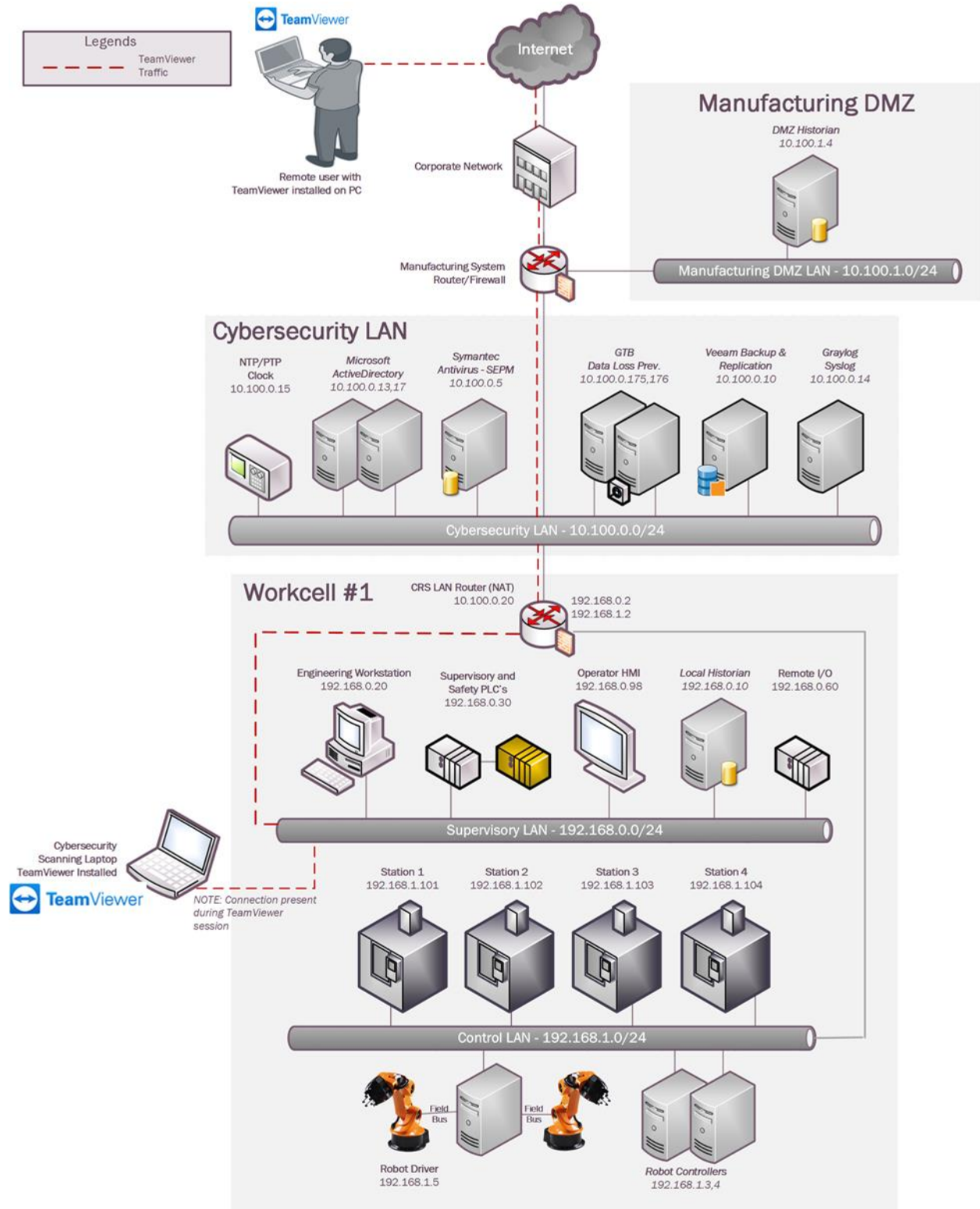
Secure Remote Access

4.7.3 Subcategories Addressed by Implementing Solution

PR.AC-5, PR.MA-2

⁶⁹ <https://www.teamviewer.com>

4.7.4 Architecture Map of Where Solution was Implemented



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

4.7.5 Installation Instructions and Configurations

Details of the solution implemented:

| Name | Version | Hardware Details |
|-------------------|---------|---|
| TeamViewer | 14 | Laptop with the following specs. <ul style="list-style-type: none"> • Processor: i7 • Memory: 16 GB • Disk: 256 GB • OS: Windows 7 Professional |

4.7.5.1 Environment setup

1. A temporary laptop (referred as Cybersecurity scanning laptop) with TeamViewer installed and was setup on an on-demand basis. The scanning laptop had internet access via wireless along with a connection to the Work-cell by connecting a physical network connection to the Layer-2 switch of the Supervisory LAN network.
2. The guest OS IP information of this system was set as follows:

IP address: 192.168.0.11
 Gateway: 192.168.0.2
 Subnet Mask: 255.255.255.0
 DNS:10.100.0.17

3. To complete a connection, the remote user needs to have TeamViewer installed on his/her computer too. The Cybersecurity scanning laptop was used a jump box for installing TeamViewer and connecting remotely to the work-cell network within.

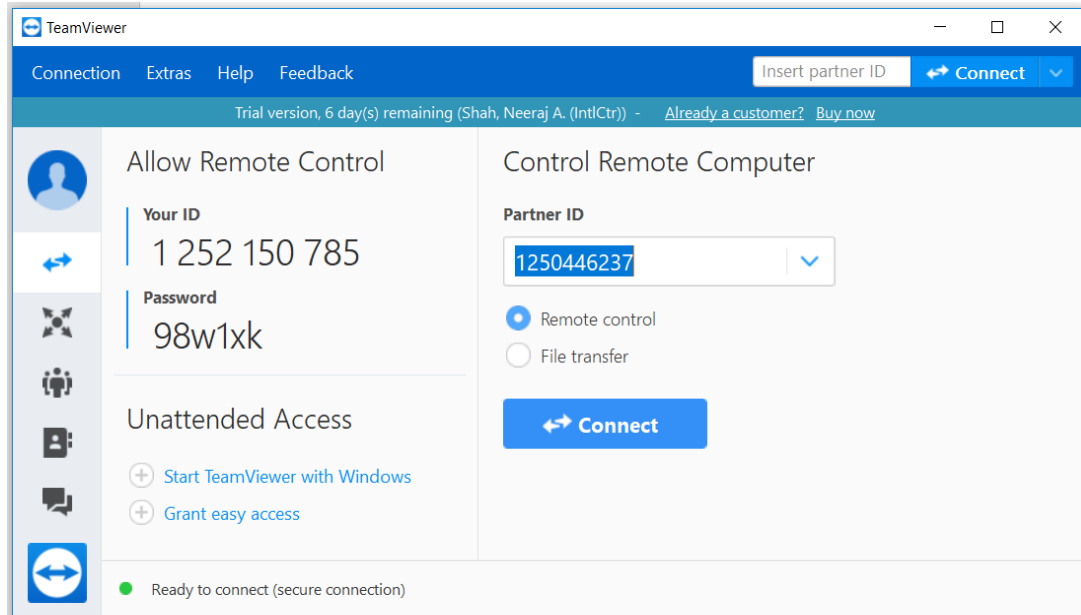
4.7.5.2 Setup Instructions

- Download TeamViewer⁷⁰ on a supported OS computer.
- Run the installer (.msi for Windows) to complete the installation. Ensure to have internet access on this computer.
- Repeat steps 1 and 2 on the remote user's computer as well.

⁷⁰ <https://www.teamviewer.com/>

4.7.5.3 Using TeamViewer

1. Perform the following steps on the on-premise system acting as the Jump box.
 - a. Launch TeamViewer. Note down the ID and password displayed on the screen. For example

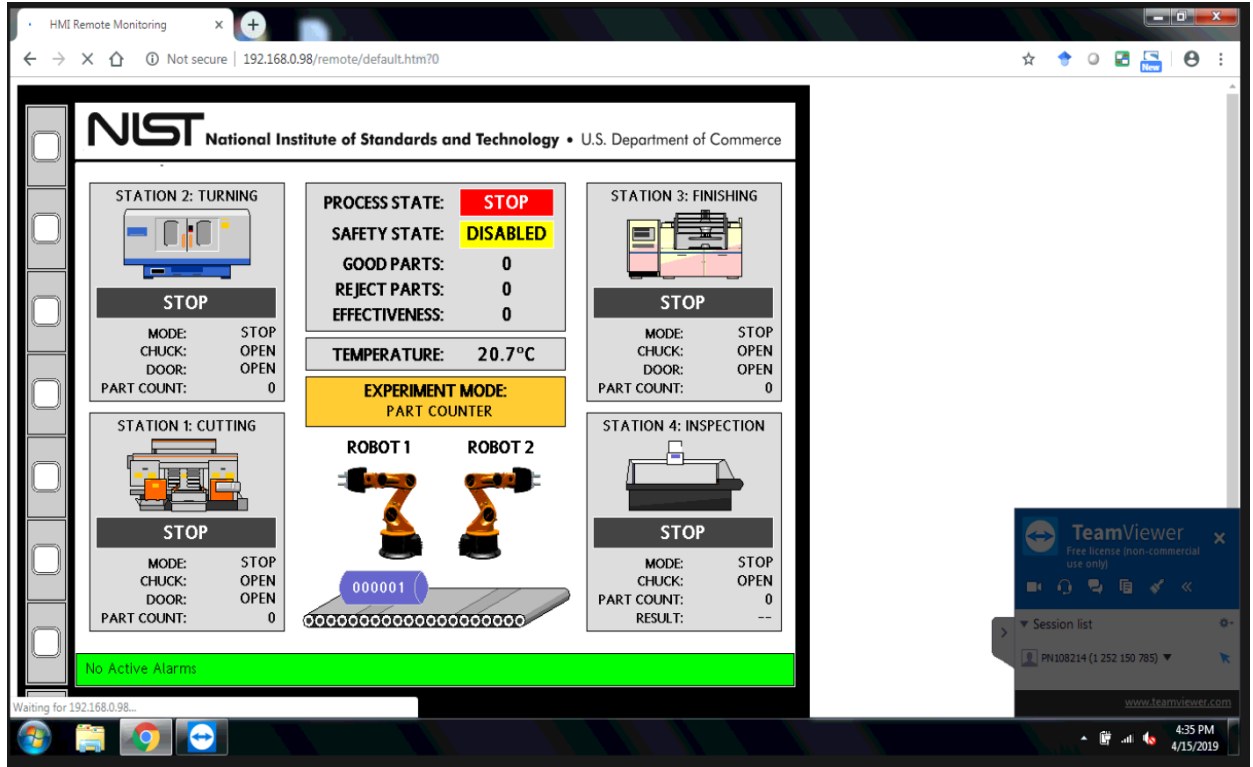


2. Convey this information (ID and password) to the remote user.
3. Perform the following actions on the remote user's computer:
 - Enter the ID provided in the **Partner ID** box.
 - Select **Remote Control**.
 - Click **Connect** button to initiate a session.
 - Enter password as prompted.

Two factor authentication⁷¹ was configured for this connection.

Once the connection is established, the remote user should be able to access the Desktop of the Destination system. For instance, in our case the HMI Panel was accessed off a browser on the Cybersecurity Scanning laptop to perform maintenance on the HMI.

⁷¹ <https://community.teamviewer.com/t5/Knowledge-Base/Two-factor-authentication-Activation-and-Deactivation/ta-p/66>



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 Links 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. 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.⁷²

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:

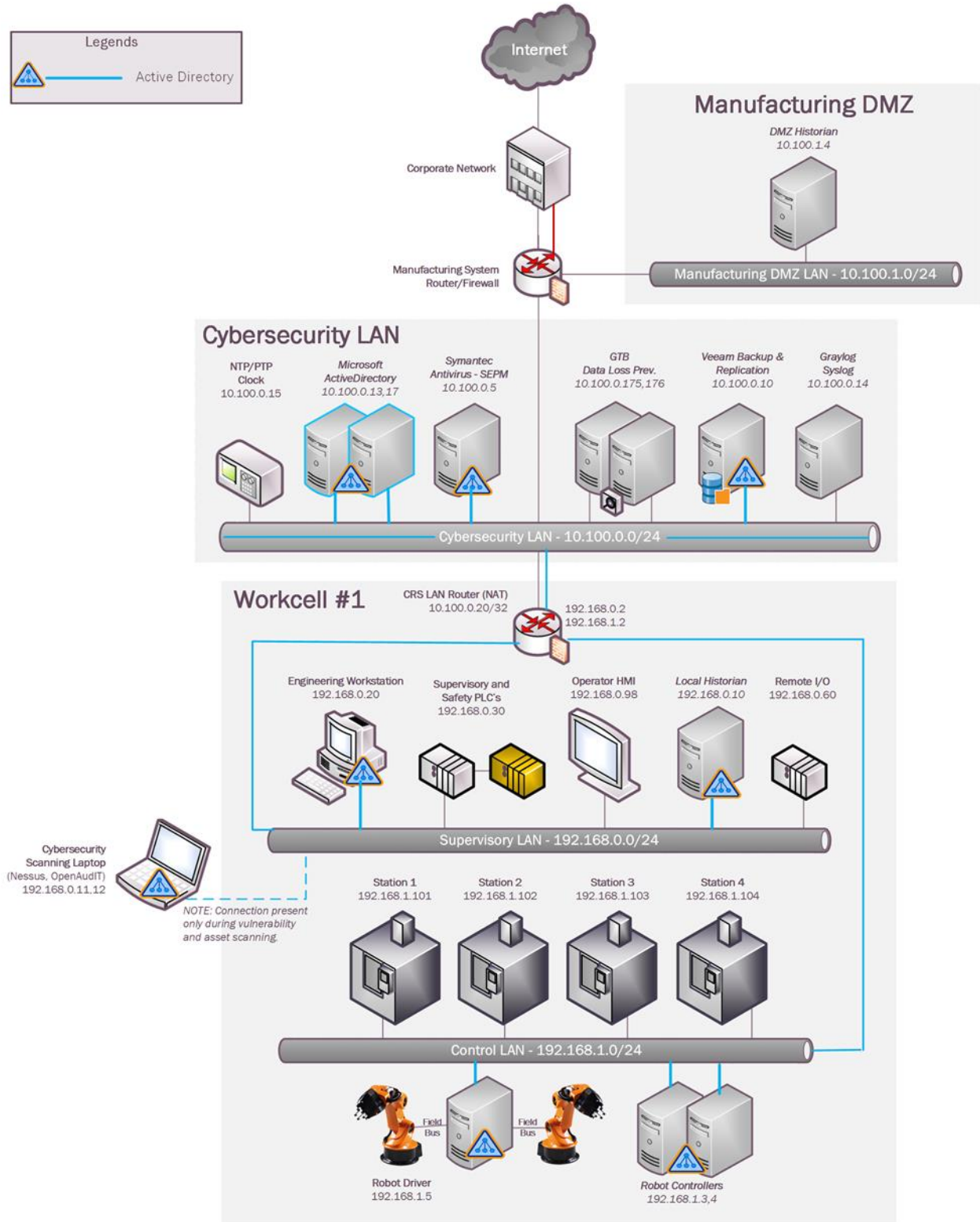
- Credential Management
- Authentication and Authorization

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

⁷² <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



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

4.8.5 Installation Instructions and Configurations

Details of the environment:

| Hostname | Roles | Domain Name | Hardware Details |
|-----------------|------------------------------|-------------|---|
| LAN-AD | Active Directory, DNS Server | LAN.lab | Hyper-V Virtual Machine (Generation 2): <ul style="list-style-type: none"> Processors: 2 virtual cores Memory: 6 GB Disk space: 70 GB Network: 1 network adapter OS: Windows 2012 R2 |
| LAN-AD02 | Active Directory, DNS Server | LAN.lab | Hyper-V Virtual Machine (Generation 2): <ul style="list-style-type: none"> Processors: 2 virtual cores Memory: 6 GB Disk space: 70 GB Network: 1 network adapter OS: Windows 2012 R2 |

4.8.5.1 Environment Setup

- Two virtual machines, each running Windows 2012 R2 were setup on a Hyper-V host server of the Cybersecurity LAN network for authenticating Linux devices. The hardware specifications of these are described in the table above.
- The guest OS IP information of these servers was set as follows:

```

Hostname: LAN-AD
IP address: 10.100.0.5
Gateway: 10.100.0.1
Subnet Mask: 255.255.255.0
DNS:127.0.0.1, 10.100.0.13
    
```

```

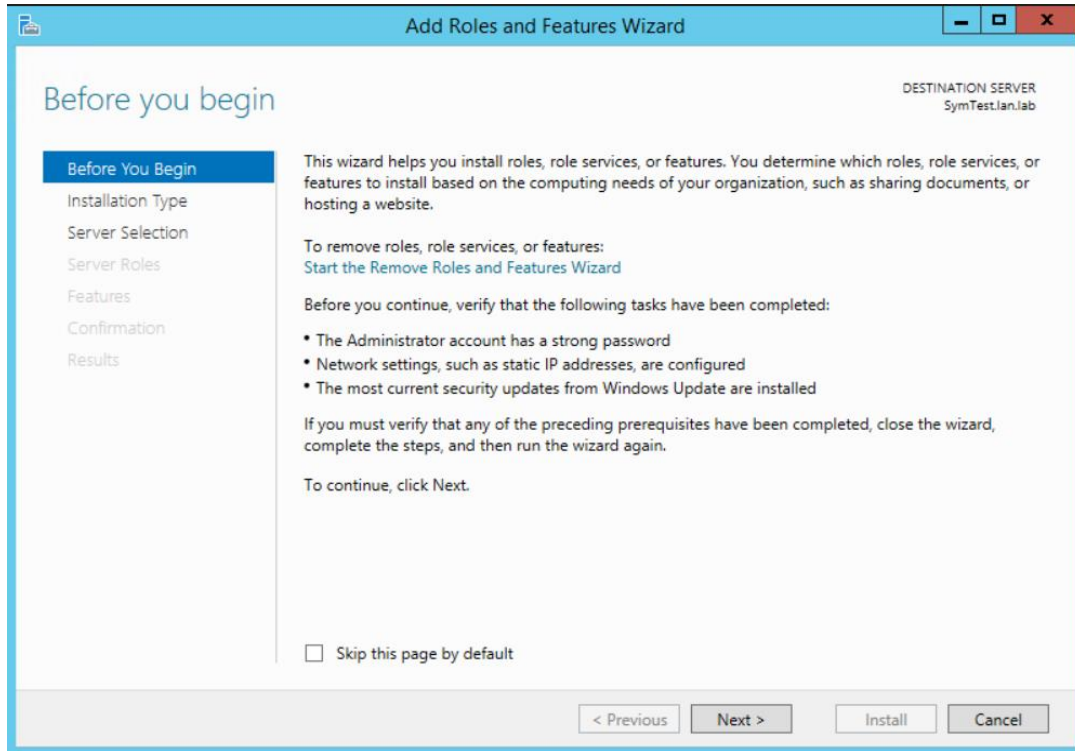
Hostname: LAN-AD02
IP address: 10.100.0.13
Gateway: 10.100.0.1
Subnet Mask: 255.255.255.0
DNS:10.100.0.17,127.0.0.1
    
```

4.8.5.2 Installing Active Directory Domain Services & DNS Server

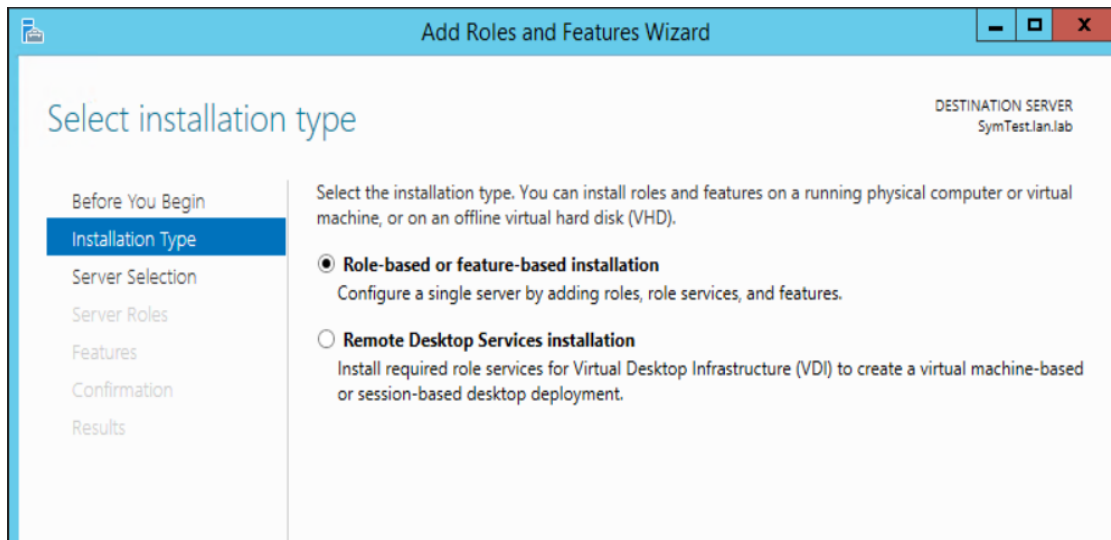
Prerequisites

Windows 2012 R2 server (preferably two for redundancy) up to date on patches, static IP address assigned with primary DNS server set to 127.0.0.1 (localhost)

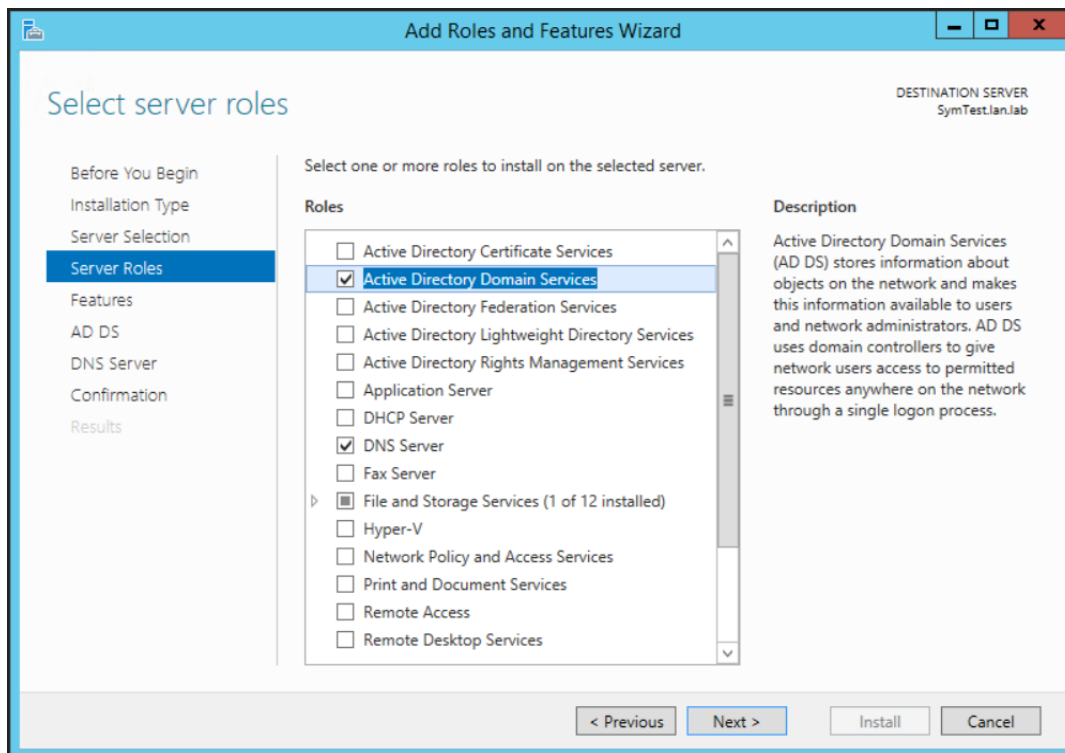
1. Launch the Windows **Server Manager** and click on **Add Roles and Features**
2. Click “**Next**” at the first page as shown below



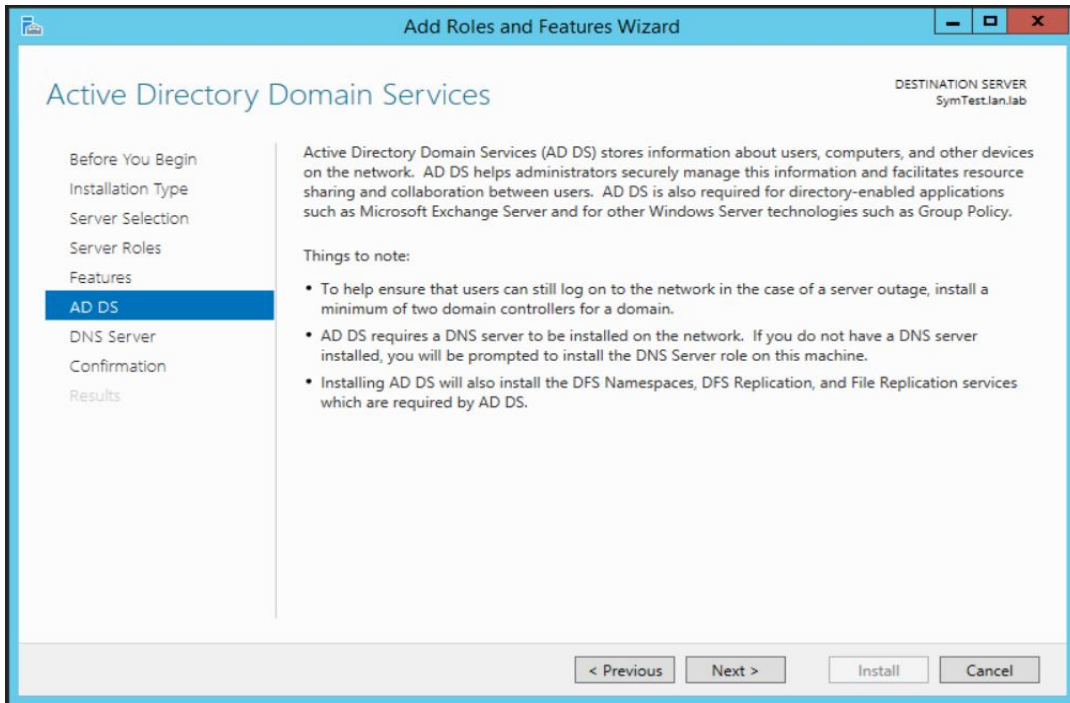
3. Select **Role Based or Feature Based Installation** under Installation Type



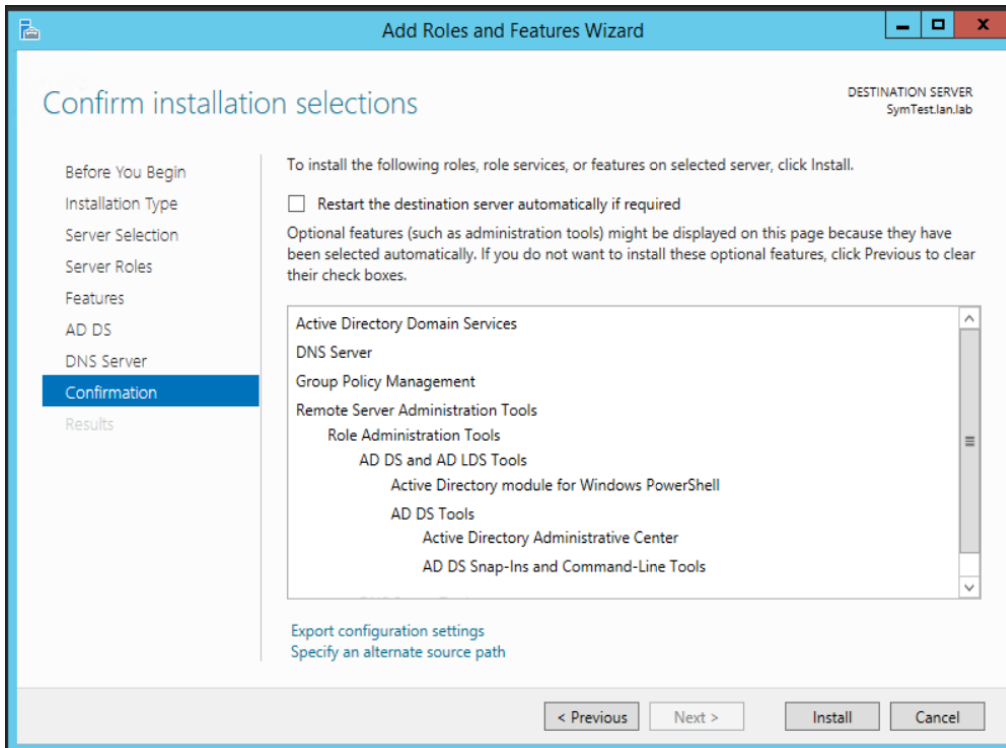
4. Select **Active Directory Domain Services** and **DNS Server** to install. Click **Next**.



5. Click **Next** on the **Features** screen, leave the default options selected,
6. Click **Next** on the **AD DS** screen and the following **DNS Server** screen as well.

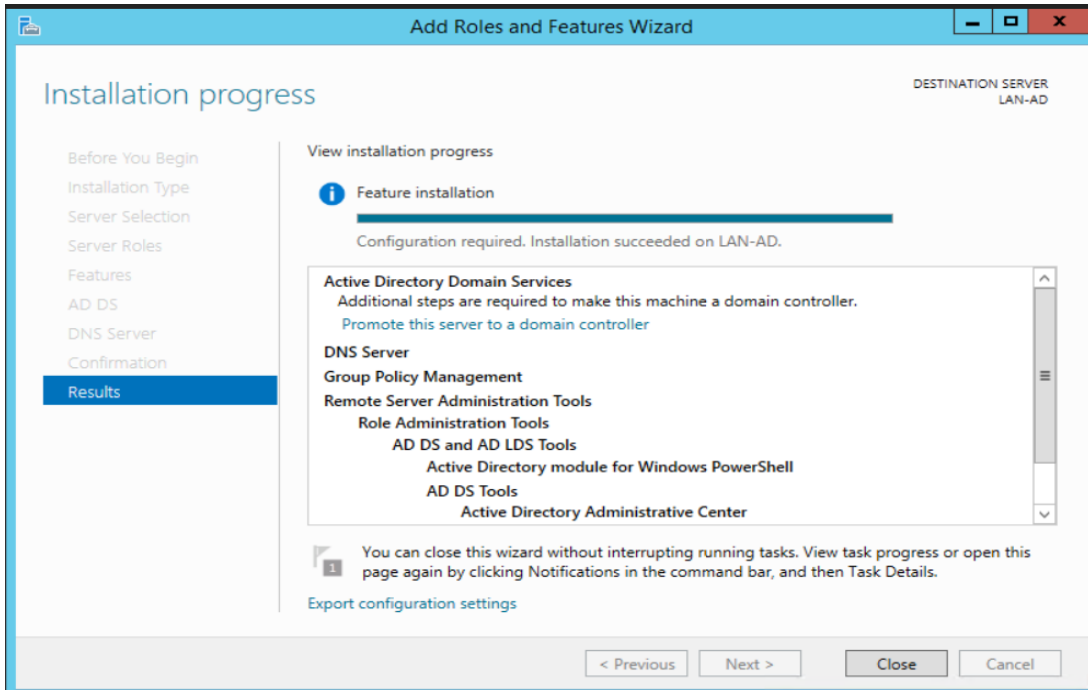


7. Verify your settings on the **Confirmation** screen. Click **Install** to proceed.

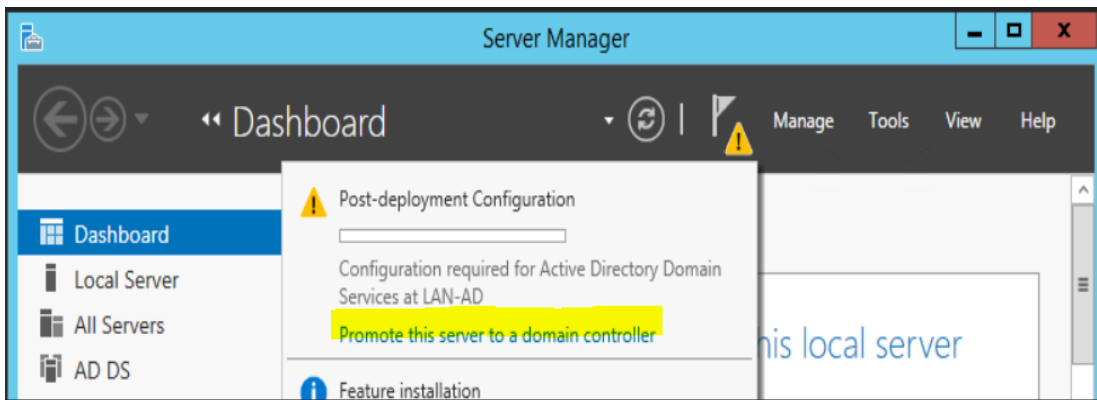


This publication is available free of charge from: <https://doi.org/10.6028/NIST.IR.8183A-3>

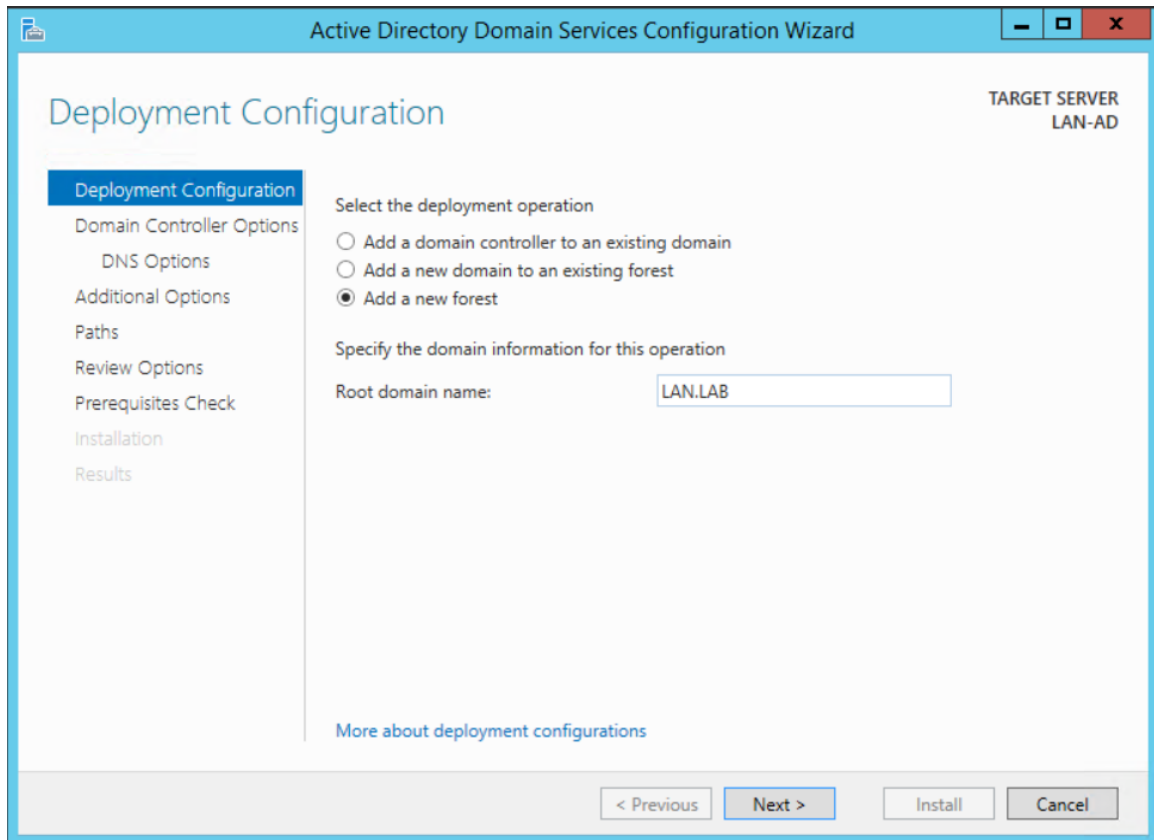
- Wait till the installation process completes and shows an **Installation succeeded** message. Hit **Close** button.



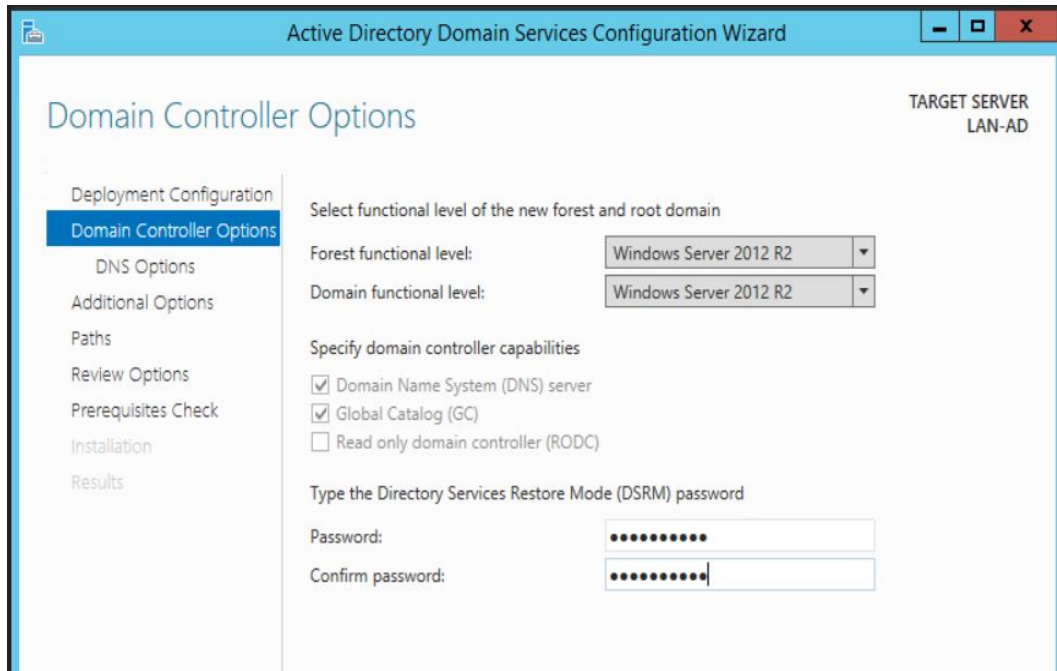
- Launch **Server Manager** again and click on **Promote this server to a domain controller**.



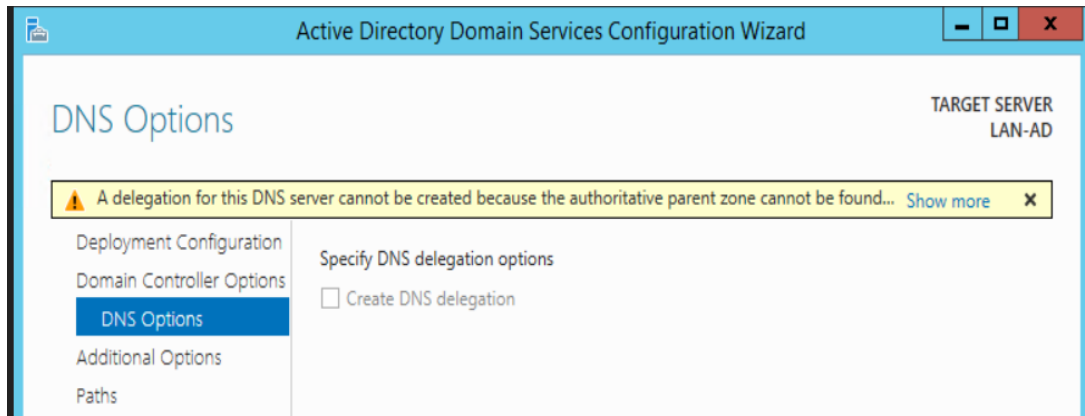
10. Select **Add a new forest** on the **Deployment Configuration** step, as this would be a new domain controller in a new forest. Mention a **Root Domain name** as applicable to your environment.



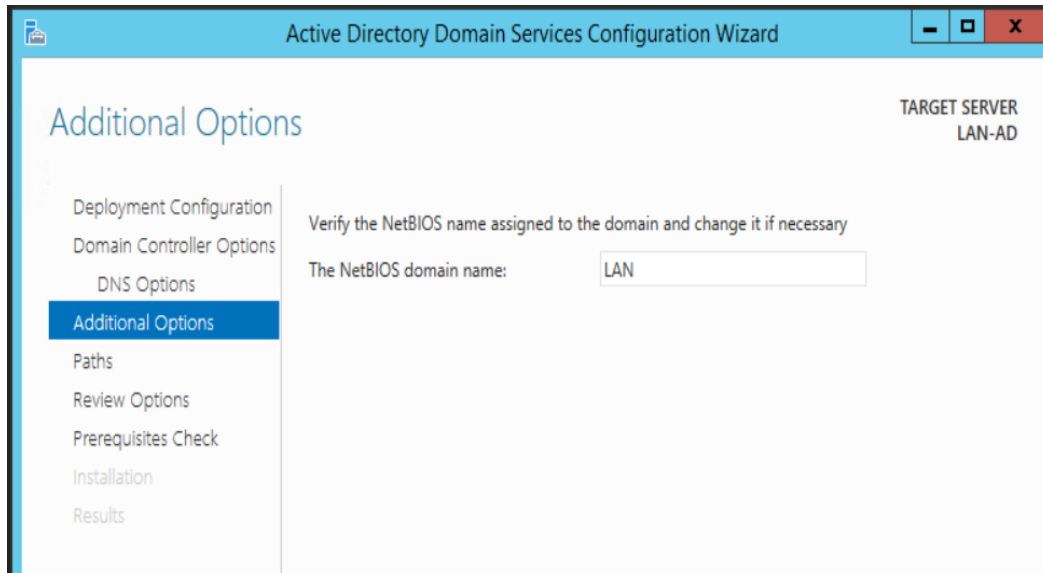
11. Set a **Directory Services Restore Mode** password in the next step. Click **Next**.



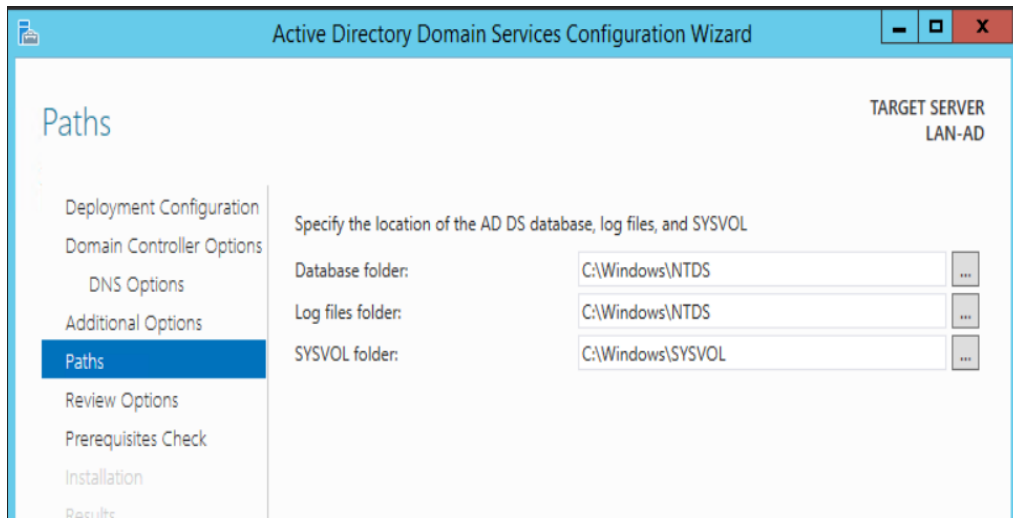
12. Under “**DNS Options**” leave the default options selected. Click **Next**.



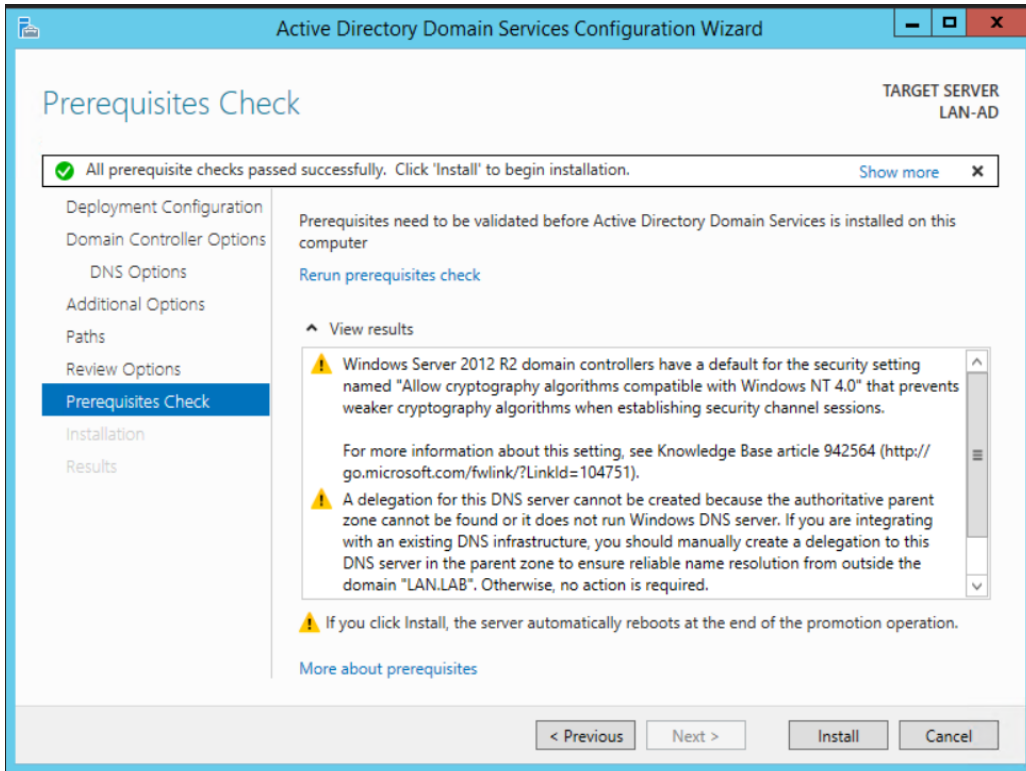
13. Confirm the NETBIOS domain name under **Additional Options**. Click **Next**.



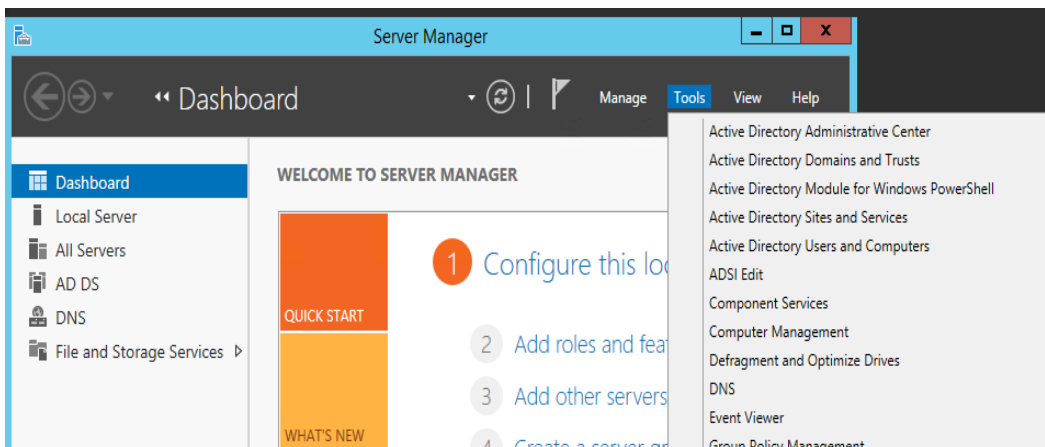
14. Leave the default folder paths as it is Under **Paths**. Click **Next**.



15. Confirm all the settings On the **Review Options** page. Click **Next**.
16. Click **Install** on the **Prerequisites Check** to launch the installation process. The server will auto reboot upon completion.



17. Login with domain administrator credentials upon reboot. Open **Server Manager** and click on **Active Directory Users and Computers** under **Tools** to manage your AD.



4.8.5.3 Joining Linux Systems to Active Directory Domain

All the Linux systems from the work-cell were joined to the AD domain **lan.lab** using **Centrify Express**. 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 is mentioned below. In addition, DNS records for each Linux host were manually created on the Active Directory server.

4.8.5.4 Installing Centrify

Prerequisites

Connectivity between your Linux clients and AD server: Ensure the Linux clients can reach the AD Domain Controller. Configure the appropriate DNS settings on the Linux client. Set the search domain to domain name of Active Directory. Verify the DNS-settings in the */etc/resolv.conf* file of your Linux server.

The following instructions are for a Debian/Ubuntu system:

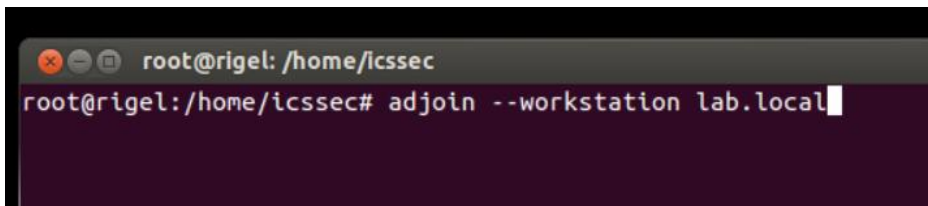
1. Download the Centrify Express (CentrifyDC) free package from <https://launchpad.net> or <https://www.centrify.com/express/linux/download/> as per CPU architecture of the Linux client.
2. Install the package: `dpkg -i <package_name>`
3. Install any dependencies if prompted. Re-run when done.

```
root@rigel:/home/icssec# dpkg -i /media/CDROM/centrifydc_5.1.1-831-0ubuntu1_amd64.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#
```

4. 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#
```

5. Run the command: `adjoin --workstation domain-name`.
This will prompt you to enter a Domain Administrator password.

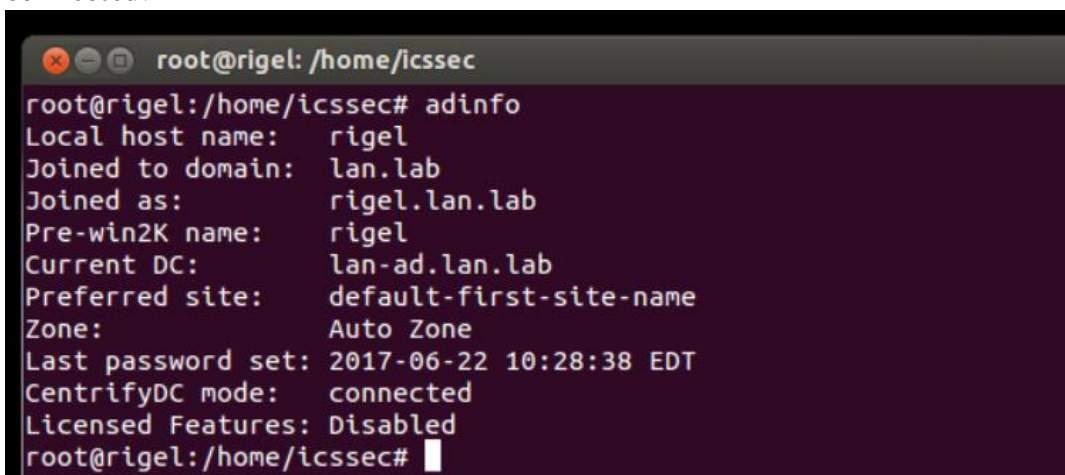


```

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

```

6. Run `adinfo` to verify the domain join status. The **CentrifyDC mode** should show as **connected**.



```

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#

```

7. Login to the Linux host using AD credentials.
 - a. For example: `ssh username.domain-name@hostname.domain-name`
 - b. OR by entering `<Domain-Name\Username>` on a Desktop based version
8. Enable sudo for AD-resources using the following steps
 - a. Add the following line in `/etc/sudoers` file (using the command `visudo`) to make an AD Domain Group a sudoer

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

Where, **adgroup**, is a group from the Active directory. The group names from active directory are transformed into all lower-case letters with underscores replacing spaces. For instance, `%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.

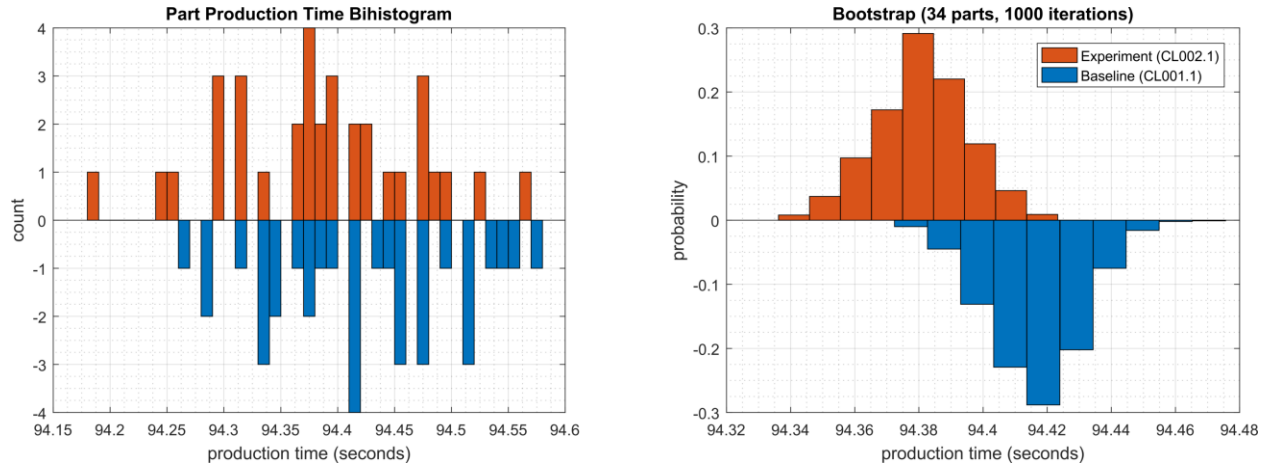


Figure 4-22 - Bihistograms showing the part production time (left) and estimated mean production time using the bootstrap method (right) using the measurements from baseline CL001.1 and experiment CL002.1.

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 (SEP)⁷³ is an endpoint protection solution that can help defend against ransomware and other emerging threats.

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 prerequisite. 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.

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:

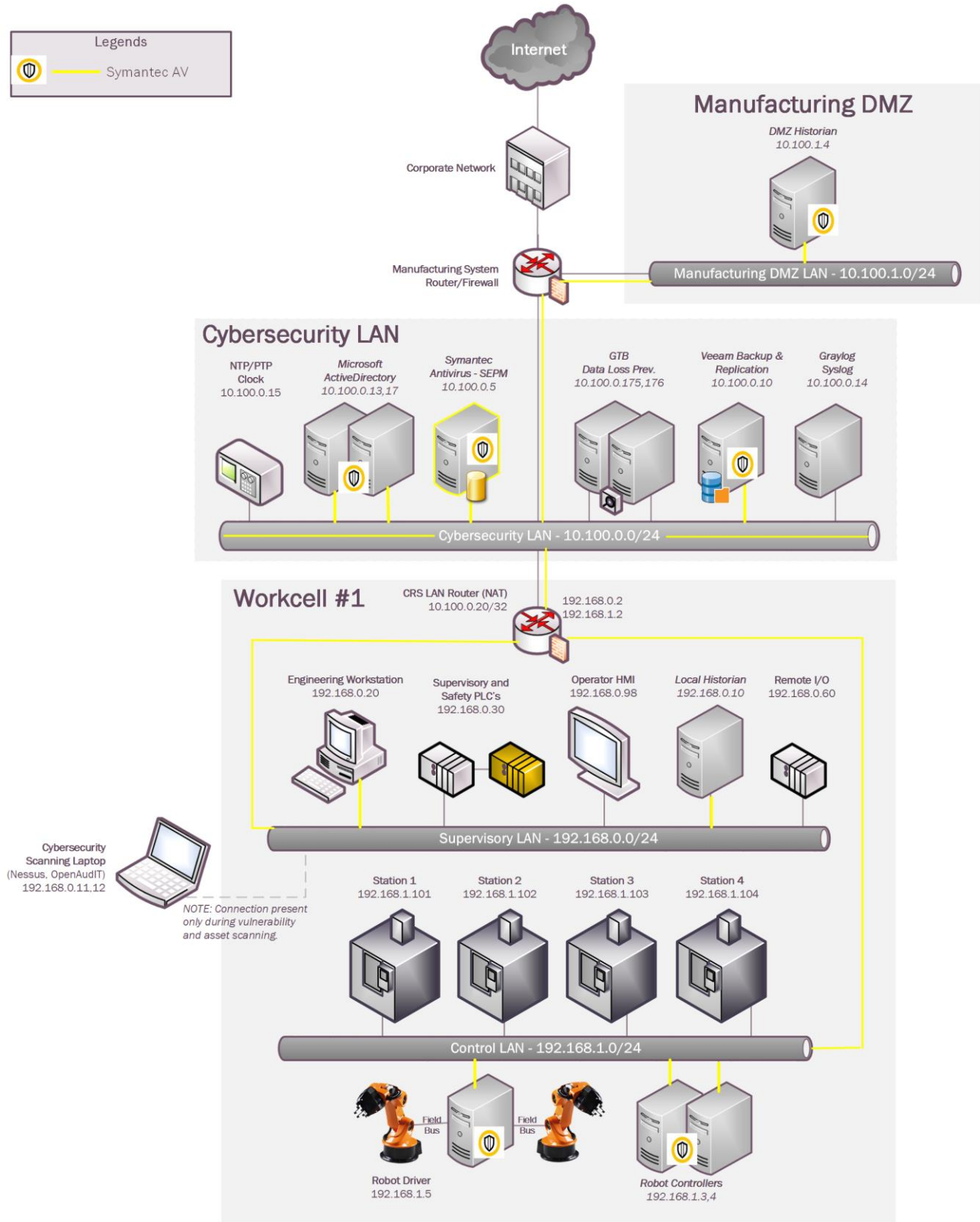
- Anti-virus/malware

4.9.3 Subcategories Addressed by Implementing Solution

DE.CM-4

⁷³ <https://www.symantec.com/content/dam/symantec/docs/data-sheets/endpoint-protection-14-en.pdf>

4.9.4 Architecture Map of Where Solution was Implemented



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

4.9.5 Installation Instructions and Configurations

Details of the solutions implemented:

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

4.9.5.1 Environment Setup

1. A virtual machine running Windows 2012 R2 was setup on a Hyper-V host server of the Cybersecurity LAN network of the workcell with hardware specifications as described in the table above.
2. The guest OS IP information of this server was set as follows:

```
IP address: 10.100.0.5
Gateway: 10.100.0.1
Subnet Mask: 255.255.255.0
DNS:10.100.0.17
```

3. The Symantec Endpoint Protection Manager (SEPM) virtual machine was deployed in the Cybersecurity LAN network of the workcell. This central instance communicates with all the endpoint agents deployed on to the workcell. 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. A detailed list⁷⁴ of firewall ports is available.

4.9.5.2 Setup of the SEPM Server

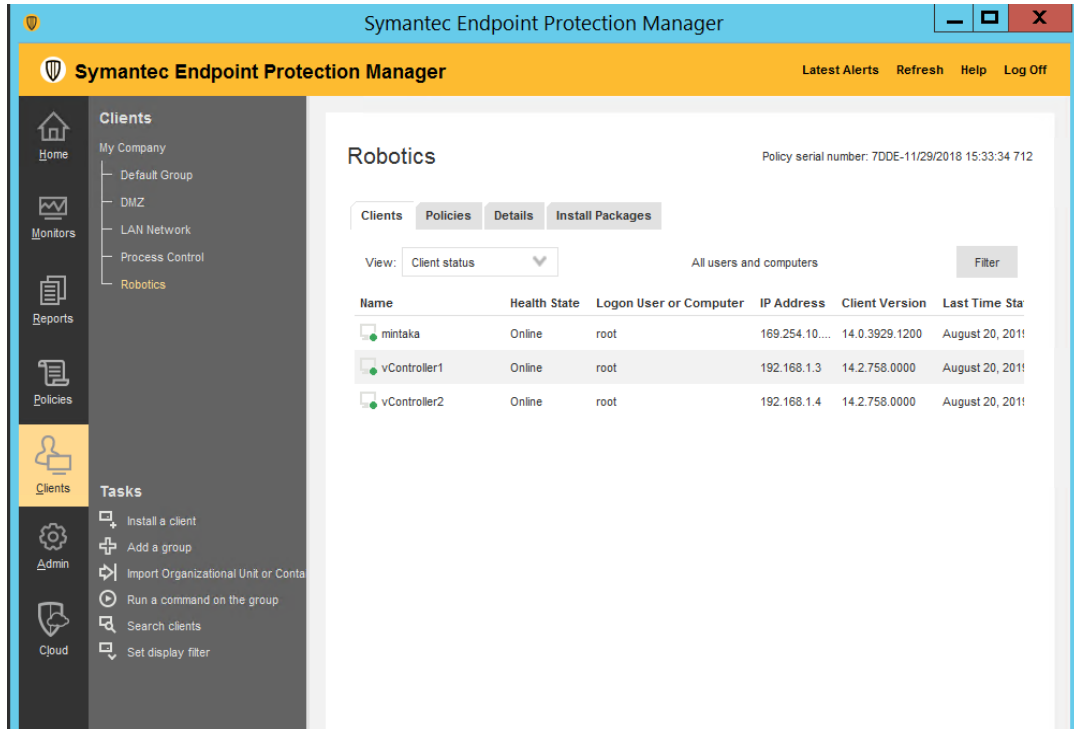
1. Download the Symantec Endpoint Protection .zip bundle from the Symantec website. A license is required to register and download the product.
2. Open the extracted folder and run the **Setup.exe** file. Mid-way during the install, enter a strong admin password when prompted.
3. Select the **Backed Database** selection page on the Database selection page. Choose the **Embedded database** if you do not have a MS SQL Server. Follow the on-screen instructions and complete the installation wizard.
4. **Reboot** the server once done.
5. Launch the Symantec Endpoint Protection Manager (SEPM) console and login with the admin user created earlier.
6. Activate the license key to begin using the product.

⁷⁴ https://support.symantec.com/en_US/article.HOWTO81103.html

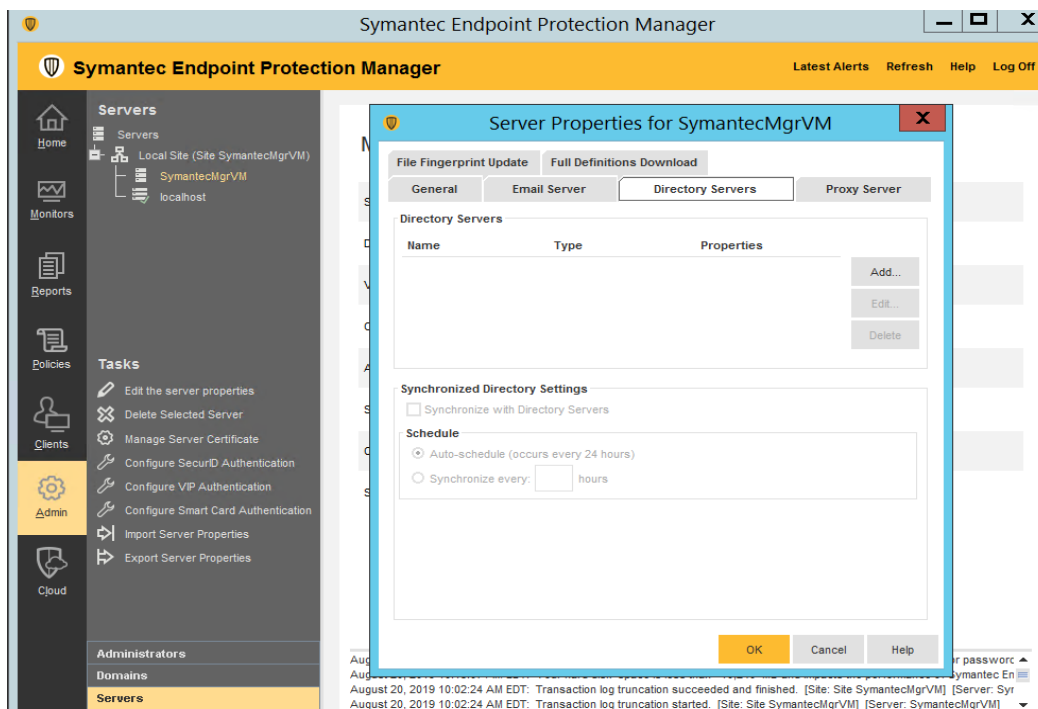
4.9.5.3 Configuration of the SEPM Server

1. Configure **Client groups** to group devices as follows
 - a. Click on **Clients** option from left-side menu
 - b. Click on **Add a group**
 - c. Enter a **Name**

For instance, the image below shows the different client groups created in our network to group devices from each of the systems.

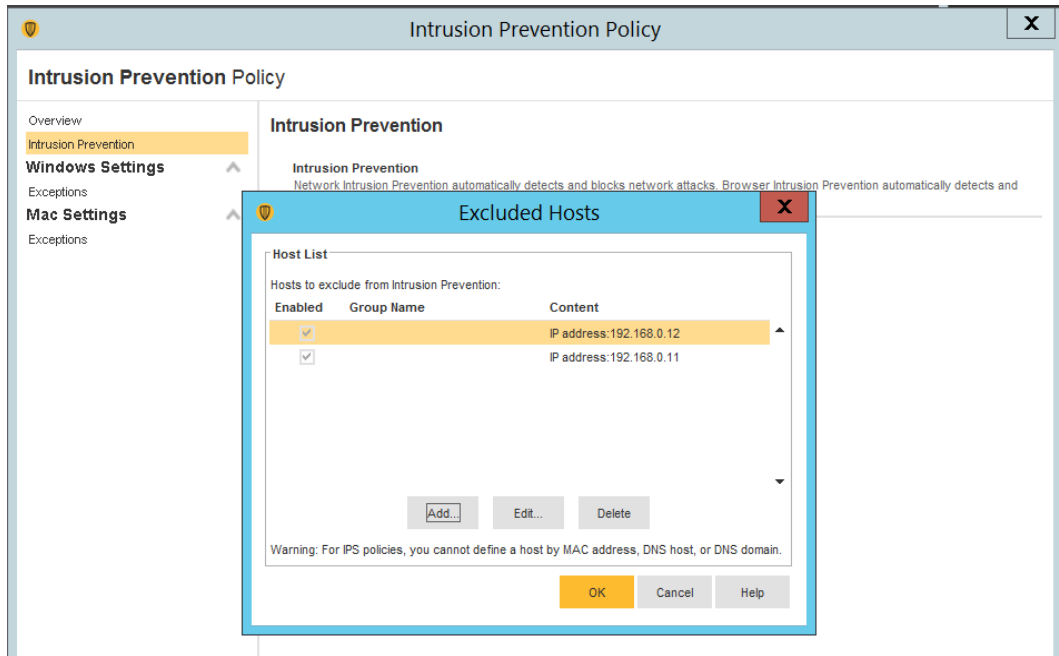


2. Integrate SEPM with Active Directory/LDAP using the following instructions
 - a. Click on **ADMIN > Servers > Local Site > Server Name > Edit Server Properties**
 - b. Click on **Directory servers** tab under **Server Properties for <Server>**.
 - c. Click further on **ADD** button as shown below to configure domain details.
 - d. Logout and log back in this time with your AD credentials.

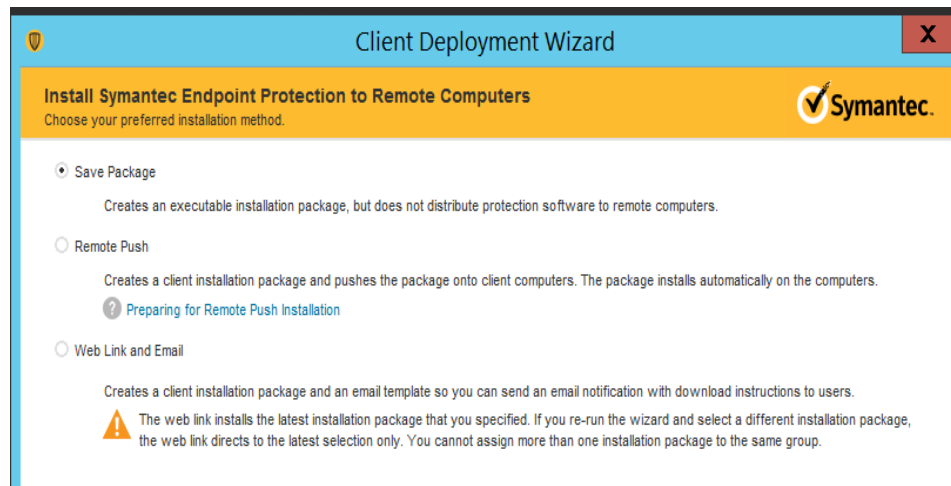


3. Configure SMTP server using the following instructions,
 - a. Click on **ADMIN > Servers > Local Site > Server Name > Edit Server Properties**
 - b. Click on **Email server** tab under **Server Properties for <Server>**.
 - c. Enter the details. Click **OK** when done.
4. Configure a policy for **Excluded Hosts** to **exclude** IP addresses of systems such as vulnerability scanners from getting blocked when performing a scan.
 - a. Click **Policies > Intrusion Prevention or Create a new Policy**
 - b. Click **Excluded Hosts**. Add the IP address of the system in question.
 - c. **Link** the policy to the appropriate client group.

The figure below shows some of our Excluded hosts such as Nessus scanner.



5. (Optional) Setup device control such as restricting USB devices using the following instructions.
 - a. Create a policy under **Application and Device Control**.
 - b. Click Device Control
 - c. Click Add under Blocked devices
 - d. Select one or more devices to block. For instance: USB
 - e. Ensure to select Keyboard and Mice under **Devices excluded from blocking**.⁷⁵



⁷⁵ <https://support.symantec.com/us/en/article.howto80866.html>

4.9.5.4 Installing Endpoint Agent on Linux Client Systems

The high-level steps in getting the AV installed on client systems are as follows:

- Create a deployment package specific for a client group
- Install the endpoint agent.
- Restart the client system to complete the install.

Creating a deployment package

- a. Login to the Symantec Manager console. Click on **Clients** > **Group Name** where the endpoint device needs to be in.
- b. 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.
- c. 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.

Client Deployment Wizard

Select Deployment Type

Welcome to the Client Deployment Wizard

Use this wizard to install the protection client on computers in your network or update existing client communication settings.

[Click to view the Install Client tour](#)

Note: For instructions to install the client on a computer that runs Symantec Mail Security or Symantec Scan Engine, see the Symantec Technical Support knowledge base article: [Click here](#)

New Package Deployment

Select packages from the server and specify client group and features.

Existing Package Deployment

Choose from previously exported packages that are located on your hard drive.

Communication Update Package Deployment

Create a package that changes the communication settings on an existing Symantec Endpoint Protection client installation. Use this option to restore communication between the client and Symantec Endpoint Protection Manager, to connect the client to a new Symantec Endpoint Protection Manager, or to convert an unmanaged client to a managed client.

Create a package for Symantec Endpoint Protection clients that run on Windows. 🌐

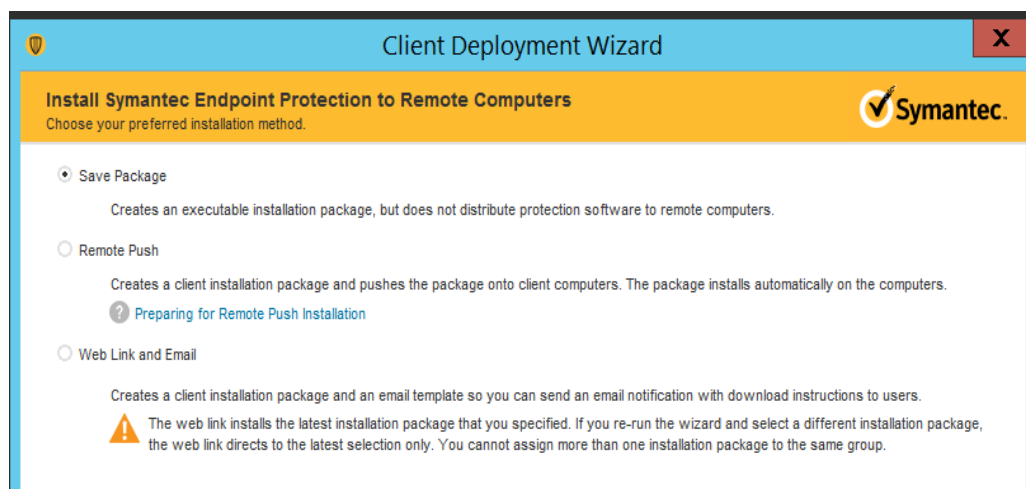
Create a package for Symantec Endpoint Protection clients that run on Mac. 🍏

< Back Next > Cancel

- d. Click **Next**. Choose the appropriate OS Platform as per the endpoint OS, from the dropdown list of Install Packages. Notice the Group Name is already prepopulated. This ensure the client will be placed directly in that group upon install.



- e. (Optional) Select **Include virus definitions in the client installation package** under Content Options. Click **Next**.
- f. Select **Save Package** to create a local installer. This is the **recommended** option for Linux clients.
- g. Click **Next**
- h. Verify if the installer bundle (.zip) was successfully created.



Installing the endpoint protection agent on Linux

Prerequisites:

- Symantec AV on Linux requires some 32-bit packages to be installed as a prerequisite.⁷⁶
- 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, for a Debian /Ubuntu system; run the following commands:

- a. Verify if the system has 64-bit architecture by running the command:

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

Expected output: amd64

- b. 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.

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

Output: i386

- c. Enable multi-arch support by running the command:

```
Sudo dpkg --add-architecture i386
```

- d. Install those 32-bit packages

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

- e. Copy the installer bundle (.zip) file created in Step.1 to the Linux client. Grant execute permissions to the “install.sh” file found in the extracted folder.

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

- f. Run the install.sh script: `sudo ./install.sh -i`

⁷⁶ https://support.symantec.com/en_US/article.TECH228118.html

g. Verify if the output shows **Installation completed**. For example,

```

youbot@vSaiph: /var/sepfiles
Pre-compiled Auto-Protect kernel modules are not loaded yet, need compile them from source code
Build Auto-Protect kernel modules from source code successfully
Running LiveUpdate to get the latest defintions...
sep::lux::Cseplux: Failed to run session, error code: 0x80010830
Live update session failed. Please enable debug logging for more information
Unable to perform update
Installation completed
=====
Daemon status:
symcfgd           [running]
rtvscand          [running]
smcd              [running]
=====
Drivers loaded:
symap_custom_3_19_0_25_generic_x86_64
symev_custom_3_19_0_25_generic_x86_64
=====
Auto-Protect starting
Protection status:
Definition:      Waiting for update.
AP:              Malfunctioning
=====
The log files for installation of Symantec Endpoint Protection for Linux are under ~/:
sepfl-install.log
sep-install.log
sepap-install.log
sepui-install.log
sepfl-kbuild.log
youbot@vSaiph:/var/sepfiles$

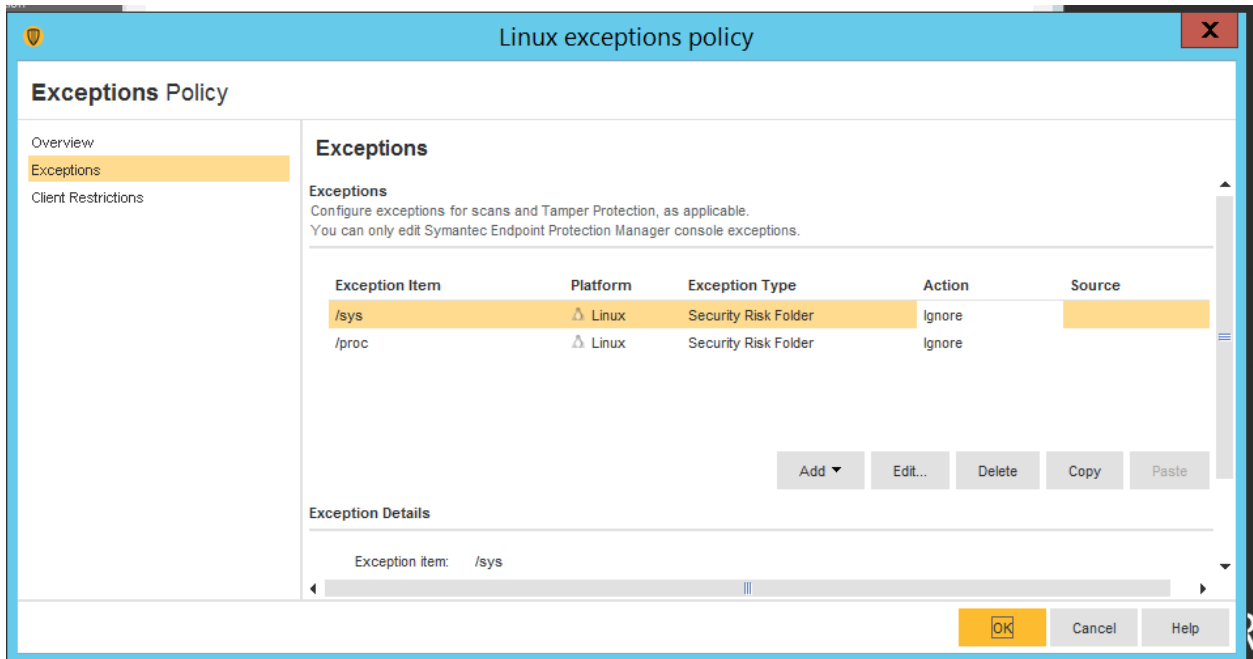
```

1. Restart the Linux client.
2. Check the SEPM console to see if the Linux client shows as **green ONLINE**

4.9.5.5 Additional Configuration for Linux

Create an **Exceptions** policy for excluding the /sys and /proc directories from scanning as follows:

- Login to the SEPM console.
- Click on **Policies > Exceptions > Default policy** or create your own > **Exceptions**
- Click **Add** to add folders to exclude from scanning.
- Click **OK**. Logout



4.9.5.6 Additional Information

- Official Symantec Endpoint Protection v14 installation guides⁷⁷
- How-to-guides from Symantec for Endpoint protection⁷⁸ can be found at
- Official install guide for Windows systems⁷⁹

⁷⁷ https://support.symantec.com/en_US/article.DOC9449.html

⁷⁸ <https://support.symantec.com/us/en/how-to-guides.html>

⁷⁹ https://support.symantec.com/en_US/article.DOC9445.html

Lessons learned

- 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 prerequisite.⁸⁰
- On 64bit Linux systems, this will install 32bit packages alongside their 64bit counterparts. This may 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 Multiarch⁸¹ mode is enabled to allow 32bit apps to install on 64bit systems.
- On the Ubuntu 12.04 servers (such as Engineering Workstation) we couldn't get the agent to install due to these package conflicts. Other compensating controls were then applied.

⁸⁰ https://support.symantec.com/en_US/article.TECH228118.html

⁸¹ <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.

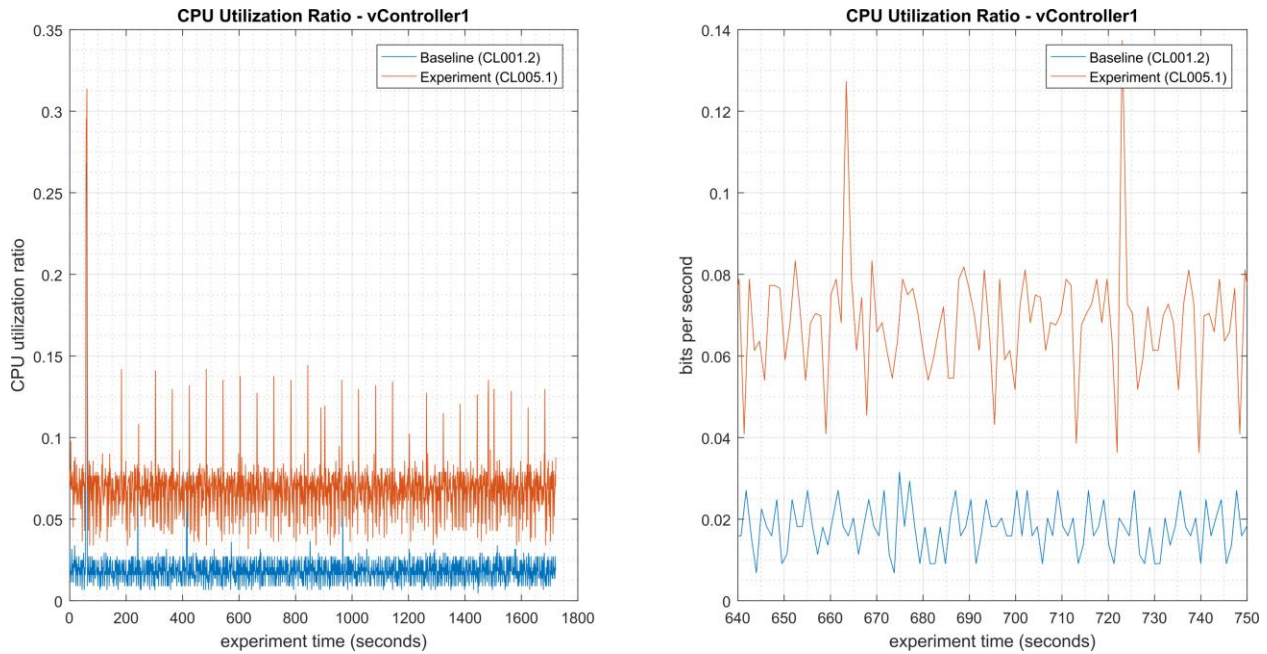


Figure 4-23 - Time series plots showing the CPU utilization ratio for vController1 during the CL005.1 experiment and CL001.2 baseline (left), and during the period of measured impact (right).

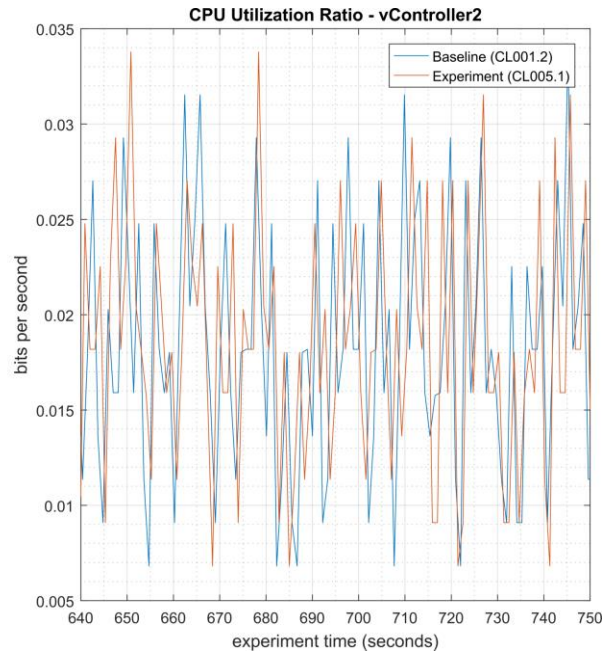
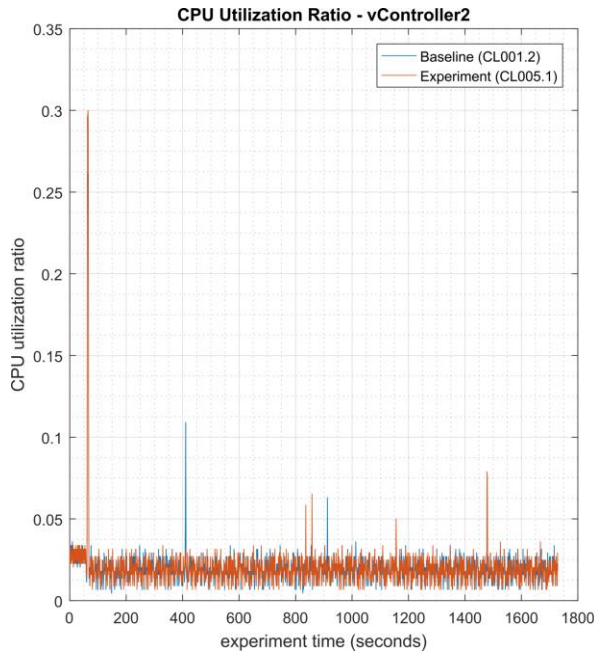


Figure 4-24 - Time series plots showing the CPU utilization ratio for vController2 during the CL005.1 experiment and CL001.2 baseline (left).

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

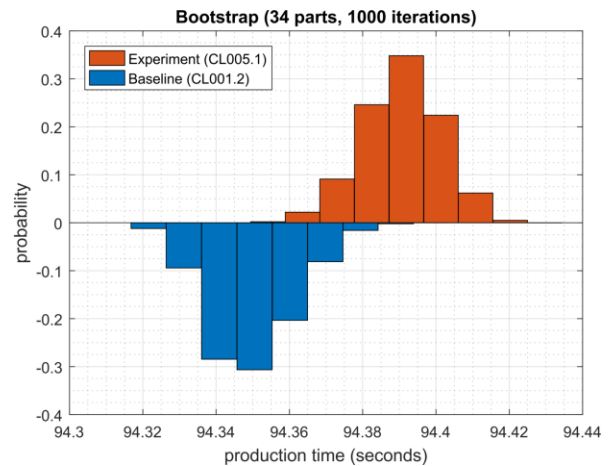
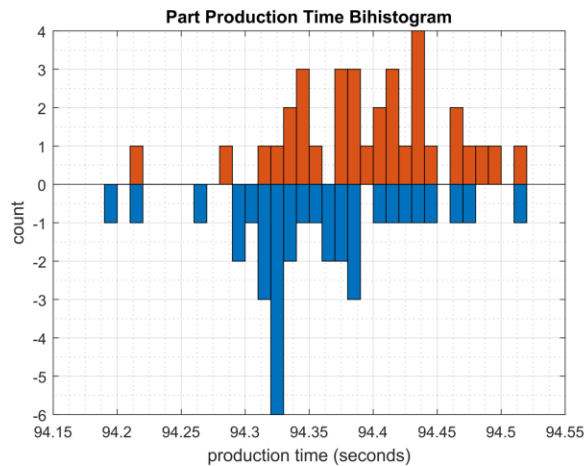


Figure 4-25 - Bihistograms showing the part production time (left) and estimated mean production time using the bootstrap method (right) using the measurements from baseline CL001.2 and experiment CL005.1.

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%.

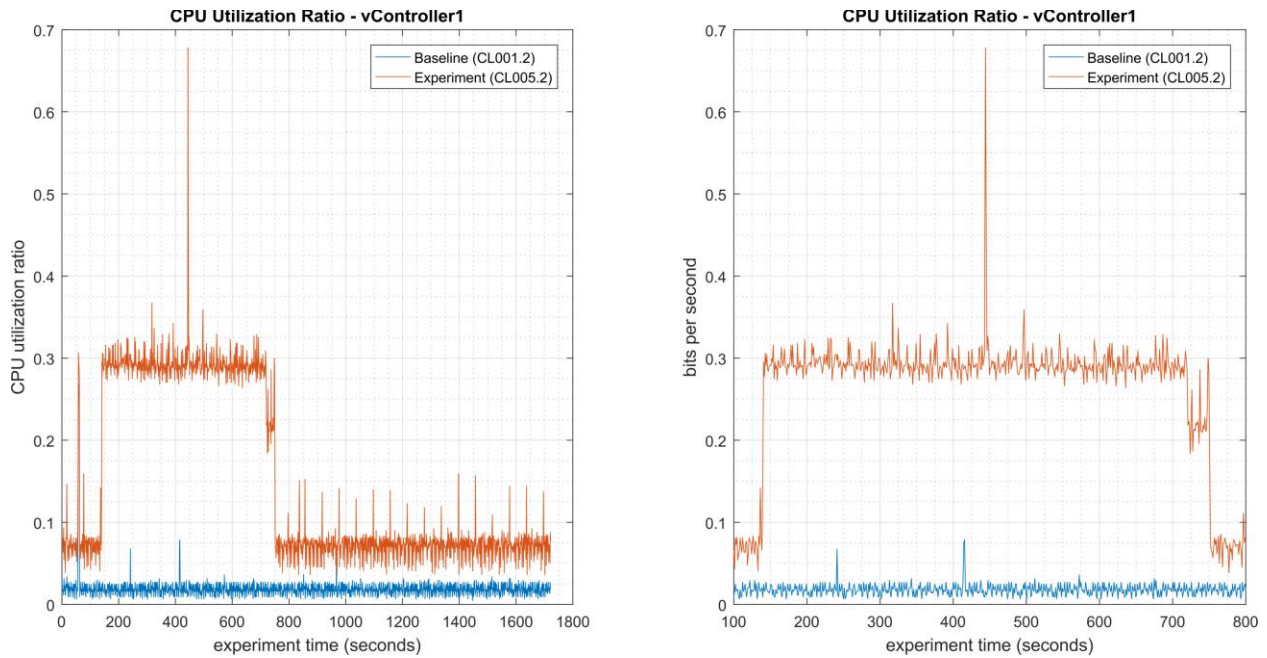


Figure 4-26 - Time series plots showing the CPU utilization ratio for vController1 during the CL005.2 experiment and the CL001.2 baseline (left), and during the period of measured impact (right).

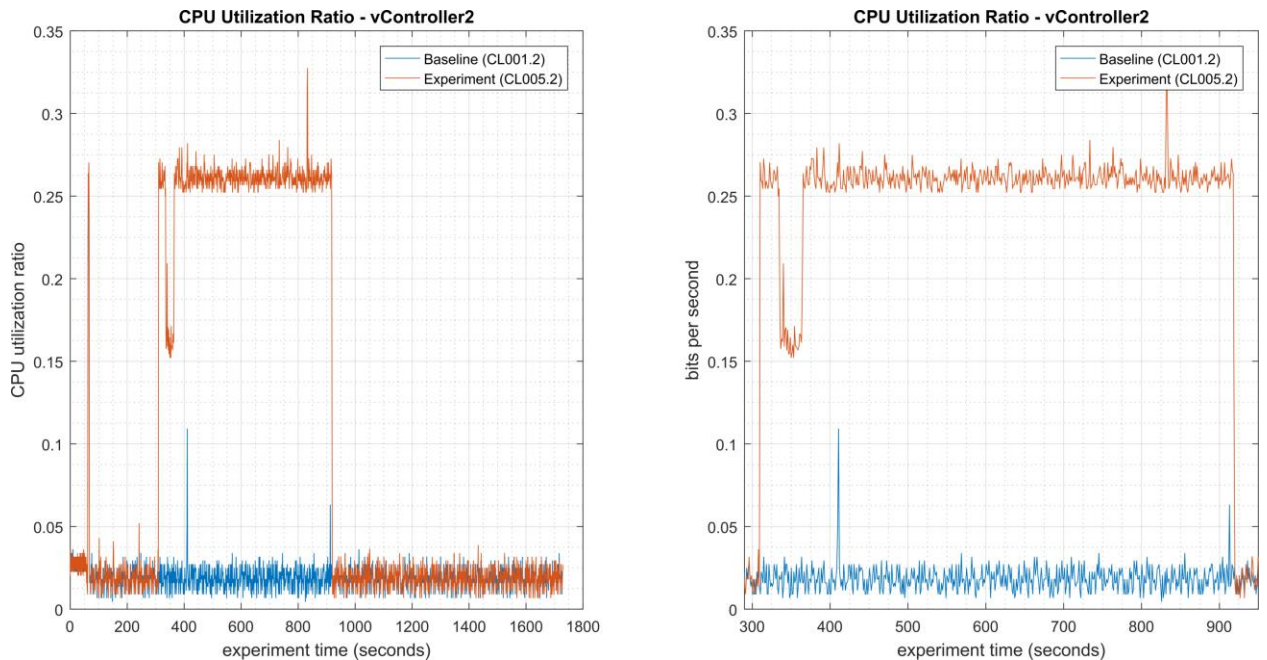


Figure 4-27 - Time series plots showing the CPU utilization ratio for vController2 during the CL005.2 experiment and the CL001.2 baseline (left), and during the period of measured impact (right).

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

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.

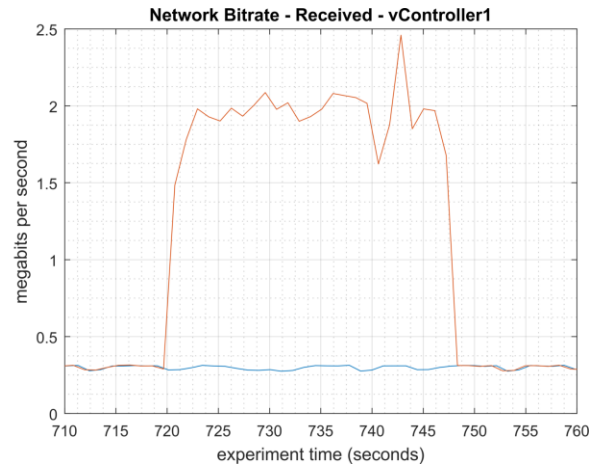
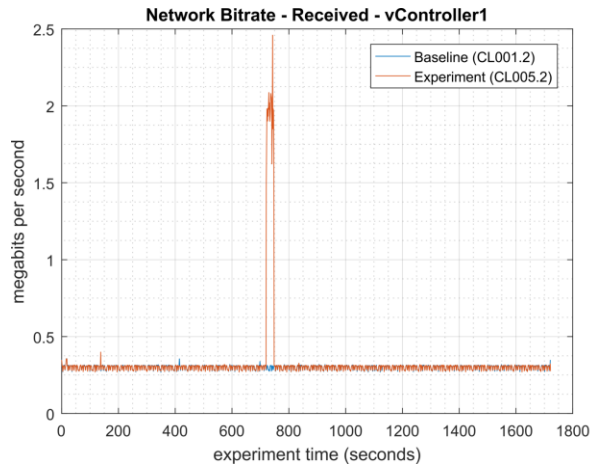


Figure 4-28 - Time series plots showing the quantity of network traffic received by vController1 during the experiment (left), and during the period of measured impact (right). The peak in traffic shown between 720 sec. to 750 sec. occurred while the scan was active.

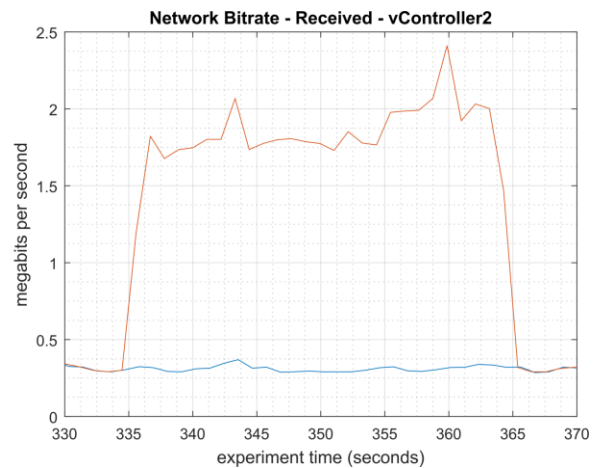
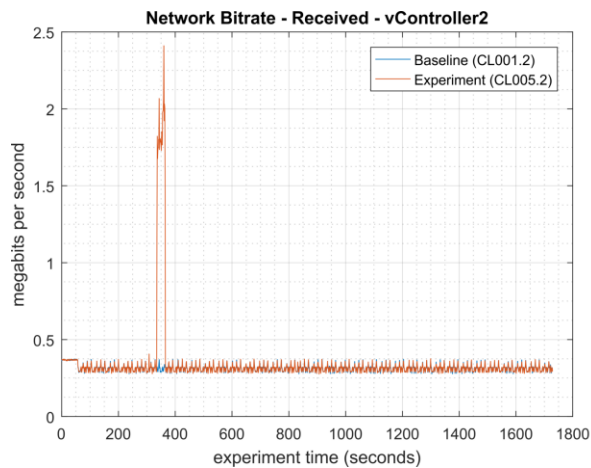


Figure 4-29 - Time series plots showing the quantity of network traffic received by vController2 during the experiment (left), and during the period of measured impact (right). The peak in traffic shown between 330 sec. to 365 sec. occurred while the scan was active.

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

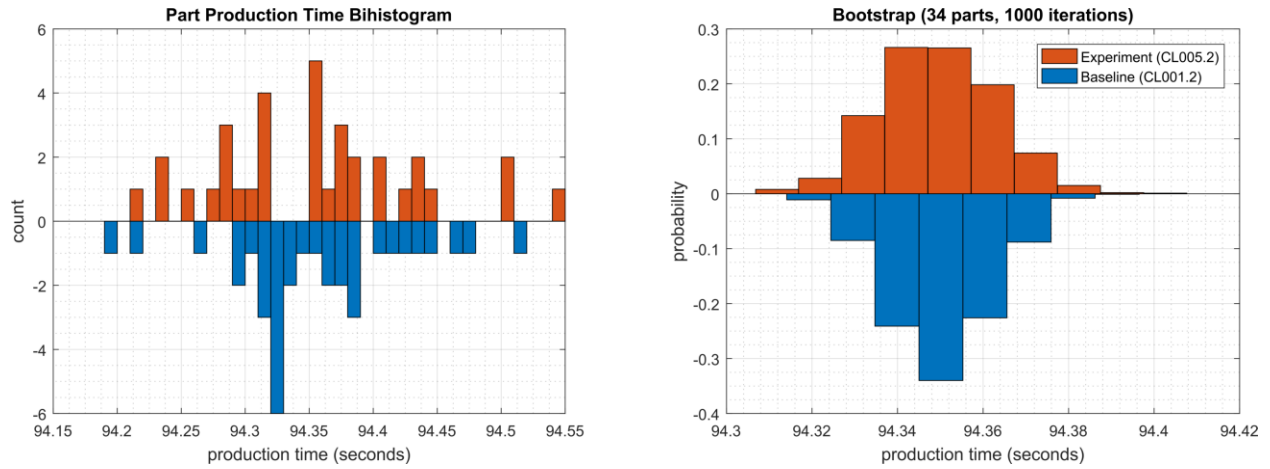


Figure 4-30 - Bihistograms showing the part production time (left) and estimated mean production time using the bootstrap method (right) using the measurements from baseline CL001.2 and experiment CL005.2.

4.9.7 Links to Entire Performance Measurement Data Set

- [CL005.1-AntivirusRealTimeScan.zip](#)
- [CL005.2-AntivirusFullScan.zip](#)

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

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.⁸² 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:

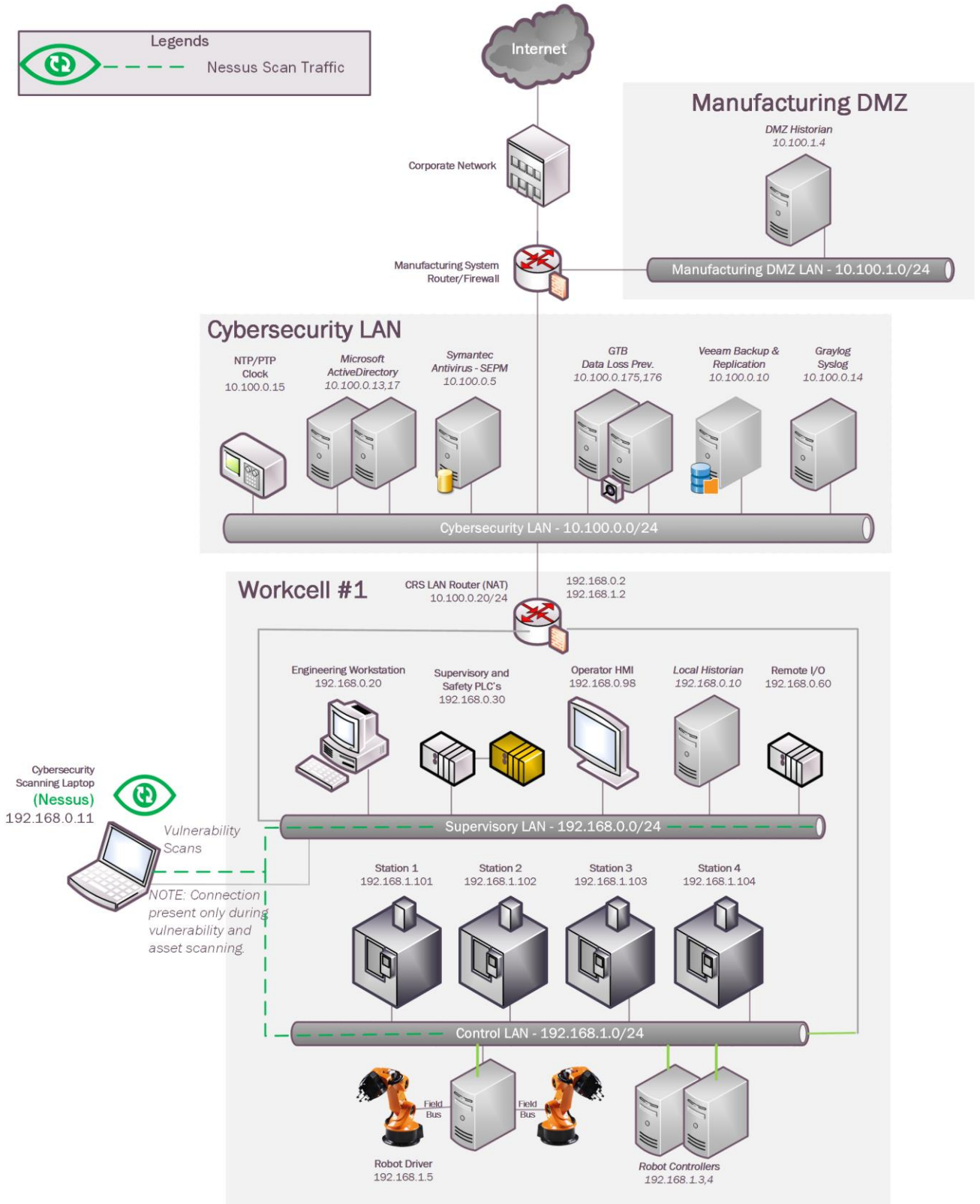
- Vulnerability Scanning
- Vulnerability Management

4.10.3 Subcategories Addressed by Implementing Solution

ID.RA-1, DE.CM-4, DE.CM-8, RS.MI-3

⁸² http://info.tenable.com/rs/934-XQB-568/images/NessusPro_DS_EN_v8.pdf

4.10.4 Architecture Map of Where Solution was Implemented



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

4.10.5 Installation Instructions and Configurations

Details of the solution implemented:

| Name | Version | Deployment Mode | Hardware Details |
|---------------------|---------|-----------------|---|
| Nessus Professional | 7.2.0 | Standalone | Laptop with the following specs. <ul style="list-style-type: none"> • Processor: i7 • Memory: 16 GB • Disk: 256 GB • OS: Windows 7 Professional |

4.10.5.1 Environment Setup

1. A temporary laptop (referred as Cybersecurity scanning laptop) running Windows and connected to Supervisory LAN network was setup on an on-demand basis.
2. The guest OS IP information of this server was set as follows:

```
IP address: 192.168.0.11
Gateway: 192.168.0.2
Subnet Mask: 255.255.255.0
DNS:10.100.0.17
```

4.10.5.2 Setup Instructions

1. Download the Nessus Professional installer.⁸³
2. Run the installer. Follow the on-screen instructions of the setup wizard.
3. Register the product during installation either in **online** or **offline** mode. An online mode⁸⁴ is suitable for environments where Nessus server has internet access while an offline mode is suitable for air-gapped environments.
4. Navigate to the Nessus web interface⁸⁵ post installation.
5. Login to the Nessus UI, Click **Settings** to configure SMTP Server, LDAP Server and Custom CA Certificate (if applicable)
6. Configure Firewall rules as described in the Nessus documentation for credentials scans to allow SSH, WMI or SNMP traffic depending on the type of hosts between the Nessus server and the scan targets. For unauthenticated scans, the firewall should be allowed for any-any communication between the Nessus server and target network.

⁸³ <https://www.tenable.com/>

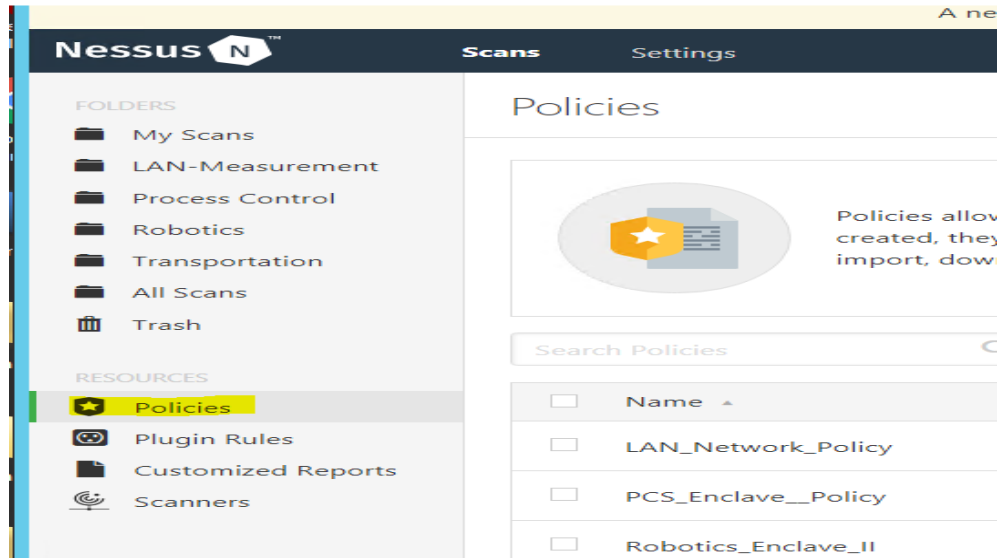
⁸⁴ <https://docs.tenable.com/nessus/Content/ManageNessusOffline.htm>

⁸⁵ <https://<IP address of Nessus server>:8834>

4.10.5.3 Configuring Scans and Policies

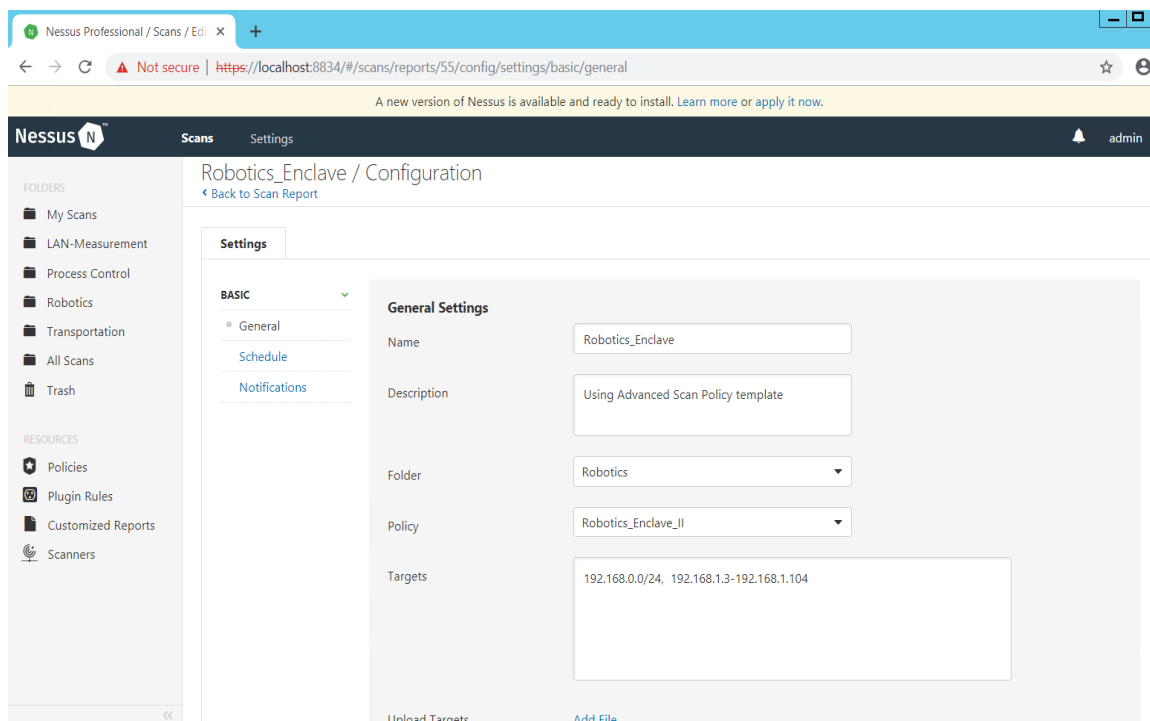
Use the **Policy** feature of Nessus for performing credentials checks. A Policy lets you create a scan template where in device credentials and other custom settings can be saved for scanning assets. Once created, a policy can then later be assigned to a scan.

1. Create a Policy using the following instructions
 - b. Click on **Policies** from the left-side explorer bar
 - c. Click on **New Policy** button.



- d. Choose from any on the default templates available. The **Advanced Scan** template was selected for our use. Click on Credentials tab under a template to configure host-based credentials (SSH, Windows, SNMP, etc.).
- e. Click **Save** when done.

2. Create a Scan using the following instructions
 - a. Click **Scans** on the Home Page > **+New Scan** > **User Defined** > **Select <Policy>**
 - b. Enter a **Name**, **Description** and **Network Range or Host IP addresses**.
 - c. Click on **Schedule** to configure a schedule
 - d. Click **Notifications** to configure Email recipients.
 - e. Click **Save**.



3. Assign the Scan created to a Policy as follows
 - a. Click **All Scans** > Click on the **<Scan>** created earlier.
 - b. Under **Policy**, Select the appropriate Policy from the drop-down list to associate the scan with a policy.
 - c. Click **Save**.
4. (Optional) Click on the **launch** button next to the scan to start on-demand scan
5. Review the scan results upon completion of the scan.

4.10.5.4 Additional Information

- Official Nessus Documentation⁸⁶
- Credentials checks for scanning Windows targets⁸⁷

⁸⁶ <https://docs.tenable.com/nessus/Content/GettingStarted.htm>

⁸⁷ <https://docs.tenable.com/nessus/Content/CredentialedChecksOnWindows.htm>

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.

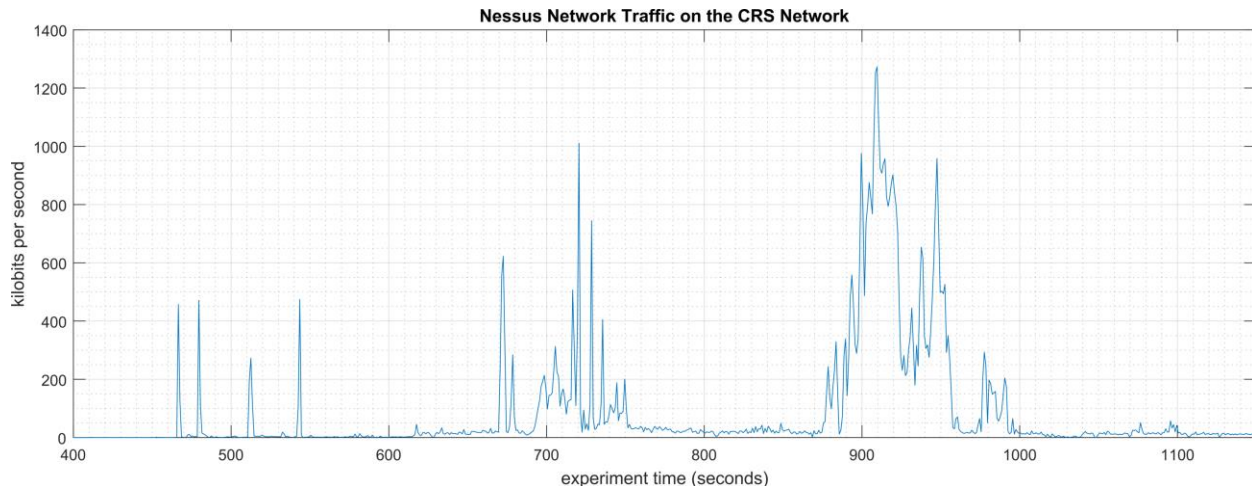


Figure 4-31 - Time series plot showing the quantity of network traffic transmitted and received by the Nessus tool during the experiment time period 400 to 1200 seconds, with the most prominent activity between 700 to 750 seconds and 875 to 1000 seconds. The Nessus GUI reported it was active between 450 to 1400 seconds experiment time.

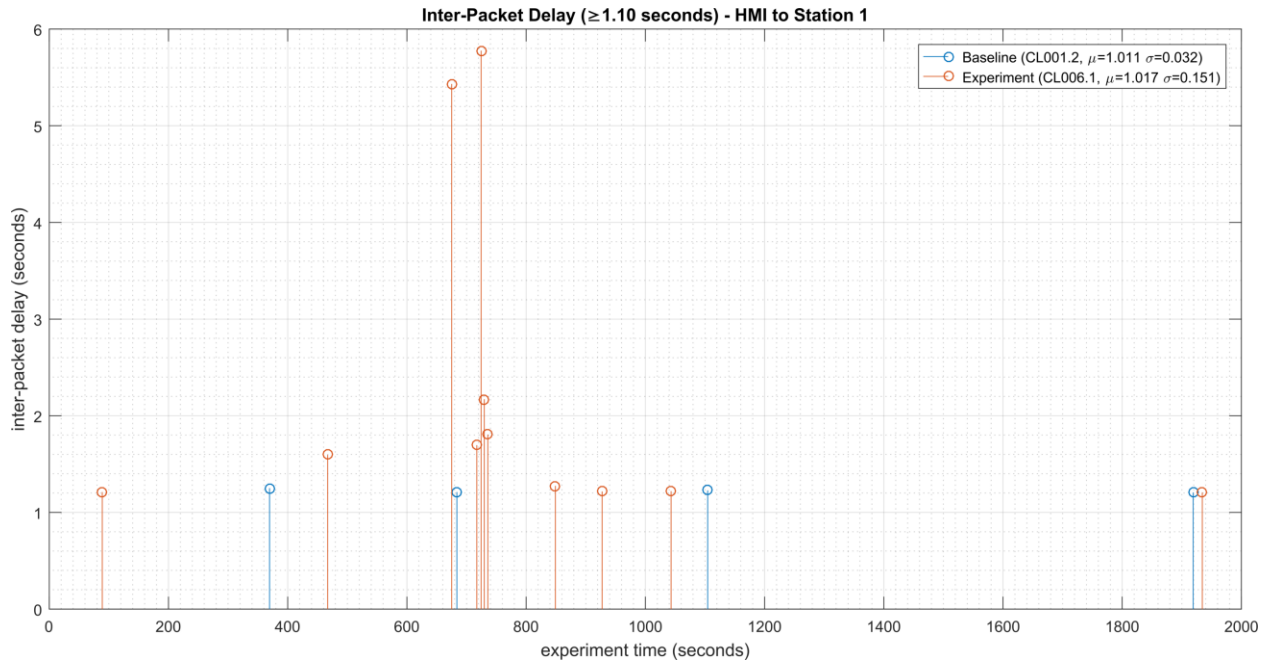


Figure 4-32 - Stem plot displaying the inter-packet delays (greater than or equal to 1.10 seconds) of Modbus TCP traffic between the HMI and Station 1, as measured during the baseline CL001.2 and experiment CL006.1. Note the large inter-packet delays between experiment time 600 to 800, resulting in HMI 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.

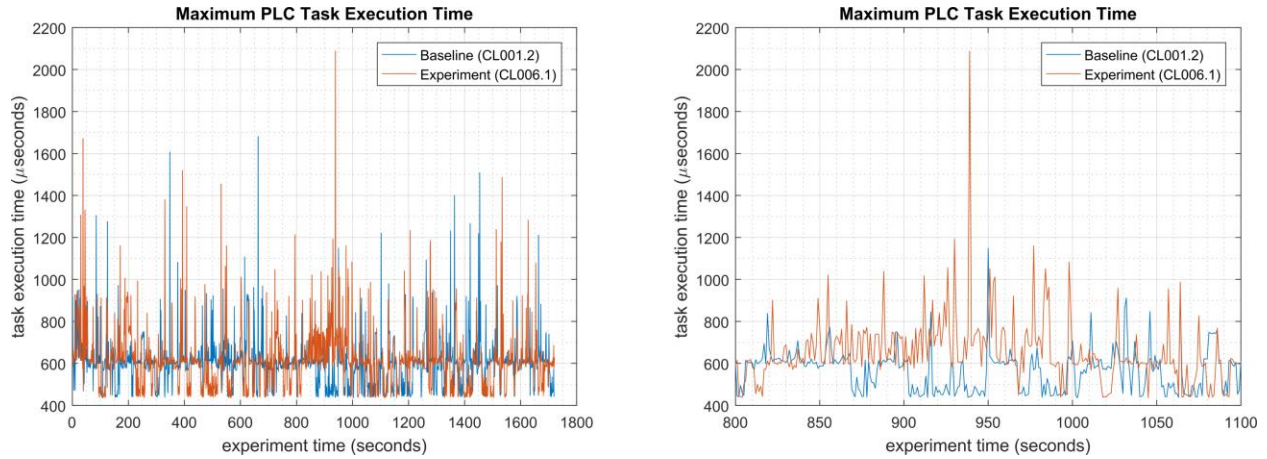


Figure 4-33 - Plots showing the maximum PLC task execution time during the experiment (left) and during the period of measured impact (right). While the Nessus tool was active, the PLC experienced periods of fluctuating and increased task execution time.

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

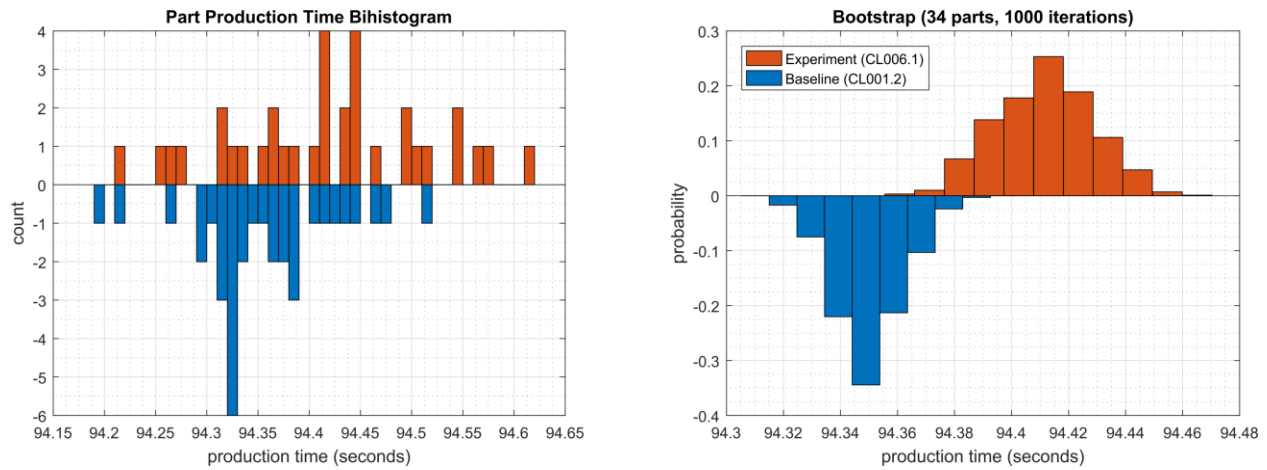


Figure 4-34 - Bihistograms showing the part production time (left) and estimated mean production time using the bootstrap method (right) using the measurements from baseline CL001.2 and experiment CL006.1.

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).

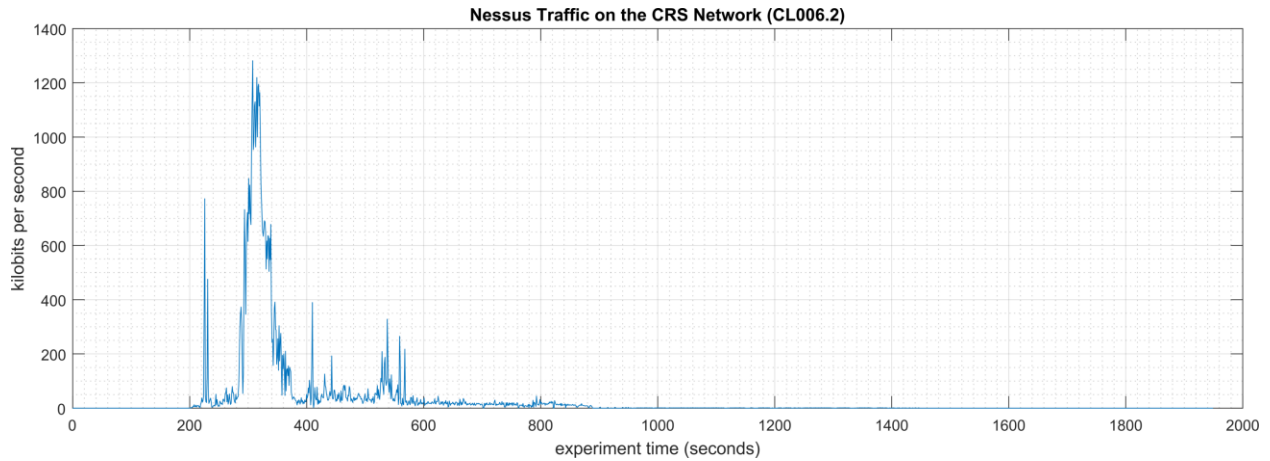


Figure 4-35 - Time series plot showing the quantity of network traffic transmitted and received by the Nessus tool during the experiment, with the most prominent activity from 200 to 600 seconds.

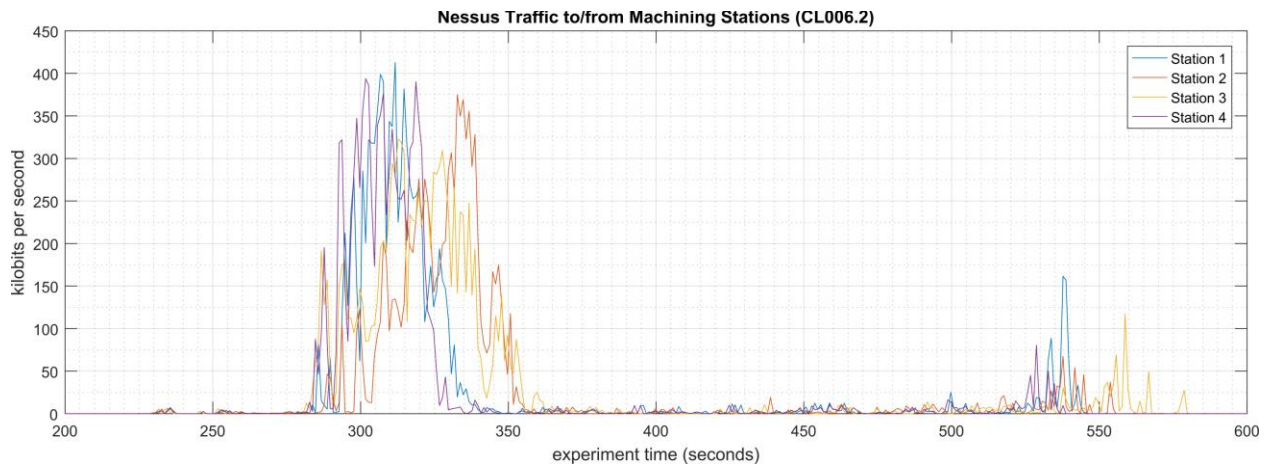


Figure 4-36 - Time series plot showing the quantity of network traffic transmitted and received by the Nessus tool and the machining stations during the experiment. Performance impacts to the PLC appear to correlate Nessus scanning the machining stations, likely due to the limited processing power of the devices.

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

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.

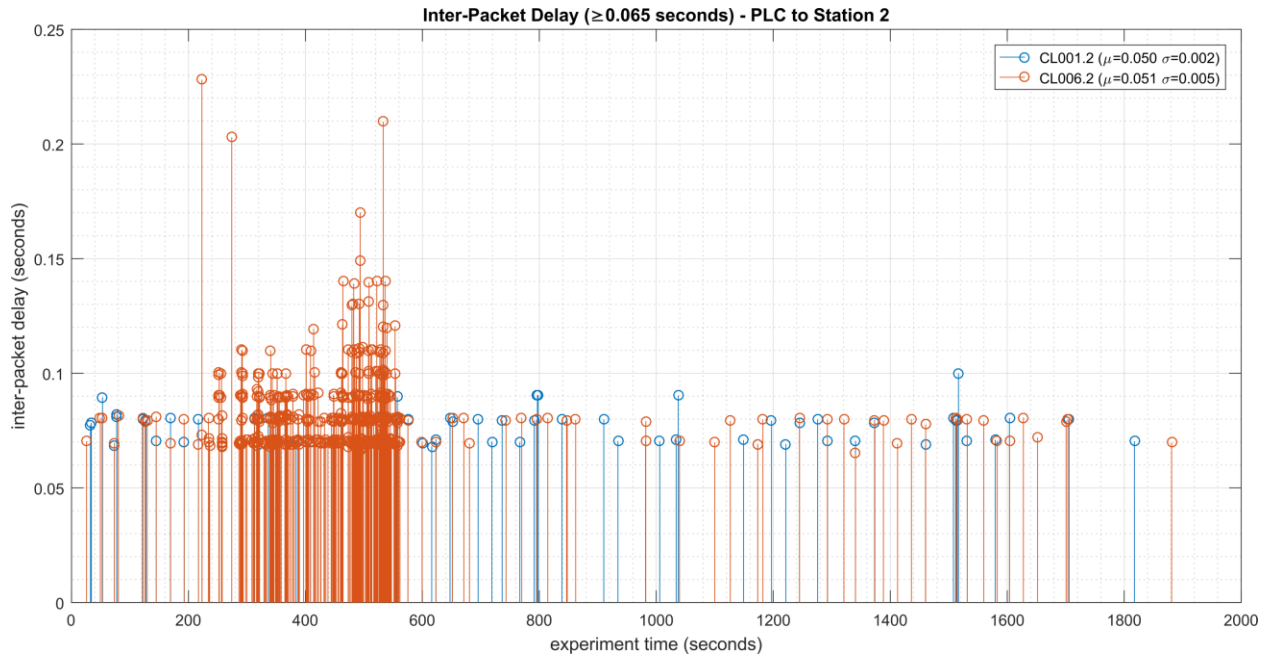


Figure 4-37 - Stem plot displaying the inter-packet delays (greater than or equal to 0.065 seconds) of Modbus TCP traffic between the PLC and Station 2, as measured during the baseline CL001.2 and experiment CL006.2. Note the large inter-packet delays between experiment time 250 to 600.

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.

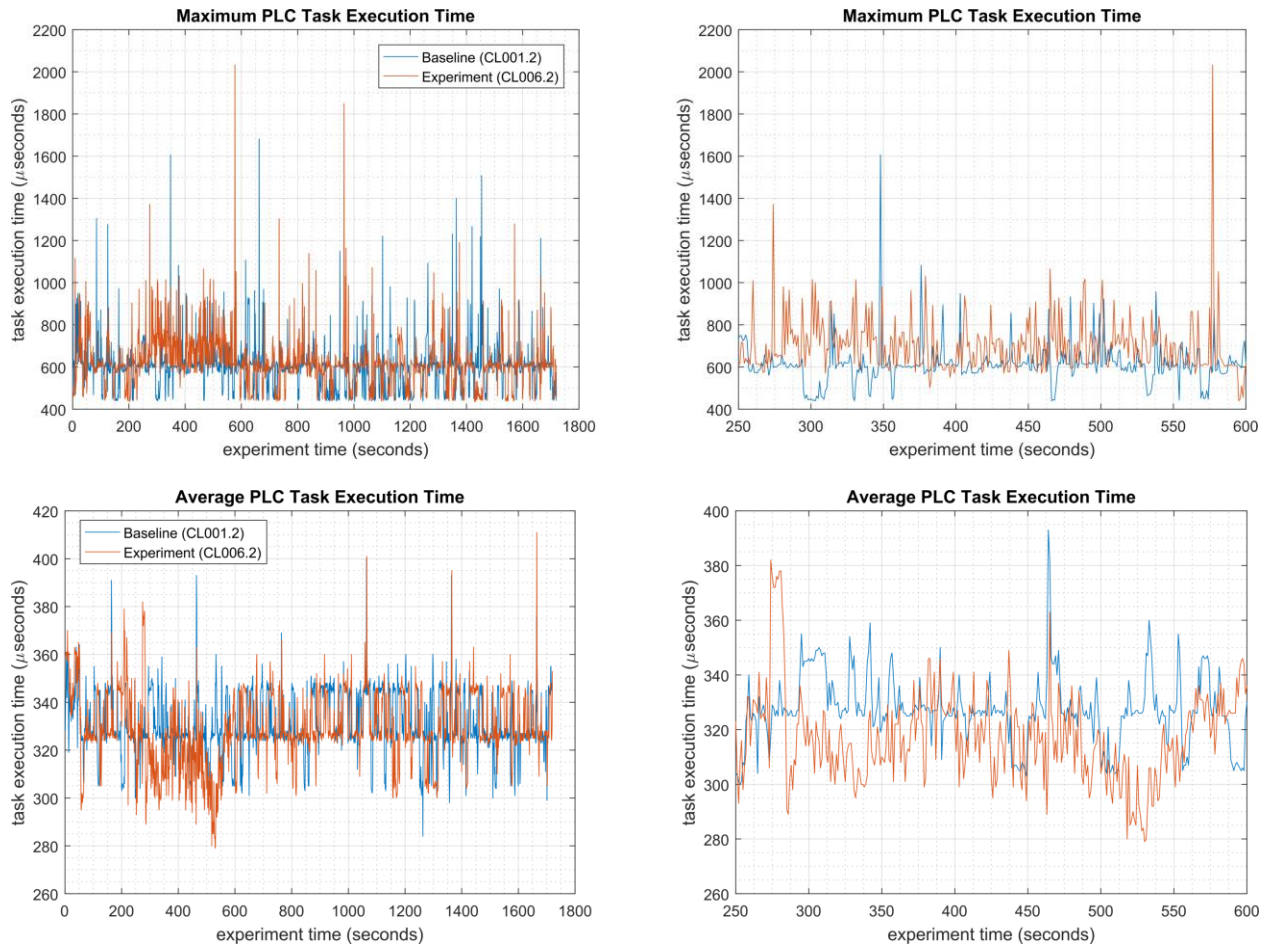


Figure 4-38 - Plots showing the maximum (top) and average (bottom) PLC task execution time during the experiment (left) and during the period of measured impact (right). While the Nessus tool was active, the PLC experienced periods of fluctuating and increased task execution time.

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

Since Nessus was configured to perform an authenticated scan, vController1 and vController2 both hosts experienced increased utilization of resources (i.e., CPU, disk, memory).

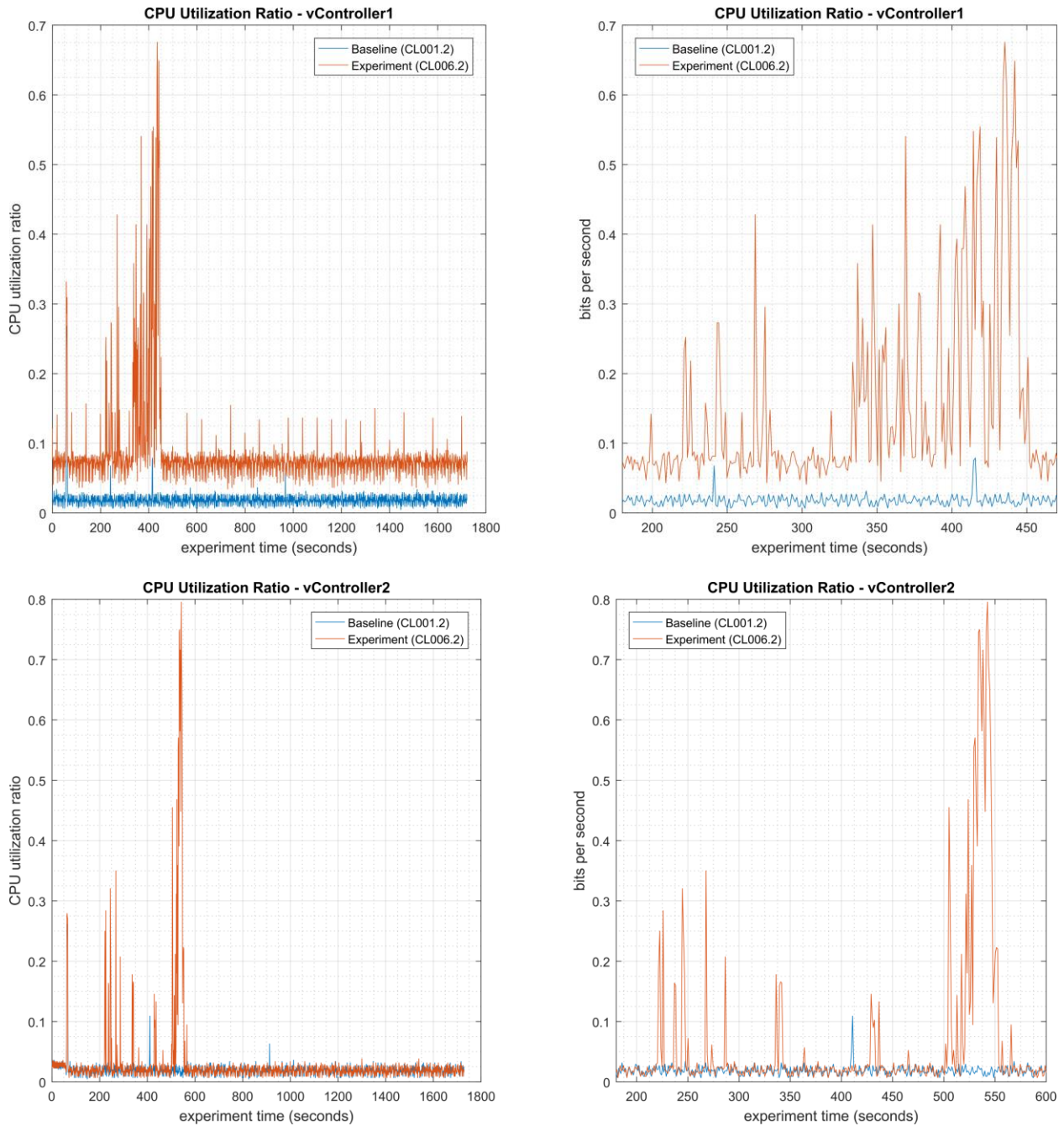


Figure 4-39 - Time series plots showing the CPU utilization of vController1 and vController2 during the CL006.2 experiment. vController1 experienced intermittent periods of increased CPU utilization from 200 sec. to 450 sec., with a maximum of 68% utilization. vController2 experienced intermitted periods of increased CPU from 225 sec. to 560 sec., and a maximum of 80% utilization.

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

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

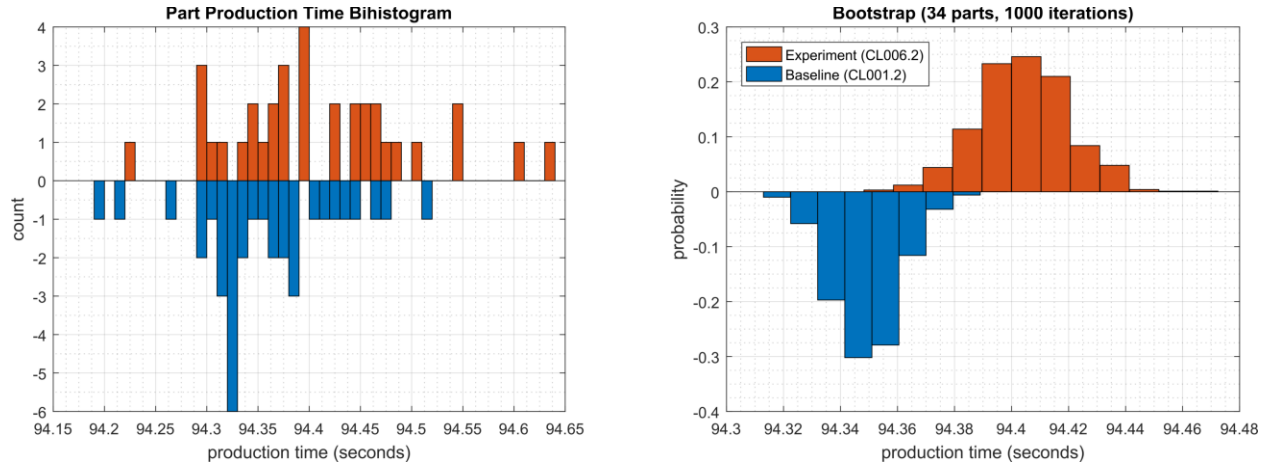


Figure 4-40 - Bihistograms showing the part production time (left) and estimated mean production time using the bootstrap method (right) using the measurements from baseline CL001.2 and experiment CL006.2.

4.10.7 Links 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 is a parser and reporting tool for Nessus, Burp, Nexpose OpenVAS and NCATS.⁸⁸

4.11.2 Technical Capabilities Provided by Solution

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

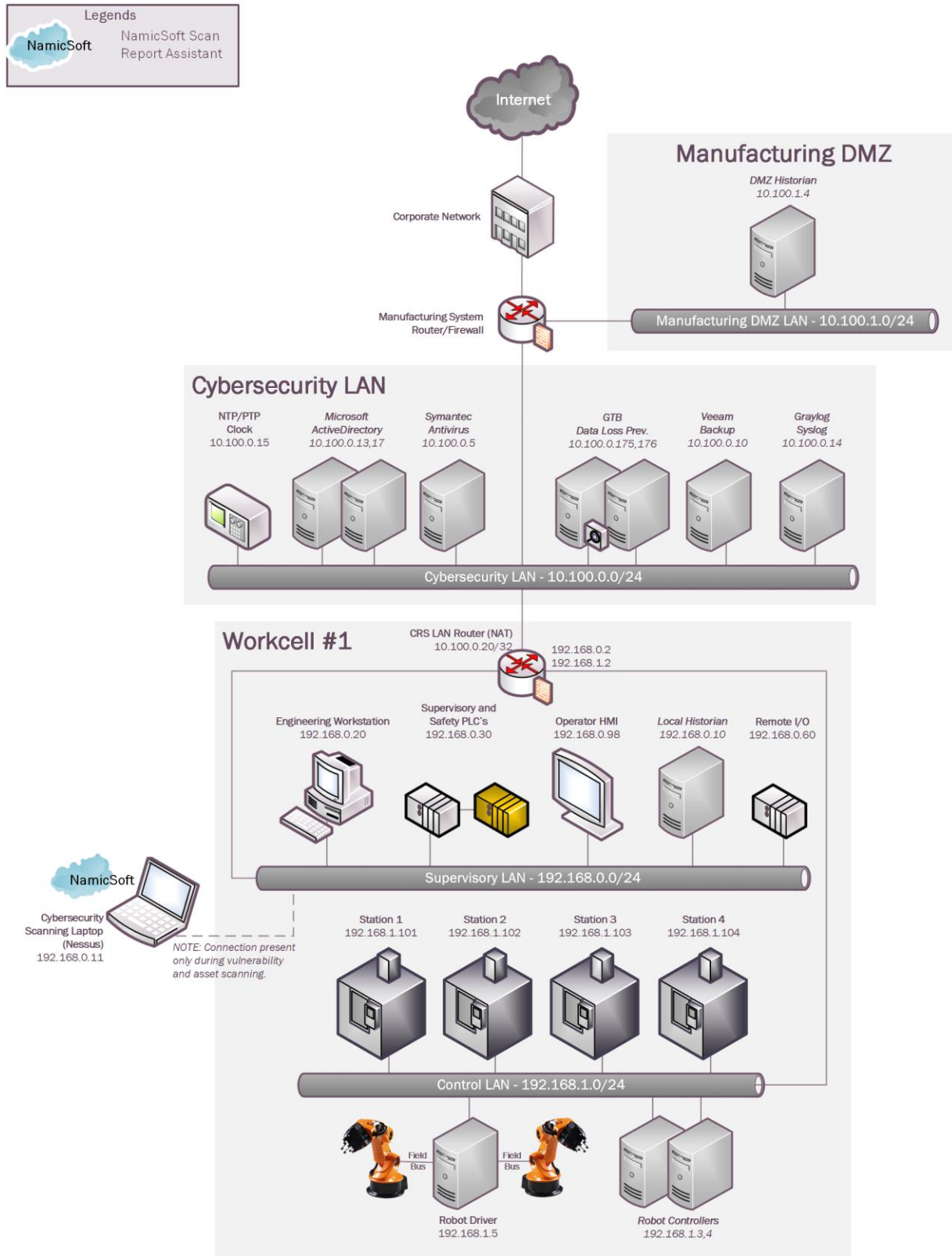
- Vulnerability Management

4.11.3 Subcategories Addressed by Implementing Solution

ID.RA-1, DE.CM-4, RS.MI-3

⁸⁸ <https://www.namicsoft.com/>

4.11.4 Architecture Map of Where Solution was Implemented



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

4.11.5 Installation Instructions and Configurations

Details of the solution implemented:

| Name | Version | Hardware Details |
|--|---------|---|
| NamicSoft Scan Report Assistant | 3.5.0 | Laptop with the following specs. <ul style="list-style-type: none"> • Processor: i7 • Memory: 16GB • Disk: 256GB • OS: Windows 7 Professional |

4.11.5.1 Environment Setup

1. NamicSoft was installed on a temp. Windows 10 laptop setup on a need-by basis.
2. The guest OS IP information of this server was set as follows:

```
IP address: 192.168.0.11
Gateway: 192.168.0.2
Subnet Mask: 255.255.255.0
```

4.11.5.2 Setup Instructions

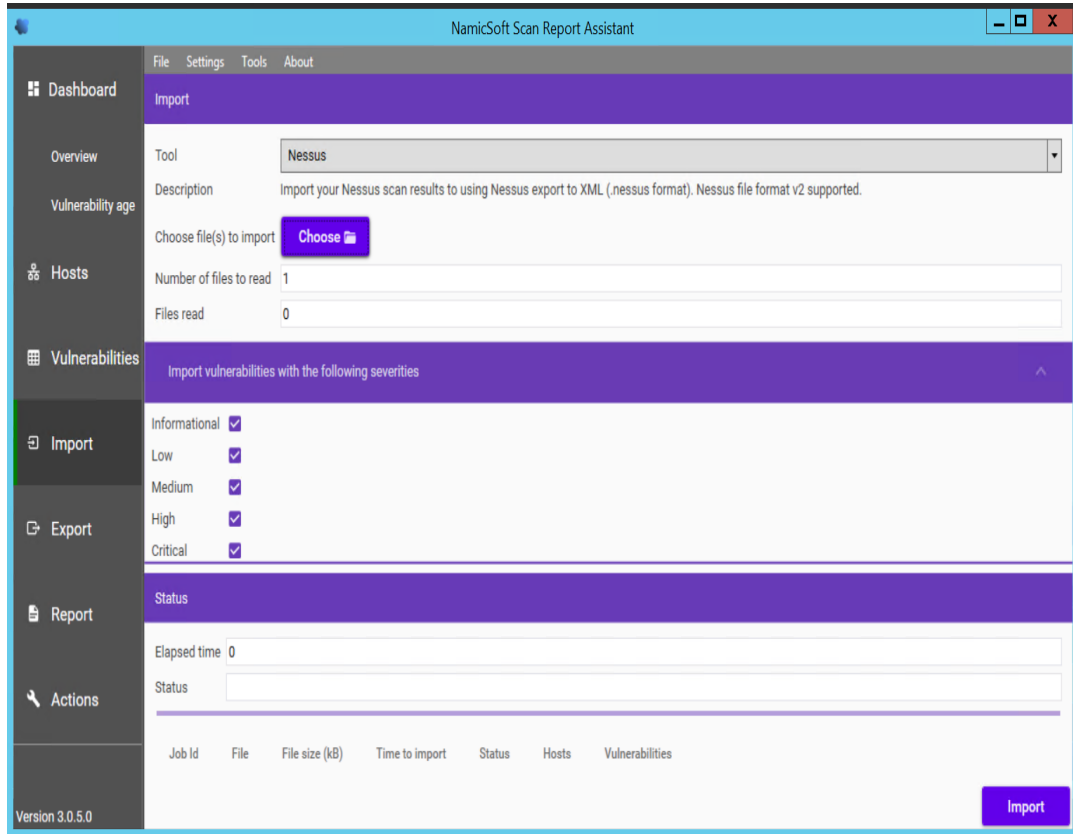
1. Download NamicSoft⁸⁹
2. Run the installer on a Windows PC. NamicSoft is currently supported on 64-bit Windows with .Net Framework 4.5 installed
3. Launch the program by double clicking its Desktop icon. If using for the first time, the installation will prompt for a license file. If a license is not entered, it runs in free mode. The free mode is limited to five hosts.

Note: The software is tied to a Windows user account. Any changes made by a user would not be visible to a different user logging in to the same system.

⁸⁹ <https://www.namicsoft.com>

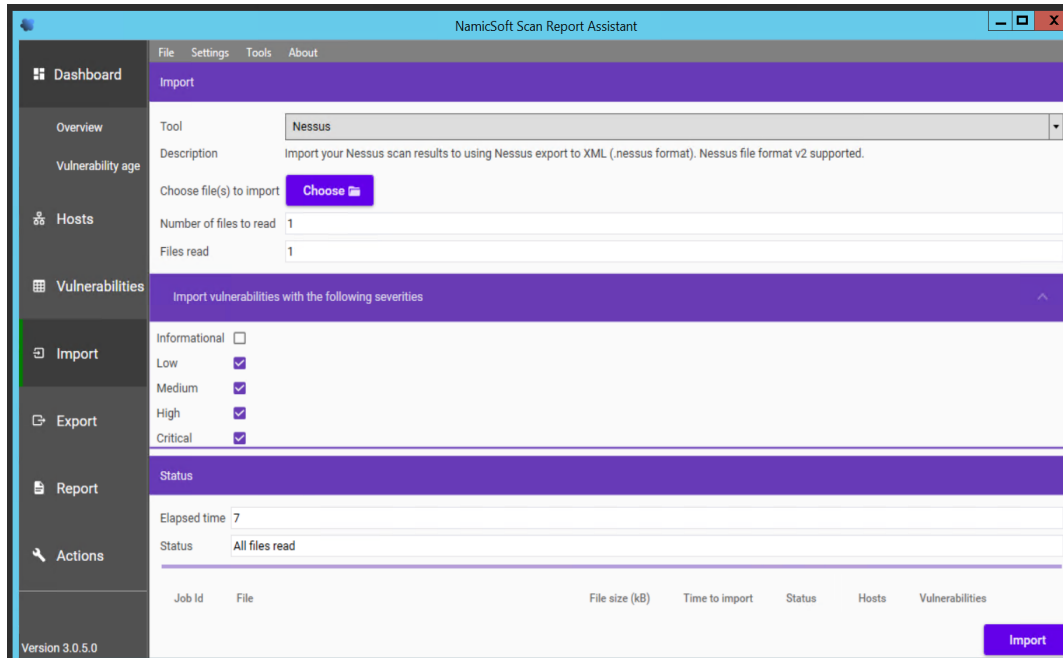
4.11.5.3 Configuration for Reporting Nessus Scans

1. Export a Scan Report of **Nessus** format from the Nessus web interface.
2. Launch NamicSoft Report Assistant. Click **Import** on left-side explorer, select **Nessus**
3. Click on **Choose** button to import files



4. Browse to the Nessus scan report. Under **Import Vulnerabilities with following vulnerabilities**, Check / Uncheck whichever severity of vulnerabilities you wish to be included in the report and click **Import**.

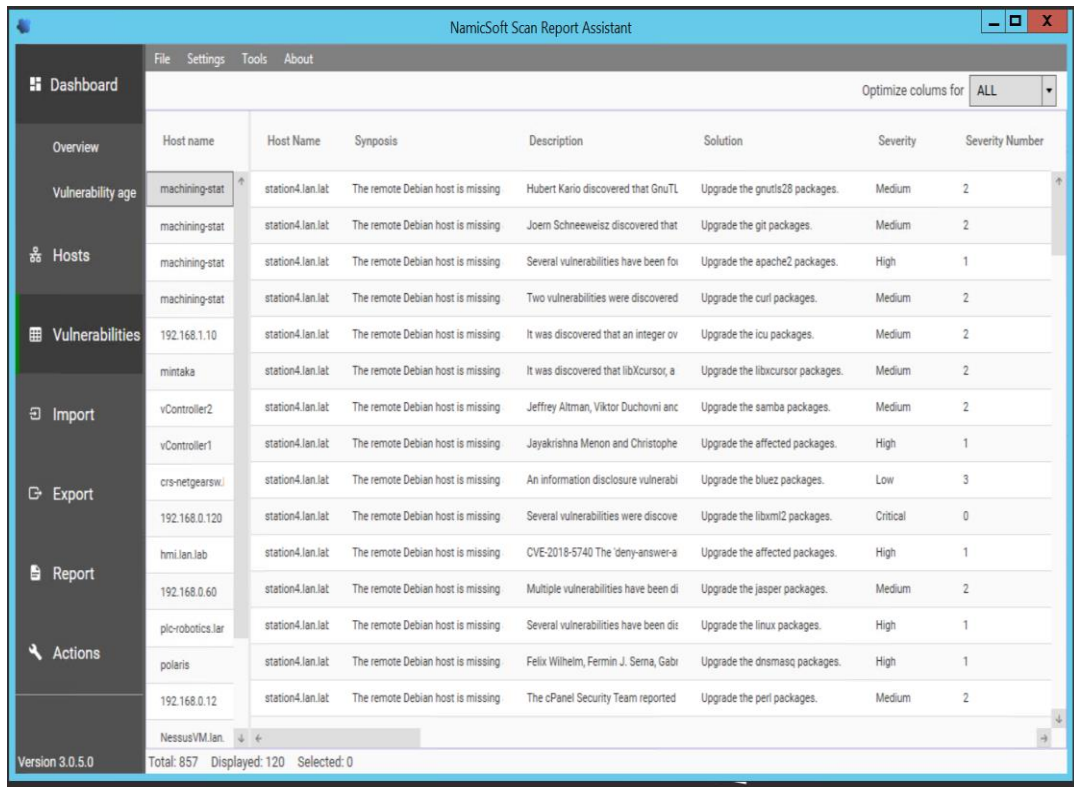
For instance, the image below shows **Informational** types being excluded and other severity levels such as **High, Critical, Medium Low** being selected. When the **Import** finishes, the Status bar should display **All files read**.



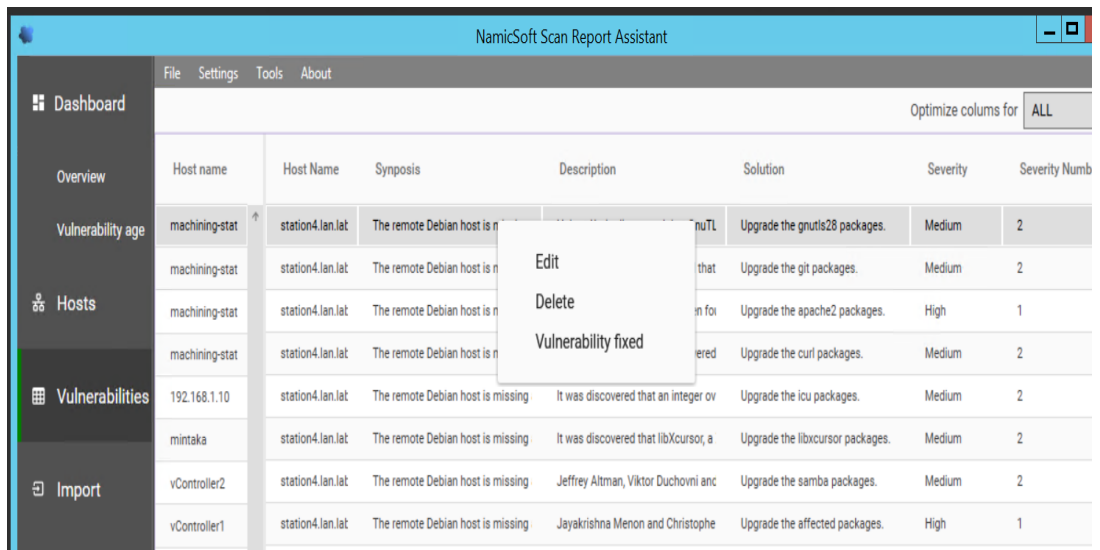
5. Click the **Hosts** page upon completion of Import, to view all the hosts level summary. Similarly, clicking on **Vulnerabilities** page shows all the vulnerabilities

| Name | IP | Operating System | MAC | NetBIOS | FQDN | System Type | Report Ni |
|----------------------|---------------|--|---|---------------------|----------------------|-----------------|------------|
| machining-station-4 | 192.168.1.104 | Linux Kernel 4.4.54-ii-r93 on Debian 8.7 | B0:D5:CC:F4:26:EC B0:D5:CC:F4:26:EE B0:D5:CC:F4:26:F1 | machining-station-4 | station4.lan.lab | general-purpose | Robotics_E |
| machining-station-3 | 192.168.1.103 | Linux Kernel 4.4.54-ii-r93 on Debian 8.7 | B0:D5:CC:FA:7A:43 B0:D5:CC:FA:7A:45 B0:D5:CC:FA:7A:48 | machining-station-3 | station3.lan.lab | general-purpose | Robotics_E |
| machining-station-2 | 192.168.1.102 | Linux Kernel 4.4.54-ii-r93 on Debian 8.7 | B0:D5:CC:FE:6E:B1 B0:D5:CC:FE:6E:B3 B0:D5:CC:FE:6E:B6 | machining-station-2 | station2.lan.lab | general-purpose | Robotics_E |
| machining-station-1 | 192.168.1.101 | Linux Kernel 4.4.54-ii-r93 on Debian 8.7 | B0:D5:CC:FA:70:C9 B0:D5:CC:FA:70:CB B0:D5:CC:FA:70:CE | machining-station-1 | station1.lan.lab | general-purpose | Robotics_E |
| 192.168.1.10 | 192.168.1.10 | | | | | | Robotics_E |
| mintaka | 192.168.1.5 | Linux Kernel 3.13.0-35-generic on Ubuntu 12.04 | A0:CE:C8:1F:BD:99 C8:1F:66:C8:6A:EB C8:1F:66:C8:6A:EC | mintaka | mintaka.lan.lab | general-purpose | Robotics_E |
| vController2 | 192.168.1.4 | Linux Kernel 3.19.0-25-generic on Ubuntu 14.04 | 00:15:5D:16:AC:03 | vController2 | vcontroller2.lan.lab | general-purpose | Robotics_E |
| vController1 | 192.168.1.3 | Linux Kernel 3.19.0-25-generic on Ubuntu 14.04 | 00:15:5D:16:AC:02 | vController1 | vcontroller1.lan.lab | general-purpose | Robotics_E |
| crs-netgears.lan.lab | 192.168.0.239 | Linux Kernel 2.4 | A0:63:91:70:D5:6F A0:63:91:70:D5:71 | | crs-netgears.lan.lab | general-purpose | Robotics_E |
| 192.168.0.120 | 192.168.0.120 | | C8:1F:66:C8:65:F9 | | | | Robotics_E |
| hmi.lan.lab | 192.168.0.98 | | 00:05:E4:03:7C:3B | | hmi.lan.lab | | Robotics_E |
| 192.168.0.60 | 192.168.0.60 | AIX 5.2 | 00:30:DE:00:C4:3C | | | general-purpose | Robotics_E |

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

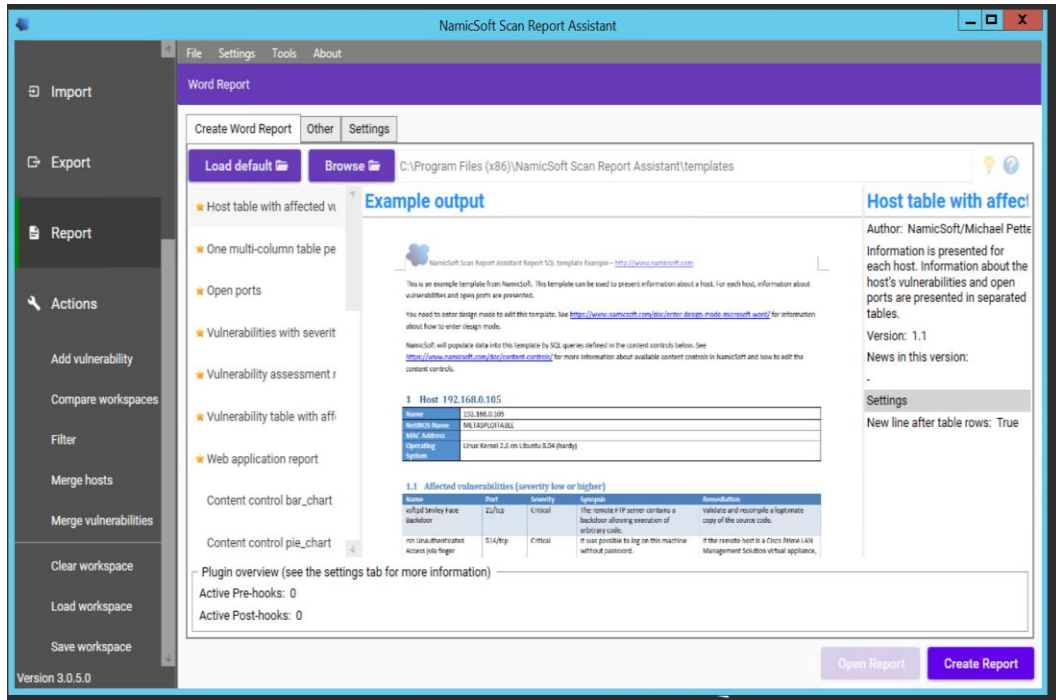


6. (Optional)Mark a Vulnerability as **Fixed**, by *Vulnerability* >> Right Click >> **Fixed**.

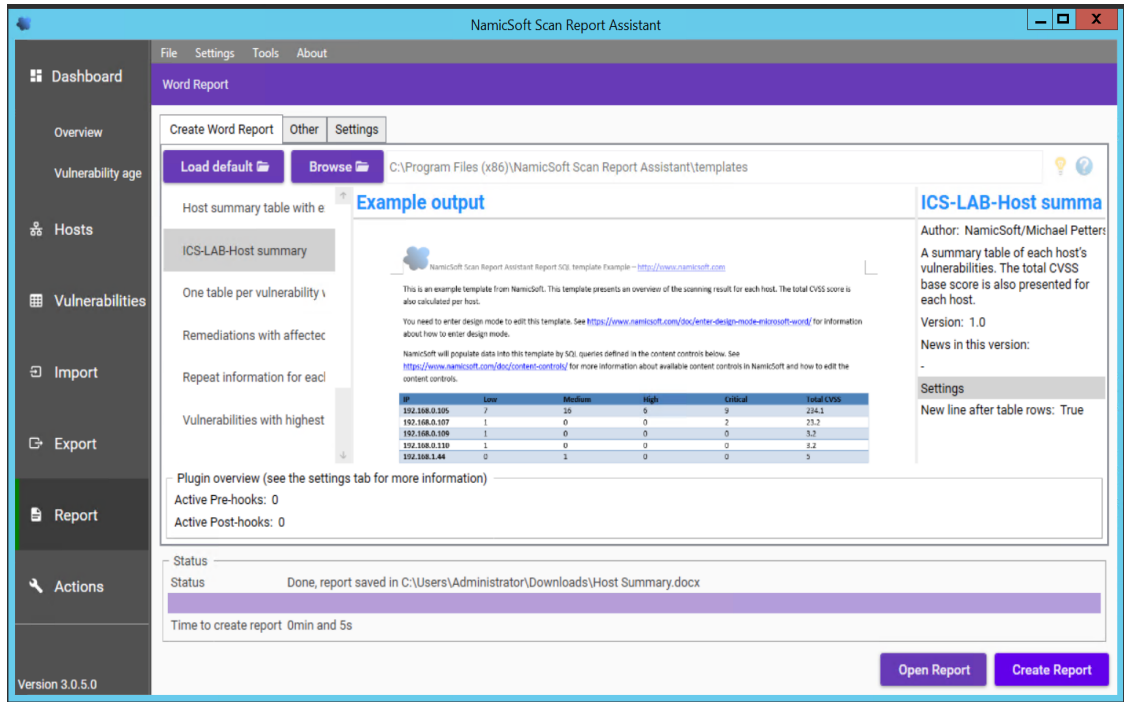


7. Click on **Save Workspace**. Ensure to Save your workspace after every change made. When running NamicSoft the next time, you can load this saved workspace file.

- Click on **Report** to generate one. Select from 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**.



- Click **Open Report** to view the report.

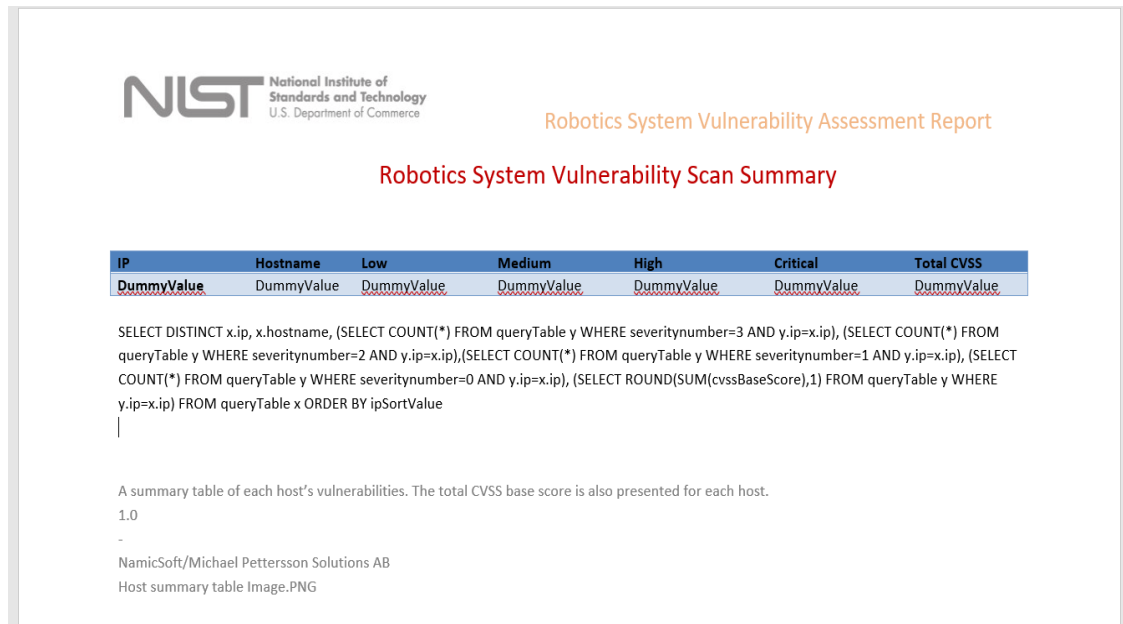


This publication is available free of charge from: <https://doi.org/10.6028/NIST.IR.8183A-3>

4.11.5.4 Creating Custom Template

1. Copy one of the existing template files located under *C:\Program Files(x86)\NamicSoft Scan Report Assistant\templates* and save it to a different folder.
2. Open the copied file in MS Word to begin editing. The image below shows a customized template file created for this work-cell. This report generates a summary of hosts and their respective vulnerabilities based on the Severity level.

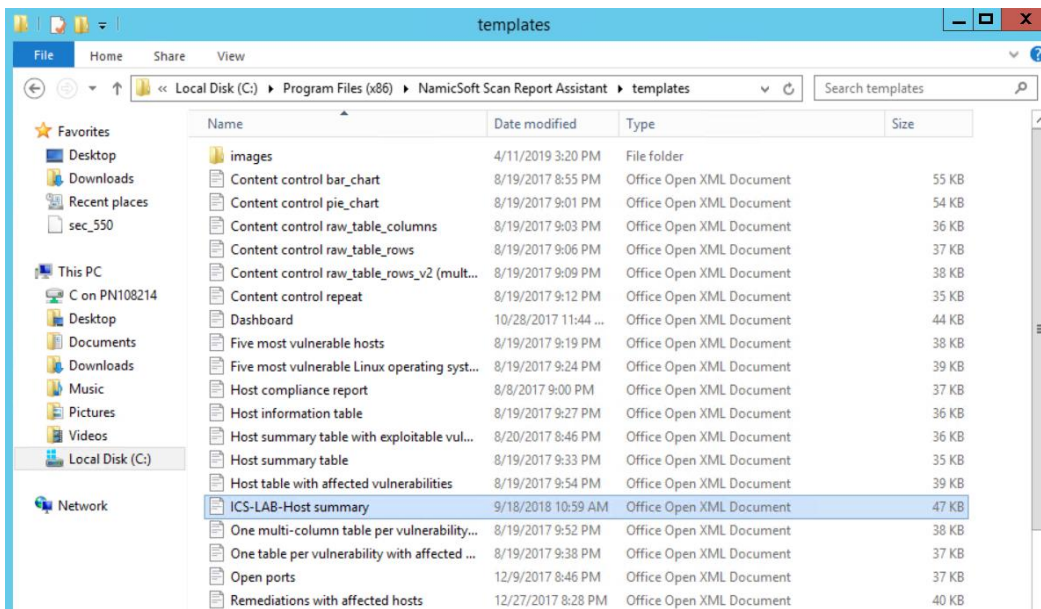
Custom reports⁹⁰ can also be created.



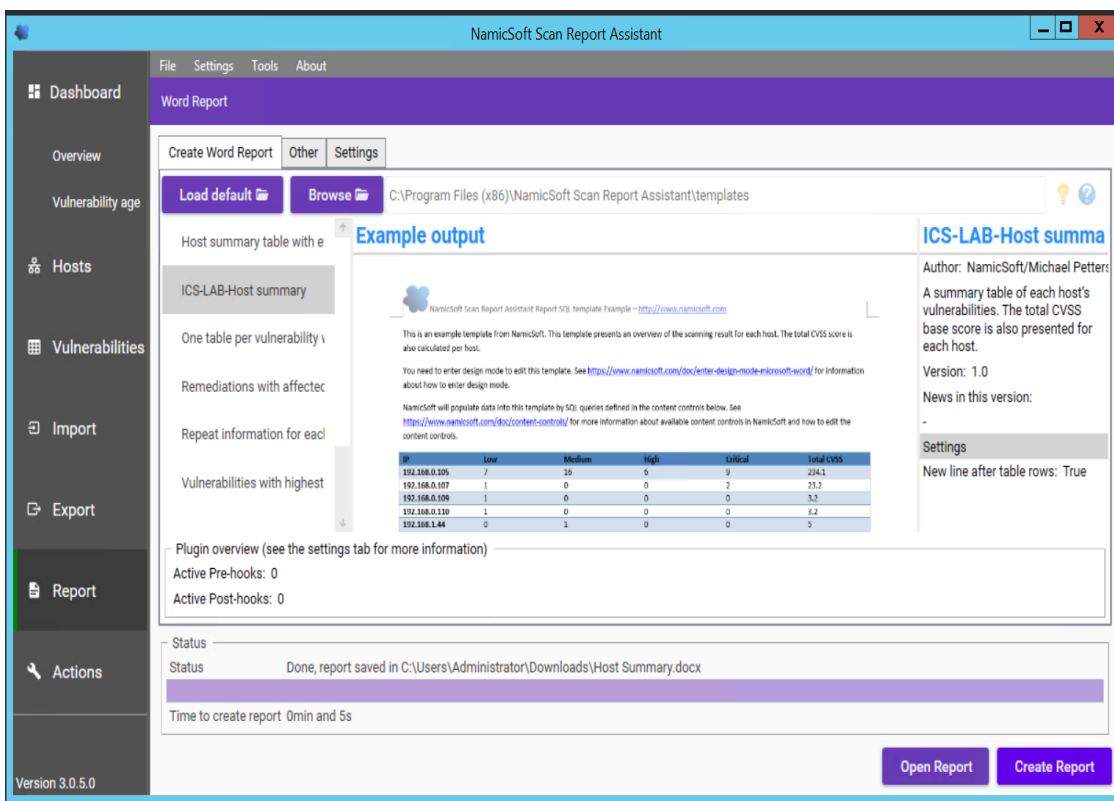
3. Save your changes and give the file a name.

⁹⁰ <https://www.namicsoft.com/doc/content-controls/>

- Copy this file back to the *templates* directory on the NamicSoft machine. For instance, the image below 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**.



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

6. Review the output to confirm your changes.

The screenshot shows a report titled "Robotics System Vulnerability Assessment Report" with a sub-section "Robotics System Vulnerability Scan Summary". The table below lists various IP addresses and their corresponding vulnerability counts across four severity levels: Low, Medium, High, and Critical, along with a Total CVSS score.

| 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-netgears.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 |

7. (Optional) Use the **Compare Workspaces** feature under Action Menu to report on Vulnerabilities remediated based off the previous vulnerability scans as follows

- a. Load Nessus result from your previous scan. Save as a **workspace**.
- b. Clear the workspace in the GUI (or restart NamicSoft)
- c. Load Nessus results from the latest scan
- d. Open **Actions > Compare workspaces**. Choose **Compare** with current workspace and point Workspace 2 to your workspace saved earlier.
- e. Choose **Excel output file (target)**
- f. 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.

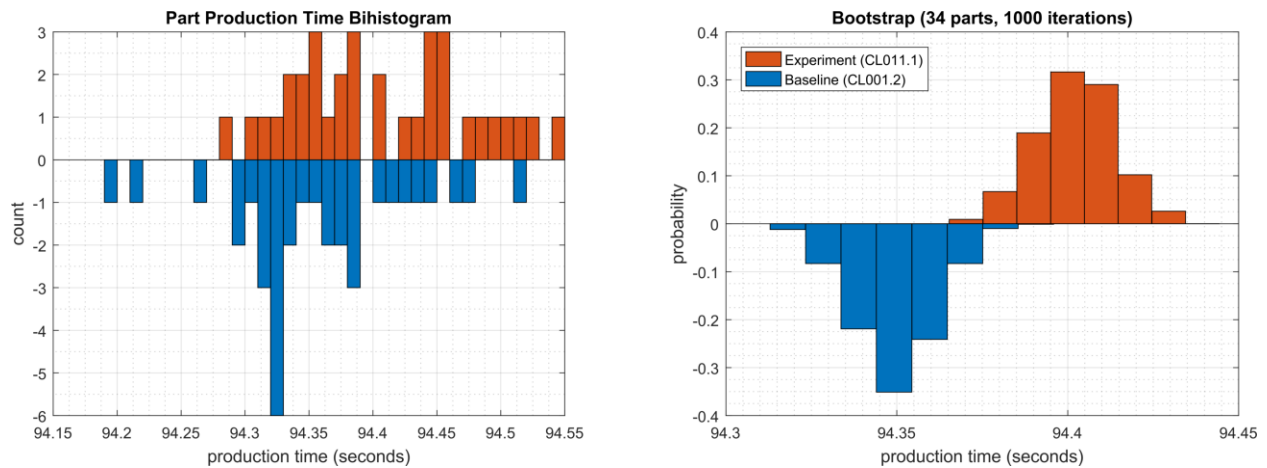


Figure 4-41 - Bihistograms showing the part production time (left) and estimated mean production time using the bootstrap method (right) using the measurements from baseline CL001.1 and experiment CL011.1.

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).

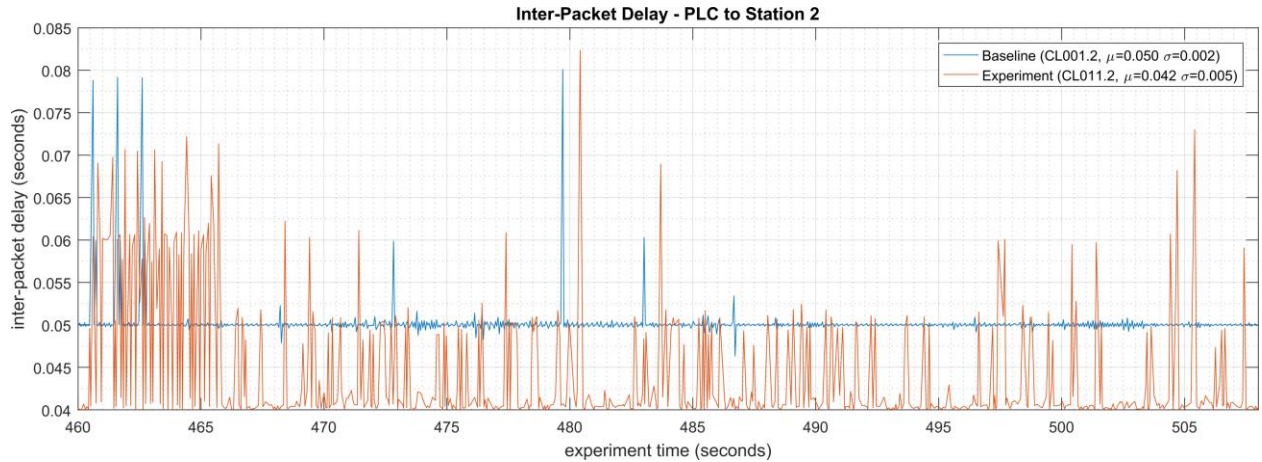


Figure 4-42 - Time series plot displaying the inter-packet delay of Modbus TCP traffic between the PLC and Station 2, as measured during the baseline CL001.2 and experiment CL011.2. Note the relatively constant baseline average delay of around 0.050 sec., while the experimental delay is decreased to an average of 0.042 sec. with large deviations.

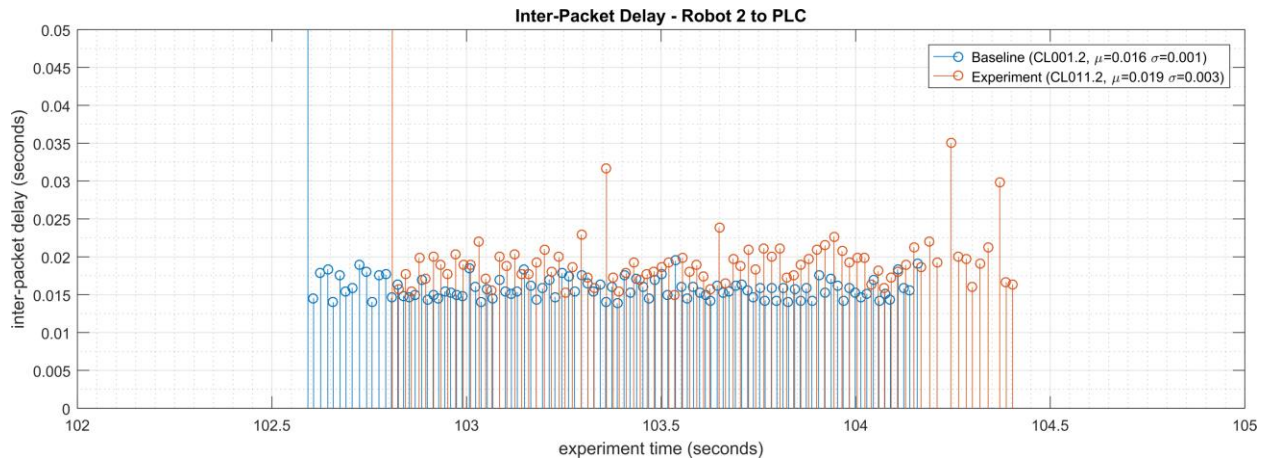


Figure 4-43 - Stem plot displaying the inter-packet delay of Modbus TCP traffic between Robot 2 and the PLC, as measured during the baseline CL001.2 and experiment CL011.2. Note the relatively constant baseline average delay of around 0.016 sec., while the experimental delay is increased to an average of 0.019 sec. and relatively unstable.

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

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.

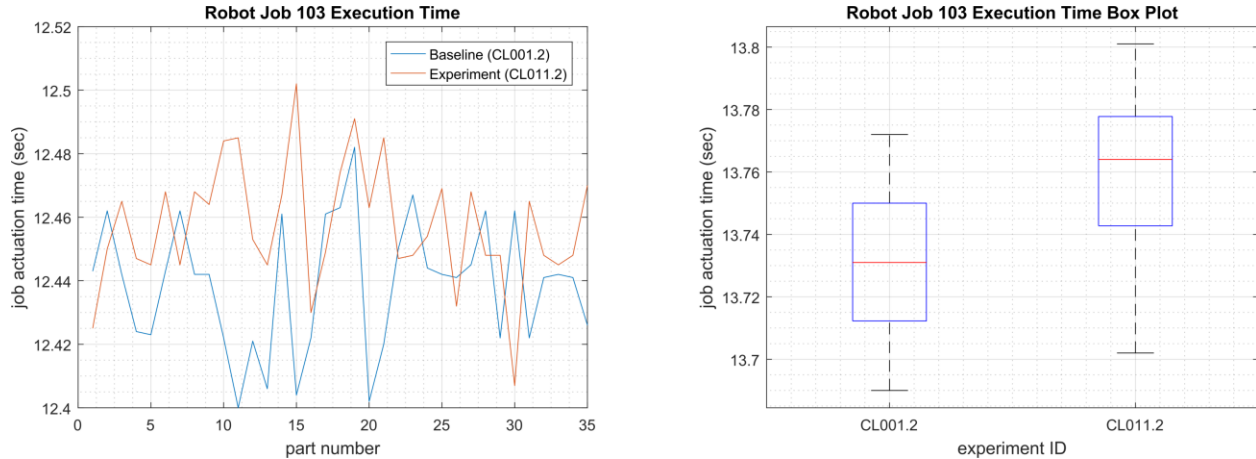


Figure 4-44 - Time-series (left) and boxplot (right) showing the job actuation times for Job 103 during the CL001.2 baseline and CL011.2 experiment.

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 μ sec. during the baseline to around 690 μ sec., with the maximum task execution time now consistently exceeding 2000 μ sec. (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.

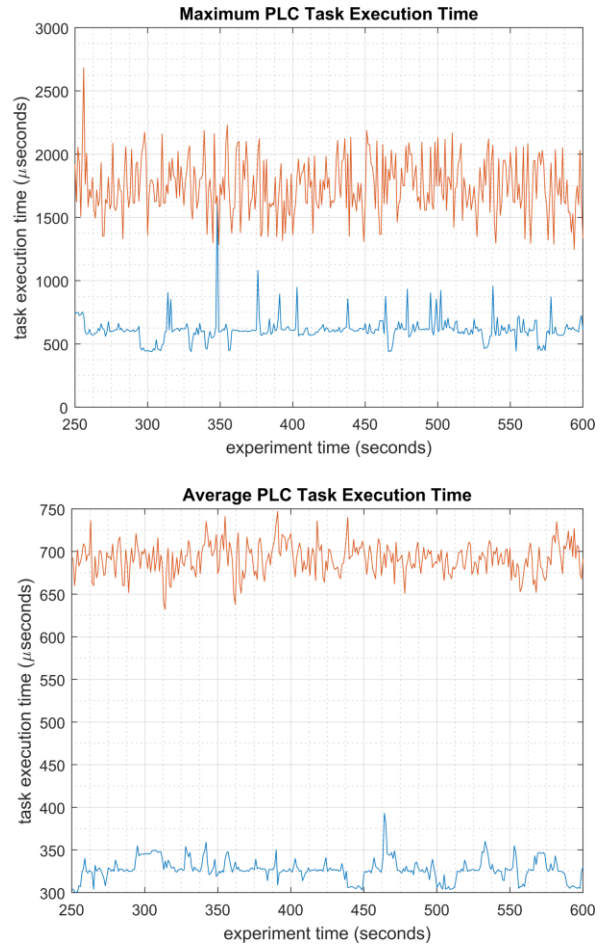
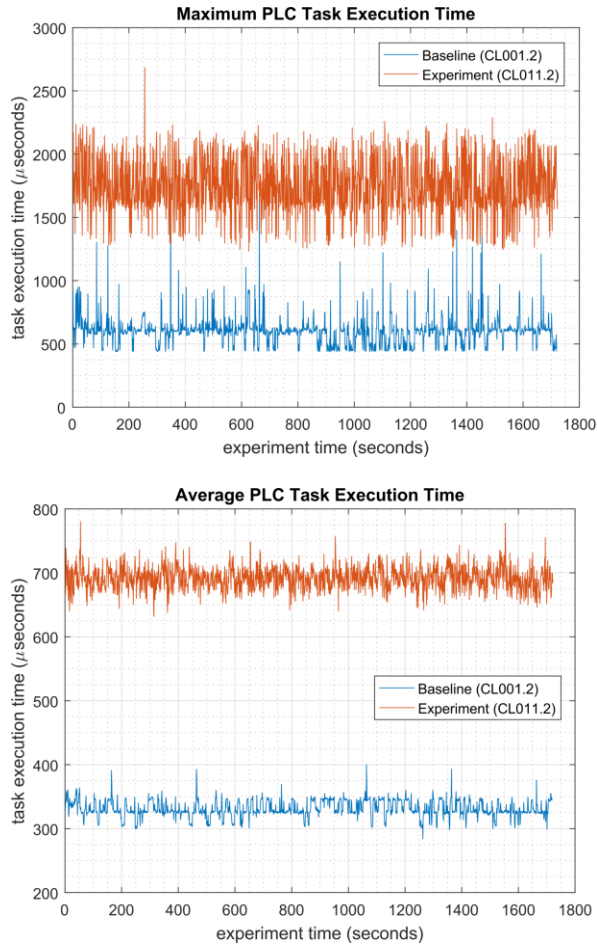


Figure 4-45 - Plots showing the maximum (top) and average (bottom) PLC task execution time during the experiment (left) and during the period of measured impact (right). The PLC task execution time characteristics changed considerably after patches were applied to the PLC and other ICS devices.

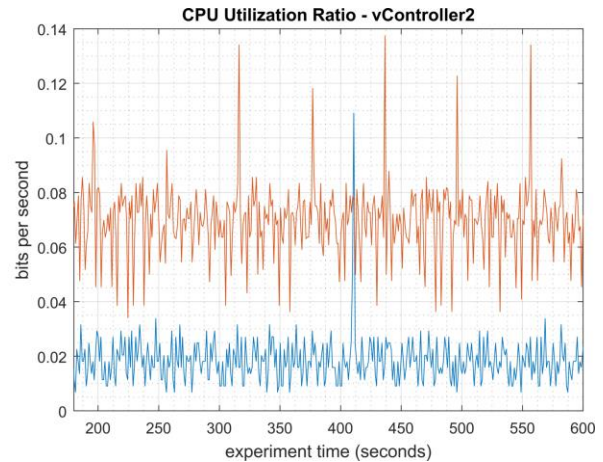
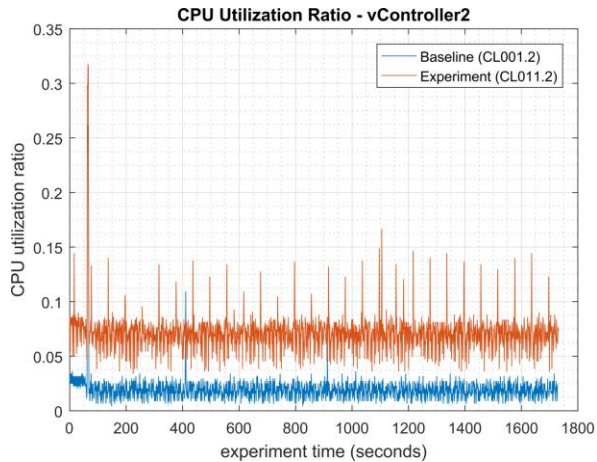


Figure 4-46 - Time series plots showing the CPU utilization ratio for vController2 during the CL011.2 experiment and the CL001.2 baseline (left), and a detailed view of the same data (right).

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

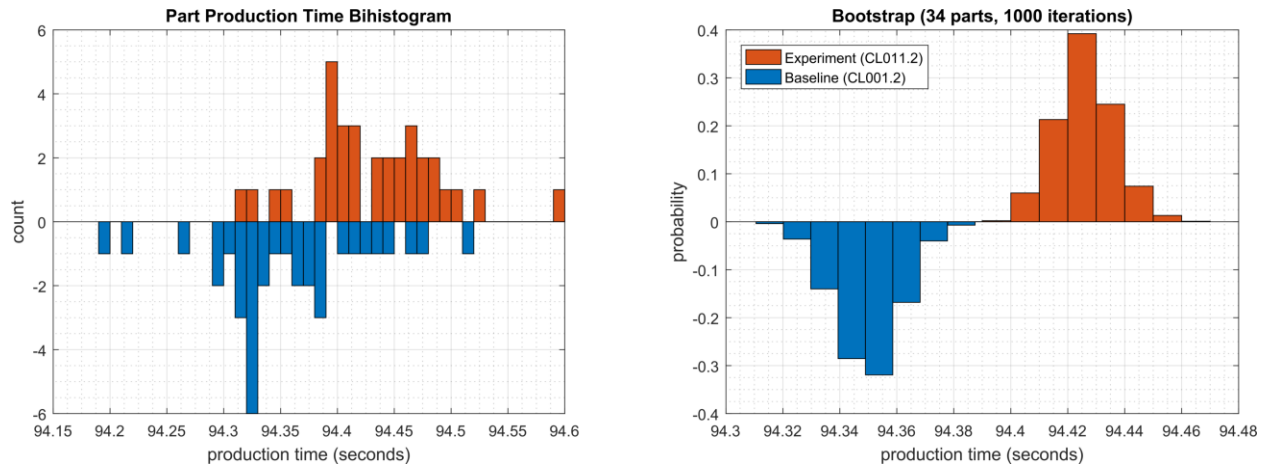


Figure 4-47 - Bihistograms showing the part production time (left) and estimated mean production time using the bootstrap method (right) using the measurements from baseline CL001.2 and experiment CL011.2.

4.11.7 Links to Entire Performance Measurement Data Set

- [CL011.1-PatchesNetworkHardware.zip](#)
- [CL011.2-PatchesServersICSDDevices.zip](#)

4.12 GTB Inspector

4.12.1 Technical Solution Overview

GTB Inspector by GTB Technologies is a Data Loss Prevention (DLP) solution that has the ability to detect, log, and block network traffic trying to leave the network. Inspector detects and blocks FTP, Email, HTTP, HTTPS (SSL/TLS), Finger Printed files, USB protection, and other configured exfiltration methods. Inspector is the main component that analyzes all network traffic. GTB Central Console is the device Inspector reports back to. Central Console allows for groups and escalation paths depending on the alerting required.

Points to consider:

- All DLP products have a high cost to implement.
- All DLP products require configuration that can be extensive.

4.12.2 Technical Capabilities Provided by Solution

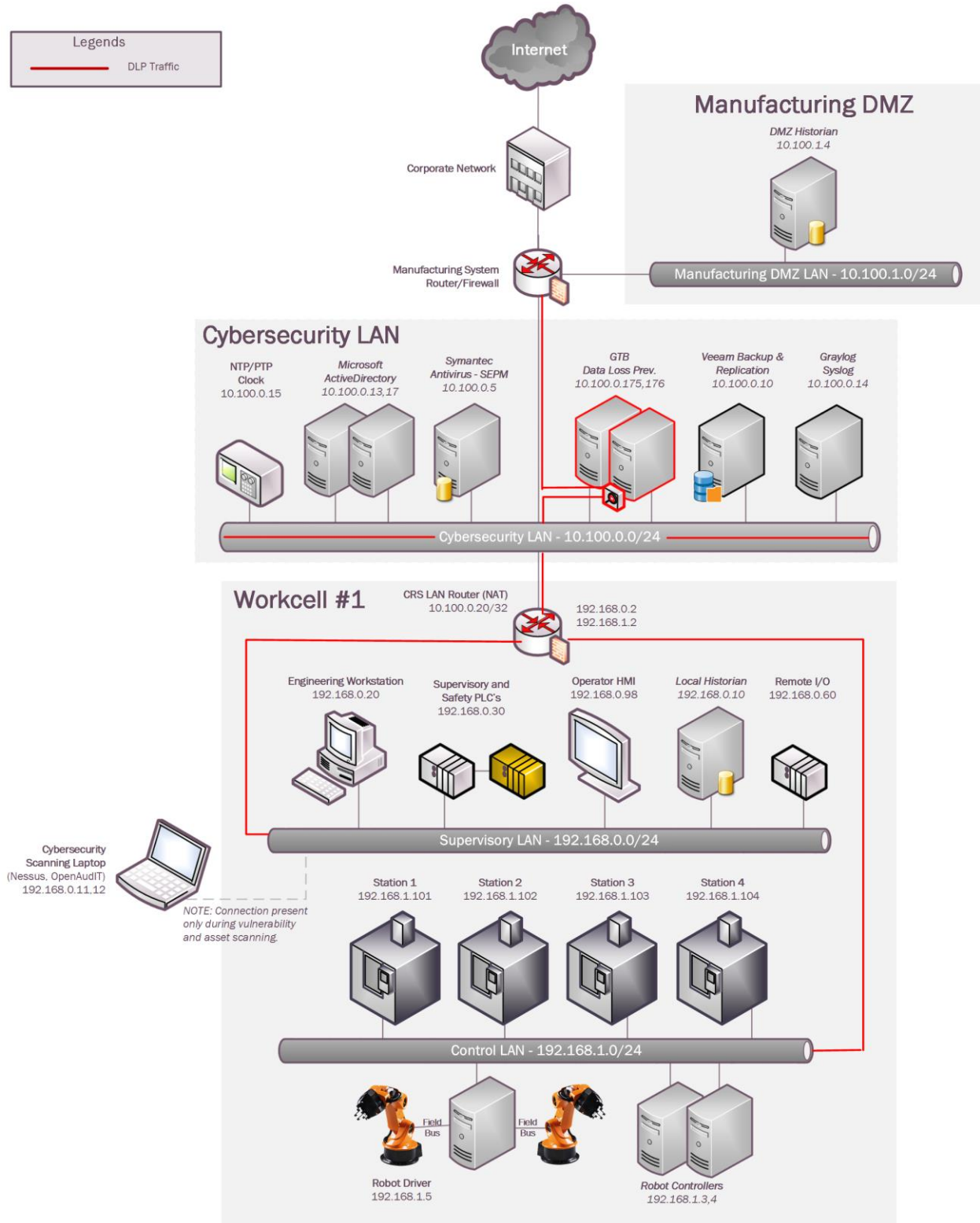
GTB Inspector provides components of the following Technical Capabilities described in Section 6 of Volume 1:

- Data Loss Prevention

4.12.3 Subcategories Addressed by Implementing Solution

PR.DS-5

4.12.4 Architecture Map of Where Solution was Implemented



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

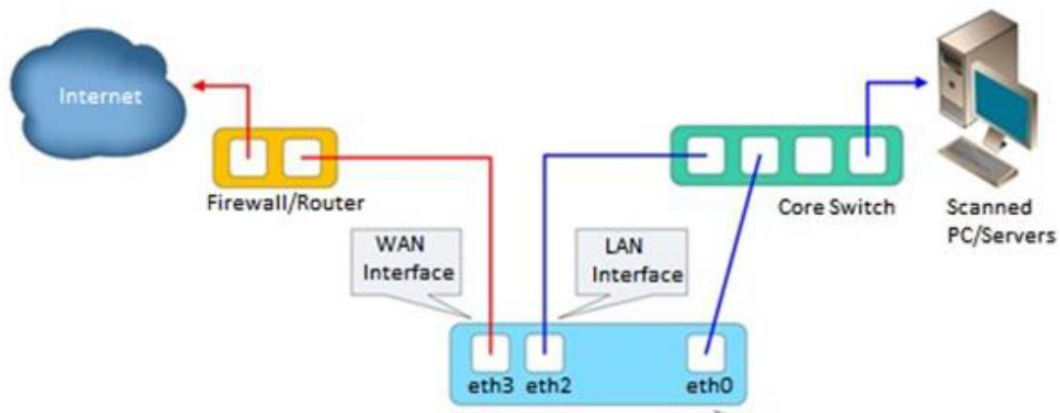
4.12.5 Installation Instructions and Configurations

Details of the solutions implemented:

| Name | Version | Purpose | Hardware Details |
|----------------------------|---------|---|--|
| GTB Inspector | 15.6.0 | Network DLP | Hyper-V Virtual Machine (Generation 1): <ul style="list-style-type: none"> Processors: 2 virtual cores Memory: 6 GB Disk space: 20 to 30GB (As per the Virtual Appliance file provided by the vendor) Network: 3 network adapters OS: CentOS Linux 7 Core |
| GTB Central Console | 15.6.0 | Central Reporting and Management for all GTB products | Hyper-V Virtual Machine (Generation 1): <ul style="list-style-type: none"> Processors: 2 virtual cores Memory: 6 GB Disk space: 20 to 30GB (As per the Virtual Appliance file provided by the vendor) Network: 1 network adapter OS: CentOS Linux 7 Core |

4.12.5.1 Environment Setup

1. Two virtual machines were setup in the Cybersecurity LAN network of the workcell, using the ISO image provided by the vendor. Their hardware specifications are described in the table above.
2. The GTB Inspector server was deployed in **Bridge [Inline]** mode as per the official diagram provided by the vendor which is shown below. For additional details, refer to the official install guide.



3. The guest OS networking information on the VM's was set as follows:

```
Virtual Machine: GTB-Inspector
Network interface:eth0
IP address: 10.100.0.175
Gateway: 10.100.0.1
Subnet Mask: 255.255.255.0
DNS:10.100.0.17
Network interface:eth2->connected to Monitor Port1 of a Network Aggregator
device
Network interface:eth3->connected to WAN interface of our Cisco-ASA firewall.
```

```
Virtual Machine: GTB-Central
Network interface:eth0
IP address: 10.100.0.176
Gateway: 10.100.0.1
Subnet Mask: 255.255.255.0
DNS:10.100.0.17
```

4.12.5.2 Setting up the GTB Central Console

1. Download the ISO file of GTB Central Console and install guides⁹¹
2. Setup the virtual machine using the ISO on your preferred Hypervisor.
3. Perform initial configuration such as creating a DNS record, assigning a Static IP address to the server, etc.
4. Login to the Central Console Web UI using the default credentials. Click **Administration** > **Licensing** to upload the license file. Restart once done.
5. Click **DLP Setup** tab > **Network** to enter the network settings.
6. Click **DLP Setup** tab > **LDAP** to configure AD server details.
7. Click **DLP Setup** tab > **Email & Alerts.** to configure smtp server settings.
8. Click **DLP Setup** tab > **Date & Time** > Enter **NTP** Server details.
9. Click **DLP Setup** tab > **SIEM** > Enter the IP address of Syslog / SIEM server

4.12.5.3 Setting up the GTB Inspector

1. Download the ISO file of GTB Inspector and install guides⁹²
2. Setup the virtual machine using the ISO files on your preferred Hypervisor.
3. Perform initial configuration such as creating DNS records, assigning Static IP address, setting up the LAN and WAN interfaces for the Inspector server, etc. For detailed instructions, refer to the GTB product install guides.
4. Login to the Inspector server Web UI using the default credentials as provided. Click **Administration** > **Licensing** to upload the license file. Restart once done.

⁹¹ <https://gttb.com/downloads/>

⁹² <https://gttb.com/downloads/>

5. Click **Configuration** tab > **Email Alerts**, to configure smtp server settings.
6. Click **Configuration** tab > **LDAP Integration**, to configure Active Directory server details.
7. Click **Configuration** tab > **Network** > Set the Deployment Mode as required.
8. Click **Configuration** tab > **SIEM** > Enter the IP address of Syslog / SIEM server.
9. Click **Configuration** tab > **SSL Proxy** > Upload a Public Certificate (if any) for SSL decryption.
10. Click **Configuration** tab > **Central Console** > Enter the hostname of the GTB Central server. Ensure the inspector can reach the Central console.

4.12.5.4 Creating ACL Rules on the Central Console

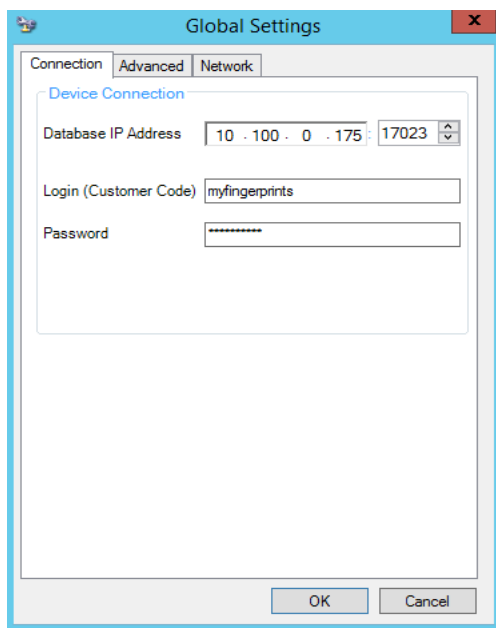
1. Login to the Central Console Web UI. Click **DLP-Setup** > **Network DLP**
2. Click on the <Inspector server name> listed under **Categories**.
3. Click **Add** button. The Add New ACL Rule window should pop-up

| Policy/Sets | Action | Alerts | File capture |
|--------------------------|--------|--------|-------------------------------------|
| <input type="checkbox"/> | Log | | <input checked="" type="checkbox"/> |

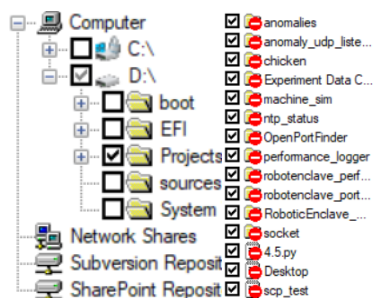
4. Enter the information as required under Name, Protocol, Source, Destination, File Type.
Selecting **Protocol = Any** will enable the Inspector to inspect all protocols.
Note: This may cause a performance impact depending on the number of clients within your organization.
5. Click **Add** under **Enforcement** to configure Policy/Sets. Select from any of the default policies for Credit Card Numbers (CCN), Social Security etc., or create a new one.
6. Select the action to be taken – Log, Block, S-Block and Pass.
7. Check mark the File Capture option to retain a copy of the offending data.
8. Click **Save**.
9. Click **Deploy-All**. This sends newly created policy to the Inspector.
10. (Optional) Order rules if more than one by clicking the **UP / DOWN** arrows. Rules always work from Top to down.

4.12.5.5 Fingerprint Files using Security Manager

1. Click **Help Tab** on the Central Console. Download **GTB Security Manager** on a Windows system.
2. Run the installer (For example *GTBSecurityManager_15.3.0.msi*). Follow the on-screen instructions to complete the install. Reboot the system once done.
3. Launch the GTB Security Manager by doing a **Run as Administrator**.
4. Click **Settings**. Enter the IP address of the Central Console server. The user and password are prepopulated. Click **OK** to save changes.

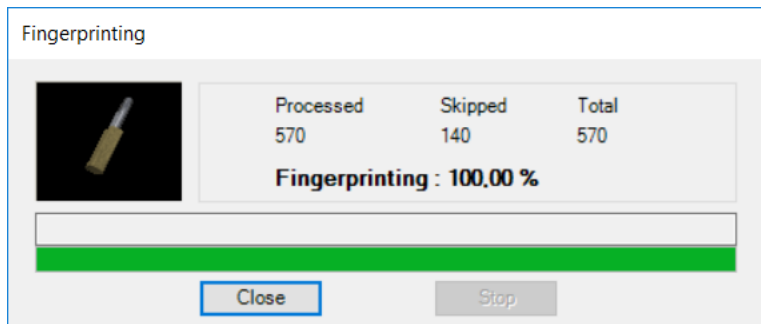


5. Click **File** from the Menu > **New** > **New File Profile**. This will launch a new window with an Explorer like interface allowing to select files/folders for fingerprinting.
6. Select the files or folders that need fingerprinting. Once a folder is selected all files within selected folder will receive a check mark indicating which files will be fingerprinted.

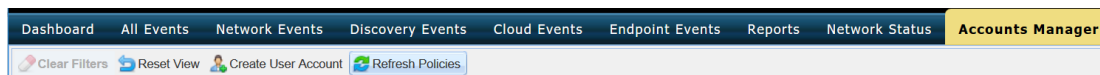


7. Click **Save**. Select a Location to save the newly created profile.
8. Click on the **padlock** icon to start the fingerprinting process.

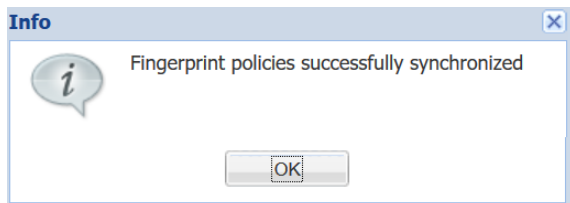
9. View the Output screen to monitor the progress of Fingerprinting. Once completed, click Close.



10. Click **View** on the Menu bar > **Profiles** > **Profiles Window** > <Profile Name>
11. Select the Profile that was created earlier. Right click > **Start Monitoring**.
Once monitoring is enabled, files will be listed under **Currently Monitoring** tab.
12. Login back to **Central Console**, navigate to **Account Manager** Tab and click **Refresh Policies**.



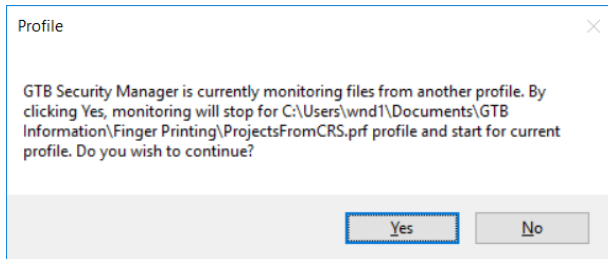
You'll see a message indicating Fingerprint policies successfully synchronized.



13. Click **DLP Setup** > **Policy Management** > Double-click **Default** to launch a new Window.
14. Click **Add Policy**.
15. Click the drop-down and select a File.
16. Click Save once done. Upon completion, 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 on Fingerprinting:

- Fingerprint feature only allows for one active Profile at a time. If another profile is set to **Start Monitoring**, a warning message as shown below will be generated



- Install **GTB Security Manager** on a machine that can be the central repository for all fingerprinted files. Creating a large folder where the files can be placed into for fingerprinting. Files need not 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.
- Fingerprinted files follow acl rules created within Central Console. Rules are processed in order from top to bottom. 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 Links 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.⁹³

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:

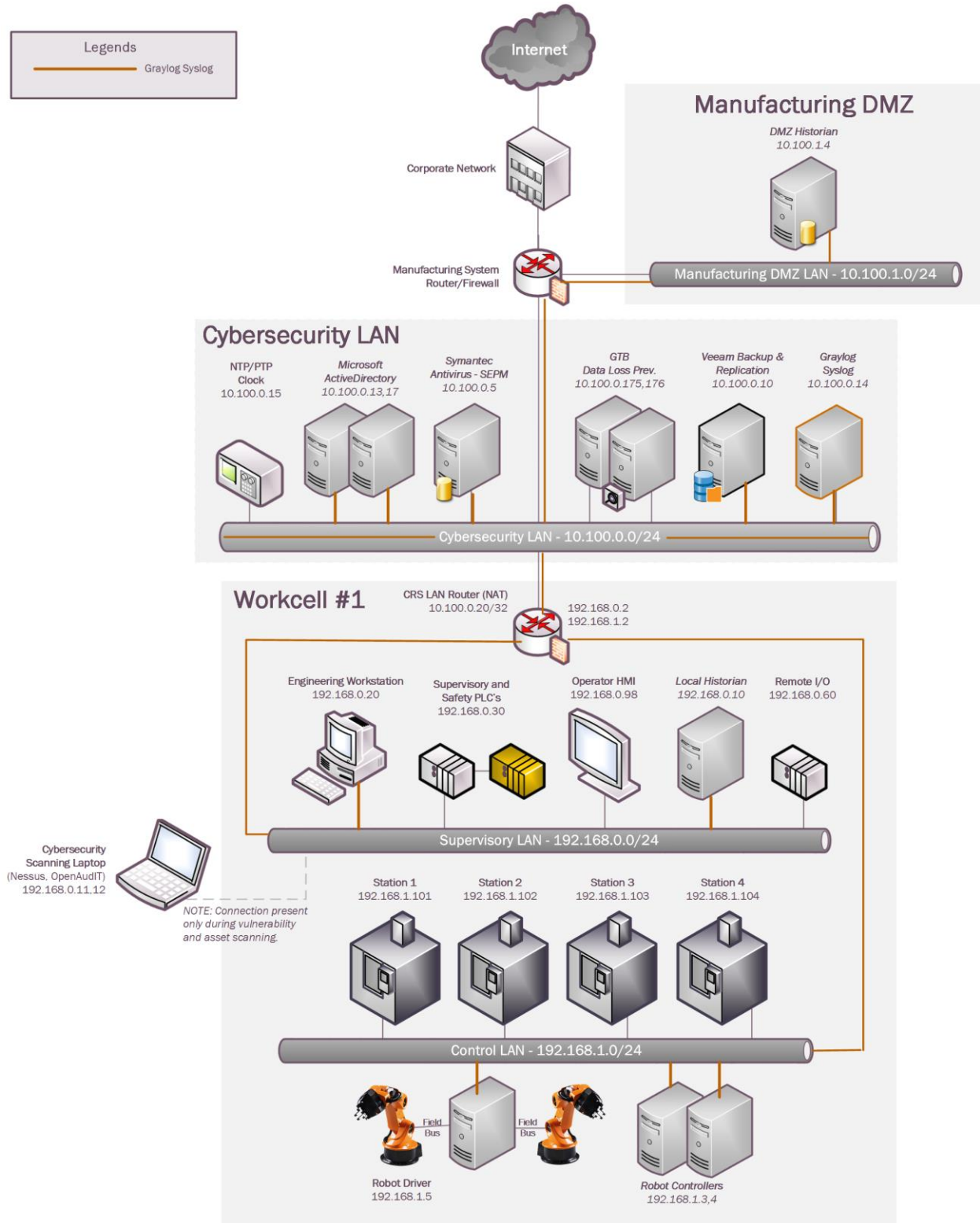
- Network Monitoring
- Event Logging
- Forensics

4.13.3 Subcategories Addressed by Implementing Solution

PR.DS-5, PR.MA-2, PR.PT-1, PR.PT-4, DE.AE-2, DE.AE-3, DE.CM-1, DE.CM-6, DE.CM-7, DE.DP-3, RS.AN-3

⁹³ <http://docs.graylog.org/en/3.0/>

4.13.4 Architecture Map of Where Solution was Implemented



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

4.13.5 Installation Instructions and Configurations

Details of the solution implemented:

| Name | Version | Hardware Details |
|--------------------|---------|--|
| Graylog Enterprise | 2.4.6 | Hyper-V Virtual Machine (Generation 1): <ul style="list-style-type: none"> • Processors: 2 virtual cores • Memory: 6 GB • Disk space: 400 GB Total <ul style="list-style-type: none"> (i) Root volume as allocated by the Virtual Appliance file provided by the vendor. (ii) 350+ GB Data volume for log storage • Network: 1 network adapter • OS: Ubuntu 14 |

4.13.5.1 Environment Setup

1. A preconfigured virtual machine (.ova) provided by the vendor was setup on a Hyper-V host server of the Cybersecurity LAN network of the workcell with hardware specifications as described in the table above.
2. The guest OS IP information of this server was set as follows:
 - a. IP address: 10.100.0.14
 - b. Gateway: 10.100.0.1
 - c. Subnet Mask: 255.255.255.0
 - d. DNS: 10.100.0.17
3. UDP ports 514, 5415 and 1202 were opened on the firewall as required by Graylog to collect syslog messages from the clients.⁹⁴

4.13.5.2 Initial Setup

1. Download the installation package as per the Operating system from the Graylog website.⁹⁵
Note: Graylog provides a preconfigured VM for use in test/training environments.
2. Assign a static IP address to the Linux system (if not already).
3. Install the package using the instructions mentioned in the Graylog documentation.⁹⁶
4. Login to the Web Interface using the default credentials and change the admin password.
5. Configure Active Directory integration as follows

⁹⁴ <http://docs.graylog.org/en/3.0/>

⁹⁵ <https://www.graylog.org>

⁹⁶ http://docs.graylog.org/en/3.0/pages/installation/operating_system_packages.html

- a. Click on **System > Authentication** on the Top menu.
- b. Click on **LDAP / Active Directory** on the Authentication Management page and enter the AD server details. Refer to the Graylog docs for detailed instructions.
- c. Click on **LDAP Group Mapping** to configure **Group Mapping** options to control the type of access to be assigned to the users. Change the Default User Role depending on your requirement.

4.13.5.3 Receiving Syslog from Linux Servers

The Rsyslog package was leveraged to forward log messages from Linux clients to Graylog. Rsyslog is available by default in majority of the Linux distributions.

1. Edit the `/etc/rsyslog.conf` file on the Linux system to enable forwarding the logs to the IP address of the Graylog server.
2. Enter the following line with IP address of the Graylog server.⁹⁷

```
# Graylog configuration
*.* @10.100.0.14:514;RSYSLOG_SyslogProtocol23Format
3. root@gitlab:/home/icssec#
```

4. Save the change.
5. Restart rsyslog service: `sudo systemctl restart rsyslog`
6. Login to the Graylog Web UI. Look for the events from these hosts.
7. Click on **Sources** in the Top menu bar to verify if the Linux host shows up under the list of **Selected sources**.
8. Search for events from a host by entering a search query and selecting the appropriate time interval in the home page.

For example: To search for events by hostname, enter `source: <server name>` in the Search *box*

4.13.5.4 Configuring Syslog on the Boundary Firewall (RuggedCom)

1. Login to the web UI of the RuggedCom firewall.
2. Click on **Edit Private** to enter configuration mode.
3. Click on **admin > logging > server**. Click on **Add a server**
4. Enter the IP address of the syslog (Graylog) server.
5. Set the logging level as required. For example: **Informational and above**
6. Click Apply. Logout of the device.

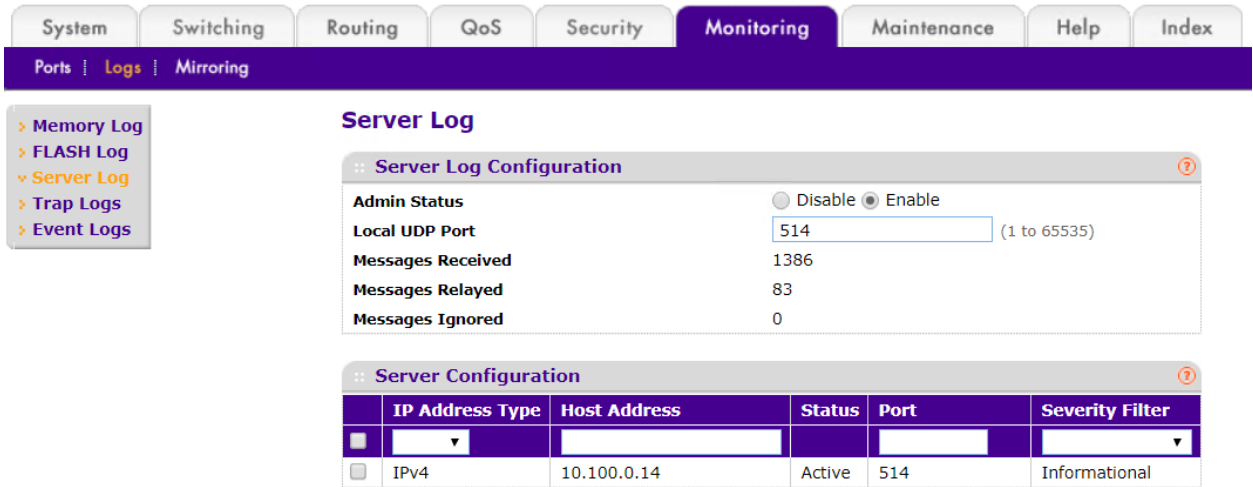
Detailed instructions can be found in the product manual.⁹⁸

⁹⁷ <https://marketplace.graylog.org/addons/a47beb3b-0bd9-4792-a56a-33b27b567856>

⁹⁸ http://www.plcsystems.ru/catalog/ruggedcom/doc/ROXII_RX1500_User-Guide_WebUI_EN.pdf

4.13.5.5 Configuring Syslog on the Layer 2 Switches on the Workcell

Both the network switches (Netgear and Siemens i800) were configured to log to the Graylog server. The image below shows Syslog server configuration on the Netgear SW pointing to the IP address of the Graylog server.



4.13.5.6 Configuring Email Notifications for Alert Conditions

Email alerts for any custom events, alert conditions can be setup. The process below shows how our Graylog was configured to send out email notifications for any events related to **Veeam Backups** that were received from the Windows clients.

Follow this process to define your custom alert conditions.

There are three configuration settings required for email notification to work:

- Creating a **stream**.
- Adding an **alert condition**.
- Creating a **notification**.

1. Click on **Streams** on the **Top-Menu > Create a Stream >** Enter **Title, Description, and Index Set** which should default to **Default index set**
2. Click **Save** to save the changes

Editing Stream
✕

Title

Description

Index Set

Messages that match this stream will be written to the configured index set.

Remove matches from 'All messages' stream

Remove messages that match this stream from the 'All messages' stream which is assigned to every message by default.

Cancel
Save

3. Click on **Alerts** in the Top menu > **Manage conditions > Add New Condition** to define a condition.
4. Click the **Drop menu** under **Alert on Stream** and select the stream created earlier. Under **Condition Type**, select **Message Count Alert Condition**.

Condition

Define the condition to evaluate when triggering a new alert.

Alert on stream

Select the stream that the condition will use to trigger alerts.

Condition type

Select the condition type that will be used.

5. Click **Add Alert Condition**. Fill out the required information in the window.

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

6. Click **Save** to complete (See below for example of current Message Count Alert Condition).

Update Veeam Backup Alerts ✕

Message Count Alert Condition description
This condition is triggered when the number of messages is higher/lower than a defined threshold in a given time range.

Title

The alert condition title

Time Range

Evaluate the condition for all messages received in the given number of minutes

Threshold Type

Select condition to trigger alert: when there are more or less messages than the threshold

Threshold

Value which triggers an alert if crossed

Grace Period

Number of minutes to wait after an alert is resolved, to trigger another alert

Message Backlog

The number of messages to be included in alert notifications

Repeat notifications (optional)
Check this box to send notifications every time the alert condition is evaluated and satisfied regardless of its state.

7. Create a notification as follows:
 - a. Click on **Manage notifications** in upper right-hand corner.
 - b. Click **Add New Notification**
 - c. Select notification created earlier from the drop-down menu under Notify on Stream.
 - d. Select **Email Alert Callback** under Notification Type
 - e. Click **Add alert notification** button
 - f. Title: < Some text> For instance: **Veeam Backup Alerts**
 - g. (For Reference) Email Subject: “Successful Veeam Backup source: `${foreach backlog message}${message.source}${end}`” without the quotes, see below for screen shot of current callback wording.
 - h. **Sender:** < sender address >

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

i. **E-mail Body:**

```
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}
```

- j. **User Receivers:** Select a Graylog user if desired
- k. **Email Receivers:** Enter email address for individuals receiving these alerts
- l. Click **Save**

8. Test new Streams / Alerts / Notifications to ensure they are configured correctly.

4.13.5.7 Additional Information

- There are many useful Content packs and plugins available⁹⁹ as per vendor specific technologies, devices such as Cisco, Microsoft DNS, Bro IDS, Cacti, Symantec etc.
- Additional guidance is available on creating pipelines.¹⁰⁰

Lessons Learned

Carefully configure the level of logging on each system. In case of Windows clients, filter out Event IDs in the *nxlog.conf* instead of enabling every event category, as this can generate a high volume of events which in turn will impact search operations in Graylog and overall performance of the Graylog server. When using Group Policy to enable auditing, select only the categories which are required. Some categories such as Process Creation generate tremendous amount of noise.

⁹⁹ <https://marketplace.graylog.org>

¹⁰⁰ <https://jalogisch.de/2018/working-with-cisco-asa-nexus-on-graylog/>

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).

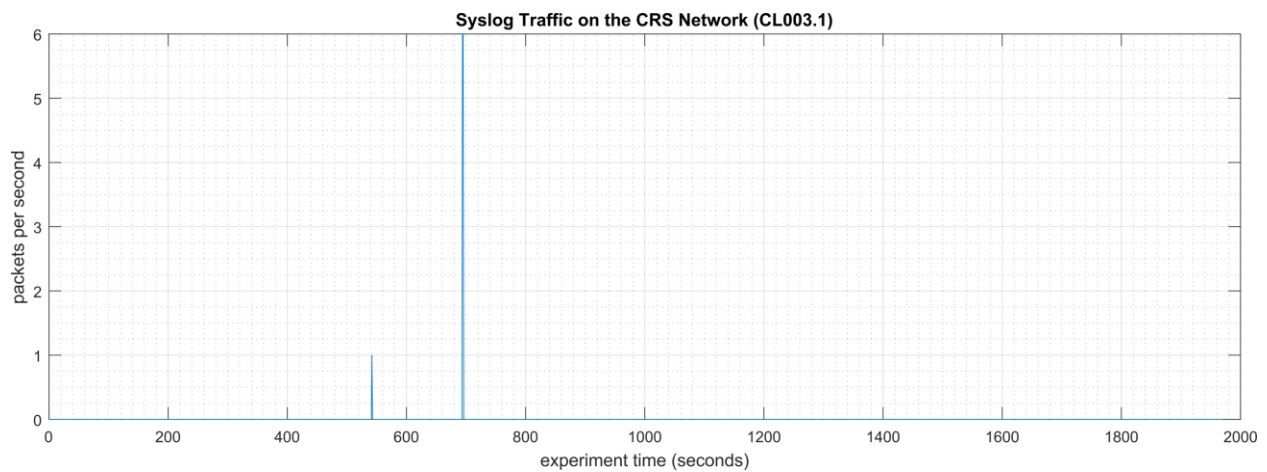


Figure 4-48 - Time series plot showing the rate of syslog network traffic (in packets per second) transmitted during the CL003.1 experiment.

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

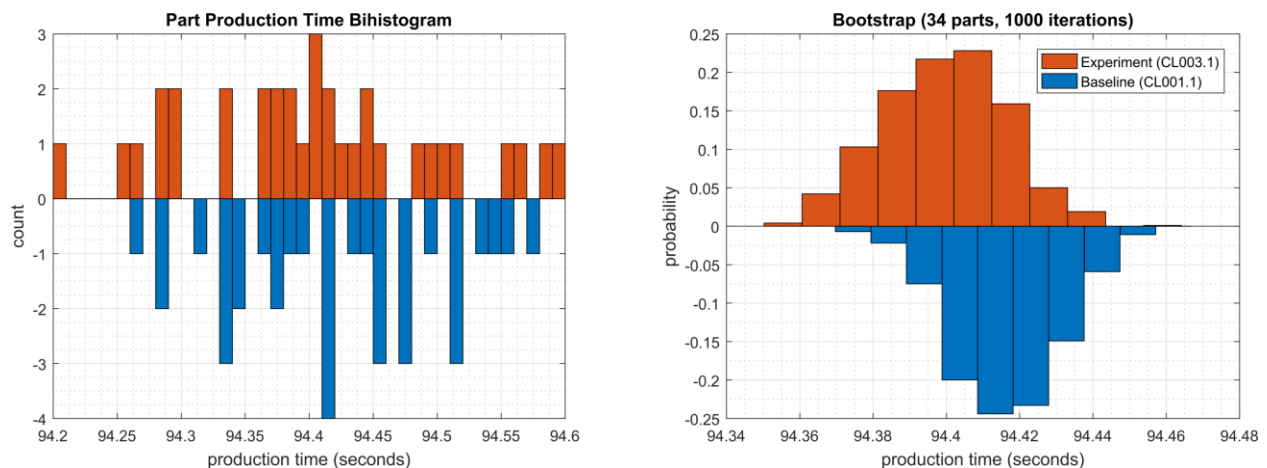


Figure 4-49 - Bihistograms showing the part production time (left) and estimated mean production time using the bootstrap method (right) using the measurements from baseline CL001.1 and experiment CL003.1.

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

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).

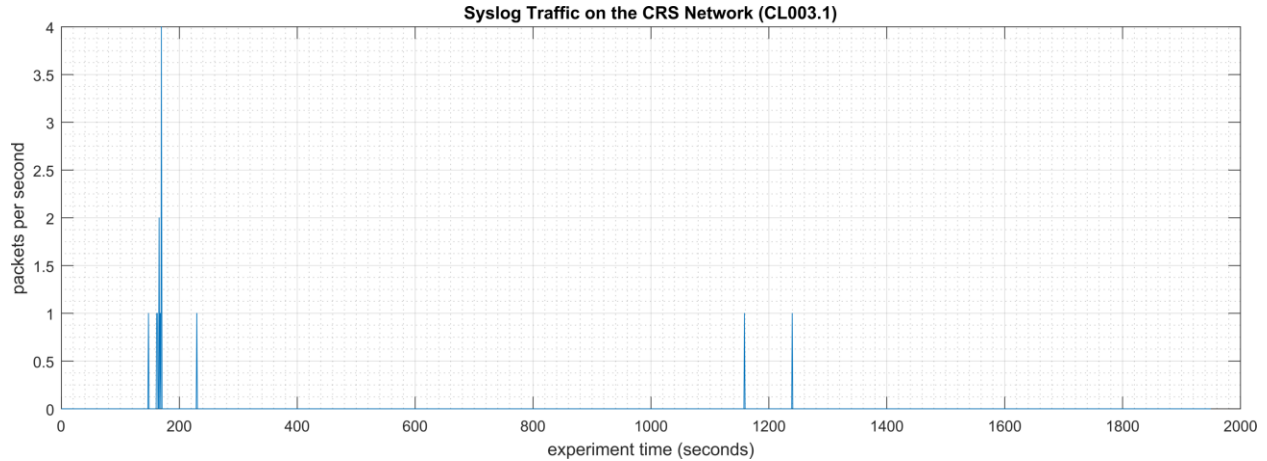


Figure 4-50 - Time series plot showing the rate of syslog network traffic (in packets per second) transmitted during the CL003.2 experiment.

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

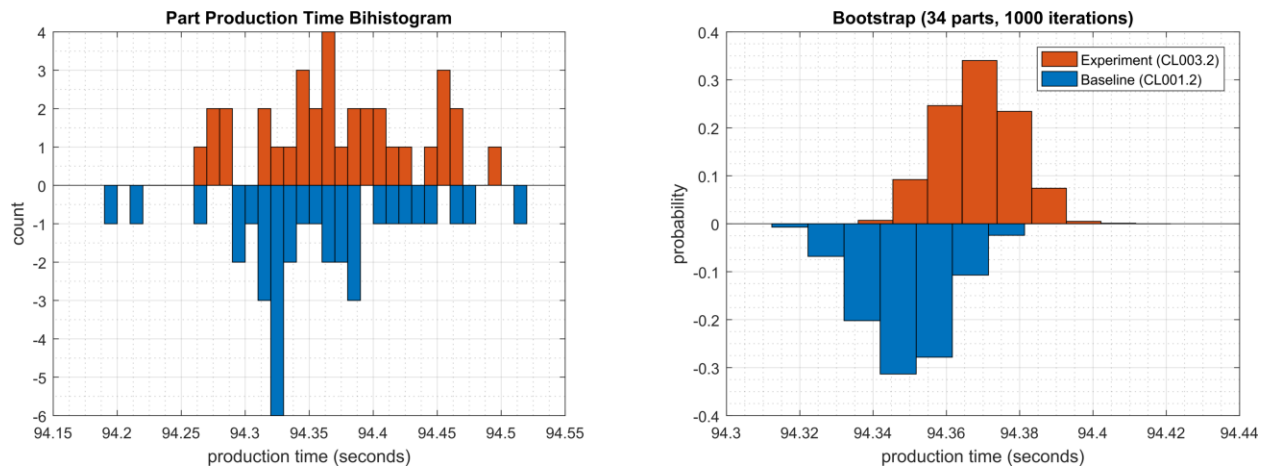


Figure 4-51 - Bihistograms showing the part production time (left) and estimated mean production time using the bootstrap method (right) using the measurements from baseline CL001.1 and experiment CL003.2.

4.13.7 Links 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

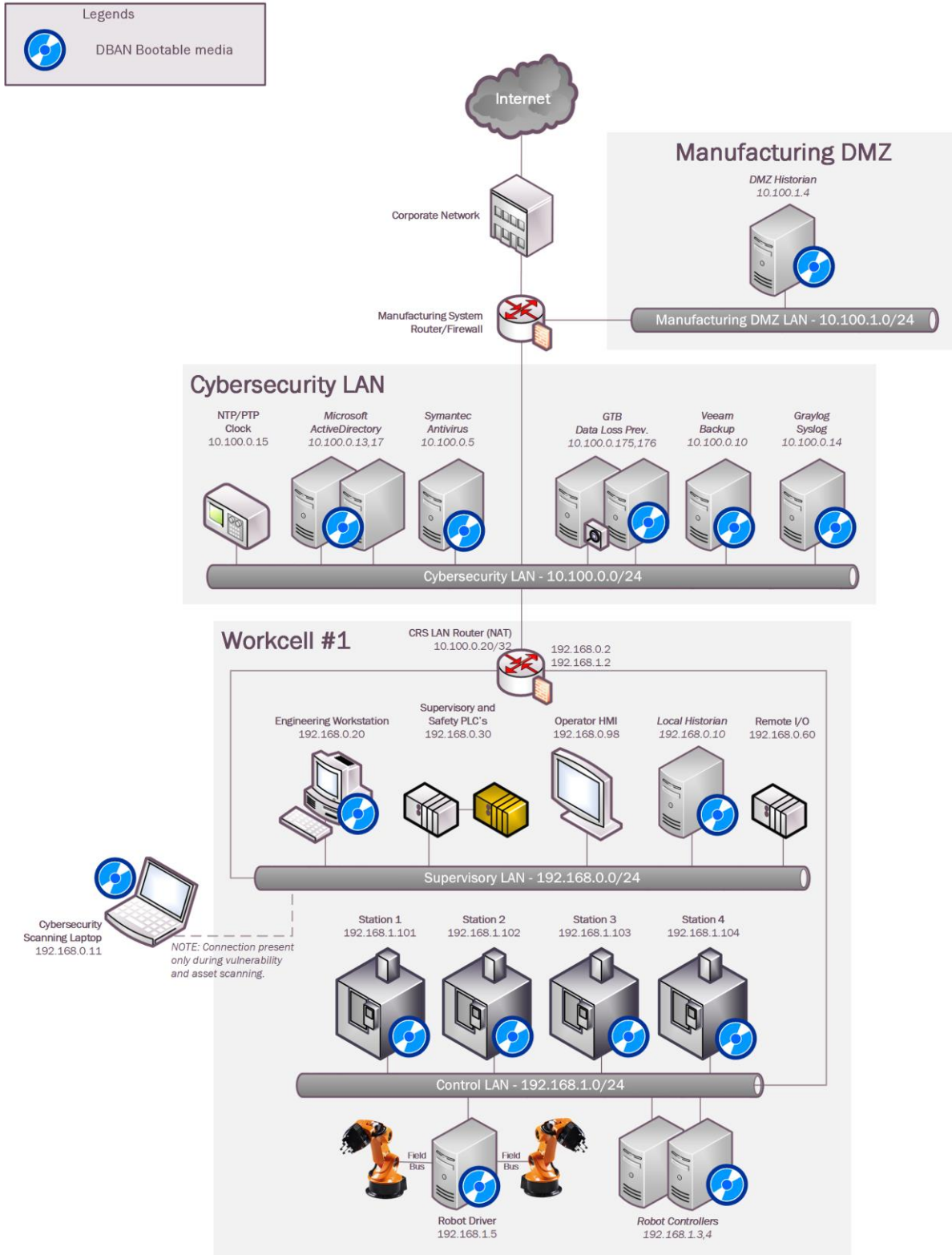
DBAN provides components of the following Technical Capabilities described in Section 6 of Volume 1:

- 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



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

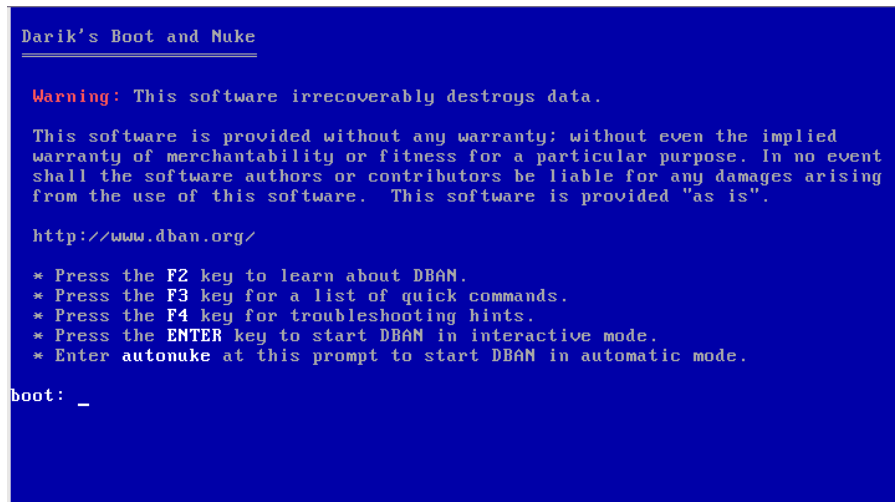
4.14.5 Installation Instructions and Configurations

4.14.5.1 Setup

1. Download the DBAN ISO file¹⁰¹
2. Burn to a CD/DVD, or USB drive using any of the available ISO bootable utilities.

4.14.5.2 Instructions

1. Boot up the computer requiring sanitization using the bootable media created earlier.
2. Select the desire option for media sanitization upon boot. Typically, the **default** mode is applicable for most cases.



```
Darik's Boot and Nuke

Warning: This software irrecoverably destroys data.

This software is provided without any warranty; without even the implied
warranty of merchantability or fitness for a particular purpose. In no event
shall the software authors or contributors be liable for any damages arising
from the use of this software. This software is provided "as is".

http://www.dban.org/

* Press the F2 key to learn about DBAN.
* Press the F3 key for a list of quick commands.
* Press the F4 key for troubleshooting hints.
* Press the ENTER key to start DBAN in interactive mode.
* Enter autonuke at this prompt to start DBAN in automatic mode.

boot: _
```

3. Hit **Enter Key** to continue. The default sanitization mode is **short DoD 5520.22-M**, but this can be changed depending on the level your security program indicates.
4. Follow the on-screen menu options to Start the Wiping process. Once the wipe has completed, you will see a screen like the image below.

¹⁰¹ <https://dban.org>

```
DBAN succeeded.  
All selected disks have been wiped.  
Remove the DBAN boot media and power off the computer.  
  
Hardware clock operation start date: Sun Aug 13 15:24:36 2006  
Hardware clock operation finish date: Sun Aug 13 15:27:00 2006  
Saving log file to floppy disk... a floppy disk in DOS format was not found.  
DBAN finished. Press ENTER to save the log file._
```

5. Remove the physical hard drive from device post completion. It is now ready for disposal.

Additional Information

Not all hard drives can 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 Links 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

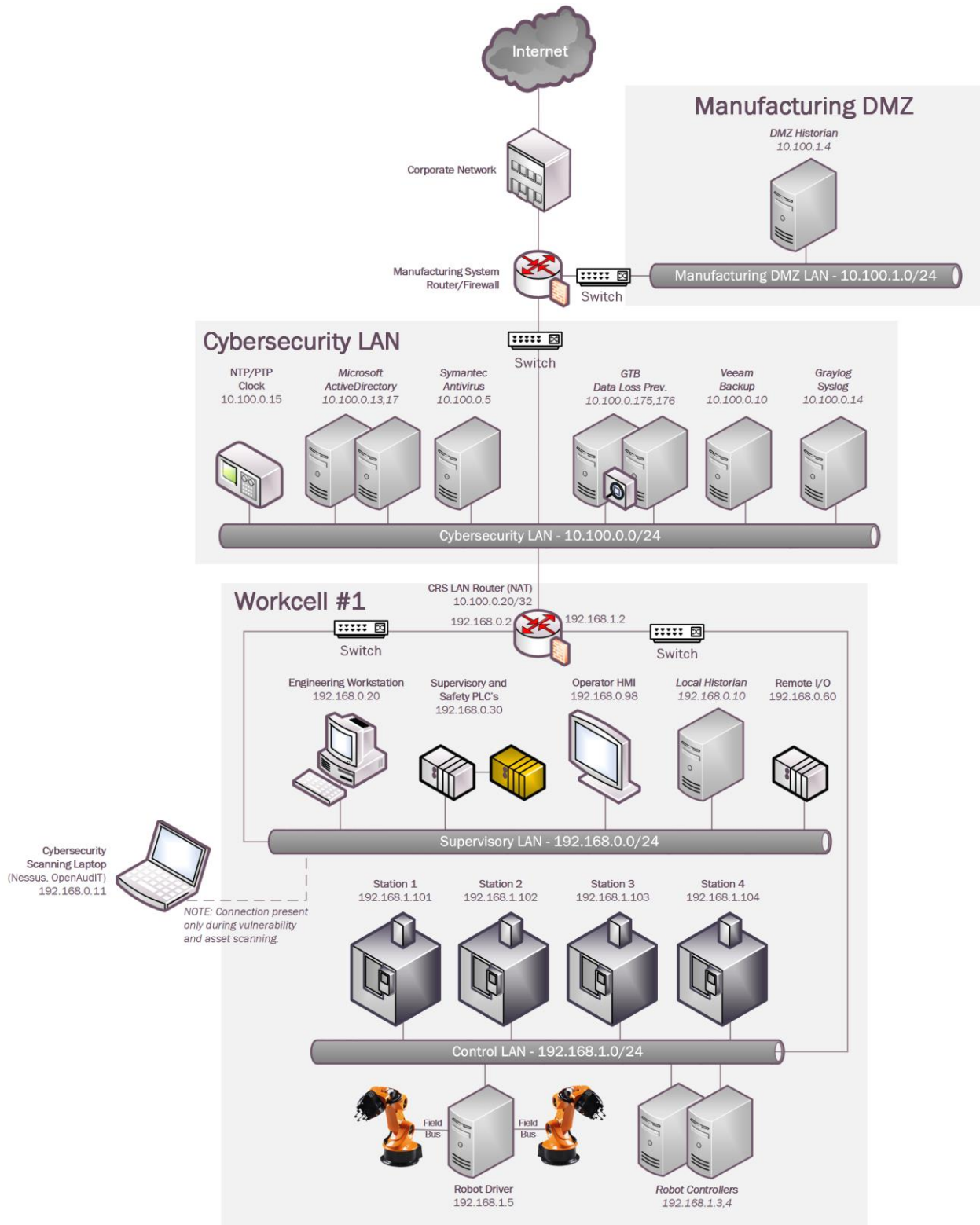
Network Segmentation and Segregation provides components of the following Technical Capabilities described in Section 6 of Volume 1:

- 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



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

4.15.5 Installation Instructions and Configurations

4.15.5.1 Environment Setup

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 | Workcell |

4.15.5.2 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 | 10.100.0.0/24 | 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 | 10.100.1.0/24 | Manufacturing DMZ LAN |

4.15.5.3 Segmentation in the Workcell

The Workcell 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 |

List of interfaces created on the firewall. There were two subnets created as listed in the table below.

| 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 Links to Entire Performance Measurement Data Set

N/A

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

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

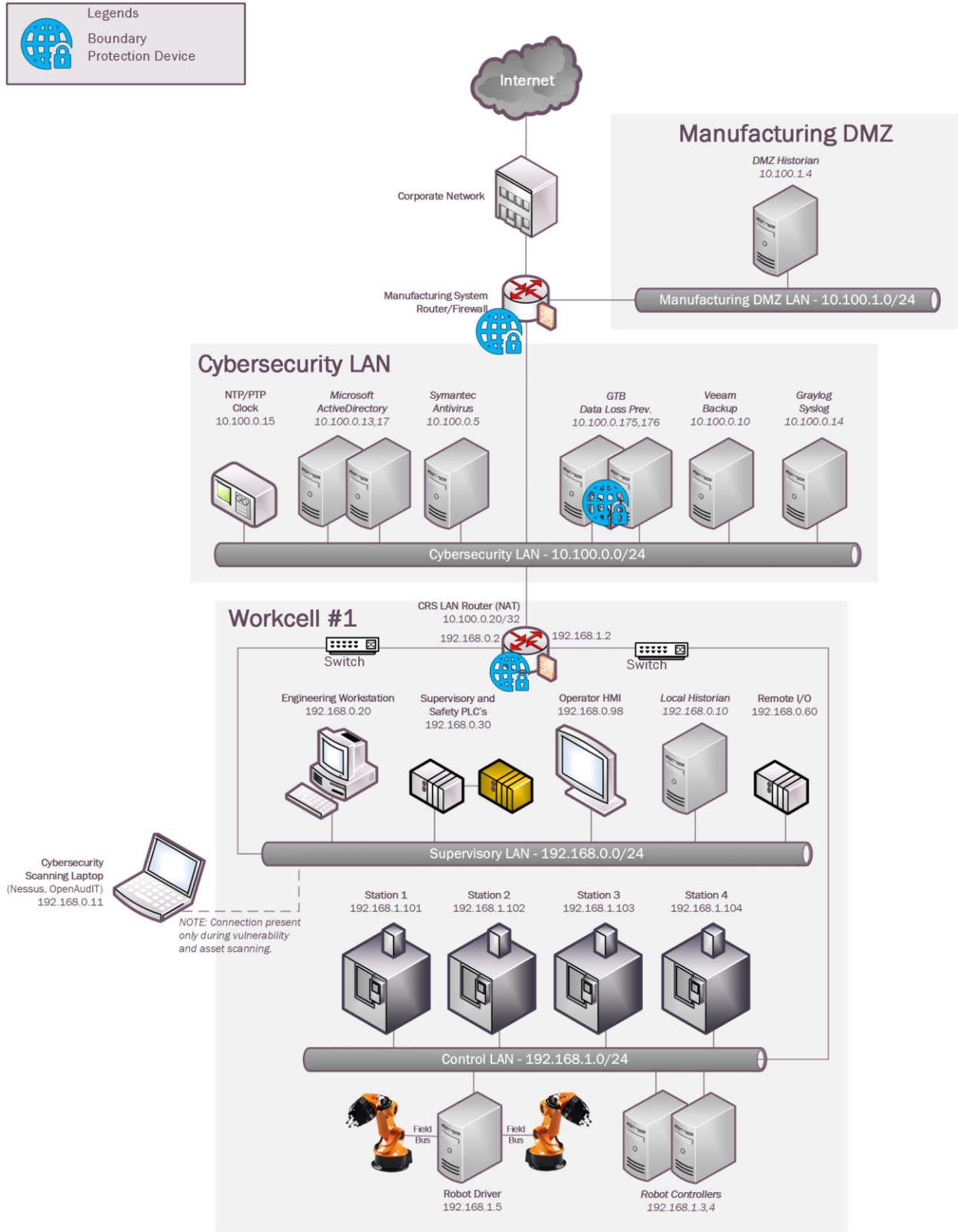
Network Boundary Protection provides components of the following Technical Capabilities described in Section 6 of Volume 1:

- 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



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

4.16.5 Installation Instructions and Configurations

4.16.5.1 Environment Setup

The following devices were setup for Boundary protection:

| 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 | Workcell |
| GTB Inspector | Data Loss Prevention (DLP) virtual appliance | Cybersecurity LAN |

4.16.5.2 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

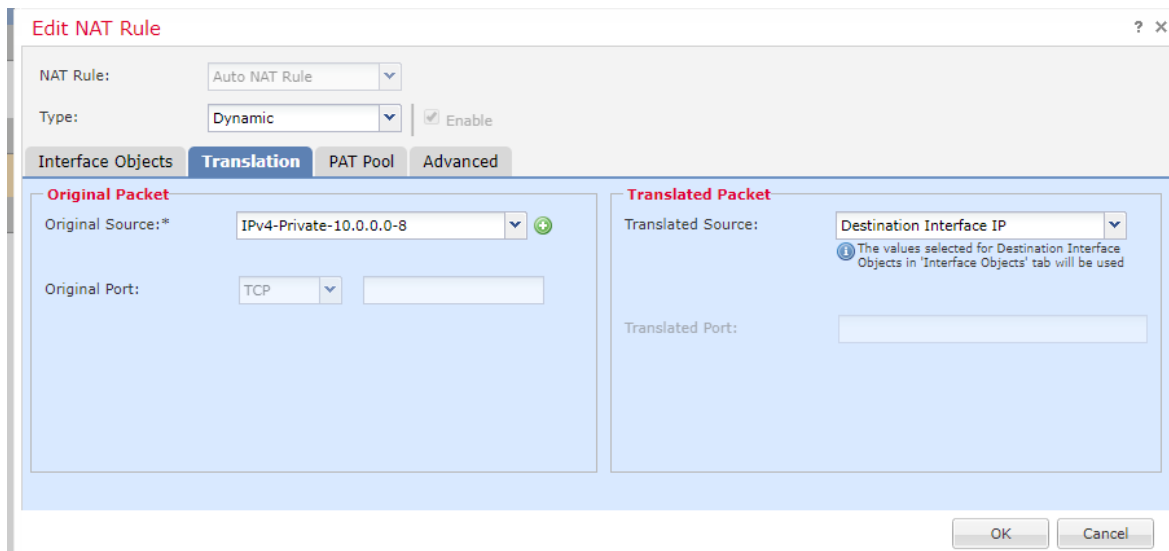
The following ACL rules were put in place on the ASA with a default Action to **Block all traffic**.

| 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 |

NAT Policy

A Dynamic NAT policy was configured to allow internet access:

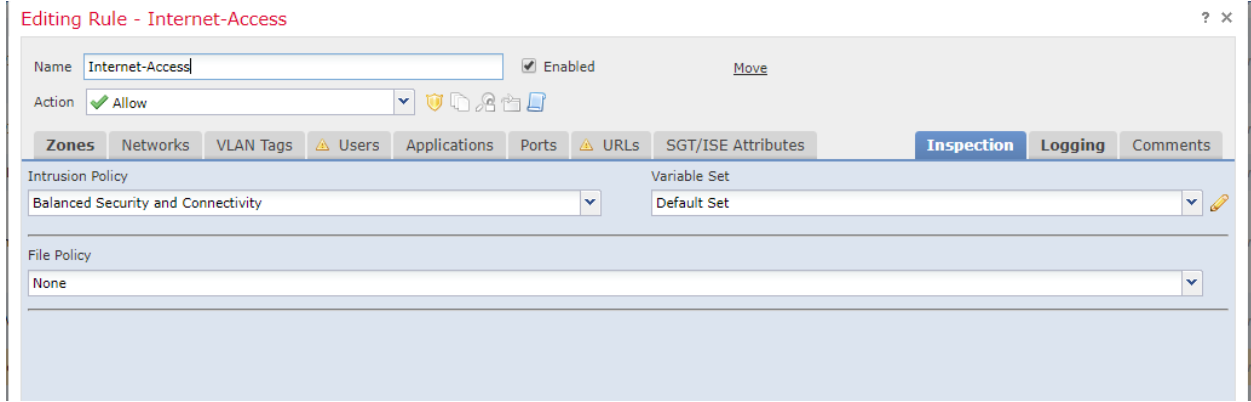
| | |
|-----------------------|---|
| | |
| Type of NAT rule | Auto NAT |
| Source Interface | inside |
| Destination Interface | outside |
| Original sources | 10.100.0.0/8 |
| Translated Source | Destination Interface IP |
| Options | Translate DNS Replies that match this Rule: False |



Snort Inspection

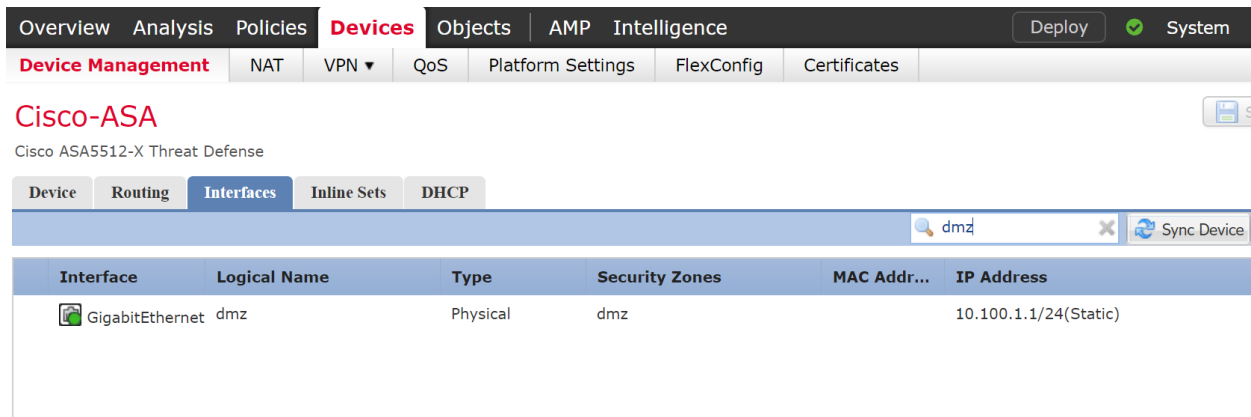
Snort Inspection was enabled on the following ACL rules:

| Name of the ACL | Intrusion Policy |
|----------------------|------------------------------------|
| Internet-Access rule | Balanced connectivity and security |



DMZ Network

A Separate interface was setup for the Manufacturing DMZ LAN Network for hosting the **DMZ Historian** server.



4.16.5.3 Configuration on RuggedCom Firewall

The following features, settings were enabled on this firewall:

- Network Segmentation
- ACL Rules
- Masquerading (NAT) rules

Network Segmentation

Separate network interfaces were configured for the different network segments as listed below:

- Supervisory LAN Interface (Network: 192.168.0.0/24)
- Control LAN Interface (Network: 192.168.1.1/24)
- LAN Interface (IP: 10.100.0.20, Uplink to Cybersecurity LAN)

Access Control List (ACL) rules

The following zones were created:

- WAN - Zone for internet-bound / uplink connections to Cybersecurity LAN.
- CTRL - Zone for the 192.168.1.0/24 subnet.
- SUPERVISORY - Zone for the 192.168.0.0/24 subnet.
- MGMT - Zone for the management interface traffic (out of scope)

The following firewall policies were created:

- 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)

| 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 | none |
| 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 |

NAT Policy

Two Masquerading rules were created (one for each LAN segment) to NAT all traffic going outbound from the Workcell to the Cybersecurity LAN network. Masquerading is a form of Dynamic NAT. Both hide a single subnetwork behind a single IP address

| 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 |

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

Configure Running Tools Logout from ruggedcom

View | Edit Private | Edit Exclusive

fwconfig

fw1

fwzone

fwhost

fwinterface

fwpolicy

fwrule


fwnat

fwmasq

snat

snat2

← ← /security/firewall/fwconfig(fw1)/fwmasq

 Masqueradings

| Masquerade Entry Name | IP Type | Outgoing Interface List | Outgoing Interface Specifics | IP Alias | Source Hosts | SNAT Address | Description |
|-----------------------|---------|-------------------------|------------------------------|----------|----------------|--------------|-------------|
| snat | ipv4 | ge-3-2 | not found | disabled | 192.168.1.0/24 | 10.100.0.20 | not found |
| snat2 | ipv4 | ge-3-2 | not found | disabled | 192.168.0.0/24 | 10.100.0.20 | not found |

4.16.5.4 Configuration on GTB Inspector

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:

1. CL009.1 - Firewall rules and Access control list (ACL) rules are implemented at the CRS boundary router.
2. 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.

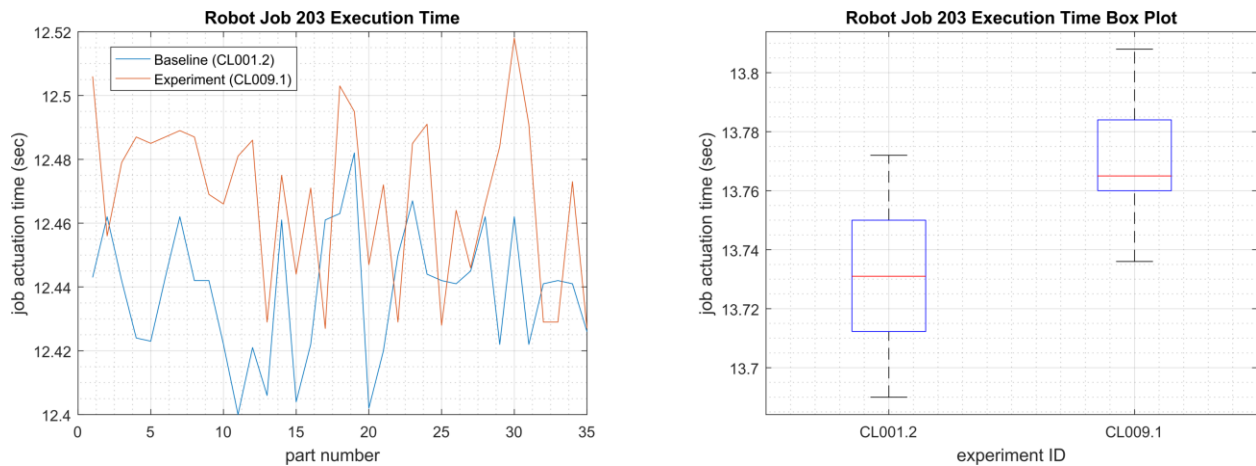


Figure 4-52 - Time-series (left) and boxplot (right) showing the job actuation times for Job 203 during the CL001.2 baseline and CL009.1 experiment.

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

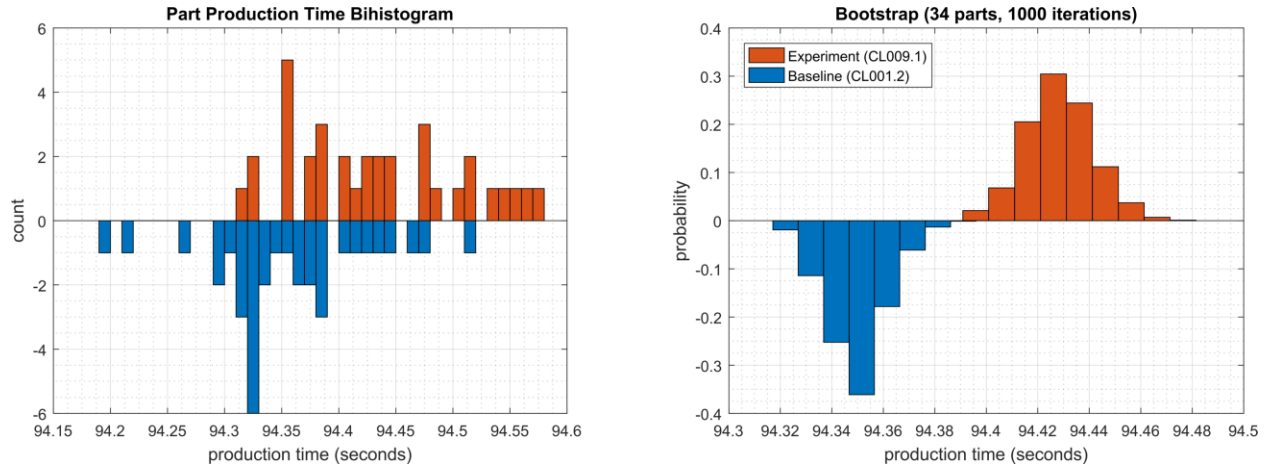


Figure 4-53 - Bihistograms showing the part production time (left) and estimated mean production time using the bootstrap method (right) using the measurements from baseline CL001.2 and experiment CL009.1.

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.

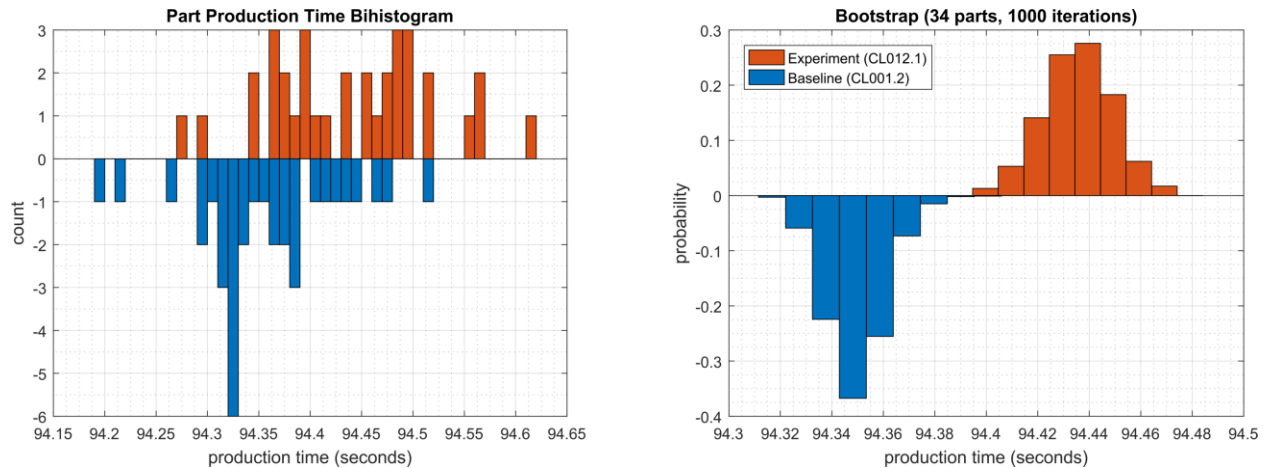


Figure 4-54 - Bihistograms showing the part production time (left) and estimated mean production time using the bootstrap method (right) using the measurements from baseline CL001.2 and experiment CL012.1.

4.16.7 Links 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 the manufacturing system, along with physical labeling of the 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.

There is a minimal cost for labeling. The effort to implement can be 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

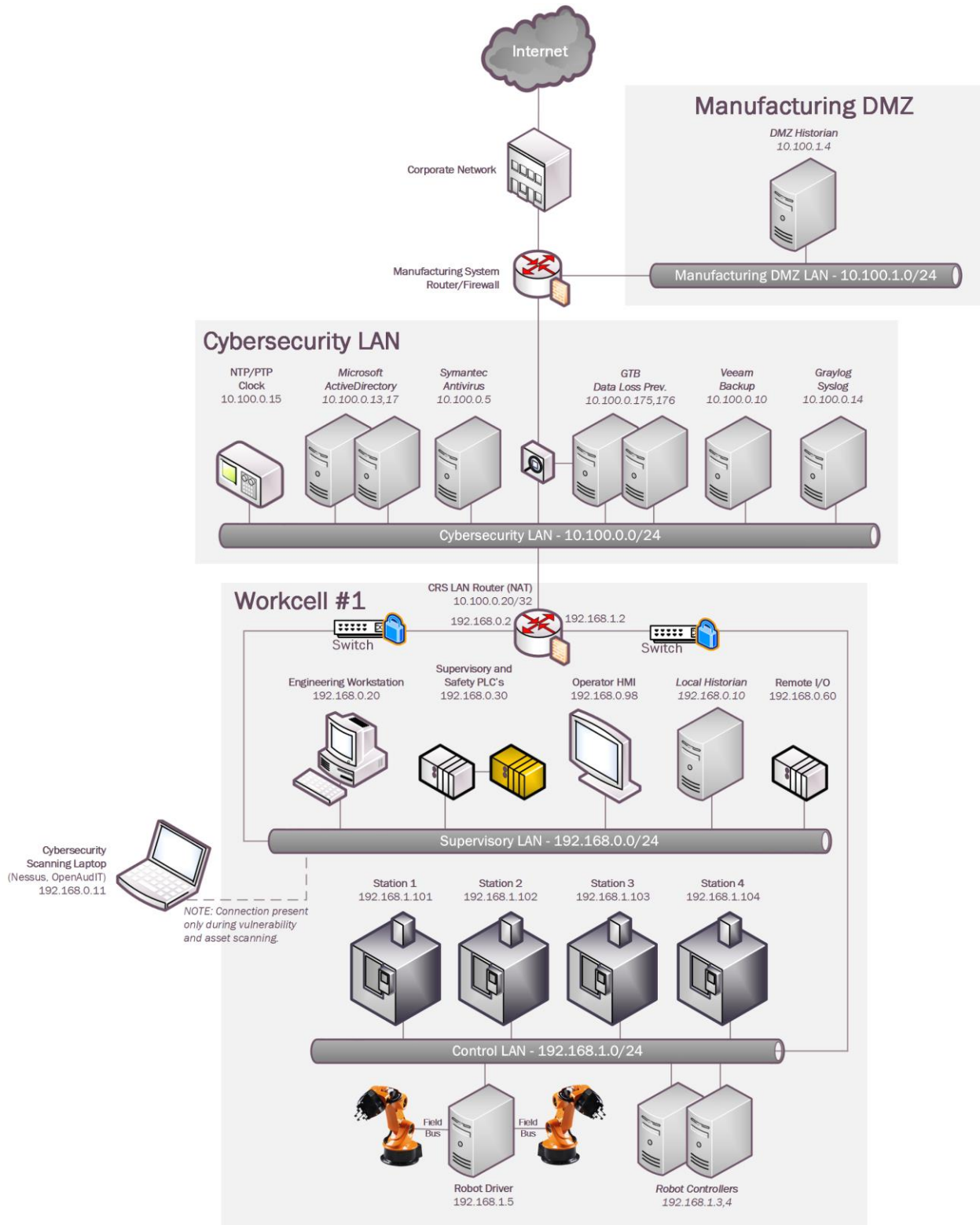
Managed Network Interfaces provides components of the following Technical Capabilities described in Section 6 of Volume 1:

- Managed Network Interfaces

4.17.3 Subcategories Addressed by Implementing Solution

PR.AC-5

4.17.4 Architecture Map of Where Solution was Implemented



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

4.17.5 Installation Instructions and Configurations

4.17.5.1 Environment Setup

The Workcell consists of the following Network Devices.

- Siemens RuggedCom RX1510 (Router/Firewall)
- Siemens RuggedCom i800 (Switch)
- NETGEAR GS724Tv4 (Switch)

The following actions were performed for implementing Managed Network Interfaces.

4.17.5.2 Port Labelling

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.

1. Configure Port Labelling on the Siemens i800 Switch as follows:
 - a. Login to switch web interface/
 - b. Click on **Ethernet > Ports > Configure Port Parameters**.
 - c. Click desired port number for renaming.
 - d. Enter a label under **Name** to identify the port. click **Apply**.
2. Configure Port Labelling on the Netgear Switch as follows:
 - a. Login to switch via web browser. <https://192.168.0.239>
 - b. Click on **Switching**
 - c. Select port that will be labeled.
 - d. Enter Description.
 - e. Click apply button

4.17.5.3 Port Security

Port security or MAC address filtering is a security method for access control. Using this method, we can blacklist, or whitelist certain devices based on their MAC address. This prevents unauthorized devices from being plugged into a network switch while trying to obtain 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.

1. Configure Port Labelling on the Siemens i800 Switch as follows:
 - a. Login to switch web interface
 - b. Navigate to **MAC Address Tables > Configure Static MAC Addresses**. The Static MAC Addresses table appears.
 - c. Click **Insert Record**. The Static mac-address form appears.
 - d. Enter a learned mac-address. Click **apply**

2. Configure Port Labelling on the Netgear Switch as follows:
 - a. Login to the switch via web browser.
 - b. Click on **Security > Traffic Control > Port Security > Interface Configuration**.
 - c. Select the ports to configure.
 - d. Specify the following settings: Port Security, Max Allowed Dynamically Learned MAC, Max Allowed Statically Locked MAC, Enable Violation Traps.
 - e. Click **Apply** button

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.

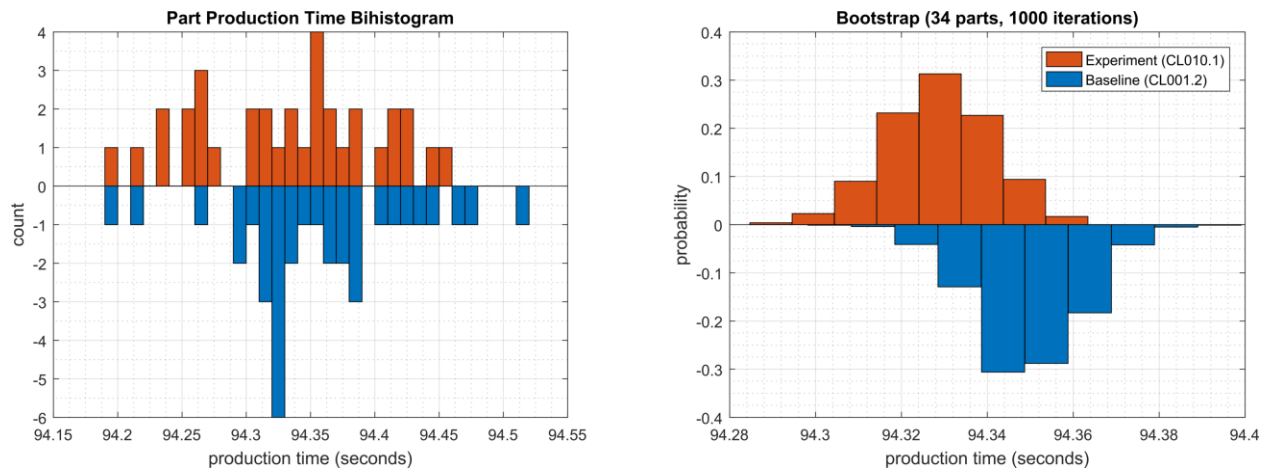


Figure 4-55 - Bihistograms showing the part production time (left) and estimated mean production time using the bootstrap method (right) using the measurements from baseline CL001.1 and experiment CL010.1.

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.

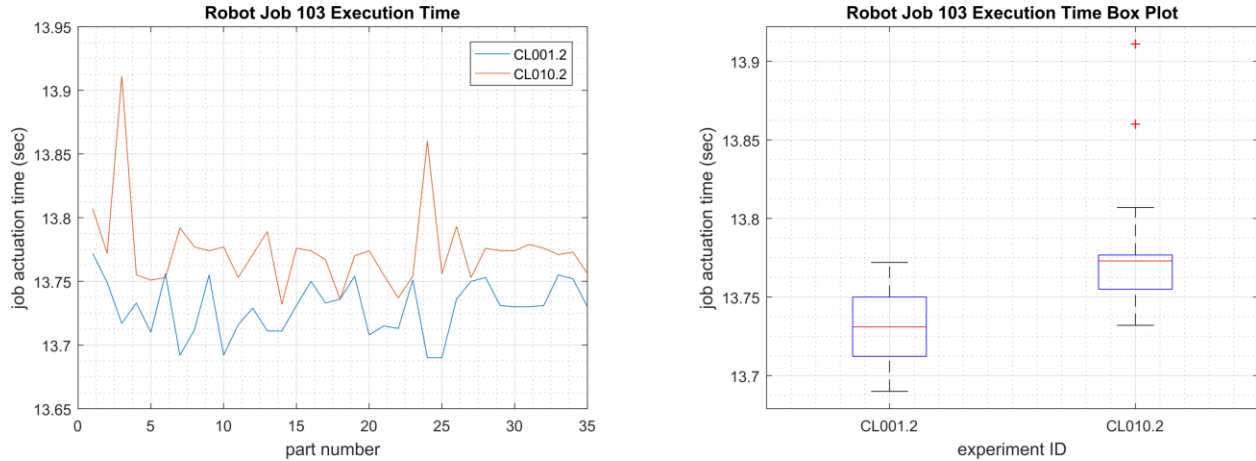


Figure 4-56 - Time-series (left) and boxplot (right) showing the job execution times for Job 103 during the CL0010.2 experiment and CL001.2 baseline.

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

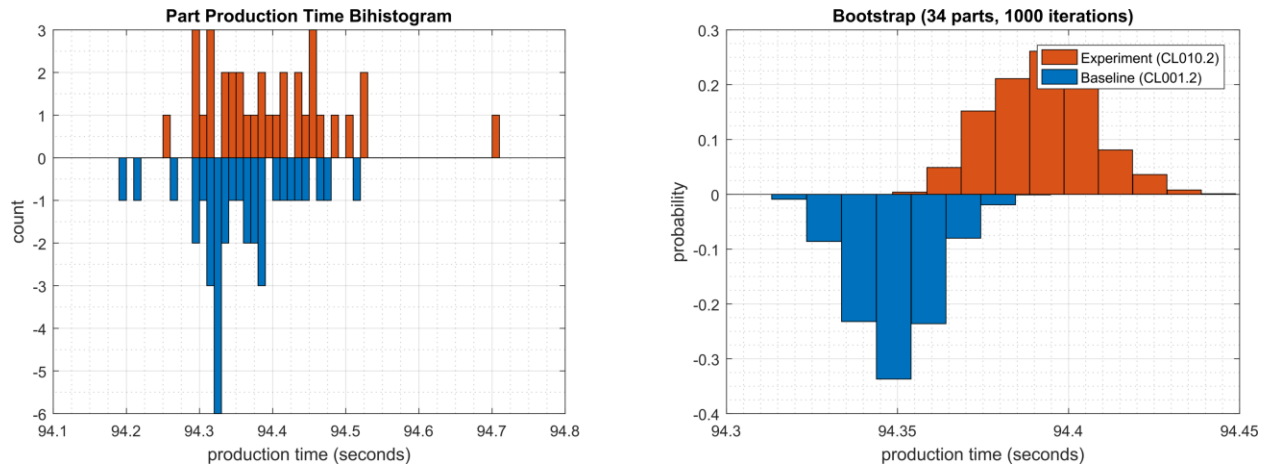


Figure 4-57 - Bihistograms showing the part production time (left) and estimated mean production time using the bootstrap method (right) using the measurements from baseline CL001.1 and experiment CL010.2.

4.17.7 Links to Entire Performance Measurement Data Set

- [CL010.1-NetworkPhysicalConnections.zip](#)
- [CL010.2-NetworkMACFiltering.zip](#)

4.18 Time Synchronization

4.18.1 Technical Solution Overview

Time synchronization allows devices to synchronize with a reliable time source. Time synchronization is vital for system logins, event tracking and all other time sensitive events occurring with a manufacturing system.

4.18.2 Technical Capabilities Provided by Solution

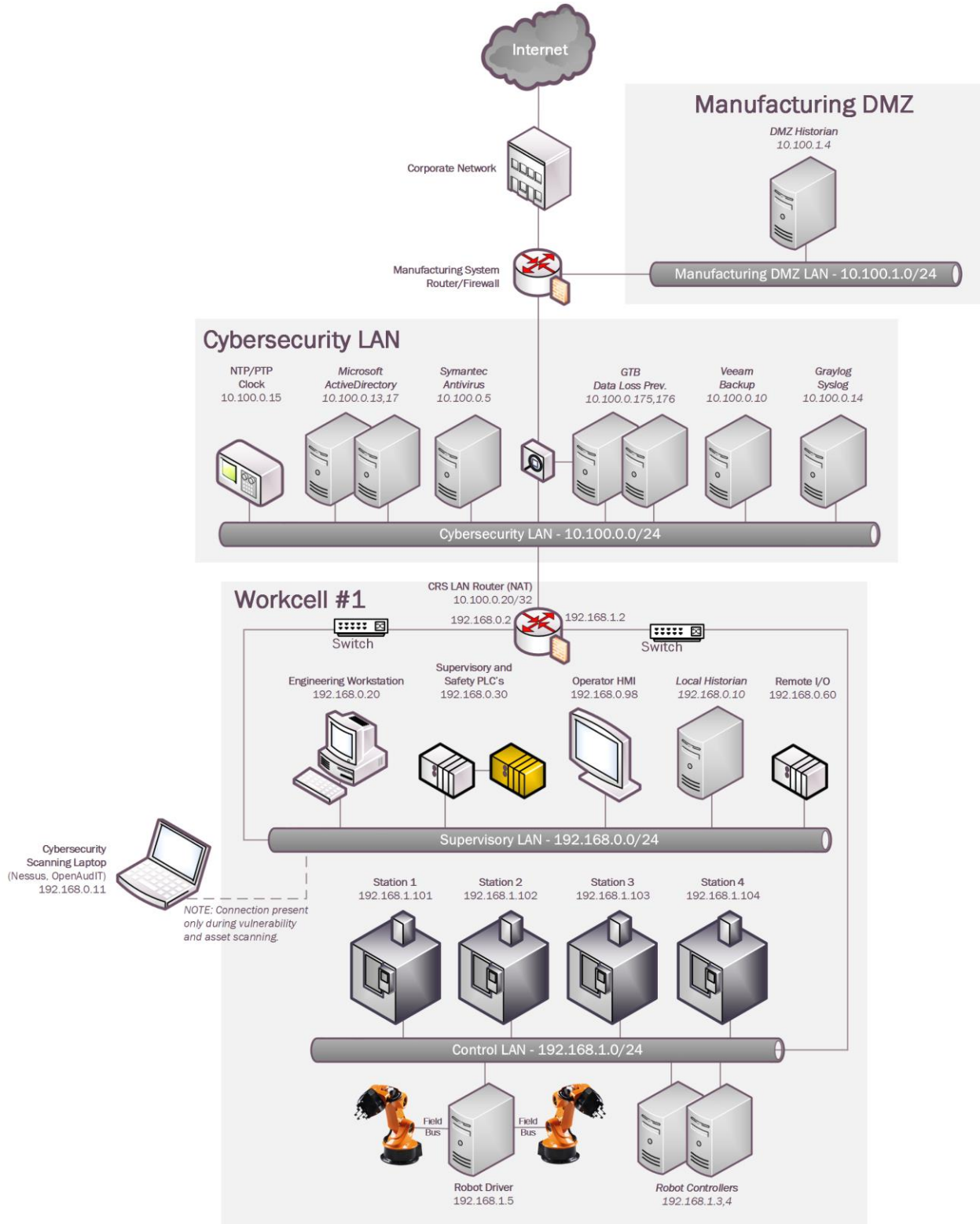
Time Synchronization provides components of the following Technical Capabilities described in Section 6 of Volume 1:

- Time Synchronization

4.18.3 Subcategories Addressed by Implementing Solution

PR.PT-1

4.18.4 Architecture Map of Where Solution was Implemented



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

4.18.5 Installation Instructions and Configurations

Details of the NTP server implemented:

| Name | IP address | Purpose | Hardware Details |
|--------------------|-------------|---------------|------------------------------|
| Grandmaster | 10.100.0.15 | NTP/PTP Clock | Model: Meinberg Lantime M900 |

4.18.5.1 Meinberg M900 Time Server

Industrial / Manufacturing environments typically need higher time accuracy than the ones provided by default capabilities of a typical Windows Active Directory environment. To accommodate this, an external hardware clock such as this one was implemented for higher time accuracy up to milliseconds level. This device was configured to obtain its Upstream time from the NIST Time server.

4.18.5.2 NTP-client Configuration on the Linux Machines of the Workcell

1. Open the `/etc/ntp.conf` file in Edit mode.
2. Add the **line server = <IP address of NTP server>** as shown below.
3. Save the file.
4. Restart ntp service using the command: `sudo service ntp restart`

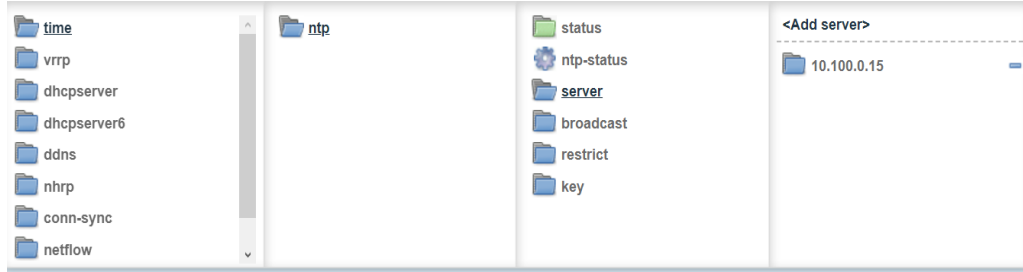
```
# Specify one or more NTP servers.

# Use servers from the NTP Pool Project. Approved by Ubuntu Technical Board
# on 2011-02-08 (LP: #104525). See http://www.pool.ntp.org/join.html for
# more information.
server 10.100.0.15 minpoll 4 maxpoll 5
#server 192.168.0.2 minpoll 4 maxpoll 5
```

5. Run `ntpq -p` to verify ntp is getting time from correct source.

4.18.5.3 NTP-client Configuration on Network Devices

1. Follow the instructions below for a Siemens RuggedCom RX1510
 - Login into RuggedCom RX 1510 web interface.
 - Click on **Edit Private** in the Top Menu to enter configuration mode
 - Click on **Services > Time > ntp > server > Add server**
 - Enter the IP address of the NTP server. Ensure to check ENABLE option.
 - Click Add button. Exit



2. Follow the instructions below to configure NTP on the Siemens i800 Layer-2 switch:
 - a. Login to the Switch web interface
 - b. Click on **Administration > System Time Manager > Configure NTP > Configure NTP Servers**
 - c. Select primary or back and make the required changes.

Server:

IP Address:

Reachable:

Update Period:

- d. Click **Apply** to save changes.
3. Follow the instructions below to configure NTP on the Netgear layer-2 switch:
 - a. Login to the switch web interface
 - b. Click **Time** from the left side explorer menu
 - c. Enter required information.
 - d. Click Apply to save the changes.

Additional Information

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 Links to Entire Performance Measurement Data Set

N/A

4.19 System Use Monitoring

4.19.1 Technical Solution Overview

System use monitoring is accomplished by multiple tools to protect manufacturing system environment from harmful activities 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 understanding of Linux systems, along with virtual machine experience.

4.19.2 Technical Capabilities Provided by Solution

System Use Monitoring provides components of the following Technical Capabilities described in Section 6 of Volume 1:

- System Use Monitoring

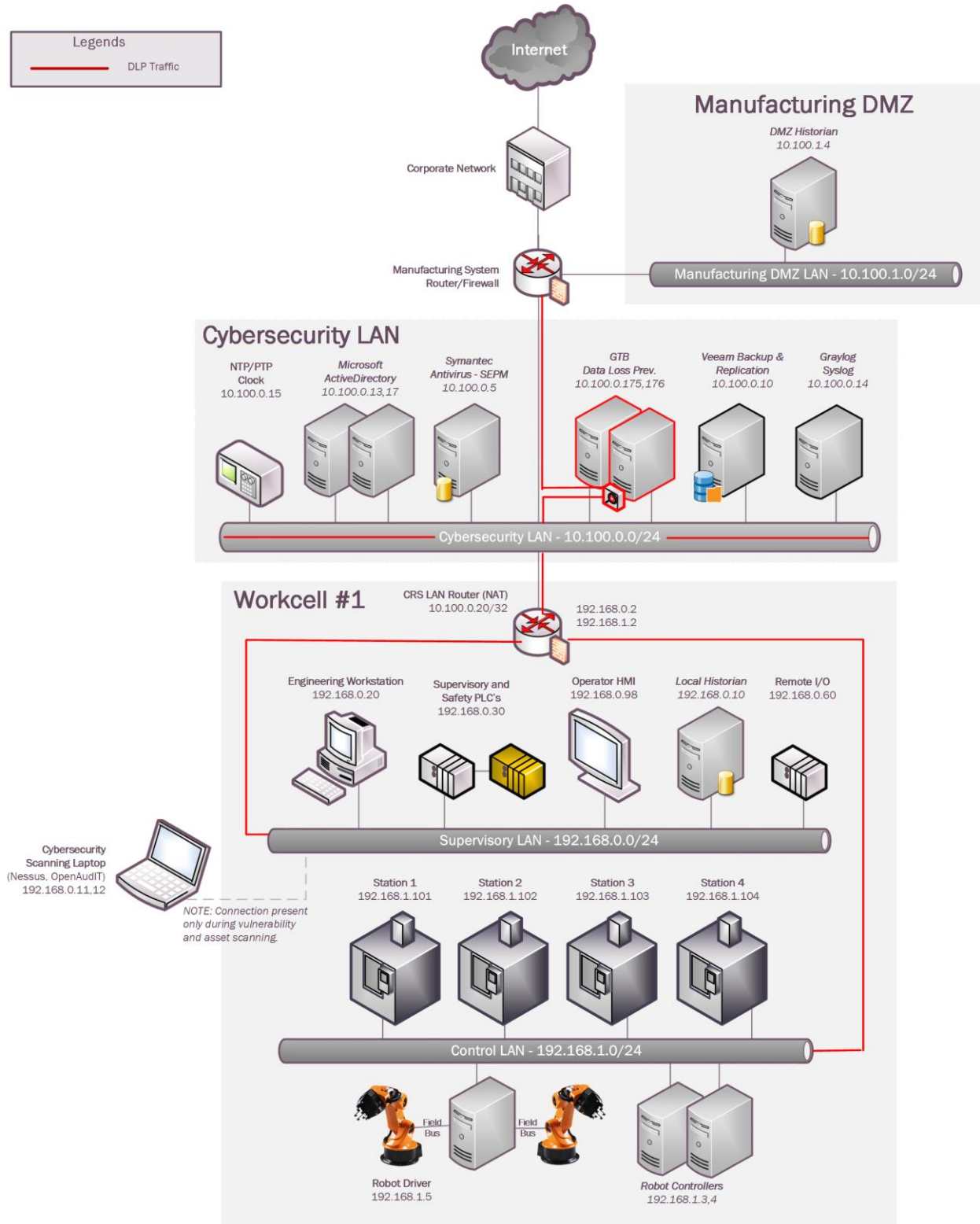
System Use Monitoring was provided by GTB Inspector, Ports and Services Lockdown, and Graylog.

4.19.3 Subcategories Addressed by Implementing Solution

PR.AC-1, PR.DS-5, PR.MA-2, DE.CM-3

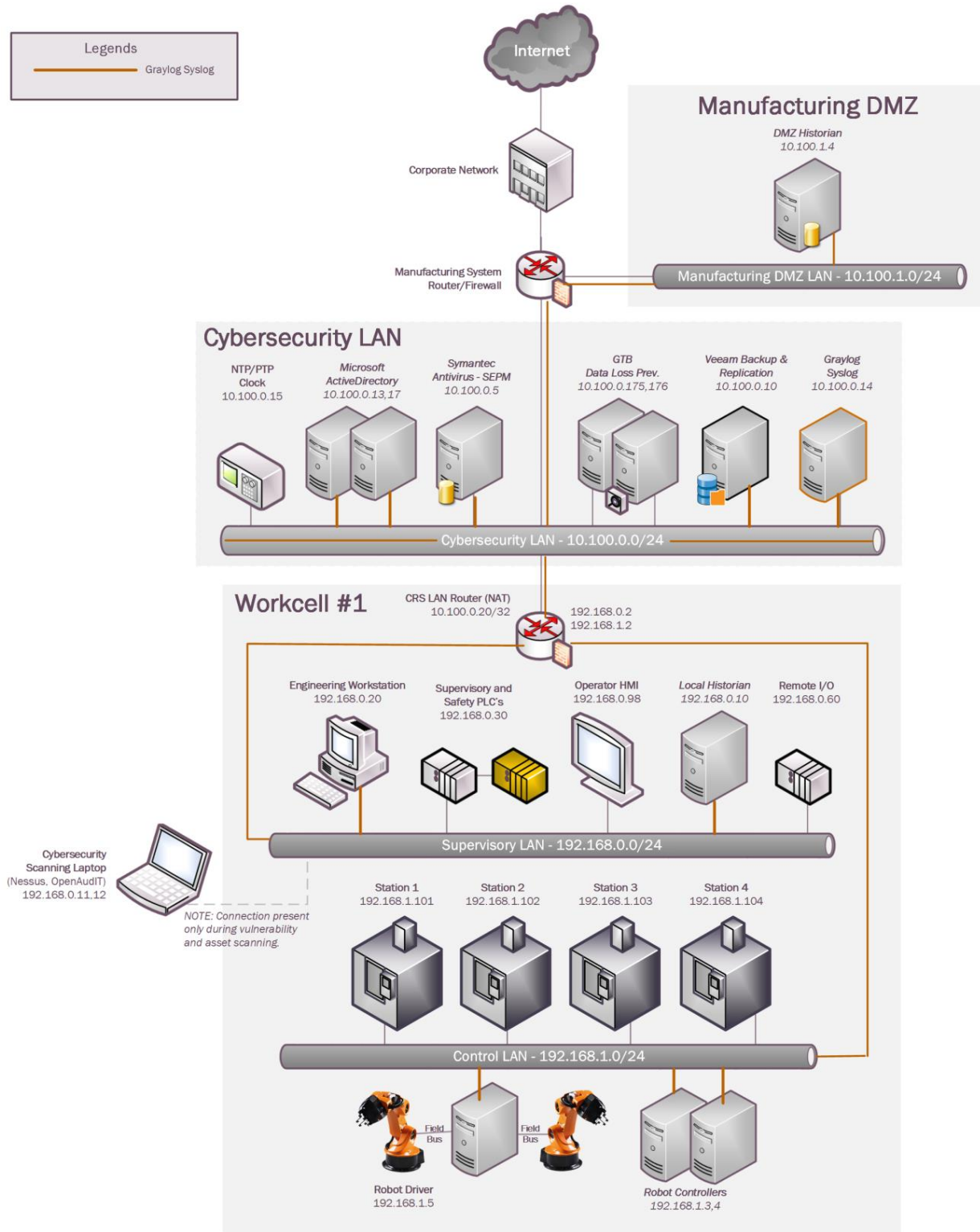
4.19.4 Architecture Map of Where Solution was Implemented

DLP Solution:



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

Graylog Solution:



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

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.

4.19.5.1 GTB Inspector

See Section 4.12.5 for instructions.

4.19.5.2 Graylog

See Section 4.13.5 for instructions.

4.19.5.3 Hardening Permissions on Linux Servers on the Workcell

Permissions on user home directories were changed from 755 to 700 to protect data from unauthorized 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 Links 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 unnecessary ports by uninstalling unnecessary 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 workcell.

4.20.2 Technical Capabilities Provided by Solution

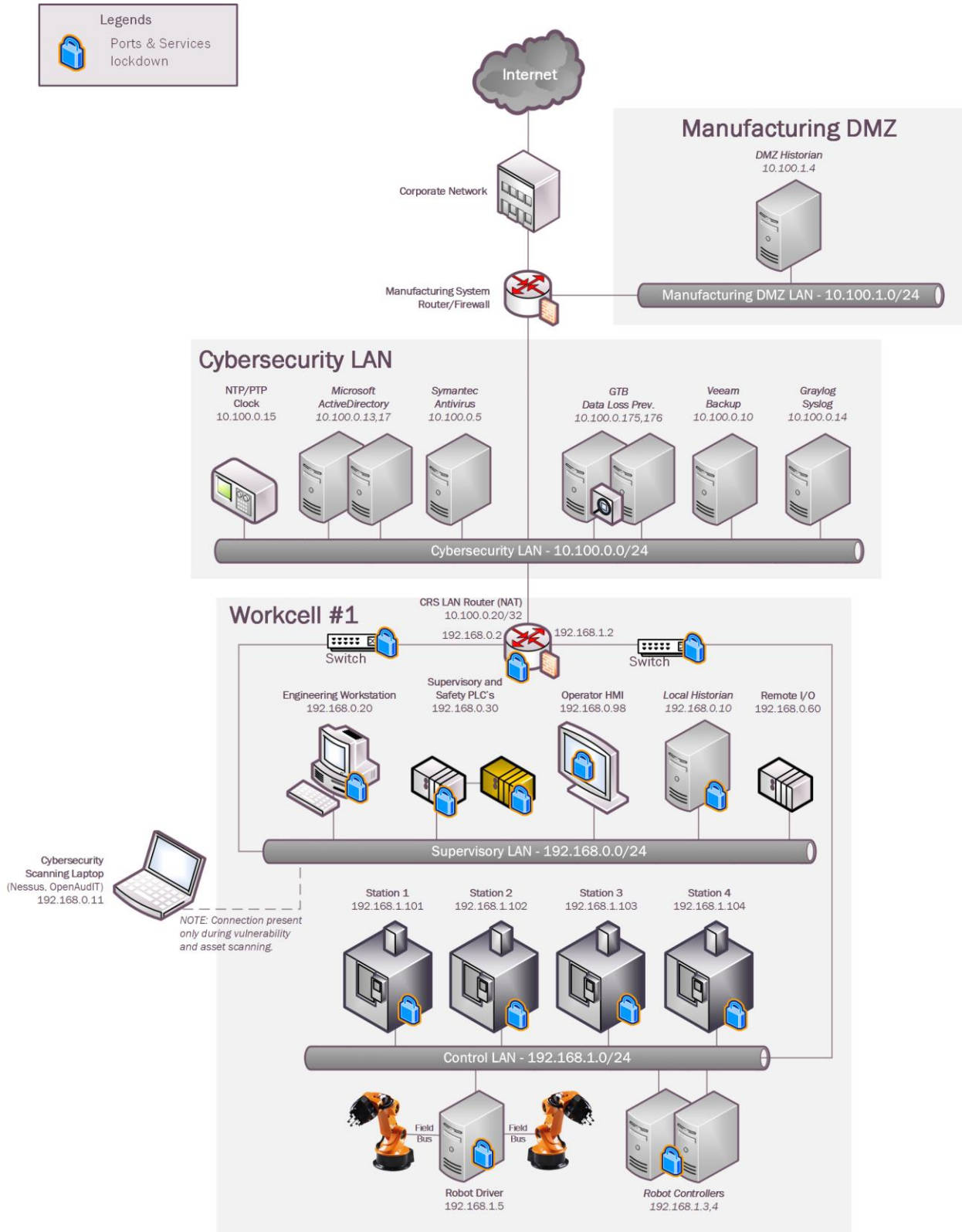
Ports and Services Lockdown provides components of the following Technical Capabilities described in Section 6 of Volume 1:

- 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



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

4.20.5 Installation Instructions and Configurations

The following steps were performed on the workcell infrastructure.

4.20.5.1 Hardening the Linux Systems

1. Perform a software inventory using the inbuilt package manager utility or via commercial tools such as Open-Audit.
2. Uninstall any unwanted software. Disable any services that are not required for operations.
3. Regulate access to device either whether Network Firewall or Host based firewall.
4. Follow any of the system hardening guidelines such as CIS, DISA.

The following actions were performed on the Linux systems of our workcell:

1. 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.
2. Hardened **/etc/exports** file on the NFS-server to export nfs-shares to specific client IP addresses with Read only permissions
3. Disabled the **dnsmasq** service and socket on machining stations, as they are not required for normal operations
4. Disabled services such as **mongodb**, **modem-manager** from Robot Driver server and Engineering Workstation.
5. Restricted SSH access to select users in the **/etc/ssh/sshd_config** file.

4.20.5.2 Hardening the Workcell HMI

1. Disable services such as HTTP, Telnet.
2. Use SNMP only if required by changing the default community string.
3. Follow vendor documentation to identify / disable other features that are not in use.

The following actions were performed on our Redlion HMI:

1. Ports 21 161 which were detected as open by Open-Audit were disabled.
2. 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.

4.20.5.3 Hardening the Workcell PLC

1. Disable services such as HTTP, Telnet and SMB (if using Windows Embedded)
2. Use SNMP only if required by changing the default community string.

The following actions were performed on our Beckhoff PLC:

1. Ports 23, 80, 139, 443, 445, 5120, and 8080 were closed by disabling services.
2. 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.
3. Remaining open TCP ports: 21, 987. FTP is used by current workcell operations
4. SMB and SNMP services were disabled. The SNMP service was disabled by modifying Windows CE registry entries.

4.20.5.4 Hardening Network Devices

1. Disable unsecure services such as Telnet, SNMP (v1 and v2). If SNMP is required, change the default community string or use SNMP v3.
2. Following vendor recommended hardening guidelines

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.

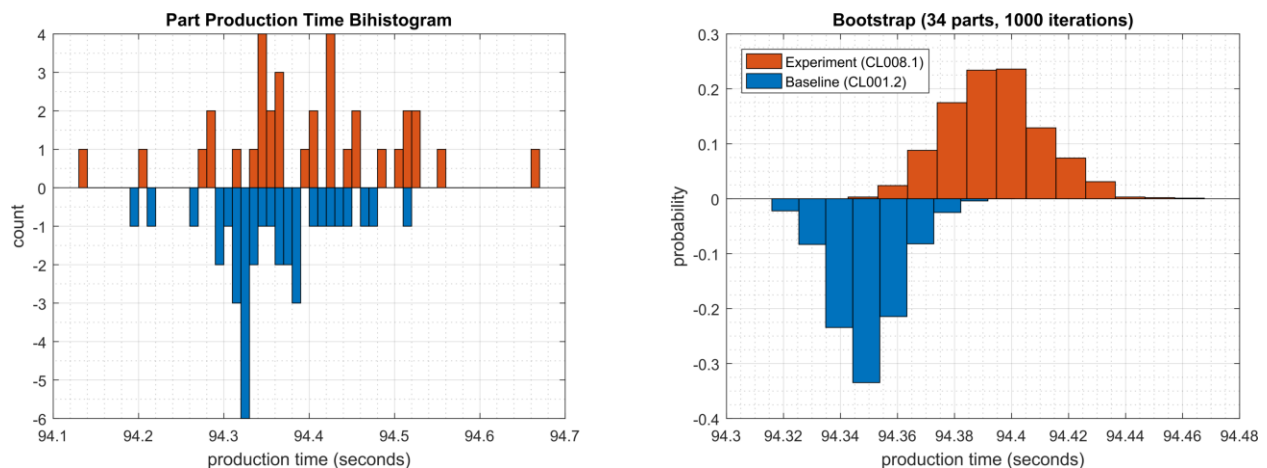


Figure 4-58 - Bihistograms showing the part production time (left) and estimated mean production time using the bootstrap method (right) using the measurements from baseline CL001.1 and experiment CL008.1

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 Linux¹⁰². 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 (preboot 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:

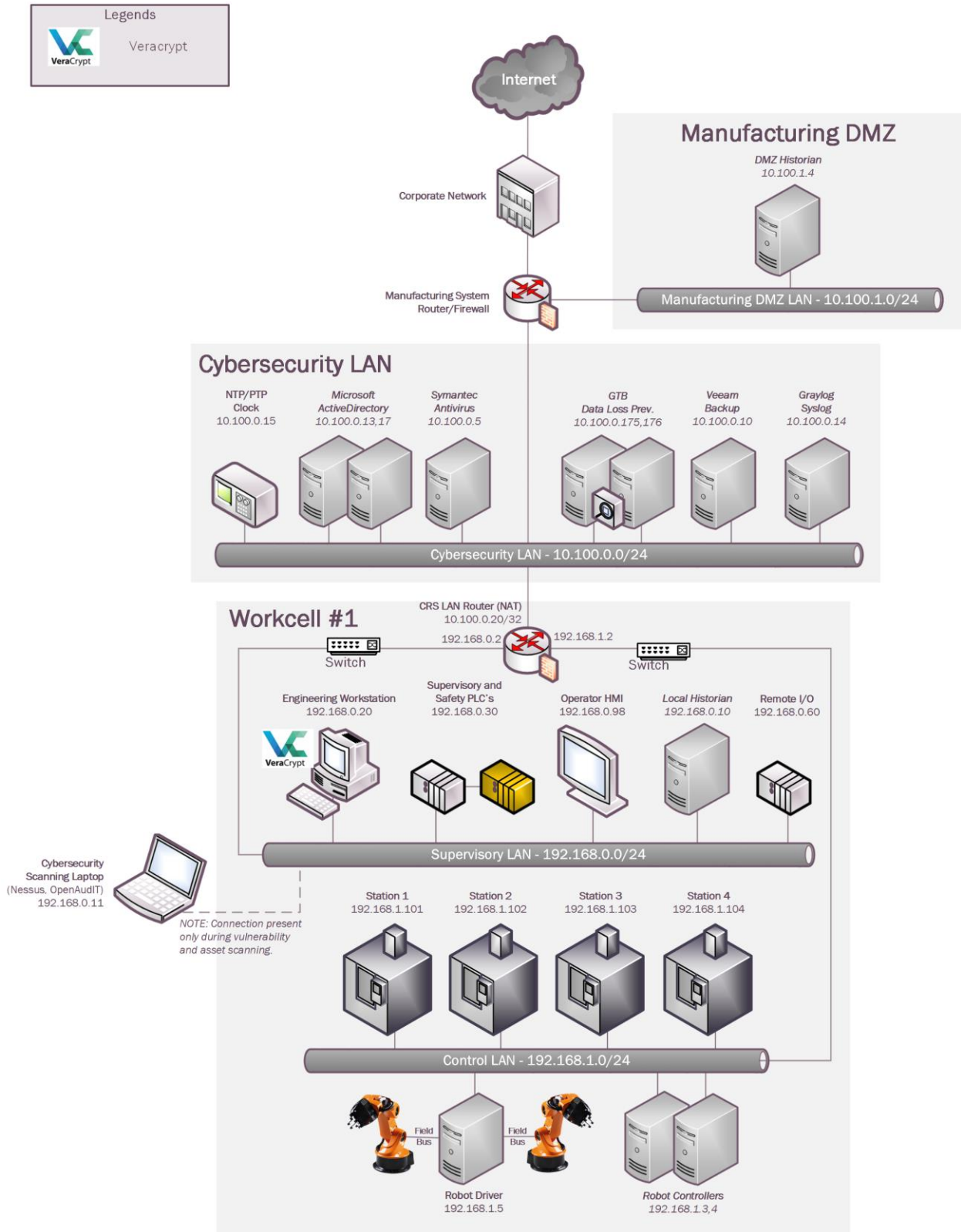
- Encryption

4.21.3 Subcategories Addressed by Implementation

PR.DS-5

¹⁰² VeraCrypt: <https://www.veracrypt.fr/en/Home.html>

4.21.4 Architecture Map of Where Solution was Implemented



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

4.21.5 Installation Instructions and Configurations

Details of the solution implemented:

| Name | Version | Location |
|-----------|---------|---------------------------|
| VeraCrypt | 1.23 | Work-Cell Supervisory LAN |

4.21.5.1 Environment Setup

VeraCrypt was installed on the Engineering Workstation (running Ubuntu Linux) to encrypt a directory containing sensitive documents and code files.

4.21.5.2 Installation

1. Download VeraCrypt¹⁰³
2. Extract the .tar.bz2 bundle 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
```

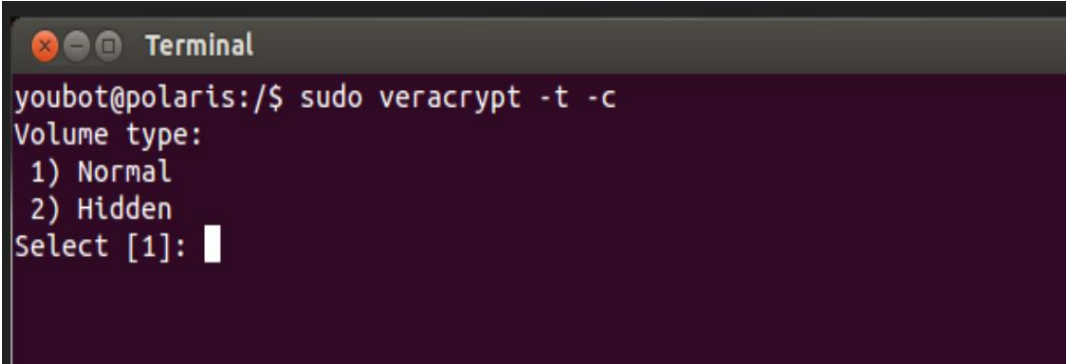
 (File name varies depending on the version used)
3. Launch the program using Unity Dash (on Ubuntu LTS) or your preferred application launcher.

4.21.5.3 Using VeraCrypt

Follow the instructions below to create an Encrypted container

1. Create an encrypted volume where you will store all folders/files you'd like to protect. Run the following command and follow the interactive menu

```
sudo veracrypt -t -c
```

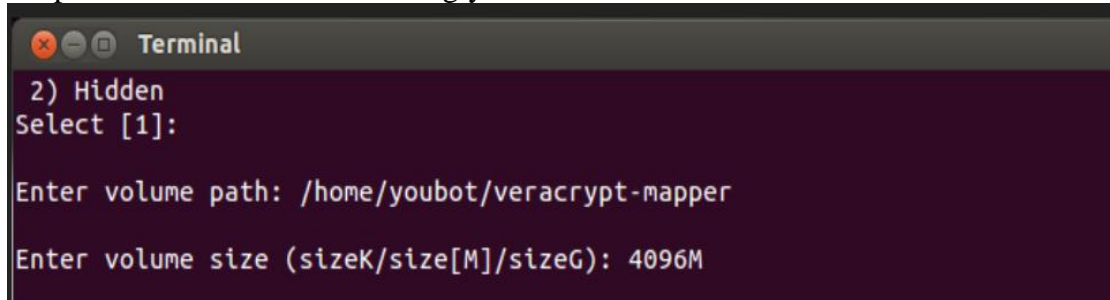


```

Terminal
youbot@polaris:/$ sudo veracrypt -t -c
Volume type:
 1) Normal
 2) Hidden
Select [1]: █
  
```

¹⁰³ <https://www.veracrypt.fr>

2. Select **1** for Normal (Standard) 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



```

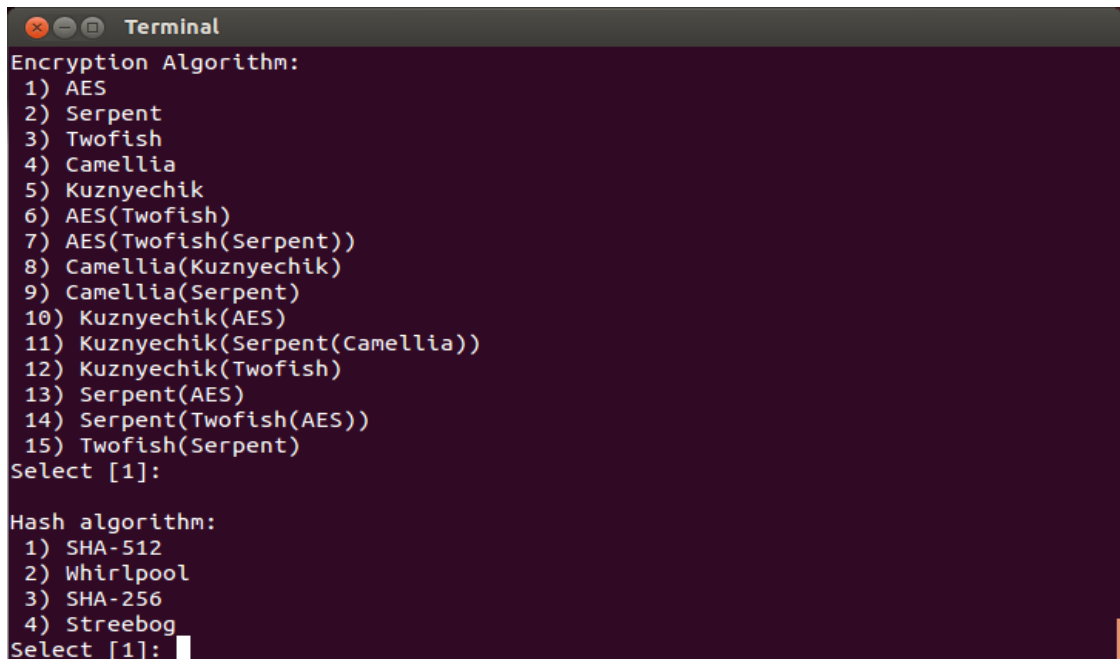
Terminal
2) Hidden
Select [1]:

Enter volume path: /home/youbot/veracrypt-mapper

Enter volume size (sizeK/size[M]/sizeG): 4096M

```

3. Select an Encryption algorithm followed by Hashing algorithm from the list



```

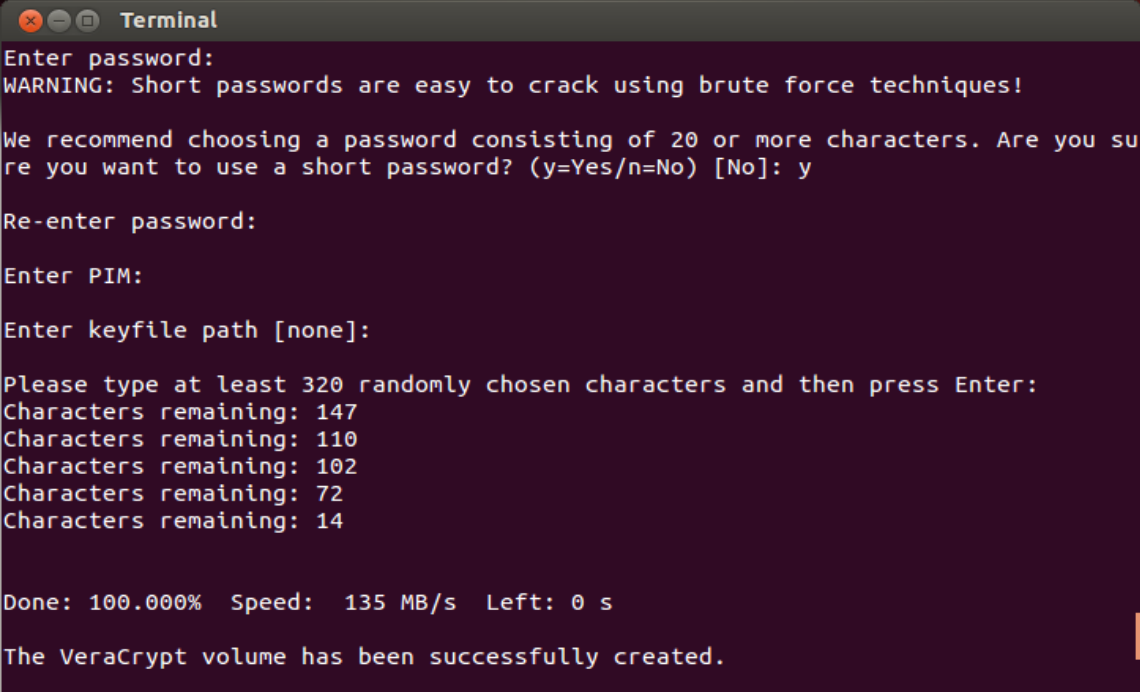
Terminal
Encryption Algorithm:
1) AES
2) Serpent
3) Twofish
4) Camellia
5) Kuznyechik
6) AES(Twofish)
7) AES(Twofish(Serpent))
8) Camellia(Kuznyechik)
9) Camellia(Serpent)
10) Kuznyechik(AES)
11) Kuznyechik(Serpent(Camellia))
12) Kuznyechik(Twofish)
13) Serpent(AES)
14) Serpent(Twofish(AES))
15) Twofish(Serpent)
Select [1]:

Hash algorithm:
1) SHA-512
2) Whirlpool
3) SHA-256
4) Streebog
Select [1]:

```

4. Select a Filesystem type depending on the OS of the computer. FAT works on all Operating systems
5. 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.

6. Enter 320 characters randomly at the prompt. This helps to increase the cryptographic strength of the encryption keys. The process should move forward.



```
Terminal
Enter password:
WARNING: Short passwords are easy to crack using brute force techniques!

We recommend choosing a password consisting of 20 or more characters. Are you su
re you want to use a short password? (y=Yes/n=No) [No]: y

Re-enter password:

Enter PIM:

Enter keyfile path [none]:

Please type at least 320 randomly chosen characters and then press Enter:
Characters remaining: 147
Characters remaining: 110
Characters remaining: 102
Characters remaining: 72
Characters remaining: 14

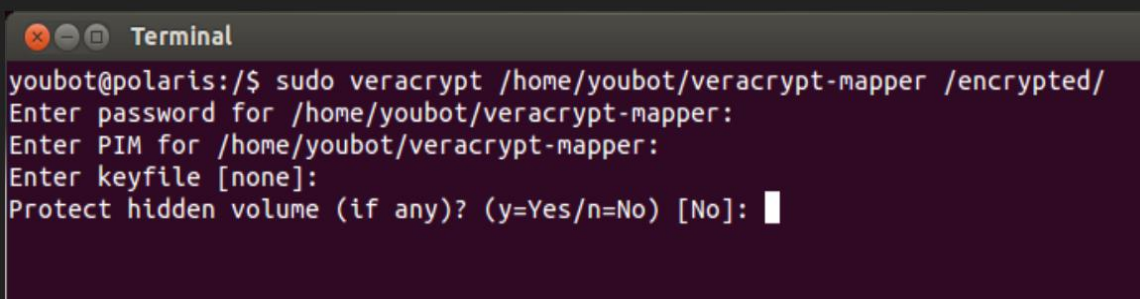
Done: 100.000% Speed: 135 MB/s Left: 0 s

The VeraCrypt volume has been successfully created.
```

7. Create a directory to mount this virtual container on. Run the following command to mount. In our case, a **/encrypted** directory was created to mount the container on.

```
sudo veracrypt <path of the container mapper file> <directory
to mount on>
```

8. 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.



```
Terminal
youbot@polaris:/$ sudo veracrypt /home/youbot/veracrypt-mapper /encrypted/
Enter password for /home/youbot/veracrypt-mapper:
Enter PIM for /home/youbot/veracrypt-mapper:
Enter keyfile [none]:
Protect hidden volume (if any)? (y=Yes/n=No) [No]:
```

9. Verify the mount by running `df -kh`

```

youbot@polaris:~$ df -kh
df: /home/zimmermant/.gvfs': Permission denied
Filesystem      Size  Used Avail Use% Mounted on
/dev/sda1        1.8T   44G  1.7T   3% /
udev             7.8G   4.0K  7.8G   1% /dev
tmpfs            1.6G   936K  1.6G   1% /run
none             5.0M     0   5.0M   0% /run/lock
none             7.9G   324K  7.9G   1% /run/shm
/dev/mapper/veracrypt1 4.8G   10M  4.6G   1% /encrypted
youbot@polaris:~$ █

```

Additional Information

- By default, other system users would only have **Read** access to the mounted directory. 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 in case 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.
- Veracrypt official documentation¹⁰⁴

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 Links to Entire Performance Measurement Data Set

N/A

¹⁰⁴ <https://www.veracrypt.fr/en/Documentation.html>

4.22 Media Protection

4.22.1 Technical Solution Overview

Hardware-based 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 the lock device without damaging the USB port unless a 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

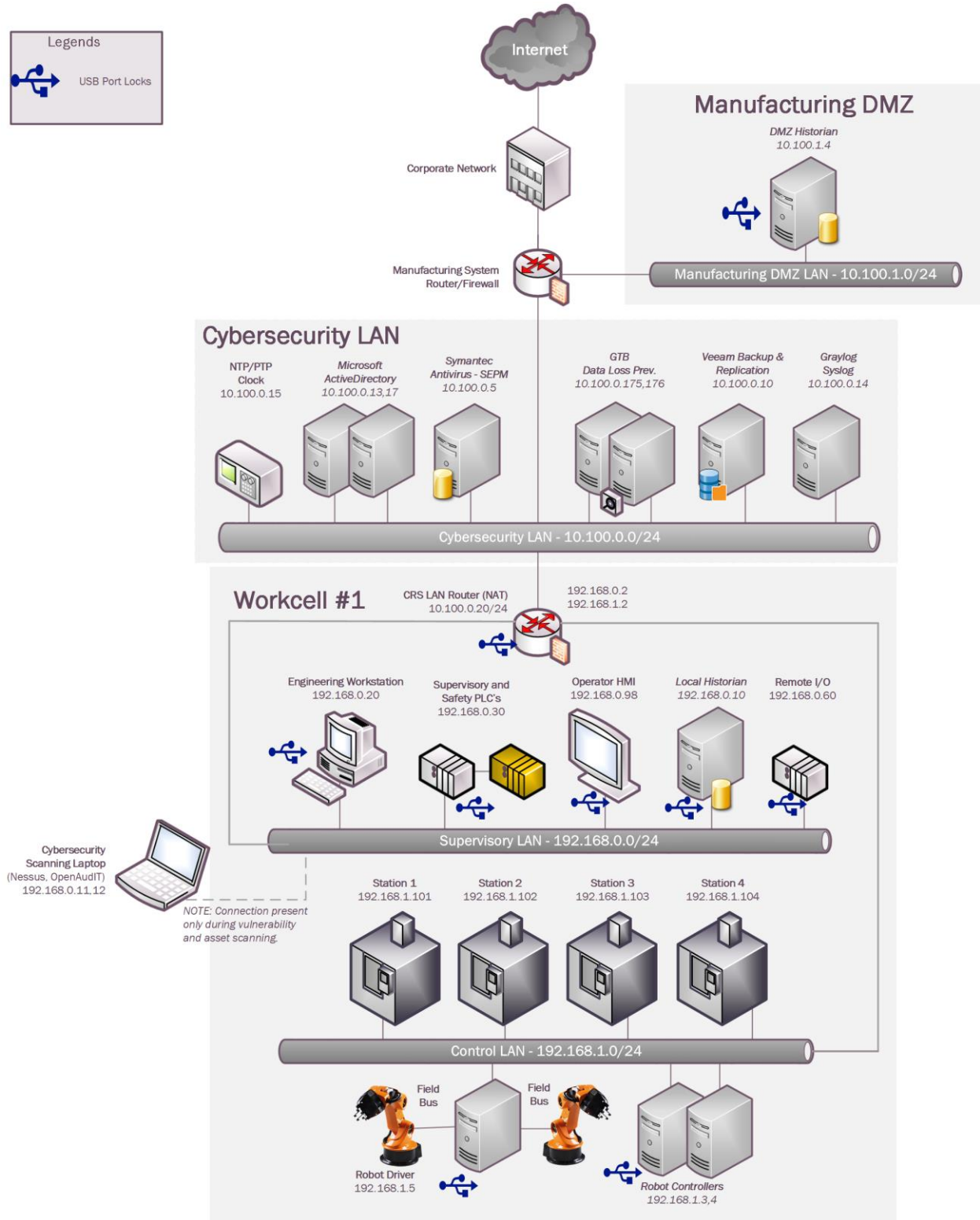
Media Protection provides components of the following Technical Capabilities described in Section 6 of Volume 1:

- Media Protection

4.22.3 Subcategories Addressed by Implementation

PR.PT-2

4.22.4 Architecture Map of Where Solution was Implemented



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

4.22.5 Installation Instructions and Configurations

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.

Patience is required when using this product so as not to inadvertently damage the 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 Links to Entire Performance Measurement Data Set

N/A

Appendix A - Acronyms and Abbreviations

Selected acronyms and abbreviations used in this document are defined below.

| | |
|-----------------|--|
| ACL | Access Control List |
| AD | Active Directory |
| API | Application Programming Interface |
| ARP | Address Resolution Protocol |
| AV | Anti-Virus |
| CCN | Credit Card Number |
| CD | Compact Disk |
| CNC | Computer Numerical Control |
| COTS | Commercial Off-The-Shelf |
| CSET | Cyber Security Evaluation Tool |
| CSF | Cybersecurity Framework |
| DC | Domain Controller |
| DCS | Distributed Control System |
| DHCP | Dynamic Host Configuration Protocol |
| DHS | Department of Homeland Security |
| DLP | Data Loss Prevention |
| DMZ | Demilitarized Zone |
| DNS | Domain Name System |
| DS | Domain Services |
| EFS | Encrypted File System |
| FIPS | Federal Information Processing Standards |
| FTP | File Transfer Protocol |
| GID | Generator ID |
| HIDS | Host Intrusion Detection System |
| HMI | Human Machine Interface |
| HR | Human Resources |
| HTTP | Hypertext Transfer Protocol |
| HTTPS | Hypertext Transfer Protocol Secure |
| HVAC | Heating, Ventilation, and Air Conditioning |
| ICMP | Internet Control Message Protocol |
| ICS | Industrial Control System |
| ICS-CERT | Industrial Control Systems Cyber Emergency Response Team |
| ICSJWG | Industrial Control System Joint Working Group |
| IDE | Integrated Drive Electronics |
| IDS | Intrusion Detection System |

| | |
|----------------|--|
| IEEE | Institute of Electrical and Electronics Engineers |
| IG | Implementation Guide |
| IP | Internet Protocol |
| ISA | The International Society of Automation |
| ISE | Identity Services Engine |
| ISO | International Organization for Standardization |
| IT | Information Technology |
| KPI | Key Performance Indicator |
| LAN | Local Area Network |
| LDAP | Lightweight Directory Access Protocol |
| LDAPS | Secure LDAP |
| MAC | Media Access Control |
| MFG | Manufacturing |
| MGMT | Management |
| NAT | Network Address Translation |
| NCCIC | National Cybersecurity and Communications Integration Center |
| NETBIOS | Network Basic Input/Output System |
| NIDS | Network Intrusion Detection System |
| NIST | National Institute of Standards and Technology |
| NISTIR | National Institute of Standards and Technology Internal Report |
| NPS | Network Policy Server |
| NSA | National Security Agency |
| NTFS | New Technology File System |
| NTP | Network Time Protocol |
| NVD | National Vulnerability Database |
| OPC | Open Platform Communications |
| OS | Operating System |
| OSSEC | Open Source HIDS SECURITY |
| OT | Operational Technology |
| PC | Personal Computer |
| PCS | Process Control System |
| PLC | Programmable Logic Controller |
| PPD | Presidential Policy Directive |
| PPP | Point to Point protocol |
| PPTP | Point to Point tunneling protocol |
| PTP | Precision Time Protocol |
| RDP | Remote Desktop Protocol |
| ROS | Robot Operating System |
| SCADA | Supervisory Control and Data Acquisition |

| | |
|----------------|---|
| SDLC | System Development Lifecycle |
| SEC | Security |
| SEPM | Symantec End-Point Protection Manager |
| SID | Signature ID |
| SIEM | Security Information and Event Management |
| SMB | Server Message Block |
| SMTP | Simple Mail Transfer Protocol |
| SNMP | Simple Network Management Protocol |
| SSH | Secure Shell |
| SSL | Secure Socket Layer |
| SSN | Social Security Number |
| TCP | Transmission Control Protocol |
| TLS | Transport Layer Security |
| UAC | User Access Control |
| UI | User Interface |
| UNC | Universal Naming Convention |
| UPN | Universal Principal Name |
| UPS | Uninterruptable Power Supply |
| USB | Universal Serial Bus |
| US-CERT | United States Computer Emergency Readiness Team |
| VHD | Virtual Hard Drive |
| VHDX | Hyper-V virtual hard disk |
| VLAN | Virtual Local Area Network |
| VPN | Virtual Private Network |
| WAN | Wide Area Network |
| WMI | Windows Management Instrumentation |
| XML | eXtensible Markup Language |

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 workcell 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 (2019) 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>