1	DRAFT NISTIR 8183A
2	Volume 3
3	
4	<b>Cybersecurity Framework Manufacturing Profile</b>
5	Low Security Level Example
6	<b>Implementations Guide:</b>
7	Volume 3 – Discrete-based Manufacturing System Use Case
8	
9	Keith Stouffer
10	Timothy Zimmerman
11	CheeYee Tang
12	Jeffrey Cichonski
13	Neeraj Shah
14	Wesley Downard
15	
10	This publication is available free of charge from:
18	https://doi.org/10.6028/NIST.IR.8183A-3-draft
19 20	



21	DF	RAFT NISTIR 8183A
22		Volume 3
25	Cyborcocurity Fromowork Ma	nufacturing Profila
24	Cyber security Framework Ma	
25	Low Secu	rity Level Example
26	Imple	ementations Guide:
27	Volume 3 – Discrete-based Manufac	cturing System Use Case
28		
29	Keith Stouffer	Neeraj Shah
30	Timothy Zimmerman	Strativia, LLC
31	CheeYee Tang	Largo, Maryland
32 33	Intelligent Systems Division Engineering Laboratory	
34	Engineering Laboratory	
35	Jeffrey Cichonski	Wesley Downard
36	Applied Cybersecurity Division	<i>G2, Inc.</i>
37	Information Technology Laboratory	Annapolis Junction, Maryland
38		
39		
40		
41	This publication	is available free of charge from:
42	https://doi.org/	10.6028/NIST.IR.8183A-3-draft
43		
44		May 2019
45 46		
		SORTINENT OF COMMIT
47		STATES OF
49 50		U.S. Department of Commerce Wilbur L. Ross, Jr., Secretary
51 52	Na	ational Institute of Standards and Technology
53	Walter Copan, NIST Director and Under Secretary	of Commerce for Standards and Technology

54 55 56 57 58	National Institute of Standards and Technology Internal Report 8183A, Volume 3 333 pages (May 2019) This publication is available free of charge from: https://doi.org/10.6028/NIST.IR.8183A-3-draft	
59 60 61 62	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.	
63 64 65 66 67 68	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.	
69 70 71	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 <u>https://csrc.nist.gov/publications</u> .	
72		

72	
73	Public comment period: May 28, 2019through July 8, 2019
74	National Institute of Standards and Technology
75	Attn: Applied Cybersecurity Division, Information Technology Laboratory
76	100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000
77	Email: CSF_Manufacturing_Profile_Implementation@nist.gov
78	
79	All comments are subject to release under the Freedom of Information Act (FOIA).
80	······································

## Abstract

82 83	This guide provides example proof-of-concept solutions demonstrating how open-source and commercial off-the-shelf (COTS) products that are currently available today can be implemented		
84	in discrete-based manufacturing environments to satisfy the requirements in the Cybersecurity		
85	Framework (CSF) Manufacturing Profile [4] Low Security Level. The example proof-of-concept		
86	solutions include measured network, device, and operational performance impacts observed		
87	during the implementation. Depending on factors like size, sophistication, risk tolerance, and		
88	threat landscape, manufacturers should make their own determinations about the breadth of the		
89	proof-of-concept solutions they may voluntarily implement. The CSF Manufacturing Profile can		
90	be used as a roadmap for managing cybersecurity risk for manufacturers and is aligned with		
91	manufacturing sector goals and industry best practices. The Manufacturing Profile provides a		
92	voluntary, risk-based approach for managing cybersecurity activities and cyber risk to		
93	manufacturing systems. The Manufacturing Profile is meant to compliment but not replace		
94	current cybersecurity standards and industry guidelines that the manufacturer is embracing.		
95			
96	Keywords		
97 98 99 100	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.		
101	Supplemental Content		
102	Additional volumes of this publication include:		
102			
105	Draft NISTIR 8183A Volume 1, Cybersecurity Framework Manufacturing Profile Low		
103 104	Draft NISTIR 8183A Volume 1, Cybersecurity Framework Manufacturing Profile Low Security Level Example Implementations Guide: Volume 1 – General Implementation		
103 104 105	Draft NISTIR 8183A Volume 1, Cybersecurity Framework Manufacturing Profile Low Security Level Example Implementations Guide: Volume 1 – General Implementation Guidance. <u>https://doi.org/10.6028/NIST.IR.8183A-1-draft</u>		
103 104 105	Draft NISTIR 8183A Volume 1, Cybersecurity Framework Manufacturing Profile Low Security Level Example Implementations Guide: Volume 1 – General Implementation Guidance. <u>https://doi.org/10.6028/NIST.IR.8183A-1-draft</u>		
103 104 105 106	<ul> <li>Draft NISTIR 8183A Volume 1, Cybersecurity Framework Manufacturing Profile Low Security Level Example Implementations Guide: Volume 1 – General Implementation Guidance. <u>https://doi.org/10.6028/NIST.IR.8183A-1-draft</u></li> <li>Draft NISTIR 8183A Volume 2, Cybersecurity Framework Manufacturing Profile Low Security Level Example Implementations Guida: Volume 2 – Process based</li> </ul>		

108 Manufacturing System Use Case. https://doi.org/10.6028/NIST.IR.8183A-2-draft

# Acknowledgments

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

# 116

# Note to Reviewers

- 117 This guide does not describe the solution, but a possible solution. This is a draft guide. We seek
- 118 feedback on its contents and welcome your input. Comments, suggestions, and success stories
- 119 will improve subsequent versions of this guide. Please contribute your thoughts to
- 120 <u>CSF\_Manufacturing\_Profile\_Implementation@nist.gov</u>.
- 121

# **Call for Patent Claims**

123 This public review includes a call for information on essential patent claims (claims whose use 124 would be required for compliance with the guidance or requirements in this Information 125 Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be 126 directly stated in this ITL Publication or by reference to another publication. This call also 127 includes disclosure, where known, of the existence of pending U.S. or foreign patent applications 128 relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents. 129 130 ITL may require from the patent holder, or a party authorized to make assurances on its behalf, 131 in written or electronic form, either: 132 133 a) assurance in the form of a general disclaimer to the effect that such party does not hold and 134 does not currently intend holding any essential patent claim(s); or 135 136 b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in 137 138 this ITL draft publication either: 139 140 i) under reasonable terms and conditions that are demonstrably free of any unfair 141 discrimination; or 142 143 ii) without compensation and under reasonable terms and conditions that are 144 demonstrably free of any unfair discrimination. 145 146 Such assurance shall indicate that the patent holder (or third party authorized to make assurances 147 on its behalf) will include in any documents transferring ownership of patents subject to the 148 assurance, provisions sufficient to ensure that the commitments in the assurance are binding on 149 the transferee, and that the transferee will similarly include appropriate provisions in the event of 150 future transfers with the goal of binding each successor-in-interest. 151 152 The assurance shall also indicate that it is intended to be binding on successors-in-interest 153 regardless of whether such provisions are included in the relevant transfer documents. 154 155 Such statements should be addressed to: CSF\_Manufacturing\_Profile\_Implementation@nist.gov 156

157					
158	3 Table of Contents				
159	Executive Summary vii				
160	1.	Introduction	1		
161 162 163		<ul><li>1.1 Purpose and Scope</li><li>1.2 Audience</li><li>1.3 Document Structure</li></ul>	1 2 2		
164	2.	Discrete-based Manufacturing System Low Security Level Use Case	3		
165 166		<ul><li>2.1 Introduction</li><li>2.2 Discrete-based Low Security Level Use Case</li></ul>			
167	3.	Policy and Procedure Implementations	9		
168 169 170 171 172 173		<ul> <li>3.1 Security Program Document Example</li></ul>			
174	4.	Technical Solution Implementations	102		
175 176 177 178 179 180 181 182 183 184 185 186 187 188		<ul> <li>4.1 Introduction</li></ul>			
189 190 191 192 193 194 195 196		<ul> <li>4.15 Network Segmentation and Segregation</li> <li>4.16 Network Boundary Protection</li> <li>4.17 Managed Network Interfaces</li> <li>4.18 Time Synchronization</li> <li>4.19 System Use Monitoring</li> <li>4.20 Ports and Services Lockdown</li> <li>4.21 VeraCrypt</li> <li>4.22 Media Protection</li> </ul>	272 276 287 296 301 305 309 316		

197		
198	Appendix A - Acronyms and Abbreviations	
199	Appendix B - Glossary	
200	Appendix C - References	
201		

## 202 Executive Summary

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

- 210 proof-of-concept solutions they may voluntarily implement.
- 211 The CSF Manufacturing Profile can be used as a roadmap for managing cybersecurity risk for
- 212 manufacturers and is aligned with manufacturing sector goals and industry best practices. The
- 213 Manufacturing Profile provides a voluntary, risk-based approach for managing cybersecurity
- activities and cyber risk to manufacturing systems. The Manufacturing Profile is meant to
- 215 compliment but not replace current cybersecurity standards and industry guidelines that the
- 216 manufacturer is embracing.
- 217 The CSF Manufacturing Profile focuses on desired cybersecurity outcomes and can be used as a
- 218 roadmap to identify opportunities for improving the current cybersecurity posture of the
- 219 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
- 221 implemented to support key business/mission goals are then identified.
- 222 While the proof-of-concept solutions in this guide used a suite of commercial products, this
- 223 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
- 225 products that will best integrate with your existing tools and manufacturing system
- 226 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
- 228 implementing parts of a solution. This guide does not describe regulations or mandatory
- 229 practices, nor does it carry any statutory authority.

### 230 **1.** Introduction

231 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
- 235 infrastructure services.
- 236 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

239 language to address and manage cybersecurity risk in a cost-effective way based on business

- 240 needs without imposing additional regulatory requirements.
- 241 To address the needs of manufactures, a Manufacturing Profile [4] of the Cybersecurity

242 Framework was developed, through collaboration between government and the private sector, to

243 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

245 protection of the manufacturing system, its components, facility, and environment. Through use

of the Profile, the manufacturer can align cybersecurity activities with business requirements,

247 risk tolerances, and resources. The Profile provides a manufacturing sector-specific approach to

248 cybersecurity from standards, guidelines, and industry best practices.

# 249 **1.1** Purpose and Scope

250 Many small and medium sized manufacturers have expressed that they are challenged in 251 implementing a standards-based cybersecurity program. This guide provides example proof-of-252 concept solutions demonstrating how open-source and commercial off-the-shelf (COTS) 253 products that are available today can be implemented in manufacturing environments to satisfy 254 the requirements in the Cybersecurity Framework (CSF) Manufacturing Profile Low Security 255 Level. Example proof-of-concept solutions with measured network, device, and operational performance impacts for a process-based manufacturing environment (Volume 2) and a discrete-256 257 based manufacturing environment (Volume 3) are included in the guide. Depending on factors 258 like size, sophistication, risk tolerance, and threat landscape, manufacturers should make their 259 own determinations about the breadth of the proof-of-concept solutions they may voluntarily 260 implement. The CSF Manufacturing Profile can be used as a roadmap for managing 261 cybersecurity risk for manufacturers and is aligned with manufacturing sector goals and industry 262 best practices. The Manufacturing Profile provides a voluntary, risk-based approach for 263 managing cybersecurity activities and cyber risk to manufacturing systems. The Manufacturing 264 Profile is meant to enhance but not replace current cybersecurity standards and industry

265 guidelines that the manufacturer is embracing.

266 While the proof-of-concept solutions in this guide used a suite of commercial products, this

267 guide does not endorse these particular products, nor does it guarantee compliance with any

- 268 regulatory initiatives. Each organization's information security experts should identify the
- 269 products that will best integrate with their existing tools and manufacturing system

- 270 infrastructure. Organizations may voluntarily adopt these solutions or one that adheres to these
- 271 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.
- 274 This project is guided by the following assumptions: The solutions were developed in a lab
- environment. The environment is based on a typical small manufacturer. The environment does
- not reflect the complexity of a production environment. An organization can access the skills and
- 277 resources required to implement a manufacturing cybersecurity solution.

# 278 **1.2 Audience**

279 This document covers details specific to manufacturing systems. Readers of this document

- should be acquainted with operational technology, general computer security concepts, and
- 281 communication protocols such as those used in networking. The intended audience is varied and
- 282 includes the following:
- 283 • Control engineers, integrators, and architects who design or implement secure 284 manufacturing systems. 285 System administrators, engineers, and other information technology (IT) professionals • who administer, patch, or secure manufacturing systems. 286 • Managers who are responsible for manufacturing systems. 287 • Senior management who are trying to understand implications and consequences as they 288 289 justify and implement a manufacturing systems cybersecurity program to help mitigate 290 impacts to business functionality. 291 Researchers, academic institutions and analysts who are trying to understand the unique • security needs of manufacturing systems. 292 293 **1.3 Document Structure** 294 Volume 3 is divided into the following major sections: 295 • Section 2 provides an overview of the discrete-based manufacturing system use case. 296 • Section 3 provides the detailed policy and procedure documents developed for the 297 discrete-based manufacturing system use case. 298 • Section 4 provides the detailed technical capability implementations and associated 299 performance measurements for the discrete-based manufacturing system use case. 300 • 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.
- 303

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

#### 305 **2.1** Introduction

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

### 312 **2.2 Discrete-based Low Security Level Use Case**

- 313 The fictional company, Alpha Manufacturing (i.e., Alpha), is a small manufacturer that produces
- 314 common metal components for the automotive industry. These parts are typically subcontracted
- to Alpha by larger manufacturers. The finished parts are then integrated into
- 316 larger subassemblies that perform non-safety related functions within a vehicle.
- 317 To meet increasing production demand, an automated workcell was contracted and purchased
- from a manufacturing systems integrator. The first workcell was purchased to evaluate and
- 319 validate its operation, with the intent of purchasing more workcells to further increase
- 320 production. Two of the machining stations integrated into the workcell were existing at the
- 321 Alpha facility, while the other two stations were purchased by the integrator. The workcell
- 322 operates independently of all other shop operations, and is tended to by a single operator, who:
- 323 loads raw material, unloads finished parts, responds to alarm conditions, and validates the quality
- of finished parts.

## 325 **2.2.1 Facilities**

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

#### 327 **2.2.2 Employees**

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

Organizational Role	Count
President	1
HR Manager	1
Bookkeeper	1

Foreman/Supervisor	1
Machine Operators	6
Total	10

#### 331 2.2.3 External Personnel

332 Some facility operations are outsourced to external entities.

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

333

#### 334 2.2.4 Supply Chain

335 Raw material suppliers are utilized on-demand. No formal relationships or direct-order 336 networking/online/cloud connections with any suppliers currently exist. Alpha is considered a

"tier two" supplier. Alpha sends completed parts to a tier one manufacturer. At the tier one 337

338 manufacturer's facility, Alpha's parts are integrated into subassemblies that are subsequently 339

installed into a vehicle by the original equipment manufacturer (OEM).

#### 340 2.2.5 Supporting Services

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

#### 343 2.2.6 Legal and Regulatory Requirements

344 Alpha does not have knowledge of any legal or regulatory requirements in regards to its

- 345 cybersecurity. However, as a tier two supplier, it is contractually obligated to follow all
- standards, procedures, and guidance provided by the tier one manufacturer(s) and the OEM (e.g., 346

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

# 349 **2.2.7** Critical Infrastructure

- 350 The DHS Critical Manufacturing sector considers vehicle manufacturing (and its supply chain) a
- 351 core industry to be protected. However, Alpha is a tier two manufacturer that produces parts that
- are not critical to vehicle safety and can easily be produced by other tier two job shops if Alpha cannot meet its production demand. It is likely that the tier one manufacturer has already
- 353 callot meet its production demand. It is fixely that the tier one manufacturer 354 implemented supply chain redundancy to enable continuity of production.
- 355 Alpha will not be able to produce if the primary metals critical manufacturing sector cannot
- 356 provide Alpha with the required raw materials. However, this sector is outside of the scope of
- 357 Alpha's implementation of the Manufacturing Profile.

# 358 2.2.8 Manufacturing Process

- 359 Parts are created in a sequential manufacturing process with four CNC machines within a
- 360 workcell. The CNC machines are tended to by two industrial robotic arms, which transfer parts
- to each station until all of the machining processes are completed. Raw materials are loaded into
- a queue by an operator. A supervisory PLC monitors the dynamic status of each machining
- 363 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
- 365 robot, subsequently dropping into either a finished parts bin, or a rejected parts bin. The bins are
- 366 emptied by operators once they are full.

# 367 The manufacturing process is as follows:



# 368 **2.2.9 Systems**

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

# 372 2.2.10 Critical Systems

- 373 The following systems are critical for proper operation of the workcell:
- Engineering workstation
- Supervisory PLC
- 376 HMI
- Machining stations
- Robot arms

- Robot controllers
- 380•Robot driver
- Networking equipment

## 382 2.2.11 Data

- 383 Data transferred over, or stored within, Alpha's network includes:
- PLC code
- 385•Robot code
- MODBUS TCP registers
- Computer-aided Manufacturing (CAM) files (e.g., G code)
- Workcell operating manuals and documentation
- Electrical diagrams
- Network diagrams
- Computer-aided drafting (CAD) files
- Part inspection measurements
- Historical production data
- 394 NOTE: All data listed above are proprietary, trade secrets, and/or confidential.

## 395 2.2.12 Network

396 The manufacturing system network is connected to the corporate network through a dedicated

397 top-level router/firewall, and is organized into subnetworks and a DMZ. The network is managed

398 by the external IT contractor. The workcell has a dedicated router/firewall utilizing network

399 address translation (NAT) to help segment and isolate the workcell from the rest of the network.

400 The workcell itself is split into two subnets: the Supervisory LAN, and the Control LAN.

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

# 403 2.2.13 Mission Objectives

- 404 The Manufacturing Profile describes five business/mission objectives common to the
- 405 manufacturing sector. The following sections describe what Alpha must protect, in regards to406 their manufacturing process and assets, in order to meet each of the missions:

# 407 1. Maintain Personnel Safety

408
 <u>Safety PLC</u> - 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.

412	2.	Maintain Environmental Safety
413		• <u>None</u> - The workcell, and its underlying manufacturing process, do not use any raw
414		ingredients or produce any by-products that can compromise the environmental safety
415		mission.
416		
417	3.	Maintain Quality of Product
418		• <u>Machining Stations 1, 2, 3</u> - All manufacturing functions are performed by
419		sequential CNC machining stations (1, 2, and 3). Each station uses preprogrammed
420		operations (e.g., G code) to complete its required manufacturing process tasks. This
421		code, and all station functions, have direct control over the output product quality.
422		• Inspection Station 4 - If product quality has been impacted outside of product quality
423		specifications, the inspection station will reject the part. Modification of the
424		specifications within the inspection station can allow out-of-spec parts to pass
425		inspection.
426		• Robots - Tending of parts between the machines is handled by the two workcell
427		robots. This process requires accurate and repeatable placement of parts within the
428		machining station fixtures, which is performed through robot calibration and
429		preprogrammed waypoint coordinates. Parts that are not properly placed within
430		fixtures, or collide with the fixtures, may not meet product quality specifications.
431		• Supervisory PLC - The supervisory PLC tracks each part as it goes through the
432		manufacturing process and commands the robots to transport each part between
433		machines in a sequential manner. If a robot executes a job out-of-order, a part may
434		bypass one of the machining stations, impacting product quality.
435		• HMI - Through the HMI, operators can manipulate workcell operation parameters,
436		machining station programs, and inspection station acceptance parameters.
437		Modification of any of these parameters outside of expected bounds can impact
438		product quality.
439		• Engineering Workstations - Privileged control and administrative functions of
440		workcell components is granted to engineers via the Engineering Workstation.
441		
442	4.	Maintain Production Goals
443		• Machining Stations - The amount of time each machining station takes to perform its
444		manufacturing functions, and the frequency of alarm conditions, can impact
445		production goals.
446		• Robots - The amount of time the robots require to transport the parts between
447		machining stations can impact the production goals.
448		• Supervisory PLC - The amount of time it takes the PLC to disseminate jobs to the
449		robots, or communicate with the machining stations, can impact production goals.
450		• HMI - Operators have direct control over the amount of parts produced in a batch via
451		the HMI.
452		• Engineering Workstations - Numerous privileged functions available through the
453		engineering workstation can impact production goals.
454		• Operator Workstations - Operators obtain production planning goals (e.g., product
455		type and quantity), machining station data files (e.g., G code) from network shares
456		and email systems. Inability to access these systems can impact production goals.
		7

457 • Networking equipment - All coordination between workcell components occurs 458 through the installed network equipment. If this equipment degrades or ceases to 459 function, production goals will be impacted. 460 5. Protect Trade Secrets 461 • <u>Machining Stations</u> - The operations performed by each machining station are a 462 protected trade secret of the company. 463 464 • Network - The machining station data files (e.g., G code) are typically stored on 465 network shares, and must be protected.

# 466 **3.** Policy and Procedure Implementations

467 This section includes example policy and procedure documents and statements that were

468 developed for the fictional company Alpha. An overview of these documents is discussed in

469 Section 5 of Volume 1. Each organization's information security experts should identify the

470 policy and procedure documents and statements that will best integrate with their existing

471 cybersecurity program and manufacturing system infrastructure.

# 472 **3.1 Security Program Document Example**

473	Security Program				
474	for				
475	Alpha				
476					
477					
478					
	<b>Document Owner:</b>	Supervisor, Alpha			
479					

# 480 Version

481

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

482

# 483 Approval

485

Approvers	Role	Signed	Approval Date
	President		4-22-2018

486

## 487 **3.1.1 Purpose**

- 488 The Information Security Program establishes guidelines and principles for initiating,
- 489 implementing, maintaining, and improving cybersecurity management for Alpha.
- 490 This program is designed to:
- Ensure the security and confidentiality of employees and business information;

<sup>484 (</sup>By signing below, all Approvers agree to all terms and conditions outlined in this document.)

- 492 Protect against any anticipated threats or hazards to the security or integrity of such information; and
- Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to Alpha, its partners, customers, or any member.
- 496 In addition, the Supervisor (Foreman) oversees the development, implementation, and
- 497 maintenance of the information security program

## 498 **3.1.2 Who Should use this Document?**

499 This document is intended to be used by the President, HR Manager, Shop Supervisor and any

other members as deemed appropriate by the Supervisor. It supports an agencies responsibilityfor implementing an INFOSEC program.

# 502 **3.1.3 Commitment from Management**

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

# 508 3.1.4 Organization Overview

# 509 Role in the Industrial sector

- 510 Alpha produces common metal components for the automotive industry. These parts are
- 511 subcontracted to Alpha by larger manufacturers. The finished parts are then integrated into
- 512 larger subassemblies that perform non-safety related functions within a vehicle
- 513 Raw material suppliers are utilized on-demand, and supplier selection is determined in-stock
- availability. No formal relationships or direct-order networking/online/cloud connections with
- any suppliers currently exist. Alpha is considered a "tier two" supplier. Alpha sends completed
- 516 parts to a tier one manufacturer for integration into subassemblies that are subsequently installed
- 517 into a vehicle by the original equipment manufacturer (OEM).
- 518 Alpha will not be able to produce if the primary metals critical manufacturing sector cannot
- 519 provide Alpha with the required raw materials. However, this sector is outside of the scope of
- 520 Alpha's implementation of the Manufacturing Profile.

# 521 Mission Objectives:

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

### 525 1. Maintain Personnel Safety

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

## 530 2. Maintain Environmental Safety

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

#### 534 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.
- <u>Robots</u> 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.
- <u>HMI</u> 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.
- <u>Engineering Workstations</u> Privileged control and administrative functions are granted to authorized personnel via the Engineering Workstation.
- 558 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.

- <u>Robots</u> 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.
- 567 <u>HMI</u> Misconfiguration of the production settings on the HMI can impact production goals.
- <u>Engineering Workstations</u> 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.
- 574 5. Protect Trade Secrets
- Machining Stations The individual operations performed by each machining station, and all supporting information the describes these operations, are protected trade secrets of the company.
- Network The machining station data files (e.g., G code) are typically stored on network
   shares, and must be protected

# 580 **Role in the Supply chain:**

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

# 586 **Communication to Organization**

- 587 All critical and operational aspects of the Manufacturing system, key resources should be
- 588 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.
- 590 This information will be shared with all employees, contractors depending on their role in the 591 Company.
- 591 C
- 593 Critical Manufacturing System Components:
- 594

- 595 The following are a list of critical Manufacturing system components:
- 596 Engineering workstation597 Supervisory PLC
  - Supervisory • HMI
- 598 HM 599 • Mao
  - Machining stations
    - Robot arms

- Robot controllers
- 602 Robot driver
- Networking equipment

604 Supporting Services:

- 605 The only supporting service required by Alpha is electricity to power IT systems, manufacturing
- 606 machines, and lights.
- 607

# 608 **3.1.5** Information Security Policy

609 The purpose of the Information Security Policy, which can be found in Section 3.2, is to provide

an overview of the policies, standards, procedures and Technical controls that make up Alpha's

611 Information Security Program. This policy is developed and executed by the Supervisor, and

612 expectations are set for protecting Alpha's IT and OT assets.

# 613 **3.1.6 Applicable Laws and Regulations**

614 Alpha does not have knowledge of any legal or regulatory requirements in regards to its

615 cybersecurity. However, as a tier two supplier, it is contractually obligated to follow all

standards, procedures, and guidance provided by the tier one manufacturer(s) and the OEM (e.g.,

617 ISO/TS 16949, ISO 9000). Alpha does not produce any components that fall within the

618 regulatory jurisdiction of 49 CFR Part 571: Federal Motor Vehicle Safety Standards.

619

# 620 **3.1.7** Security Organization and Governance

621 Information security is an inherent part of governance and consists of the leadership,

622 organizational structures and processes that safeguard Alpha's information, its operations, its

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

- 633 The Supervisor is responsible for:
- 634 Serving as a Security Officer and as a Single point of contact for any physical or cybersecurity related incident. 635
- 636 Implementing and maintaining Security Policy documents. •
- 637 • Overall security of all IT/OT assets, operations and remediating risks and vulnerabilities.
- Acting as a liaison between plant operators, vendors and management on matters relating 638 639 to information security.
- 640 Reporting to the President about the status of the program, any security related • 641 risks or incidents via reports.
- 642 All employees, contractors and vendors are responsible for ensuring the security, confidentiality, 643 and integrity of information by complying with all corporate policies and procedures.

#### 644 3.1.8 Privacy of Personal Information

645 Employees should not assume any degree of privacy to information they create or store on 646 Alpha's systems. Alpha is a private organization and any information stored on its information 647 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. 648

#### 649 3.1.9 Operational Security

- 650 **Risk Management:**
- 651 The Organization's Risk Management Strategy can be found here in Section 3.4 Risk
- 652 Management Document. The Supervisor shall conduct yearly risk assessments to identify
- 653 potential internal and external risks to the security, confidentiality and integrity of Alpha.
- 654 Risk assessment involves evaluating risks and their likelihood along with selecting and
- 655 implementing controls to reduce risks to an acceptable level. Each risk assessment documents 656
- major findings and risk mitigation recommendations.
- 657 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 658
- 659 determined (e.g., accept the risk, seek assistance from the IT Team, contact a vendor to
- 660 remediate the risk). Similarly, a vendor or contractor can also notify the Supervisor if they
- 661 identify any threats or risks to their equipment. A detailed description of risk notification
- 662 process can be found in Section 3.4 Risk Management Document.

### 664 <u>Physical Security:</u>

- The perimeter of the facility is fenced, and the main entrance has gate that is open during
- business hours and locked after hours. There are two entrances to the main building. One is for
- 667 Employees only which is normally locked, employees need to swipe their personal
- badges to enter the building. The other entrance located at the front lobby is open during normal
- business hours. Guests and visitors are required to sign in with proper identification. Additional
- 670 details about Physical security requirements are mentioned in the Physical Security Section of
- 671 the Security Policy document.
- 672 Additionally, Personnel security is addressed through pre-employment screenings, adequate
- 673 position descriptions, terms of employment, and security education and training.

## 674 <u>Access Control:</u>

- 675 User access to IT and OT systems is based on the principle of least privilege depending on the
- 676 user's role in the organization. Proper authorization and approval by the Supervisor is required
- 677 prior to granting access or operating any manufacturing system equipment. Sets of controls are in
- 678 place to restrict access through authentication methods and other technical means. Passwords are
- 679 managed through a formal process and secure log-on procedures. Sensitive systems are explicitly
- 680 identified and audited regularly.
- 681 Appropriate authentication controls are used for external connections and remote users. Physical
- and logical access to critical infrastructure is controlled. Duties are separated to protect systems
- and data. Access rights are audited at regular intervals

# 684 3.1.10 Security Awareness Training

- 685 Security awareness information is provided to new employees at the time of hire. Online
- resources are provided to educate employees on best practices and the importance of reporting security incidents. Additionally, the Supervisor will ensure the employee understands their role
- and responsibilities in Alpha's information security program.
- 689 Any information about potential or existing cyber threats to Alpha's systems may be
- 690 exchanged routinely between the Supervisor and external vendors. Likewise, any news about
- 691 email scams, phishing attempts and other malicious actions are posted to inform users of possible
- threats.

# 693 Training for Users and Managers

- 694 Employees must perform online computer-based training or classroom-based training per
- 695 management approval. Below is a list of training options. Trade organization subscriptions to
- newsletters and magazines will offer more industry specific training classes.
- 697
- 698

699	Computer Based Training
700	• ICS CEPT VI D (Virtual Learning Dortal)
701	• ICS-CERT VEF (Vintual Leanning Foltar)
702	• DHS Pacommonded Training
703	• Dris Recommended Training
705	• SCADAbacker
705	<ul> <li>SCADAllacker com/training html</li> </ul>
707	• In Person Training
708	Sans Industrial Control Systems Training
709	https://ics.sans.org/training/courses
710	
711	Training for Privileged Users
712	Privileged Users in the Organizational Use case:
713	• Foreman/Supervisor
714	This user has complete control of the manufacturing process within Alpha.
715	Responsibilities:
716 717 718	• Any privileged user within manufacturing environment will have two accounts. A primary account used for normal activities, and a privileged "administrator" account for performing privileged functions.
719	
720	• Primary accounts are used for normal daily operations.
721	• Primary accounts will have same rights as a standard Alpha user account (e.g., email
722	access, Internet access).
723	• Privileged accounts will have administrative privileges, and must only be used when
724	performing administrative functions within manufacturing system (e.g., system updates
725	of firmware or software, system reconfigurations, device restarts).
726	
727	• Privileged users will adhere to securely using Administrative account when performing
728 729	auties within manufacturing system. If a privilege account becomes compromised this could have a damaging impact on the manufacturing process.

- 731 <u>Training</u>:
- Training for privileged users will include the training for regular users. Advance training will
   be provided from industry trade group specializing in automation process, or other specialty
   training organization focusing on manufacturing security for ICS environments.
- 735 736 Examples:
- 737 o International Society of Automation (ISA) <u>https://www.isa.org</u>
- 738oSANS (Information Security Training) <a href="https://www.sans.org">https://www.sans.org</a>
- 739 Training for Third Party contractors
- 740 There are many different training options available. Training can be completed in person at a ٠ 741 training facility, or online in a virtual classroom environment. In person training at a facility 742 will have a cost associated and it not always appropriate depending on the level of training 743 required. Online training can also have a cost depending on the level required, but there are 744 also options that a free and provide a good understanding of the difference between a 745 traditional Information Technology (IT) environment and Operations Technology (OT) 746 environment. 747 Payed Training Options. •
  - <u>https://www.sans.org/course/ics-scada-cyber-security-essentials</u> (Offers hands on training with experienced instructors).
- Free Online Training Options.
  - <u>https://ics-cert-training.inl.gov/learn</u> (Offers virtual classroom environment at no cost).
- 752 753

749

751

# 754 **3.1.11 Third Party Responsibilities and Requirements**

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

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

# 770 **3.1.12 Fire and Safety Regulations**

- Fire Protection Systems will compile with Local, State, and Federal laws. This is to include
   Fire Protection Systems specially designed for manufacturing process. Fire Protection
   System will place emphasis on human safety first and for most, before concern for
   manufacturing system. Fire Protection Systems will be checked minimum once per year
   unless shorter intervals are required from superseding regulations.
- Only Industry approved Environmental Controls will be used within manufacturing systems,
   to included compliance with all Local, State, Federal laws. Environmental Control will be
   implemented to place human/community safety first before manufacturing systems.
- Fire protection for a manufacturing environment should be designed to safeguard electrical equipment. Fire Protection should be designed and implemented to protect human life first and equipment second. Installed fire protection systems will be certified compliant with existing/new environment by a licensed and accredited vendor. Check industry standards for any required baselines.
- 784

## 785 **3.1.13 Emergency Power**

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

## 788 3.1.14 Incident Management

Alpha's Incident Response and Recovery Plan describes the detection, analysis, containment,

readication, recovery and review of security incidents. The process for responding to security

incident is designated in Incident Response Plan, while the procedures for incident recovery and

resilience requirements are defined in the Incident Recovery Plan. Security incidents are

managed by the Supervisor who ensures that security incidents are promptly reported,

investigated, documented and resolved in a manner that restores operation quickly and, if

required, maintains evidence for further disciplinary, legal, or law enforcement actions. The

796 Incident Response Plan and Recovery Plans are reviewed annually and updated as needed.

797 Lessons learned from cybersecurity events will be used to revise and improve device detection

ability while increasing protection for the organization and manufacturing system.

799

# 800 **3.1.15 Information Sharing Plan**

801 Information sharing with outside entities like trade organizations and local, state, and federal

agencies can help strengthen cybersecurity. Information sharing, especially when receiving

803 information from other outside entities, will improve Alpha's situational awareness, and result in

a more secure manufacturing system.

## 805 **Trade Organizations:**

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

## 814 Local Government:

815 Relationships with any local government organization whose purpose is to share cybersecurity 816 incident data should be established.

## 817 State Government:

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

## 821 Federal Government:

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

824

- 825 DHS (CISA) Agency for reporting incidents of Phishing, Malware, Vulnerabilities.
- 826 <u>https://www.us-cert.gov/report</u>
- B27 DHS (NCCIC) Agency for reporting cybersecurity incidents relating to Industrial ControlSystems.
- 829 https://ics-cert.us-cert.gov/Report-Incident
- 830

# 831 **3.1.16** Periodic Reevaluation of the Program

- 832 The Security Program document will be continuously updated to reflect changes made to
- 833 manufacturing system and to improve cybersecurity. Lessons learned will be incorporated to
- help improve this document in the event a cybersecurity incident occurs.
- 835 The Supervisor shall reevaluate and update the Program from time to time as deemed
- 836 appropriate. The Supervisor shall base such reevaluation and modification on the following:
- The results of the risk assessment and monitoring efforts;
- Any material changes to the Alpha's operations, business or infrastructure components.
- Any cybersecurity incident.

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

## 841 **3.1.17 References**

- Implementing Effective Information Security Program by SANS Resources
   <u>https://www.sans.org/reading-room/whitepapers/hsoffice/designing-implementing-</u>
   <u>effective-information-security-program-protecting-data-assets-of-1398</u>
- 845
   845
   and Sec Program Plan by University of Tennessee Knoxville <a href="https://oit.utk.edu/wp-content/uploads/2015-11-11-utk-sec-prog-plan.pdf">https://oit.utk.edu/wp-content/uploads/2015-11-11-utk-sec-prog-plan.pdf</a>
- 847 3. GCADA Sample Information Security Procedure
   848 <u>http://www.gcada.org/pdf/Sample%20Information%20Security%20Procedure%20(safeg</u>
   849 <u>uard%20policy).pdf</u>
- 850
   851
   4. IT Security Program by Old Dominion University
   851
   https://www.odu.edu/content/dam/odu/offices/occs/docs/odu-it-security-program.pdf
- 852

## 854 **3.2 Security Policy Document Example**

*			
855		Security Policy	
856		for	
857		Alpha	
858			
859			
860			
	<b>Document Owner:</b>	Supervisor, Alpha	

## 861

# 862 Version

863

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

# 864

# 865 Approval

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

867

Approvers	Role	Signed	Approval Date
	President		4-22-2018

868

## 869 **3.2.1** Purpose

870 This Security Policy document defines the security requirements for the proper and secure use of

871 IT and OT services in the organization. The goal of the policies defined within is to protect the

872 organization and its users to the maximum extent possible against cybersecurity threats that

873 could jeopardize their integrity, privacy, reputation, and business outcomes.

## 874 **3.2.2 Scope**

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

## 876 3.2.3 Policy Maintenance

877 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 needto be preapproved by the Supervisor.

- 880 This policy document will be reviewed by the Supervisor on an annual basis. The Supervisor will
- 881 notify all employees for any updates made to the policy.
- 882 **3.2.4** Role-based Security Responsibilities
- 883 Security responsibilities vary depending on an individual's role in the company. Each is defined884 below.

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

## 887 External Personnel

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

888

# 889 3.2.5 Employee requirements

- Employees must complete security awareness training and agree to uphold the acceptable
   use policy.
- 892
  893
  2. Employees must immediately notify the Supervisor if an un-escorted or unauthorized individual is found in the facility.
- 894 3. Employees must always use a secure password on all systems as per the password policy.
   895 These credentials must be unique and must not be used on other external systems or
   896 services.
- 4. Terminated employees must return all company records, in any format.
- 898 5. Employees must verify with the Supervisor that authorizations have been granted before899 allowing external personnel to connect to the IT or OT network.
- 900 6. Employees must report any physical security incidents to the Supervisor.
- 9019017. Employees must understand and diligently follow the physical security requirements stated902902903904905905906906907907908908908909</

903

# 904 3.2.6 Physical Security

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

913 914	6.	Any visitors, contractors and/or maintenance personnel must always be escorted by an employee
915	7	Unauthorized removal of any documentation, equipment, or media from is restricted.
916	,.	unless authorized. Authorization can be obtained from the Supervisor.
917	8.	All activities of visitors, contractors, and maintenance personnel will be subject to
918		monitoring while onsite. An employee from the IT team will be assigned to monitor all
919		computer activities if the visitor, contractor, or maintenance personnel is connected to
920		any company network.
921	9.	A supervisor will conduct monthly security status monitoring of the company to check
922		for any physical security incidents.
923		
924	3.2.7	Information Technology (IT) Assets
925	1.	IT assets must only be used for the business activities they are assigned and authorized to
926		perform.
927	2.	Every employee is responsible for the preservation and proper use of the IT assets they
928		have been assigned.
929	3.	IT assets must not be left unduly exposed.
930	4.	Desktops and laptops must be locked if left unattended. This policy should be
931	<i>_</i>	automatically enforced whenever possible.
932	5.	IT assets must not be accessed by non-authorized individuals. Authorization can be
933	6	obtained from Supervisor.
934	6.	Configuration changes are to be conducted through the change control process,
933	7	All assets must be protocted by outbentiestion technologies (a group management.
930	/. o	All assets must be protected by authentication technologies (e.g., passwords).
937	ð. 0	The Supervisor must be notified immediately after an asset is discovered to be lost or
030	9.	stolen
940	10	Use of personal devices to access IT resources is prohibited
9/1	10.	Storage of sensitive information on portable media is prohibited unless authorized by the
942	11.	Supervisor
943	12	Any sensitive information stored on IT assets, or being transported on a portable device.
944	12.	must be protected in such a way to deny unauthorized access, and must be encrypted in
945		line with industry best practices and any applicable laws or regulations.
946		

# 947 3.2.8 Operational Technology (OT) Assets

- 948 1. OT assets must not be used for operations they are not assigned or authorized to perform.
- 949
   950
   2. The Supervisor and Operators are responsible for the preservation and correct use of the ICS assets they have been assigned.
- 951
   951
   952
   953
   954
   955
   955
   955
   956
   957
   958
   958
   959
   959
   950
   950
   951
   951
   952
   953
   953
   954
   955
   955
   955
   956
   957
   957
   958
   958
   959
   959
   950
   950
   951
   951
   952
   953
   953
   954
   955
   955
   956
   957
   957
   958
   959
   959
   950
   950
   951
   951
   951
   952
   953
   954
   955
   955
   954
   955
   955
   956
   957
   957
   957
   958
   958
   959
   959
   959
   950
   950
   951
   951
   952
   952
   953
   952
   953
   954
   954
   955
   955
   956
   957
   957
   958
   958
   958
   958
   959
   959
   959
   959
   950
   950
   950
   950
   950
   950
   951
   951
   951
   952
   953
   952
   953
   954
   954
   954
   954
   954
   954
   955
   956
   957
   956
   957
   956
   956
- 4. All personnel interacting directly with OT assets must have proper training.
- 5. The Supervisor is responsible for all OT devices. Supervisor is solely responsible for
  maintenance/configuration of the device they are assigned. No other personnel are
  authorized to modify OT asset configurations, including any modification to interfacing
  hardware or software.
- 9596. Usage of security tools on the OT network must be approved by the Security Officer, andall affected Operator must be notified.
- 961 7. Concept of least privilege must be followed when authorizing access to OT assets.
- 962 8. OT assets, such as PLCs, safety systems, etc., should have their keys in the "Run"
  963 position at all times unless being actively programmed.
- 9649. Accessing IT devices or internet use from the OT network, or OT assets, unless965 authorized, is prohibited.
  - 10. Use of personal devices to access OT resources is prohibited.
- 966 967

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

968

**OT Assets Inventory** 

969

# 970 **3.2.9** Lifecycle Accountability of assets

- Any IT or OT asset that needs to be decommissioned must be sanitized of all data, as per
   the manufacturer guidelines.
- 973
  973
  2. In case of an employee termination, an IT asset such as desktop PC or laptop must be reimaged prior to assigning it to a different employee.

## 976 3.2.10 System Maintenance

- Any maintenance tasks involving external resources such as Vendors, Contractors or
   other non-employees must be pre- approved by the Supervisor. This can be coordinated
   by filling out the Maintenance Order approval form.
- 980
  980
  981
  2. It is the responsibility of Vendors, Contractors and/or Maintenance personnel with access to resources that due care is ensured to properly secure their own resources.
- 9829839833. It is Alpha's responsibility that due care is ensured when using vendor devices on networks.
- 4. All remote maintenance activities provided by a vendor will be controlled and monitored to ensure no harmful or malicious activities occur. Detailed logging of the activity will be performed by an Alpha employee using in-house tools.
- 5. All systems and/or technical controls must be verified upon the completion ofmaintenance for any cybersecurity related impact.
- 6. All maintenance work details will be logged in a Maintenance Tracker Excel sheet. The
  Supervisor will update all details of the work performed in the sheet.

### 992 3.2.11 Data

991

993 1. Access to sensitive data must be authorized by Supervisor. 994 2. Data should not be shared informally. When access to sensitive information is required, 995 personnel can request it from their supervisors and should take all necessary steps to 996 prevent unauthorized access. 997 3. You must immediately notify the Supervisor in the event a device containing sensitive 998 data is lost (e.g. mobiles, laptops, USB devices). 999 4. It is recommended personnel use encrypted portable media or secure protocols while 1000 transferring data across systems. Supervisor can provide you with systems or devices that fit this purpose. You must not use other mechanisms to handle sensitive data. 1001 5. If you have been permitted to work remotely, extra precautions must be taken to ensure 1002 1003 sensitive data is appropriately protected. 6. Physical copies of data should be stored in a secure location where unauthorized 1004 1005 personnel cannot access it. 1006 7. Personnel should ensure physical copies of sensitive data are not left unattended on a 1007 printer. 1008 8. Physical copies of sensitive data should be shredded or disposed in a secure manner. 1009

Description	Digital Files	Physical Copies	Databases
PLC programs	✓	✓	
Robot programs	✓	✓	
CAM/G code	✓	✓	
Operating manuals and documentation	<b>√</b>	~	
Electrical diagrams	✓	✓	
Network diagrams	~	✓	
CAD Files	<b>√</b>	✓	
Inspection measurement files	$\checkmark$		
Historical production data	✓		✓

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

1012

#### 1013 **3.2.12 Credentials Management**

1014 The purpose of this policy is to establish a standard for the creation of strong passwords,

1015 protection of those passwords, frequency of change and employee expectations.

1016 All staff, vendors, contractors or other stakeholders who use Alpha's IT and OT systems should

1017 be given authenticated access to those systems by assigning individual credentials [username and

1018 password]. All access and restrictions to those access will be controlled by these credentials.

1019 The creation and removal of IT system accounts is managed via Microsoft Active Directory. In 1020 addition, The Supervisor will determine and authorize user access to IT or OT systems.

1021 Alpha reserves the right to suspend without notice access to any system or service.

#### **3.2.13 Password Policy for Active Directory Accounts**

1023 1. All employee and system passwords must be at least 10 characters long and contain a combination of upper-case and lower-case letters, numbers, and special characters.
1025	2. Passwords must be changed every 90 days and cannot match a password used within the
1026	past 12 months.
1027	3. Passwords must not be a dictionary name or proper name.
1028	4. Passwords must not be inserted into email messages or other forms of electronic
1029	communication.
1030	5. Employees must choose unique passwords for all company accounts and may not use a
1031	password that they are already using for a personal account.
1032	6. Whenever possible, use of multi-factor authentication is recommended.
1033	7. Default passwords, such as those preconfigured in newly-procured assets, must be
1034	changed before the asset is installed or connected to any organizational network.
1035	8. Sharing of passwords is forbidden.
1036	9. Passwords must not be revealed or exposed to public sight.
1037	10. Personnel must refrain from writing passwords down.
1038	11. Personnel must not use the "remember password" feature prevalent on many applications.
1039	
1040	3.2.14 Privileged Accounts
1041	The following standards will be used for determining Privileged access to systems.
1042	Privileged Users
1043	• Foreman/Supervisor
1044	• This user has complete control of the manufacturing process within Alpha.
1045	Responsibilities
1046	• Any privileged user within manufacturing environment will have two accounts. A primary
1047	account used for normal activities, and a privileged "administrator" account for performing
1048	privileged functions.
1049	
1050	<ul> <li>Primary accounts are used for normal daily operations.</li> </ul>
1051	• Primary accounts will have same rights as a standard Alpha user account (e.g., email
1052	access, Internet access).
1053	<ul> <li>Privileged accounts will have administrative privileges, and must only be used when</li> </ul>
1054	performing administrative functions within manufacturing system (e.g., system updates
1055	of firmware or software, system reconfigurations, device restarts).
1056	
1057	• Privileged users will adhere to securely using Administrative account when performing
1058	duties within manufacturing system. If a privilege account becomes compromised this could
1059	have a damaging impact on the manufacturing process.
10.50	
1060	3.2.15 Antivirus

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

- 10642. All devices within OT environment will be configured to receive daily update to include virus signatures.
- 10663. Installed antivirus will be configured to receive push updates from central management1067server, or others antivirus clients if supported.

#### 1069 **3.2.16 Internet**

1068

- 1070 1. Internet access is provided for business purposes.
- 1071
   2. Limited personal navigation is permitted from IT networks if no perceptible consumption
   1072
   of organizational system resources is observed, and the productivity of the work is not
   affected.
- 1074
   3. Only authorized Internet access from the OT network is permitted. Authorized access can be obtained from Supervisor
- 1076 4. Inbound and outbound traffic must be regulated using firewalls in the perimeter.
- 1077 5. All Internal and External communications must be monitored and logged by in-house
   1078 network security tools. Logs must be reviewed regularly by the plant operators and
   1079 reported to the Supervisor.
- 1080
  6. When accessing the Internet, users must behave in a way compatible with the prestige of the organization.
  1082

#### 1083 3.2.17 Continuous Monitoring

- Alpha will implement a Security Continuous Monitoring program. This will include performing comprehensive network monitoring using Commercial or Open source tools to detect attacks, attack indicators and unauthorized network connections.
  - 2. The Manufacturing system will be monitored for any cybersecurity attack indicators or IOC's.
- 1089 3. All External boundary network communications will be monitored.
- 4. All cybersecurity incidents must be logged in the Incident Response Management tool for documentation purposes.
- 1093
  5. All Local, State, and Federal detection activities applying to organization or manufacturing system will be followed in accordance within the law. Detection activities are to include any industry regulations, standards, policies, and other applicable requirements.
- 1097
  6. Monitoring activity levels will be increased during periods of increased risk and/or any other factors as necessitated by the Alpha Management.
  1099
  7. All cybersecurity events detected will be communicated to the below list of defined
  - 7. All cybersecurity events detected will be communicated to the below list of defined personnel identified by the Supervisor.
- 1100 1101

1087

1088

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

High (Requiring Urgent	Machine Operators, Supervisor
Attention)	

- 8. Details of cybersecurity events will be shared with agencies such as ICS-CERT
  (https://ics-cert.us-cert.gov/). to help secure the organization, including helping secure
  the industry. Cyber + Infrastructure (CISA) is an agency of Department of Homeland
  Security which provides reporting capabilities for manufactures related to cybersecurity
  events.
- 1108

#### 1109 **3.2.18 External Service Provider Communications:**

- All communications from External Service Providers to Alpha's systems will be monitored to ensure work provided by service provider is done correctly, including following all cybersecurity best practices and complying with Alpha's security policies. Monitoring will include designated employee to oversee all activities performed.
- Any Indicator of Compromise (IOC's) detected while monitoring external service
  provider communications will be reported and escalated via appropriate communication
  channels. The Supervisor will reach out to the External service provider upon verifying
  the threat to discuss and seek an immediate remediation path accordingly.
- 1118 3.2.19 User Access Agreement

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

- 1121 As an employee of Alpha
- 11221. You may use Alpha's IT, OT systems and networks to which you have been granted1123access for work related purposes only. Accounts and access are granted based on each1124individual's roles and responsibilities.
- 11252. You should not expect any privacy on Alpha's premises or when using Alpha's propertyor networks either when onsite or accessing remotely
- 3. You will act responsibly to maintain the security and integrity of the information systems that you use, to minimize the chance of any problems or security breaches for Alpha.
- 4. You agree to co-operate with any audit by Alpha or our Contractors of your access to theSystem.
- 1131
  1132
  1132
  1132
  1133
  5. You understand your responsibility for respecting other employee's privacy and protecting the confidentiality of information to which you have access, and will comply with all privacy laws, codes and guidelines including,
- 1134
  6. Internet access must not be used for activities that are not authorized under existing laws, regulations, or organization policies.
- 11367. Any company laptops assigned to you should only be used for the purpose of conducting1137Alpha's business. You are expected to take due care while using laptops.

- 1138 8. All laptops must be returned at the end of employment.
- 9. You understand that Transmission or intentional receipt of any inappropriate material or material in violation of law or district policy is prohibited. This includes but is not limited to: copyrighted material; threatening or obscene material: material protected by trade secrets; the design or detailed information pertaining to explosive devices: criminal
- 1143 activities or terrorist acts; gambling; illegal solicitation; racism; inappropriate language.
- 1144 10. You shall be subject to disciplinary action up to and including termination for violating 1145 this agreement or misusing the internet.
- 1146

1147 **3.2.20 Remote Access** 

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

- 11501. Remote access for personnel requires pre-approval by the Security Officer1151(Supervisor). Please refer to the approval process for Maintenance to have the
- 1152 Maintenance Order Approval form approved by the Supervisor
- 1153 2. The Supervisor will determine list of authorized users for remote access.
- Remote access to sensitive or confidential information is not permitted on an unencrypted
   connection. Exception to this rule may only be authorized in cases where strictly
   required.
- 4. For temporary remote access tasks, an approved desktop sharing program such as TeamViewer will be used. A temporary laptop (workstation) will be arranged with TeamViewer client installed on it. The laptop may have dual network connections, one for internet access and other from the manufacturing network to access the necessary systems. The remote connection will be disconnected upon completion of work.
- 5. All remote connection activities will be monitored by an employee of Alpha. Monitoring will start and continue until remote session is no longer required, or work has been completed. Appointed individual will indicate when remote session is active and ensure manufacturing system environment has been returned to same state before remote connection was established
- 6. Installation and use of remote access software (desktop sharing software) etc. onauthorized devices must be approved by the Security officer.
- 11697. Any device used for remote access work must have Anti-virus installed along with up to date antivirus signatures.

# 1171 **3.2.21 Usage Restrictions**

- To avoid confusing official company business with personal communications, employees, contractors, and temporary staff with remote access privileges must never use non-company e-mail accounts (e.g. Hotmail, Yahoo, etc.) to conduct business.
- 1175
  2. No employee is to use Internet access through company networks via remote connection for illegal transactions, harassment, competitor interests, or obscene behavior, in accordance with other existing employee policies.
- 3. Where supported by features of the system, session timeouts are implemented after a
  period of no longer than 30 minutes of inactivity. Where not supported by features of the
  system, mitigating controls are implemented.

# 1182 **3.2.22 Remote Maintenance Approval Process**



REMOTE MAINTENANCE APPROVAL PROCESS & WORKFLOW

1183

#### 1185 **3.2.23 Maintenance Approval Form**

1186

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

1187

#### 1188 **3.2.24** Communicate Information to Organization

1189

1190 All critical and operational aspects of the Manufacturing system, key resources should be

documented in network diagrams, manuals or other artifacts. The documentation will be

1192 reviewed on a yearly basis by the Supervisor.

1193

1194 This information will be shared with all employees, contractors depending on their role in the 1195 Company.

# 1197 **3.2.25 Definitions and Acronyms**

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

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

# 1199 **3.2.26 References**

1200	1.	Security Policies by SANS Resources https://www.sans.org/security-resources/policies
1201	2.	Template for Security Policy by Project Management Docs
1202		http://www.projectmanagementdocs.com/template/Security-Policy.doc
1203 1204	5.	Data Security Policy by Sophos labs <u>https://www.sophos.com/en-</u> us/medialibrary/PDFs/other/sophos-example-data-security-policies-na.pdf?la=en

#### 1205 **3.3 Standard Operating Procedures Document Example**

-			
1206		Standard Operating Procedures	
1207		for	
1208		Alpha	
1209			
1210			
1211			
	<b>Document Owner:</b>	Supervisor, Alpha	

# 1212

# 1213 **Version** 1214

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

# 12151216 Approval

- 1217 (By signing below, all Approvers agree to all terms and conditions outlined in this document.)
- 1218

Approvers	Role	Signed	Approval Date
	President		4-22-2018

1219

#### 1220 **3.3.1** Introduction

1221 This document defines the procedural steps management and employees will follow ensuring 1222 consistence daily actives along with response to events occur within the manufacturing system 1223 for Alpha. Within this document contains content which should be referred to often ensuring all 1224 employees/individuals performing work within manufacturing system are not inadvertently

1225 compromising cybersecurity posture by not following Standard Operation Procedures (SOPs).

#### 1226 **3.3.2** Purpose

1227 To provide a consistent repeatable process that can be followed to perform tasks within

1228 manufacturing system.

#### 1229 **3.3.3 Scope**

- 1230 Management, employees, contractors, or individuals requiring access to manufacturing system
- 1231 for changes should be familiar with the contents included within this document.
- 1232

# 1233 **IDENTIFY**

#### 1234 **3.3.4 Asset Inventory**

1235 Identifying assets within manufacturing system for Alpha is a vital first step in protecting

1236 organization from malicious activates that could result in disruption to production. Alpha uses

- 1237 multiple tools for asset inventory, some manual processes and other automated. Knowing the
- 1238 environment and what devices are installed allows the ability to detect devices not approved to
- 1239 be on the network which could be an indication of malicious activity. Keeping devices updated
- 1240 with the latest software patches ensure to mitigate potential weakness within manufacturing
- 1241 system. All patches will be carefully examined to determine if there is any performance impact
- 1242 effecting production within manufacturing system.

# 1243 <u>Manual</u>

- 1244 Devices not having ability to be automatically scanned will be added to excel spreadsheet and
- 1245 updated quarterly. Devices included in manual process would be PLC and machine stations,
- 1246 including any additional devices that are not able to be scanned automatically with a tool. All
- 1247 inventory will be conducted during manufacturing system planned down time and inventory will
- 1248 include hardware and software.

# 1249 <u>Automated</u>

- 1250 Devices with the ability to be scanned will be added to Alpha's asset inventory tool and scanned
- 1251 quarterly. Scanning quarterly will ensure manufacturing process is not affected. All scanning
- 1252 should be performed when manufacturing system has been placed into a non-production mode
- 1253 (system down time). Alpha has chosen an asset inventory tool that has multiple version from
- 1254 open source to enterprise edition. Alpha has selected Enterprise edition since this version
- 1255 provides the ability to schedule scans, baseline systems for monitoring changes. For additional
- 1256 information and references see.
- 1257 Alpha inventory management tools will be configured for group access to ensure only
- 1258 individuals requiring access are allowed. This ensure that people within the organization only
- 1259 needing read accesses are not granted a higher level, which could lead to inadvertent changes to
- 1260 scanning tools configuration. See reference for how groups are created.
- 1261 Scans of manufacturing system will be conducted quarterly ensuring not to effect manufacturing
- 1262 process. Scans will audit software including license information, version, and configuration.
- 1263 Devices within the manufacturing systems will have software inventory audited and reviewed
- 1264 quarterly. Changes occurring to devices' software before the next update will trigger a required

- inventory to remain compliant. See reference for additional details for performing scanningwithin manufacturing system.
- 1267 Alpha will apply updates to asset inventory software as they become available. Updates are
- 1268 required to keep systems patched and free from known vulnerabilities while adding additional
- 1269 features. See reference for additional information.

# 1270 **3.3.5** Network Baseline

- 1271 Network baseline is important as it provides the ability to detect malicious active occurring on
- 1272 manufacturing system network. Alpha will periodically perform baseline scans to identify any
- 1273 unusual traffic, which could be indication of malicious activity. All traffic observed during1274 scanning should be reconciled to help create a securer network. See reference for network
- 1275 baseline performed.

# 1276 **3.3.6 External Connections**

- 1277 Using company provided network diagram tools all network connection for external
- 1278 communication will be mapped. Mapping will include all relevant information for connection
- 1279 service provided. Example of information required would be assigned IP address for device
- 1280 providing service, support phone number, customer number, person of contact, and support level
- agreement and hours. External providers will include cloud services. Network diagram will beupdated quarterly.

# 1283 **3.3.7 Baseline Configurations**

- Baseline configurations was captured using two methods since some ICS devices don't allow
  automated tool scanning; for these devices' spreadsheet tracking is the preferred method.
- 1286 Devices lacking SSH, SNMP, WMI ability will require manual entry in spreadsheet.
- 1287 Steps used to perform automated scanning for Alpha.
- Baseline configurations Alpha implemented within Manufacturing systems helps to ensure
   inadvertent changes are detected before systems' integrity has been compromised.
- 1290 Open-AudIT<sup>1</sup> has been chosen for Alpha due to scalable configuration depending on required
- needs. Instruction are listed for performing scanning. Once scanning has been performed changes
- 1292 with ICS devices are detectable by running reporting identifying new software changes.
- 1293 Manufacturing systems was scanned to get initial baseline. Steps performed are listed below.
- 1294 Once scan/s have been completed information was exported to CSV file for storage. See end of 1295 instructions for exported configuration.
- 1275 instructions for exported
- 1296

<sup>&</sup>lt;sup>1</sup> Open-Audit: https://www.open-audit.org

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

1299 Initial Configuration:

1302

1300 • Login via web portal

#### • Navigate to $\rightarrow$ Discovery $\rightarrow$ Credentials $\rightarrow$ Create Credentials

Discover -	Report <del>-</del>	Manage <del>-</del>
Credentials	5	List Credentials
Discoveries	s 🕨	Create Credentials

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

ID		
Name	CRS Scans	?
Organisation	Default Organisation •	?
Description	Perform Linux Scans	?
Туре	SSH 🗸	?
Username	icsuser01	
Password	•••••	٩
Edited By	nmis	?
Edited Date	2018-09-26 13:56:53	?
	Submit	

- 1310 button.
- 1311 Organization Groups Creation:
- 1312 Click on Manage  $\rightarrow$  Orgs  $\rightarrow$  Create Orgs

	Manage - Applications Attributos Baselines Connections Dashboards Devices Fields Groups Licenses Locations Maps Networks Queries Orgs Roles Summaries	List Orgs List Orgs Create Orgs
1313	Widgets	
1314	•	Now enter Name: Description: and click submit at the bottom of the page to save.
		Name CRS Machines ?
		Description Robotics Machines within Work Cell ?
		Parent ID Default Organisation • ?
1315		Type Organisation
1316 1317	•	If you have multiple machines / equipment in different locations you can make Organizational groups based on the business units, or related task.
1318	Confi	gure Discovery Scan:
1319	•	Now click on Discover → Discoveries → Create Discoveries Discover → Report → Manage → Credentials Discoveries List Discoveries
1320		Files Create Discoveries
1321	٠	Enter a meaningful name for discover being created
1322		Name     CRS Scans     ?
1323	•	Next, enter the subnet that'll be used for performing this scan. This scan is using
1324		192.168.0.0/23 <sup>subnet</sup> 192.168.0.0/23 ? Search online for additional
1525		subnetting information / calculators if you d like to learn more.
1326 1327	•	<b>Network address:</b> should already be defaulted to Open-AudIT installed location, if this is not true, click the drop-down arrow and select your installed location.
1328	•	Now, click on the advanced button to see more options.
1329 1330	•	Once <b>Advanced</b> has been expanded you'll have additional options to select if desired. These options are <b>Org, Type, Devices Assigned to Org,</b> and <b>Devices Assigned to</b>

- Location. These options aren't required but allow you to start placing found devices intodifferent Organizational groups.
- Once all are selected click on **Submit** button to continue.
- 1334 **Discoveries:**

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

•	Collaborative Robotics	Collaborative Robotics System	subnet	Subnet -	2018-09-19	<b>√</b>	(512 of 512)	Î
	System 192.168.0.0/23	192.168.0.0/23		192.168.0.0/23	14:45:53			

- Once discovery has started you'll be taken to a new page allowing you to view status or cancel if needed.
- 1343 Newly found devices are added to My Devices which is found on the home screen.

- 1344 Collaborative Robotics System CRS Baseline.zip
- 1345 Detailed baseline reports generated out of Open-AudIT can be obtained from <u>CRS Baseline</u>
   1346 <u>Reports</u>
- 1347 Shown below is a sample export of the baseline data from one of the devices using Open Audit
- 1348 in the Robotics system.

A	utoSavi	•	011	•ა - ⇔					EngineeringWorkstation-	Polaris.csv -	Excel		~		Shah, N	eeraj A. (Intk	Ctr) 🗗		σ
	le	Hom	ie Inser	t Draw	Page Layout Forr	mulas Data Revi	ew View	Developer H	elp 🛛 🖓 Tell me what you wa	nt to do									1st
Past	⊨ X C □ In C >e In C Clipb	iut iopy orma pard	at Painter	Calibri B I U	• 11 • A A •		ab Wrap Tex	tt Gene Center - \$ -	ral ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓	Format as Table -	Normal Neutral	Ba Ca Styles	d Go Iculation Cl	ood neck Cell	Insert Delet	e Format	∑ AutoSum Fill ∽ Clear ∽	Sort & F Filter - S	Find &
B1/	1			x J	fr 307														
	A		В	с	D	E	F	G	н	1	J	к	L	м	N	0	Р	0	F
2	id		system ic	current	last seen	first seen	manufacture	serial	description	smversion	version	revision	date	asset tag	id	-			_
3		36	307	v	12/12/2018 15:40	12/12/2018 15:40	Dell Inc.	319SJ02	Dell BIOS - Firmware Rev. A	2.7	A06	4.6	2/28/2014		307				
4																			
5	id	:	system ic	db table	db row	db action	details	user id	ack time	external I	external i	note	change id	change to	timestamp	id			
6	7	368	307	system	307	create	Item added t		1/1/2000 0:00		_		0		12/12/2018 15:39	307			
7	7	375	307	ip	473	create	Item added t		1/1/2000 0:00				0		12/12/2018 15:40	307			
8																			
9																			
10	id	:	system_ic	current	first_seen	last_seen	manufacture	model	serial	device	caption	hard_driv	e interface_type	partition	cscsi_bus	scsi_logica	scsi_port	size	statu
11		77	307	y y	12/12/2018 15:40	12/12/2018 15:40		ST2000DM001	Z1E7DOXP	/dev/sda	/dev/sda	sda	sata	3				1907729	1
12																			
13	id	1	system_ic	current	first_seen	last_seen	name	fqdn	ip	id	ip_padded	4							
14		46	307	y	12/12/2018 15:40	12/12/2018 15:40	polaris	polaris.lan.lab	192.168.0.20	307	192.168.0	00.020							
15																			
16																			
17	id	1	system_ic	current	first_seen	last_seen	mac	net_index	ip	netmask	cidr	version	network	set_by	interface	id	ip_padded		
18		166	307	y y	12/12/2018 15:39	12/12/2018 15:40	f8:b1:56:ba:0	1	192.168.0.20	255.255.2	24	4	192.168.0.0/24	static		307	192.168.0	00.020	
19		173	307	y y	12/12/2018 15:40	12/12/2018 15:40	f8:b1:56:ba:0	1 1	fe80::fab1:56ff:feba:9a8		64	6	5	static		307			
20																			

#### CSF MFG PROFILE LOW SEC LVL EXAMPLE IG DISCRETE-BASED MFG SYSTEM USE CASE

105 id		system_id	current	first_seen	last_seen	mac	manufacturer	model	descriptio	r alias	ip_enable	net_index	dhcp_enabled	dhcp_server	dhcp_leas	dhcp_lease	d
106	302	307	У	12/12/2018 15:40	12/12/2018 15:40	f8:b1:56:ba:	Intel Corporation	82579LM Gigabit Network	82579LM	Gigabit Net	TRUE		2 FALSE				p
107	303	307	у	12/12/2018 15:40	12/12/2018 15:40	68:05:ca:1c:	Intel Corporation	C600/X79 series chipset PC	C600/X79	series chip	FALSE		4 FALSE				p
108	304	307	у	12/12/2018 15:40	12/12/2018 15:40	68:05:ca:2e:	Intel Corporation	Ivytown PCI Express Root	Vivytown P	CI Express	FALSE		3 FALSE				p
109																	
110 id		system_id	current	first_seen	last_seen	name	size	initial_size	max_size	id							
111	21	307	У	12/12/2018 15:40	12/12/2018 15:40	/dev/sda5	(	8331260	8331260	307							
112																	
113 id		system_id	current	first_seen	last_seen	serial	name	description	device	hard_drive	partition_	mount_type	mount_point	size	free	used	fc
114	137	307	у	12/12/2018 15:40	12/12/2018 15:40	8e974296-03	369-487c-8f59-6db7b6	144483	/dev/sda1	L sda	sda	partition	1	1899591	1735038	39624	e:
115	138	307	У	12/12/2018 15:40	12/12/2018 15:40				/dev/sda2	2 sda	sda	partition		0	0	0	
116	139	307	у	12/12/2018 15:40	12/12/2018 15:40	9c155e7d-fc	f8-4911-bc63-7c28963	ifb5b6	/dev/sda5	i sda	sda	partition	[SWAP]	8136	8135	0	S١
117																	
118 id		system_id	current	first_seen	last_seen	physical_cou	core_count	logical_count	descriptio	rspeed	manufactu	architecture	socket	id			
119	46	307	У	12/12/2018 15:40	12/12/2018 15:40	2	8	8 8	Intel Xeor	1200	Intel		Socket LGA201	307			
120																	
121 id		system_id	current	first_seen	last_seen	destination	mask	metric	next_hop	protocol	type	id	destination_pa	next_hop_padded			
122	297	307	У	12/12/2018 15:40	12/12/2018 15:40	0.0.0.0	0.0.0.0	0	192.168.0	).2	UG	30	7 000.000.000.00	192.168.000.002			
123	298	307	у	12/12/2018 15:40	12/12/2018 15:40	169.254.0.0	255.255.0.0	1000	0.0.0.0		U	30	7 169.254.000.00	000.000.000.000			
124	299	307	У	12/12/2018 15:40	12/12/2018 15:40	192.168.0.0	255.255.255.0	1	0.0.0.0		U	30	7 192.168.000.00	000.000.000.000			
125																	

1350

# 1351 List of services running:

126 id		system_id current	first_seen	last_seen	name	description	executable	user	start_mo	d state	id
127	6208	307 y	12/12/2018 15:40	12/12/2018 15:40	acpid	acpid start/running,	process 1552 (using upstart	.)	Auto	Running	307
128	6209	307 y	12/12/2018 15:40	12/12/2018 15:40	alsa-restore	alsa-restore stop/w	aiting (using upstart)		Manual	Stopped	307
129	6210	307 y	12/12/2018 15:40	12/12/2018 15:40	alsa-store	alsa-store stop/wai	ting (using upstart)		Manual	Stopped	307
130	6211	307 y	12/12/2018 15:40	12/12/2018 15:40	anacron	anacron stop/waitir	ng (using upstart)		Manual	Stopped	307
131	6212	307 y	12/12/2018 15:40	12/12/2018 15:40	apport	apport start/runnin	g (using upstart)		Auto	Running	307
132	6213	307 y	12/12/2018 15:40	12/12/2018 15:40	atd	atd start/running, p	rocess 1553 (using upstart)		Auto	Running	307
133	6214	307 y	12/12/2018 15:40	12/12/2018 15:40	avahi-daem	avahi-daemon start	/running, process 1245 (usir	g upstart)	Auto	Running	307
134	6215	307 y	12/12/2018 15:40	12/12/2018 15:40	binfmt-sup	binfmt-support stor	p/waiting (using upstart)		Manual	Stopped	307
135	6216	307 y	12/12/2018 15:40	12/12/2018 15:40	bluetooth	bluetooth start/run	ning, process 1226 (using up	start)	Auto	Running	307
136	6217	307 y	12/12/2018 15:40	12/12/2018 15:40	centrifydc	centrifydc start/run	ning, process 1650 (using up	start)	Auto	Running	307
137	6218	307 y	12/12/2018 15:40	12/12/2018 15:40	console-set	console-setup stop,	/waiting (using upstart)		Manual	Stopped	307
138	6219	307 y	12/12/2018 15:40	12/12/2018 15:40	console	console stop/waitin	ng (using upstart)		Manual	Stopped	307
139	6220	307 y	12/12/2018 15:40	12/12/2018 15:40	container-d	container-detect st	op/waiting (using upstart)		Manual	Stopped	307
140	6221	307 y	12/12/2018 15:40	12/12/2018 15:40	control-alt-	control-alt-delete s	top/waiting (using upstart)		Manual	Stopped	307
141	6222	307 y	12/12/2018 15:40	12/12/2018 15:40	cron	cron start/running,	process 1551 (using upstart)		Auto	Running	307
142	6223	307 y	12/12/2018 15:40	12/12/2018 15:40	cups	cups start/running,	process 1247 (using upstart)		Auto	Running	307
143	6224	307 y	12/12/2018 15:40	12/12/2018 15:40	dbus	dbus start/running,	process 1213 (using upstart		Auto	Running	307
144	6225	307 y	12/12/2018 15:40	12/12/2018 15:40	dmesg	dmesg stop/waiting	g (using upstart)		Manual	Stopped	307
145	6226	307 y	12/12/2018 15:40	12/12/2018 15:40	failsafe	failsafe stop/waitin	g (using upstart)		Manual	Stopped	307
146	6227	307 y	12/12/2018 15:40	12/12/2018 15:40	failsafe-x	failsafe-x stop/wait	ing (using upstart)		Manual	Stopped	307
147	6228	307 y	12/12/2018 15:40	12/12/2018 15:40	flush-early-	flush-early-job-log	stop/waiting (using upstart)		Manual	Stopped	307
148	6229	307 y	12/12/2018 15:40	12/12/2018 15:40	friendly-rec	friendly-recovery st	top/waiting (using upstart)		Manual	Stopped	307
149	6230	307 y	12/12/2018 15:40	12/12/2018 15:40	gssd	gssd stop/waiting (u	using upstart)		Manual	Stopped	307
150	6231	307 y	12/12/2018 15:40	12/12/2018 15:40	hostname	hostname stop/wai	ting (using upstart)		Manual	Stopped	307
151	6232	307 y	12/12/2018 15:40	12/12/2018 15:40	hwclock-sav	hwclock-save stop/	waiting (using upstart)		Manual	Stopped	307
152	6233	307 y	12/12/2018 15:40	12/12/2018 15:40	hwclock	hwclock stop/waitir	ng (using upstart)		Manual	Stopped	307
153	6234	307 y	12/12/2018 15:40	12/12/2018 15:40	hybrid-gfx	hybrid-gfx stop/wai	iting (using upstart)		Manual	Stopped	307
154	6235	307 v	12/12/2018 15:40	12/12/2018 15:40	idmand	idmand start/runnin	ng, process 1198 (using upst	art)	Auto	Running	307

1352

# 1353 List of patches/packages installed:

255 io	ł	system_id current	first_seen	last_seen	name	version	description	location	uninstall	install_da i	nstalled_by	installed_on	pub
256	54348	307 y	12/12/2018 15:40	12/12/2018 15:40	Ubuntu 12.04.5 LTS	12.04	Operating System					1/1/2000 0:00	)
257	54349	307 y	12/12/2018 15:40	12/12/2018 15:40	accountsservice	0.6.15-2ubuntu9.7						1/1/2000 0:00	J
258	54350	307 y	12/12/2018 15:40	12/12/2018 15:40	acl	2.2.51-5ubuntu1						1/1/2000 0:00	J
259	54351	307 y	12/12/2018 15:40	12/12/2018 15:40	acpi-support	0.140.2						1/1/2000 0:00	J
260	54352	307 y	12/12/2018 15:40	12/12/2018 15:40	acpid	1:2.0.10-1ubuntu3						1/1/2000 0:00	J
261	54353	307 y	12/12/2018 15:40	12/12/2018 15:40	activity-log-manager-cor	0.9.4-0ubuntu3.2						1/1/2000 0:00	J
262	54354	307 y	12/12/2018 15:40	12/12/2018 15:40	activity-log-manager-cor	0.9.4-0ubuntu3.2						1/1/2000 0:00	J
263	54355	307 y	12/12/2018 15:40	12/12/2018 15:40	adduser	3.113ubuntu2						1/1/2000 0:00	J
264	54356	307 y	12/12/2018 15:40	12/12/2018 15:40	adium-theme-ubuntu	0.3.2-0ubuntu1						1/1/2000 0:00	J
265	54357	307 y	12/12/2018 15:40	12/12/2018 15:40	) alsa-base	1.0.25+dfsg-0ubuntu1.1						1/1/2000 0:00	)
266	54358	307 y	12/12/2018 15:40	12/12/2018 15:40	alsa-utils	1.0.25-1ubuntu5.2						1/1/2000 0:00	J
267	54359	307 y	12/12/2018 15:40	12/12/2018 15:40	anacron	2.3-14ubuntu1						1/1/2000 0:00	J
268	54360	307 y	12/12/2018 15:40	12/12/2018 15:40	) apg	2.2.3.dfsg.1-2						1/1/2000 0:00	)
269	54361	307 y	12/12/2018 15:40	12/12/2018 15:40	app-install-data	0.12.04.4						1/1/2000 0:00	J
270	54362	307 y	12/12/2018 15:40	12/12/2018 15:40	) app-install-data-partner	12.12.04.1						1/1/2000 0:00	J
271	54363	307 y	12/12/2018 15:40	12/12/2018 15:40	apparmor	2.7.102-0ubuntu3.11						1/1/2000 0:00	)
272	54364	307 y	12/12/2018 15:40	12/12/2018 15:40	appmenu-gtk	0.3.92-0ubuntu1.1						1/1/2000 0:00	J
273	54365	307 y	12/12/2018 15:40	12/12/2018 15:40	) appmenu-gtk3	0.3.92-0ubuntu1.1						1/1/2000 0:00	)
274	54366	307 y	12/12/2018 15:40	12/12/2018 15:40	appmenu-qt	0.2.6-0ubuntu1						1/1/2000 0:00	J
275	54367	307 y	12/12/2018 15:40	12/12/2018 15:40	apport	2.0.1-0ubuntu17.15						1/1/2000 0:00	J
276	54368	307 y	12/12/2018 15:40	12/12/2018 15:40	) apport-gtk	2.0.1-0ubuntu17.15						1/1/2000 0:00	)
277	54369	307 y	12/12/2018 15:40	12/12/2018 15:40	apport-symptoms	0.16.1						1/1/2000 0:00	J
278	54370	307 y	12/12/2018 15:40	12/12/2018 15:40	) apt	0.8.16~exp12ubuntu10.27						1/1/2000 0:00	J
279	54371	307 y	12/12/2018 15:40	12/12/2018 15:40	apt-transport-https	0.8.16~exp12ubuntu10.27						1/1/2000 0:00	)
280	54372	307 y	12/12/2018 15:40	12/12/2018 15:40	apt-utils	0.8.16~exp12ubuntu10.27						1/1/2000 0:00	J
281	54373	307 y	12/12/2018 15:40	12/12/2018 15:40	) apt-xapian-index	0.44ubuntu5.1						1/1/2000 0:00	J
282	54374	307 y	12/12/2018 15:40	12/12/2018 15:40	) aptdaemon	0.43+bzr805-0ubuntu10						1/1/2000 0:00	)
283	54375	307 y	12/12/2018 15:40	12/12/2018 15:40	) aptdaemon-data	0.43+bzr805-0ubuntu10						1/1/2000 0:00	J
284	54376	307 y	12/12/2018 15:40	12/12/2018 15:40	) apturl	0.5.1ubuntu3						1/1/2000 0:00	)
285	54377	307 v	12/12/2018 15:40	12/12/2018 15:40	apturl-common	0.5.1ubuntu3						1/1/2000 0:00	

#### 1355 **3.3.8 Update Baseline after Modifications**

1356 Manufacturing baseline will be reviewed quarterly and updated with any changes that have

1357 occurred since last review. During period between baseline updates any new equipment added,

1358 or configuration changes implemented will initiate a new baseline scan to be performed.

1359 GRASSMARLIN<sup>2</sup> and Wireshark<sup>3</sup> are the tools used for updating baseline after modification

- 1360 have occurred. Examples of changes within the manufacturing system would be updating
- 1361 software, license, system patches, firmware updates, new devices like PLCs' or HMIs' and other
- 1362 ICS components required for operations.

# 1363 **3.3.9** Network Operations Baseline

- 1364 Network baseline will be created within manufacturing system to identify all crucial components
- 1365 required for production to operate. Tools used for this process are as listed, GRASSMARLIN

and Wireshark. Each tool listed provides slightly different capabilities and detail.

1367 GRASSMARLIN generates a diagram for easy visualization, compare to Wireshark which

1368 provides data without diagrams. These tools provide the required network operations baseline

1369 required for manufacturing process.

# 1370 **3.3.10** Priorities for Manufacturing Missions

- 1371 The priorities for manufacturing missions have been identified in the "Organization Overview"
- 1372 Section of the Security Program document.

# 1373 **3.3.11** Critical Manufacturing system components and functions

- 1374 The critical manufacturing system components and functions have been identified in the
- 1375 Organization Overview Section of the Security Program document.
- 1376

# 1377 **PROTECT**

# 1378 3.3.12 Security

- 1379 Security within the organization including the manufacturing system will be followed at all time
- 1380 to reduce risk of cybersecurity incidents. Sections below contain multiple references to
- 1381 procedures used at Alpha for security manufacturing system.

<sup>&</sup>lt;sup>2</sup> GRASSMARLIN: https://github.com/nsacyber/GRASSMARLIN

<sup>&</sup>lt;sup>3</sup> WireShark: https://github.com/nsacyber/GRASSMARLIN

#### 1382 3.3.13 Training

1383 Training is a vital role for keeping the company safe for Cybersecurity threats. All employees,

1384 contractors and vendors should have completed required training before being allowed to work

1385 within manufacturing system. Awareness and Training for Third Party Contractors and Vendors

should be reviewed and signed before being allowed to access manufacturing systems.

#### 1387 **3.3.14 Port Security**

1388 Port security allows the ability to configure network ports to be associated with individual

1389 device's Media Access Control (MAC) addresses. Enabling port security ensures only designated

- devices are allowed access, any device not already in the approved list will be denied access.
- 1391 Port Security along provides additional protection, when used with defense-in-depth strategies.
- 1392 See reference for steps required for setup within Alpha.

# 1393 3.3.15 Network Segmentation

- 1394 Alpha's manufacturing network has been segmented to improve speed and security within the
- 1395 environment. Network segmentation provides ability to control traffic from each network,
- ensuring only allowed communication can pass between each network. See reference for steps
- 1397 used for Alpha.

# 1398 **Task: Implement network segmentation**.

- The Work Cell consists of the following network hardware.
- 1400

Туре	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

#### 1401

- Network segmentation was implemented using the RuggedCom firewall. The firewall has
- 1403 the following interfaces defined. There were two subnets created as listed in the below table.
- 1404

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

- 1407 The Siemens i800 switch is connected to the Ge-2-1 interface of the RX1510 and used for the 1408 Control LAN network. Devices connected to this i800 switch such as the 4 Machining 1409 stations, Robot Driver server were assigned an IP address from the Control LAN subnet 1410 (192.168.1.0/24).
- 1411
- 1412 • The Netgear switch is connected to the Ge-3-1 interface of RX1510 and used for the
- 1413 Supervisory LAN network. Devices connected to this switch such as the PLC, HMI,
- 1414 Engineering workstation were accordingly assigned an IP address from this Supervisory 1415 LAN subnet (192.168.0.0/24)
- 1416

# Task: Identify and control connections.

1417

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

1418

#### 1419 3.3.16 Monitor Boundary Connections

1420 Network traffic will be monitored for external and internal communications using a firewall, or 1421 other type of device that allows for the ability to control connection traffic. Required network 1422 traffic leaving the manufacturing system will be allowed, all other traffic will be explicitly dropped. Traffic to manufacturing system will be limited to only those machines required for 1423 1424 monitoring from corporate network to manufacturing system and machines won't be allowed 1425 internet access. Device monitoring external/internal connection/communications will forward all

- logging to internal Syslog server for archival purposes. 1426
- 1427 • External Boundary communications are monitored using Cisco ASA Firewall in the Cybersecurity LAN network. 1428
- 1429 Internal Boundary communications are monitored using RuggedCom RX series Firewall in • 1430 the Work Cell.
- 1431 **Tool: Boundary Protection Device**

# 1432 The table below lists the boundary protection devices implemented

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

1433

# 1434 **Boundary protection device configuration.**

1435 Refer to section 4.16 Network Boundary Protection

#### 1436 **3.3.17** Actions with/without Authentication

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

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

1438 1439

		HMI User	Actions Re	quiring Auth	nentication		
	View Workcell Settings	Modify Workcell Settings	View Station Settings	Modify Station Settings	Reboot Station	Silence/Clear Alarms	Access HMI HTTP Server
All Users*	Ν	Ν	N	N	N	Ν	Y

1440

	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	

# 

# 

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	Ν	N	Y		

# 

# PLC Actions Requiring Authentication

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

1450 \* Authentication for *all users* does not imply authorization has been granted to any specific user1451 or role.

#### 1452 **3.3.18 Network Connections**

- All network connection with manufacturing system will be documented to include port numbersand cables will be labeled indicating their designated purpose.
- 1455 Using company provided network diagram tools, all network connection for internal
- 1456 communication will be mapped. Mapping will include all relevant information for connection.
- 1457 Example of information required would be assigned IP address for device providing service and
- 1458 person of contact. Network diagram will be updated quarterly.
- 1459 All connection will be reviewed and authorized before being placed into production.

#### 1460 **3.3.19 Remote Maintenance**

- 1461 Remote maintenance activities will be coordinated and approved before vendor access is
- allowed. All remote maintenance activities provided by a vendor will be controlled and
- 1463 monitored to ensure no harmful or malicious activities occur. Any vendors or contractors
- 1464 connecting to Alpha for remote maintenance will require approval before connecting. Requests
- 1465 will be documented to ensure proper audit trail for activity conducted within manufacturing
- 1466 system. See reference for detailed plan.

# 1467 **3.3.20 System Maintenance**

1468 Please see System Maintenance Section within Security Policy document.

# 1469 **3.3.21 Change Control**

- 1470 Changes to manufacturing system will be submitted to a change control process ensuring that all
- 1471 applicable parties are aware and agree on actions being performed. Management will have final
- 1472 approval since production could be affected by down time.
- 1473 Changes within the manufacturing systems will be scheduled during non-production hours as not
- 1474 to affect processing within manufacturing system. Changes will be reviewed and authorized
- 1475 before being implemented. Potential system performance issues from the potential change must
- 1476 be determined before the change is made. Once changes have been completed a review will be
- 1477 conducted ensuring same security level continues to be maintained after changes have been
- 1478 implemented.

- 1480 Responsible parties will evaluate security impact on change controls being performed within the
- 1481 manufacturing system environment. Change control reviewers will have final say for changes
- 1482 being implemented along with changes having an impact on security
- 1483 An Excel sheet will be used to document all change control items.

#### 1485 Below is a list of items that need to be configuration controlled.

1486

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

1487

#### 1488 **3.3.22 Backup Procedures**

- 1489 <u>Servers, Workstations:</u>
- 1490 Refer Section 4.6 Veeam Backup and Replication
- 1491
- 1492 <u>Network Devices Switches:</u>
- 1493 1. Login to the Web UI of the device from the Engineer Workstation
- 1494 2. In the Web UI, browse to the Backup option, select the type of backup and click Download
- 1495 3.Ensure to manually save the configuration backup at a central secure location
- 1496 <u>Network Devices RuggedCom Router:</u>
- 1497 1. Login to the Web UI of the device from the Engineer Workstation
- 1498 2.Click Admin >> Full-Configuration-Save >> Format- Cli >> Enter a File Name >> Perform

onfigure Running	Tools	Logout from ruggedcom	
iew   Edit Private	Edit Exclusive		
<ul> <li>admin</li> <li>chassis</li> <li>global</li> <li>interface</li> <li>interfaces</li> <li>switch</li> <li>tunnel</li> <li>ip</li> </ul>		<ul> <li>reboot</li> <li>set-system-clock</li> <li>restore-factory-defau</li> <li>delete-logs</li> <li>install-files</li> <li>backup-files</li> <li>full-configuration-sa</li> <li>full-configuration-lo</li> </ul>	×
		/admir	n/full-configuration-save
Format Cli  File Name * Backup-April21-2019 <string, 1="" chars<="" min:="" th=""><th>) max: 255 chars&gt;</th><th></th><th></th></string,>	) max: 255 chars>		
Trigger Action	ation to a file, clic	r Perform. Perform	

1500 3.Click on Tools >> Download >> Choose File Type – Configuration >> Click on the file to
 1501 download

# SIEMENS



- 1504 <u>ICS Devices:</u>
- 1505 Follow the Manufacturer's product manual to perform a backup
- 1506 Ensure to manually save the configuration backup at a central secure location
- 1507

#### 1508 **3.3.23 Media Sanitization for Devices**

Assets / Device type	Method used	Details
Hard Drives on servers, workstations	CLEAR	<ul> <li>Tool: DBAN <sup>4</sup>, Category: Software, Type: Open-Source <u>Instructions:</u></li> <li>(1) Download and create a bootable media of DBAN</li> <li>(2) Boot the server using the bootable media</li> <li>(3) Follow the on-screen instructions to run the multiple passes of data wipe.</li> <li>(4) Once complete, verify if wipe was successful by booting the server without the DBAN media</li> </ul>
Dealth off DL C		<ul> <li>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.</li> <li>(1) Obtain a copy of the base image of the Windows CE prior to reimaging.</li> <li>(2) Remove the MicroSD and load it in a card reader. Clear the data on the SD card using the procedure recommended in Section 2 above for SD cards.</li> </ul>
Becknoff PLC	CLEAR	(3) Load the base image on the SD card and plug it in back. As per the manufacturer's official documentation <sup>5</sup>
Red Lion HMI	CLEAR	<ol> <li>When making selections in the system menu, you must touch and hold your selection until it turns green.</li> <li>When system menu is display, touch and hold <b>Database</b> <b>Utilities</b>. Then in the next window, touch and hold <b>Clear</b> <b>Database</b>, then select yes. Then hit back, then hit continue. You will get a page invelid database which</li> </ol>

<sup>4</sup> <u>https://dban.org/</u>

<sup>&</sup>lt;sup>5</sup> <u>http://www.redlion.net/sites/default/files/1299/6670/Crimson%203.0%20-</u> %20System%20Menu%20Tech%20Note.pdf

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

<sup>&</sup>lt;sup>6</sup> https://www.plcsystems.ru/catalog/ruggedcom/doc/ROXII\_RX1500\_User-Guide\_WebUI\_EN.pdf

<sup>&</sup>lt;sup>7</sup> <u>https://support.industry.siemens.com/cs/attachments/109737193/ROS\_v4.3\_i80x\_User-Guide\_EN.pdf?download=true</u>

Wago Modular IO	CLEAR	
		<ul> <li>The below instructions are found in Netgear GS724T Manual<sup>8</sup></li> <li>Clear: <ol> <li>Login to Web Admin console of the switch.</li> <li>Click on Maintenance Tab</li> <li>Click on Factory Default and hit Apply.</li> </ol> </li> </ul>

#### 1510 **3.3.24 Priority Analysis**

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

<sup>&</sup>lt;sup>8</sup> <u>http://www.downloads.netgear.com/files/GDC/GS716TV2/GS716T\_GS724T-SWA-October2012.pdf?\_ga=2.154219964.507023277.1517932216-1121248166.1517932216</u>

#### 1515 **3.3.25 Vendor Requirements**

- 1516 Service Level Agreements (SLA) will be outlined and discussed, along with the need
- 1517 for required notification when an employee transfers departments', leaves the company, or is
- 1518 terminated that had direct network connectivity into Alpha network. An example SLA developed
- 1519 for Alpha is below.

1520	Service Level Agreement (SLA)	٦
1521	for Vendor	
1522	by	
1523	Alpha	
1524	Effective Date: 02-22-2019	
1505	6	

#### 1525 1526

Document Owner:		
	Document Owner:	

1527

# 1528 Version1529

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

1530

# 1531 Approval

1532 (By signing below, all Approvers agree to all terms and conditions outlined in this Agreement.)

1533

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

1534 1535

# 1536 Agreement Overview

- 1538 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
- 1540 sustain the Product or Service.

1541 This Agreement remains valid until superseded by a revised agreement mutually endorsed by the 1542 stakeholders. 1543 This Agreement outlines the parameters of all IT/OT services covered as they are mutually 1544 understood by the primary stakeholders. This Agreement does not supersede current processes 1545 and procedures unless explicitly stated herein. 1546 1547 **Goals and Objectives** 1548 1549 The **purpose** of this Agreement is to ensure that the proper elements and commitments are in 1550 place to provide consistent IT/OT service support and delivery to Alpha by the Service 1551 Provider(s). 1552 The goal of this Agreement is to obtain mutual understanding for IT/OT services provision 1553 between the Service Provider and Alpha. 1554 1555 The objectives of this Agreement are to: 1556 • Provide clear reference to service ownership, accountability, roles and/or responsibilities. 1557 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. 1558 1559 1560 Stakeholders 1561 1562 The following Service Provider and Alpha will be used as the basis of the Agreement and represent the primary stakeholders associated with this SLA: 1563 1564 IT Service Provider: Service Provider IT/OT Customer: Alpha 1565 **Periodic Review** 1566 1567 1568 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 1569 review during any period specified, the current Agreement will remain in effect. 1570

1571 The **Business Relationship Manager** ("Document Owner") is responsible for facilitating regular 1572 reviews of this document. Contents of this document may be amended as required, provided 1573 mutual agreement is obtained from the primary stakeholders and communicated to all affected 1574 parties. The Document Owner will incorporate all subsequent revisions and obtain mutual 1575 agreements / approvals as required.

1577 1578 1579 1580 1581	Business Relationship Manager: Alpha (President) Review Period: Yearly (12 months) Previous Review Date: 02-22-2019 Next Review Date: 02-22-2020
1582 1583 1584 1585 1586 1587 1588	Service Agreement The following detailed service parameters are the responsibility of the Service Provider in the ongoing support of this Agreement. Service Scope
1589 1590 1591 1592 1593 1594 1595 1596 1597 1598 1599 1600 1601 1602	<ul> <li>The following Services are covered by this Agreement:</li> <li>Apply system updates to manufacturing environment per vendor's recommendation</li> <li>Apply system updates to IT equipment when patches are released per vendor.</li> <li>Backup configure information for all IT/OT equipment within Alpha</li> <li>Ensure cybersecurity tools are operating correctly within the environment</li> <li>Provide liaison service between OT vendor and Alpha</li> <li>Product recommendation for new equipment being purchased and installed with Alpha's manufacturing environment</li> <li>Manned telephone support</li> <li>Monitored email support</li> <li>Remote assistance using Remote Desktop and a Virtual Private Network where available</li> <li>Planned or Emergency Onsite assistance (extra costs apply)</li> <li>Monthly system health check</li> </ul>
1603 1604 1605 1606	Customer Requirements Alpha's responsibilities and/or requirements in support of this Agreement include:
1607 1608 1609 1610 1611 1612 1613 1614 1615 1616 1617	<ul> <li>Payment for all support costs at the agreed interval.</li> <li>Reasonable availability of customer representative(s) when resolving a service related incident or request.</li> <li>Service Provider Requirements</li> <li>Service Provider responsibilities and/or requirements in support of this Agreement include:</li> <li>Meeting response times associated with service related incidents.</li> <li>Appropriate notification to Customer for all scheduled maintenance.</li> </ul>

1618 1619	Service Assumptions
1620	Assumptions related to in-scope services and/or components include:
1621	Changes to services will be communicated and documented to all stakeholders.
1622	Service Management
1623	
1624	Effective support of in-scope services is a result of maintaining consistent service levels. The
1625	following sections provide relevant details on service availability, monitoring of in-scope
1626	services and related components.
1627 1628	Service Availability
1629	Coverage parameters specific to the service(s) covered in this Agreement are as follows:
1630	• Telephone support: 8:00 A.M. to 5:00 P.M. Monday – Friday
1631	• Calls received out of office hours will be forwarded to a mobile phone and
1632	best efforts will be made to answer / action the call, however there will be a
1633	backup answer phone service
163/	• Email support: Monitored 8:00 A M to 5:00 P M Monday. Eriday
1625	<ul> <li>Emails received outside of office hours will be collected housen to action</li> </ul>
1626	• Emans received outside of office hours will be conected, however no action
1030	can be guaranteed until the next working day
1637	• Onsite assistance guaranteed within 72 hours during the business week
1638	
1639	Service Requests
1640	
1641	In support of services outlined in this Agreement, the Service Provider will respond to service
1642	related incidents and/or requests submitted by Alpha within the following time frames:
1643	• 0-8 hours (during business hours) for issues classified as <b>High</b> priority.
1644	• Within 48 hours for issues classified as <b>Medium</b> priority.
1645	• Within 5 working days for issues classified as <b>Low</b> priority.
1646	Remote assistance will be provided in-line with the above timescales dependent on the
1647	priority of the support request.
1648	
1649	

#### 1650 **Personal Changes:**

1651When an individual user with remote access leaves service provider, is transferred, or is1652terminated the service provider will notify Alpha. If user had access to Alpha's network,1653that access will be disabled, or deleted as soon as possible. System account passwords the1654service provider had will need to be changed to ensure user access into the network has1655been completely removed.

1656

# 1657 **DETECT**

# 1658 **3.3.26 Event Logging**

1659 Devices within manufacturing system shall be configured to send log data to central repository

1660 (Syslog Server) when supported. Logs sent from devices allow additional forensics analysis,

which will be useful after a cybersecurity event. Alpha logs all devices event alerts to central log

- server for review and archive purpose. Recorded events help identify any malicious activity
- 1663 within the manufacturing systems. Logs will be checked periodically looking for abnormal alerts
- being generated from manufacturing system. See reference for additional information.

# 1665 **3.3.27 Event Impacts**

- 1666 Logged events will be examined to determine the impact if any against the manufacturing
- 1667 system. Events impacting manufacturing system will be reviewed to determine correlation with
- 1668 risk assessment outcomes. Once correlation has been completed action will be taken if required
- 1669 to increase cybersecurity posture to lessen future threats.

# 1670 **3.3.28 Monitor**

1671 All personnel within the manufacturing system will be required to sign-in upon entering ICS

- 1672 environment with date and time of entry, including when leaving work space. Any person found
- 1673 in violation of mandatory sign-in/sign-out sheet will be escorted out of the manufacturing
- 1674 environment. Individuals will be challenged to ensure they are employees or are being
- 1675 escorted around the environment.
- 1676 All network switches will be configured for port security, so unauthorized devices won't be able1677 to access manufacturing network without prior approval.
- Weekly wireless scans will be completed using a laptop within manufacturing system. Rouge orunknown wireless devices will be brought to management's attention for additional review.
- Periodic hardware and software scans with be performed on devices within manufacturingsystem to detect any unauthorized hardware or software changes.
- 1682 Switch logs within manufacturing system will be checked regularly to ensure no rogue devices
- have attempted to connect. Output from switch logs will be compared against hardwareinventory performed in.

- 1685 Manufacturing system environment will be monitored for unauthorized personnel, connections,
- 1686 devices, access points, and software using multiple tools. Each tool provides a specify purpose
- and is designed to record and archive data. Syslog monitoring will be configured to captures all
- 1688 system generated logs and stored for archival/forensics purposes. Inventory management is used
- 1689 to detect rogue devices, include unauthorized software installations via scheduled scans within
- 1690 the manufacturing system.

# 1691 3.3.29 Forensics

- 1692 Syslog server will be used for collection of system logs. Logs can analysis to understand the
- attack target along with determining the method that was used during the attack against deviceswithin manufacturing system.

# 1695 **3.3.30 Ensure resources are maintained**

- 1696 Systems performance and resources can have a drastic effect on manufacturing
- 1697 process. Individual in charge of manufacturing systems will be responsible for performing daily
- 1698 checks on all systems within the manufacturing system environment (OT). Checks will include,
- 1699 but not limited to physical observation of all operational components ensuring any warning
- 1700 lights or other area of concern are investigated further. System logs of
- all manufacturing devices will be checked at the beginning and end of every shift looking for
- any deviation from the normal baseline performance.

# 1703 **3.3.31 Detect non-essential capabilities**

- 1704 System scanning/auditing tool will be used to identify non-essential software applications
- installed on devices within manufacturing system. Software not required for operations will be
- 1706 removed and baseline configuration updated to reflect new configuration state.
- 1707

# 1708 **RESPOND**

# 1709 3.3.32 Fire Protection Systems

- 1710 Fire protection for a manufacturing environment should be designed to safeguard electrical
- 1711 equipment. Manufacturing systems requiring protection can be PLCs', HMIs', Robots,
- 1712 Machining equipment, computers and other required devices. Fire Protection should be designed
- and implemented to protect human life first and equipment second. Installed fire protection
- 1714 systems will be certified compliant with existing/new environment by a licensed and accredited
- 1715 vendor. Check industry standards for any required baselines.

# 1716**3.3.33Emergency and Safety Systems**

- 1717 Emergency and Safety Systems will compile with Local, State, and Federal laws. This is to
- 1718 include safety regulations for workers' safety from Occupational Safety and Health

- Administration (OSHA). Industry regulation for safety will be followed per guidance from
- 1720 regulating industry.
- 1721 Fire Protection Systems will compile with Local, State, and Federal laws. This is to include Fire
- 1722 Protection Systems specially designed for manufacturing process. Fire Protection System will
- 1723 place emphasis on human safety first and for most, before concern for manufacturing system.
- 1724 Fire Protection Systems will be checked minimum once per year unless shorter intervals are
- 1725 required from superseding regulations.
- 1726 Only Industry approved Environmental Controls will be used within manufacturing systems, to
- 1727 included compliance with all Local, State, Federal laws. Environmental Control will be
- 1728 implemented to place human/community safety first before manufacturing systems.

# 1729 **3.3.34 Detected Events**

- 1730 Detected cybersecurity event notification will be investigated to determine root cause and
- appropriate remediation steps will be taken to clear events returning the organization /
- 1732 manufacturing system to known good operating state.

# 1733 **3.3.35 Vulnerability Management Process**

- 1734 Vulnerability management is an essential component of any information security program and
- the process of vulnerability assessment is vital to effective vulnerability management
- 1736 <u>Vulnerability Scanning and Management Tool</u>
- 1737 Tenable- Nessus will be used to perform vulnerability scans. The Results report generated by
- 1738 Nessus at the completion of the scan, is then fed into NamicSoft which is a vulnerability
- 1739 management, parsing and reporting tool.
- 1740 NamicSoft can create customized reports and logically group results for a consistent workflow
- within the organization. The reports are reviewed by the foreman and then shared with the machine operators.
- 1743 <u>Vulnerability Scan Targets</u>
- All devices connected to both Control and Supervisory network segments are scanned. There is apolicy and scan configured for scanning all network segments of Alpha.
- 1746 A new scan can be established, or an existing one changed, by submitting a request to the1747 Foreman.
- 1748 <u>Vulnerability Scan Frequency/Schedule</u>
- 1749 Scans are performed by engaging the IT Contractor on an on-demand, per-request basis as
- 1750 needed. The Supervisor shall make provisions for an assessment once per month. Running

- 1751 vulnerability scans using automated tools once per month will ensure continuous monitoring of
- 1752 the Manufacturing system is in place.
- All IT/OT device scans should be scheduled between the 1st and the 15th of each month.
- 1754 This accommodates critical patches released by vendors such as Microsoft.
- All device scans should be performed during hours appropriate to the business needs of the organization and to minimize disruption to normal operations
- Any new device discovered needs to be classified under its appropriate group.
- 1758 General Rules
- The Supervisor or machine operators will not make any temporary changes to information
   systems, for the sole purpose of "passing" an assessment. Vulnerabilities on information
   systems shall be mitigated and eliminated through proper analyses and repair methodologies.
- No devices connected to the network shall be specifically configured to block vulnerability
   scans from authorized scanning engines.
- Use caution when running vulnerability scans against OT Networks such as the Supervisory
   LAN and Control LAN Network. Scans should be scheduled off hours and during periods of
   maintenance.
- It is recommended to run authenticated scans from the vulnerability scanner.
- 1768 <u>Vulnerability Reporting</u>
- 1769 Upon completion of a vulnerability scan, the data is fed into NamicSoft out of which report is 1770 generated. A report will always be generated as proof that an assessment occurred.
- 1771 All IT/OT devices are organized into appropriate groups in NamicSoft as per the system they
- 1772 reside in. A device may belong to one or more systems. Reporting is done system wide so that
- the devices and vulnerabilities can more easily be distributed to the Supervisor and machine
- 1774 operators. Below is a table of type of reports that will be sent out.

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

#### 1776 <u>Remediation Management and Priorities</u>

- 1777 All vulnerabilities discovered must be analyzed by the Supervisor and Control Engineers with
- assistance from IT/OT Contractor if needed to decide on the next course of action.
- 1779 All vulnerabilities discovered should be remediated.
- 1780 The below chart should be used for remediation timelines.

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

1781

#### 1782 Exceptions Management

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

1785 Vulnerabilities may exist in operating systems, applications, web applications or OT devices.

1786 While every effort must be made to correct issues, some vulnerabilities cannot be remediated.

1787 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

1789 the developer and manufacturer. In these cases, additional protections may be required to

1790 mitigate the vulnerability. Exceptions may also be made so that the vulnerabilities are not

1791 identified as items of risk to the system and organization.
- 1792 False Positives identification may be documented through emails or the NamicSoft tool with the
- security staff. Acceptable Risk exceptions must be requested through the IT Team with an
- 1794 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.



#### 1801 **Process Overview**

1802

# 1803 **RECOVER**

# 1804 **3.3.36 Recovery Plan**

# 1805 **Purpose and Objective:**

1806 Alpha developed this incident recovery plan (IRP) to be used in the event of a significant

- disruption to the features listed in the table below. The goal of this plan is to outline the keyrecovery steps to be performed during and after a disruption working to return to normal
- 1809 operations as quickly as possible.
- 1810
- 1811

#### 1812 Scope:

- 1813 The scope of this IRP document addresses technical recovery only in the event of a significant
- 1814 disruption. The intent of the IRP is to be used in conjunction with the business continuity plan
- 1815 (BCP) Alpha developed. The IRP is a subset of the overall recovery process contained in
- 1816 the BCP. Plans for the recovery of people, infrastructure, and internal and external dependencies
- 1817 not directly relevant to the technical recovery outlined herein are included in the Business
- 1818 Continuity Plan and/or the Corporate Incident Response and Incident Management plans that
- 1819 Alpha has in place.
- 1820

1822

1823

1824

- 1821 The specific objectives of this incident recovery plan are to:
  - Establish a core group of leaders to assess the technical ramifications of a situation;
  - Set technical priorities for the recovery team during the recovery period;
  - Minimize the impact of the disruption to the impacted features and business groups;
- Stage restoration of operations back to full processing capabilities;
- Enable rollback operations once disruption has been resolved and determined appropriate
   by recovery team.
- 1828

1829 Within the recovery procedures there are significant dependencies between and supporting

1830 technical groups within and outside Alpha. This plan is designed to identify the steps that are

- 1831 expected to take to coordinate with other groups / vendors to enable their own recovery. This
- plan is not intended to outline all the steps or recovery procedures that other departments need totake in the event of a disruption, or in the recovery from a disruption.

## 1834 Incident Recovery Strategies:

1835 The overall IR strategy of Alpha is summarized in Section 3.6 Incident Recovery Plan.

#### **3.4** Risk Management Document Example

t			
1837		Risk Management Procedures	
1838		for	
1839		Alpha	
1840			
1841			
1842			
	<b>Document Owner:</b>	Supervisor, Alpha	

# 

# **Version**

1	ð	4	Э

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**

1848 (By signing below, all Approvers agree to all terms and conditions outlined in this document.)

Approvers	Role	Signed	Approval Date
	President		4-22-2018

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

#### **3.4.1 Scope**

1857 Any employee, contractor, or individual with access to the organization's systems or data.

#### 1859 **3.4.2** Risk Management Process

#### 1860 Process

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

accomplishing this are outlined in the following sections.

### 1864 **Risk Identification**

1865 Risk identification will involve the shop Supervisor, Machine operators, evaluation of
1866 environmental factors, organizational culture and the project management plan including the
1867 project scope. There are many different types of threats that can affect IT and OT infrastructure.
1868 These can include:

- 1868 These can include:
- 1869 Technical threats disruption caused by technological advances or failures
  1870 Structural threats anything related to the building that houses your IT/OT
- 1871 infrastructure that could cause it to be harmed
- Financial threats If the business loses funding or experiences another significant financial change
- Human threats human error or loss of important individual
- Natural threats weather and natural disasters such as earthquakes, tornadoes, and floods
- 1877

1878 A Risk Management Log will be generated and updated as needed, a sample of which is shown1879 in the latter half of this document.

Software tools such as CSET<sup>9</sup> will be used to perform RISK Assessments. The reports generated
 will be discussed with the President.

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

1884 This is an iterative process. As the program progresses, more information will be gained 1885 about the program and the risk statement will be adjusted to reflect the current understanding. 1886 New risks will be identified as the project progresses through the life cycle.

# 1887 Risk Analysis

- 1888 All risks identified either manually or via CSET will be assessed to identify impact on
- operations. Qualification will be used to determine which risks are the top risks and which onescan be ignored.

<sup>&</sup>lt;sup>9</sup> CSET: <u>https://ics-cert.us-cert.gov/Assessments</u>

#### 1891 Qualitative Risk Analysis

- 1892 The probability and impact of occurrence for each identified risk will be assessed by the shop
- 1893 supervisor with input from the machine operators using the following approach:

- 1895
  - High Greater than <70%> probability of occurrence in a year
- Medium Between <30%> and <70%> probability of occurrence in a year
- 1897 Low Below <30%> probability of occurrence in a year
   1898

# 1899 **Impact**

- High Risk that has the potential to greatly impact project cost, project schedule or performance
- Medium Risk that has the potential to slightly impact project cost, project schedule or performance
- 1904
- Low Risk that has relatively minor impact on cost, schedule or performance
- 1905

# 1906Quantitative Risk Analysis

- 1907 This involves assigning a numeric value to the risk calculated as the product of probability of
- 1908 occurrence and impact score. Analysis of risk events that have been prioritized using the
- 1909 qualitative risk analysis process and their effect on project activities will be estimated, a
- numerical rating applied to each risk based on this analysis, and then documented in the risk
- 1911 management log.

# 1912**3.4.3** Risk Monitor and Control

- 1913 The Supervisor and IT/OT contractors will conduct yearly risk assessments which includes
- 1914 CSET assessments, vulnerability scans of the manufacturing system taking into account
- 1915 vulnerabilities and potential impact to the manufacturing operations. An identified risk can be
- 1916 bought to Supervisor's attention either by Alpha's employees or by external contractors.
- 1917 The IT Contractor will scan the IT and OT assets when called upon; with Nessus to monitor for
- any software-based risks. Nessus results will be fed into NamicSoft. Reports will be generated
- 1919 out of this tool and shared with the Supervisor. Any other type of risks like hardware based,
- 1920 physical, environmental will be identified and documented manually.
- All software-based vulnerabilities discovered using Nessus should be mitigated as per theVulnerability Management Plan.
- 1923 If a software vulnerability has been remediated; a Nessus scan be re-run to see whether the
- situation has changed in a way that affects the manufacturing operations. For any corrective
- 1925 action has been taken, the risk management log will be updated.

#### 1926 **Risk Notification Process** 3.4.4



1927

#### 1928 **Risk Response / Remediation Strategy** 3.4.5

- 1929 For each major risk, one of the following approaches will be selected to address it:
- 1930 • Avoid – eliminate the threat by eliminating the cause
- 1931 • Mitigate – Identify ways to reduce the probability or the impact of the risk
- 1932 • Accept – Nothing will be done
- 1933 • Transfer – Make another party responsible for the risk (buy insurance, outsourcing, etc.)
- 1934
- For each risk that will be mitigated, the Supervisor and operators will identify ways to prevent 1935 1936 the risk from re-occurring or reduce its impact or probability of occurring. This may include
- 1937 Prototyping. •
  - Adding tasks to the project schedule •
- Determining and allocating resources. 1939 •
- 1940

1938

For each risk that needs to be "Accepted", a document containing the list of accepted risks will 1941 be maintained by the Supervisor. 1942

1943 The Supervisor will reach out to an IT/OT Contractor for any risks and request remediation1944 assistance.

### 1945 **3.4.6 Risk Appetite**

- Risk appetite is the broad-based amount of risk an organization is willing to accept in pursuit ofits mission/vision. [4]
- 1948 Risk Appetite scale [5]:
- High the manufacturing system accepts disciplined risk taking because the organization has determined the potential benefits outweigh the potential risk.
- Moderate the manufacturing system accepts some risk taking, assuming the organization has reviewed the potential benefits and potential risks.
- Low the manufacturing system accepts minimal risk taking.
- None the manufacturing system accepts no risk taking because the risk is intolerable.
- 1956 **3.4.7** Risk Tolerance
- Risk tolerance is the acceptable level of variance in performance relative to the achievement of
  objectives. In setting risk tolerance levels, management considers the relative importance of the
  related objectives and aligns risk tolerance with risk appetite. [4]
- 1960 Risk tolerance scale [6]:
- Low the level of risk will not considerably impact the ability of the manufacturing system to meet its mission objectives.
- Moderate the level of risk may impact the ability of the manufacturing system to meet its mission objectives.
- High the level of risk will significantly impact the ability of the manufacturing system to meet its mission objectives.
- 1967

1955

- 1968 3.4.8 Risk Categories
- 1969 Risk Categories are used to classify a risk. This table represents a sample of potential categories1970 that may be applied to each risk.
- Safety the risk that human and/or environmental safety are compromised by an incident in the manufacturing system.
- Production the risk that product quality and/or production goals are compromised by an incident in the manufacturing system.
- Trade Secrets the risk that intellectual property and sensitive business data are compromised by an incident in the manufacturing system.

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

1978

# 1979 **3.4.9** Risk Reporting

1980 This table describes the frequency and format of how the Supervisor will document, analyze,

1981 communicate, and escalate outcomes of the risk management processes.

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

1982

1983 The Supervisor will share the results of risk assessments (either the Risk Management Log or

1984 CSET Report) with the appropriate stakeholders of Alpha and the President.

1985

# 1987 **3.4.10 Sample Risk Management Log**

1988 A Risk Log will be maintained by the Supervisor and Book keeper. These will be reviewed in the

1989 project team meetings. This log captures the results of a qualitative and quantitative risk analysis

and the results of planning for response.

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

1991

#### 1992 **3.4.11 Periodic Review**

1993 This document will be reviewed and updated annually by the Supervisor in consultation with the 1994 machine operators.

Annual reviews will be conducted determining component value within the manufacturing process being performed. Values will be used to determine required devices for continued

1997 manufacturing process and the effects if a cyber incident occurs against a device.

#### 1998 **3.4.12 Asset Criticality Matrix**

1999After a list of Alpha's assets or systems of value requiring protection have been identified by the2000Hardware 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.

2002

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

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

2005

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

2009 **High** - Loss or damage of this asset would have serious impact to the Operations of the

2010 Manufacturing system directly impacting production. This can result in major loss of primary

2011 services, core processes or functions. These assets can also be single point of failure.

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

2014 processes or functions.

2015 Low - Loss or damage of this asset would have minor to no impact on the Operations of the

2016 Manufacturing system or Production. This can result in little or no loss of primary services, core

2017 processes or functions.

# 2019 A list of assets belonging to Alpha with assigned value is presented below.

# 

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

# **3.4.13 Definitions and Acronyms**

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

# **3.4.14 References**

2026	1.	Risk Management plan – Maryland Department of Information Technology
2027		doit.maryland.gov/SDLC/Documents/Project%20Risk%20Managment%20Plan.doc
2028		
2029	2.	Sample Risk Management plan – State of North Dakota
2030		https://www.nd.gov/itd/sites/itd/files/legacy/services/pm/risk-management-plan-
2031		sample.pdf

2032		
2033	3.	Office of Management and Budget, "Management's Responsibility for Enterprise Risk
2034		Management and Internal Control", Office of Management and Budget, OMB Circular
2035		No. A-123, 2016. [Online]. Available:
2036		https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-
2037		<u>17.pdf</u> .
2038		
2039	4.	United States Agency for International Development, "U.S. Agency for International
2040		Development Risk Appetite Statement", United States Agency for International
2041		Development, 2018. [Online]. Available:
2042		https://www.usaid.gov/sites/default/files/documents/1868/USAID_Risk-Appetite-
2043		Statement_Jun2018.pdf.
2044		
2045	5.	Office of the Comptroller of the Currency, "Enterprise Risk Appetite Statement", Office
2046		of the Comptroller of the Currency, 2016. [Online]. Available:
2047		https://www.occ.treas.gov/publications/publications-by-type/other-publications-
2040		

2048 <u>reports/risk-appetite-statement.pdf</u>.

#### 2049 **3.5** Incident Response Plan Document Example

2050		Incident Response Plan	
2051		for	
2052		Alpha	
2053			
2054			
2055			
	<b>Document Owner:</b>	Supervisor, Alpha	

# 2056

#### 2057 2058

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

# 2059

# 2060 Approval

Version

- 2061 (By signing below, all Approvers agree to all terms and conditions outlined in this document.)
- 2062

Approvers	Role	Signed	Approval Date
	President		4-22-2018

#### 2063

#### 2064 3.5.1 Statement of Management commitment

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

#### 2072 **3.5.2** Purpose

2073 An incident can be defined as any event that, if unaddressed, may lead to a business interruption

2074 or loss. This document describes the plan for responding to information security incidents at

2075 Alpha Inc. It defines the roles and responsibilities of participants, characterization of incidents,

2076 relationships to other policies and procedures, and reporting requirements. The purpose of this

- 2077 plan is to detect and react to security incidents, determine their scope and risk, respond
- 2078 appropriately to the incident, communicate the results and risk to all stakeholders, and reduce the
- 2079 likelihood of the incident from reoccurring.
- 2080 This Plan is to be executed during or after a cybersecurity incident.
- 2081 **3.5.3 Scope**
- 2082 This plan applies to all the employees of Alpha.

#### 2083 **3.5.4** Roles and Responsibilities

2084 The Alpha Incident Response Team is comprised of:

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

# 2085 **3.5.5 Categories of Incidents**

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

2088	•	Intrusion
2089	•	Denial of Service
2090	•	Loss of Power
2091	•	Virus / Malware
2092	•	Social Engineering (Phishing, Phone, Email, etc.)
2093	•	Data Breach
2094	•	Hardware Stolen
2095	•	User account compromise
2096	•	System Misuse
2097	•	Technical Vulnerability
2098		-
2099	3.5.6	Severity Classification

- 2100 The Severity of an incident is determined based on the impact to the company and the urgency of
- 2101 restoration.

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

2102

#### 2104 **3.5.7** Restoration Priorities

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

2105

# 2106 **3.5.8 Incident Alert Thresholds**

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

#### 2112 **3.5.9 Incident Response Policy**

- An incident upon detection or being reported needs to be thoroughly investigated as per the
   process defined under "Detection and Analysis" step of the IR process in the next section.
   The investigation may be performed by the Supervisor or by convening an IR Team.
- 2116 2. The incident needs to be classified as per the categories defined previously.
- Upon Investigation, the impact to the Manufacturing system must be determined. The IR
  Team may co-relate detected event information with Risk assessment outcomes to achieve
  perspective on the incident impact across the Organization. The incident will accordingly be
  assigned a Severity level and reported to the President. The Incident Report Template form
- should be used for this purpose.

- 2122 4. During the "Detection and Analysis" step, detailed troubleshooting or forensic analysis
  2123 should be performed to determine the root cause. This may be done using in place log
  2124 management tools or commercial products such as Wireshark.
- 5. Upon investigation, the incident must be mitigated as per the "Containment, Eradication and Recovery" step of the IR Process.
- 6. The Supervisor upon consultation with the President. The Incident Report Template formshould be used for this purpose.
- 2129 7. will communicate, co-ordinate and share incident response plan with Alpha's stakeholders.
- 8. The President will share information about any cybersecurity incidents and its mitigationwith its designated sharing partners.
- 2132 9. The overall Incident Response program and plan will be revised or improved upon after
  2133 every incident. Procedures must be updated regularly to address evolving threats such as
  2134 APTs, Organizational changes, Manufacturing changes and/or after any problems discovered
- 2135 during implementation, execution or testing
- 2136 10. User awareness Training and Testing procedures will be updates after every incident.
- 2137 11. The Supervisor will communicate any changes or updates made to this policy.
- 2138

# 2139 3.5.10 Incident Plan Response Steps / Workflow

- 2140 The <u>NIST Computer Security Incident Handling [1] Guide</u> divides the incident response lifecycle
- 2141 into the following four steps:
- 2142 1. Preparation
- 2143 2. Detection and Analysis
- 2144 3. Containment, Eradication and Recovery
- 2145 4. Post-incident Activity
- 2146





2148

#### 2149 **3.5.11** Guidelines for Information Sharing

#### 2150 Interactions with Law Enforcement

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

#### 2155 **Communications Plan**

- The President will share information about any cybersecurity incidents and its mitigation 2157 with its designated sharing partners. Refer to the Next section for additional details
- All public communications about an incident or incident response to external parties outside
   of Alpha are made in consultation with the President.
- The minimum information necessary to share for a particular incident is determined by the
   Supervisor in consultation with President or administrative authorities such as the
   bookkeeper.
- 2163
- 2164 **3.5.12** Guidelines for Reporting to Stakeholders

### 2165 **Overview:**

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

# 2175 Who will be responding:

- Depending on the severity of the security incident this role can be filled by President, or the
   Supervisor
- If the severity of a security incident requires additional resources, they should be contacted and brought in to help gather forensic information along with responding to inquiries.
- 2180 o Examples:
- 2181 Legal Counsel
  - Forensic Investigator
  - IT consultant (Work in conjunction with IT Manager)
  - Security Consultant (Work in conjunction with IT Manager and Supervisors)
    - Law Enforcement (Depends on severity)

# 2186 Notification:

2182

2183

2184

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

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

#### 2193 **Communications:**

- The President will contact primary partners/vendors via phone call to inform them of the
   security incident. This should be done once all information has been gathered and a corporate
   response has been prepared.
- No voicemails will be left concerning the security incident in question. If recipient is
   unavailable schedule a follow up call.
- The Supervisor is the **only** Alpha employee authorized to call partners/vendors not already contacted by the President.
- Responses to partners/vendors should be scripted to ensure the delivered message is consistent, while ensuring only information regarding security incident are discussed.
- Email communication will be completed as a follow-up to a phone.
- Any email communications being sent will have additional proof reading completed by the President.
- Depending on the impact of security incident a Public Relation firm may be required to help with a response when providing communications via electronic or verbal.
- Media communication can **ONLY** be approved by President.
- 2209

#### 2210 **Restoring Trust:**

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

# 2220 3.5.13 Incident Report Form Template

Incident Reporting Template Form						
		Contact information				
Date Reported : Time Reported:						
Name:	lame: Title: Dept:					
Office Phone:						
		Details				
Date of Incident	:		Time of Inc	ident:		
		Type of Incident - Check all that apply				
Intrusion		Social Engineering ( Phishing, Phone, Email etc )	Technical	Vulnerability		
Denial of Service		Data breach	System m	nisuse		
Loss of power		Hardware stolen	Others, pl	Is specify		
Virus / Malware		User account compromise				
		Incident Description				
Provide a brief d	escription:					
Im	pact / Potent	ial impact - Check all of the following that appl	y to this inci	ident.		
Loss / Compromi	ise of Data	Financial Loss				
Damage to syste	ms	Other Organizations affected				
Damage to publi	c	Damage to Integrity or Delivery of Goods, Services				
System downtim	e	Unknown at this time				
Frovide a brief d	escription.					
		Affected System(s) information				
Host	IP	Application (if any)		0.S		
			L			
	Sei	nsitivity of Data compromised ( incase of Data l	oss)			
Public (Informa	tion is already ap	pproved for release & unauthorized disclosure will not caus	e problems for	the Company).		
Internal Use ( Inf Unauthorized dis example: Email o	ormation is inter closure may be a ontacts, emails e	ded for internal use within the Company or with other affili against laws, regulations and may harm the Company or its tc).	ated orgnaziati business partn	ions, business partners. ers or its customers. For		
Confidential ( Re business need fo Customers. For e	lated to Privacy r access. Unauth xample: Trade se	Violation. Information is private & sensitive in nature. It mus orized disclosure is against laws, regulations and will harm t crets, Software code, Citizen's data etc).	st be restricted he Company o	to those with legitimate r its business partners or		
		Details of the Data loss				
Provide a descrip	tion of what	was compromised:				
Follow up action taken so far						
Law enforcement	t notified	System disconnected from Network.				
Restored backup	s	Log files examined				
AV Virus definitio	AV Virus definition updated Any other action taken, pls specify					
System reimaged	for quarantined	No action taken				
Supervisor's Nam	Supervisor's Name: Supervisor's Signature: Date:					

# **3.5.14 Definitions and Acronyms**

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

# 

# **3.5.15 References**

2225 2226	1.	NIST Publication for handing Computer Security Incident https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
2227		
2228		
2229		

#### 2230 **3.6** Incident Recovery Plan Document Example

*			
2231		Incident Recovery Plan	
2232		for	
2233		Alpha	
2234			
2235			
2236			
	<b>Document Owner:</b>	Supervisor, Alpha	

#### 2237 2238

Version

### 2239

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

#### 2240 2241 **Approval**

- 2242 (By signing below, all Approvers agree to all terms and conditions outlined in this document.)
- 2243

Approvers	Role	Signed	Approval Date
	President		4-22-2018

2244

#### 2245 **3.6.1** Scope

- 2246 The scope and purpose of this document is to inventory all of infrastructure and capture
- 2247 information relevant to the Alpha's ability to recover its IT/OT environment from a
- 2248 cybersecurity incident. It, in turn also aims to provide an effective and efficient recovery effort.

#### 2249 **3.6.2** Objectives

- 2250 This plan has been developed to accomplish the following objectives:
- Limit the magnitude of any loss by minimizing the duration of a critical application service interruption.
- 2253 2. Assess damage, repair the damage, and activate the repaired computer center.
- 2254 3. Manage the recovery operation in an organized and effective manner.
- 2255 4. Prepare technology personnel to respond effectively in an incident recovery situation.

- 2256 Incident Response:
- 2257 This IR Plan is to be executed during or after a cybersecurity incident.
- 2258 The person discovering the incident must notify the Supervisor, who collectively assume
- responsibility for deciding which if any aspects of the IR plan should be implemented, and for
- 2260 establishing communication with employees, management, partners and customers

#### 2261 **3.6.3 RPO and RTO Targets**

2262 Alpha defines the following SLA's or Restoration times for operations recovery

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

2263

#### 2264 **3.6.4** Incident Recovery Team

2265 Alpha's Incident Recovery (IR) Team will consists of the following individuals.

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

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

# **Contact Information**

# **3.6.5** Contact Information

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

# 2271 External Contacts

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

2272

# 2274 **3.6.6 Notification Calling Tree**



### 2284 **3.6.7** Communications

#### 2285 Notification

- The Supervisor in consultation Machine Operators will periodically update the President 2287 on the progress of Recovery Activities.
- A Legal Counsel may be hired to oversee notification planning since the potential for legal actions against Alpha arising from security incident in question.
- If required, an outside Public Relations firm may be required depending on the severity level of the incident to help with crafting a response.
- The President's approval is required for work with any outside agency.

### 2293 **Communications**

The President will contact primary partners/customers via phone call to inform them 2294 • 2295 about Recovery activities. This should be done once all information has been gathered 2296 and a corporate response has been prepared. 2297 The Supervisor is the **ONLY** Alpha employee authorized to call partners/vendors not • 2298 already contacted by the President. 2299 Responses to partners/vendors should be scripted to ensure the delivered message is • consistent, while ensuring only information regarding security incident are discussed. 2300 2301 Email communication will be completed as a follow-up to a phone. ٠ 2302 Any email communications being sent will have additional proof reading completed by • 2303 the President. 2304 Depending on the impact of security incident a Public Relation firm may be required to • 2305 help with a response when providing communications via electronic or verbal.

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

# 2307 Restoring Trust

- Alpha's President or Supervisor with the advice consultants and Forensic experts will
   notify partners/vendors and customers with the steps being taken to restore and strength
   system security.
- The Supervisor will discuss with employees what caused security incident and what is being done to avoid a similar issue in the future.
- Once the security incident has been resolved and all fact are known, Alpha's leadership team will provide a full report which will be made publicly available containing facts relating to the security incident, along with the steps being taking to safe guard IT/OT infrastructure ensuring this and future events don't happen again.
- 2317 **3.6.8** Plan Testing and Maintenance

# 2318 Maintenance

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

# 2326 Testing

2322

2323

2324

2325

- Walkthroughs- IR Team members will verbally go through the specific steps as
   documented in the plan to confirm effectiveness, identify gaps or other weaknesses. The
   team should be familiar with procedures, equipment and operations.
- Simulations- An incident is simulated so that normal operations will not be interrupted.
   Hardware, software, personnel, communications, procedures, supplies and forms,
   documentation and utilities should be thoroughly tested in a simulation test.
- Full-Interruption Testing- IR Team members will perform a full-interruption test to activate a total IRP scenario. Caution must be exercised as this type of test disrupts normal operations.

### 2337 **3.6.9** Hardware Information

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

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

2338

# 2339 3.6.10 Backup Strategy

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

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

# 2341 **3.6.11 Recovery Procedures**

- The Incident Recovery plan will be executed following a cybersecurity incident.
- Any exceptions or issues during the Recovery process must be communicated to the
   Supervisor and/or President.
- Depending on the incident, and on the number and nature of the IT services affected, one or more of the following IR procedures may be activated by the IR team:
- 2347

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

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

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

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

# 2349 File System Layouts

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

2350

# 2351 **Restoration Priorities**

2352 Should an incident occur and Alpha need to exercise this plan, this section will be referred to

2353 reference restoration priorities in bringing systems online.

# 2354 IT Systems

Priority	IT System	Description	
High	LAN-AD	Active Directory / DNS Server	
High	Veeam	Veeam Backups Server	
High	MINTAKA	Robot Driver	
High	vController1, 2	Robot Controllers	
High	POLARIS	Engineering Workstation	
High	Robotics-PI	Local Historian Database	
--------	------------------	---------------------------------	--
Medium	PI-DMZ	DMZ-Historian	
Medium	SymantecMgr	Symantec Antivirus Manager SEPM	
Low	GTB Inspector	DLP	
Low	Graylog	Syslog server	
Low	Hive	Incident Response Server	

### 2356 Networking Equipment

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

#### 2357

### 2358 OT Systems

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

#### **3.6.12 Definitions and Acronyms**

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

#### 

#### **3.6.13 References**

2363	1.	SANS Guide for DR: https://www.sans.org/reading-room/whitepapers/recovery/disaster-
2364		recovery-plan-strategies-processes-564
2365	2.	NIST SP 800-34 Contingency planning guide for Federal Systems
2366		https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-34r1.pdf
2367	3.	Allen Bradley ControlLogix 5571 Manual
2368		https://literature.rockwellautomation.com/idc/groups/literature/documents/um/1756-
2369		um001en-p.pdf

#### **Technical Solution Implementations** 4.

#### 2372 4.1 Introduction

2373 This section includes proof-of-concept technical solution implementations developed for the 2374 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 2375 2376 organization's information security experts should identify the technical solutions that will best

2377 integrate with their existing cybersecurity program and manufacturing system infrastructure.

All of the technical solutions were installed and configured within the Collaborative Robotics 2378 2379 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 2380 2381 modes of operation were tested for each mode that aligned with the requirements of the low 2382 security level and the applicability of the mode to the use case [7].

2383 Three types of performance measurements were performed during the implementation: baseline 2384 measurements of the initial workcell performance, impact of individual technologies or configurations, and impact of the completed security level implementation. The process of 2385 sequentially implementing and measuring enabled the detection of performance-impacting 2386 2387 interactions between the technical solutions.

- Security level baseline Before any changes were made to the workcell, baseline 2388 • 2389 measurements were captured. Since all experiments are meant to be comparative, a baseline reference of system performance must be obtained to determine if the 2390 2391 manufacturing process or its sub-systems have been impacted after a technical solution is installed or reconfigured. 2392
- Technology/configuration implementation impact These measurements were 2393 2394 performed after each technical solution was installed and configured to meet the security 2395 level requirements. Some technical solutions provided multiple modes of operation that 2396 met the security level requirements and had the potential to affect the manufacturing process differently. Measurements were performed for each unique configuration to 2397 compare its impact to the previous configurations. 2398
- 2399 Security level implementation impact - These measurements were performed after all • technical solutions have been installed and configured. These measurements are used to 2400 determine the total impact to the manufacturing process and compared with other security 2401 2402 level implementation impact measurements to determine the relative performance impact 2403 between the security levels. The final technology implementation impact (if it not a 2404 multi-mode measurement) can also be used as the security level implementation impact.

2405 Before the security level baseline measurements were performed, the workcell manufacturing 2406 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 2407 process was in-control, stable, and random. 2408

- 2409 The primary key performance indicator (KPI) used to determine if the manufacturing process
- 2410 experienced a performance impact was "part production time" (KPI 2.1 in [6]), which measures
- 2411 the amount of time required for a part to travel through the manufacturing process. Numerous
- 2412 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
- 2414 determining the root cause of any realized performance impacts.

#### 2415 **4.1.1** Implementation Note – Due Diligence Implementing Technical Solutions

- 2416 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
- 2418 using any technical solutions, especially those that actively scan the manufacturing system ICS
- network and its devices; manufacturers should first conduct an assessment of how these tools work and what impact they might have on the connected control equipment [3]. Technology
- work and what impact they might have on the connected control equipment [3]. Technologyevaluations may include testing in similar, non-production control system environments to
- 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
- ature 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
- 2425 actively scans the manufacturing network should be scheduled to occur only during planned
- 2426 downtimes. [3]

### 2427 **4.1.2** Implementation Note - Sensor Error and Adaptation of KPI

2428 After the Low baseline implementation was completed, an analysis of the KPI was performed.

2429 During this analysis, a small but consistent increase in the Station 4 allocation ratio was observed

- 2430 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
- 2432 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).

#### CSF MFG PROFILE LOW SEC LVL EXAMPLE IG DISCRETE-BASED MFG SYSTEM USE CASE



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.

2441 After further analytical review of the testbed measurements, the problem was isolated to a

2442 retroreflective proximity sensor located in the workcell on Station 4. The sensor specification

2443 defined a 20 mm sensing distance, but testing revealed the sensor intermittently reporting part

2444 presence after the part was removed upwards of 100 mm from the sensor. This effect was

2445 exacerbated by the motion of the robot, which keeps the part within the sensor field of view

2446 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 sensorspecification 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.

244) response time). The response time when a part was placed into the station was not affected

2450 The faulty sensor data was reviewed to determine if it could be eliminated from the KPI

2451 measurements. Since the only measurements affected were when parts were *removed* from

2452 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

2454 method proved to be feasible. All mentions of this KPI throughout the remainder of this

2455 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

2457 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,

2462



#### 2463

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.

#### 2467 **4.1.3** Implementation Note - Availability of Measurement Data

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

- 2471 <u>CL001.1-Baseline.zip</u>
- <u>CL001.2-BaselineUpdate.zip</u>
- <u>CL002.1-ActiveDir.zip</u>
- 2474 <u>CL003.1-Syslog.zip</u>
- CL003.2-Syslog.zip
- 2476 <u>CL004.1-HostBackups.zip</u>

CL004.2-FullImageBackup.zip \*\* 2477 • CL004.3-DirectoryBackup.zip \*\* 2478 • CL005.1-AntivirusRealTimeScan.zip 2479 • CL005.2-AntivirusFullScan.zip 2480 • CL006.1-NessusNetworkScan.zip 2481 • CL006.2-NessusAuthenticatedScan.zip 2482 • CL007.1-OpenAudITNetworkScan.zip 2483 • CL007.2-OpenAudITAuthenticatedNetworkScan.zip 2484 • 2485 • CL008.1-LeastPrivilege.zip CL009.1-BoundaryFirewall.zip 2486 • 2487 CL010.1-NetworkPhysicalConnections.zip • CL010.2-NetworkMACFiltering.zip 2488 • 2489 CL011.1-PatchesNetworkHardware.zip • CL011.2-PatchesServersICSDevices.zip 2490 • 2491 CL012.1-CiscoASA5506.zip • 2492 2493 \*\* - The network capture files provided for CL004.2 and CL004.3 (capture.pcap) have been 2494 modified to exclude all Veeam traffic recorded during the experiment, as the traffic contains 2495 sensitive testbed data in clear-text. To obtain access to these files, please contact the authors 2496 directly. 2497

#### 2498 **4.2 Open-AudIT**

#### 2499 4.2.1 Technical Solution Overview

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

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

2507

2508 Open-AudIT is a downloadable OVA which is easy to install. OVA install allows installation in

- 2509 a Hyper-Visor environment allowing for installation within an existing virtual environment
- 2510 without requiring purchasing additional hardware. Configure for initial discovery scans are
- straight forward and easy to configure and perform.

#### 2512 **4.2.2** Technical Capabilities Provided by Solution

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

- Hardware Inventory
- Software Inventory
- System Development Lifecycle Management
- Configuration Management
- Baseline Establishment (Enterprise Edition)
- Change Control
- 2521

#### 2522 **4.2.3** Subcategories Addressed by Implementing Solution

2523 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,

2524 PR.IP-6, PR.MA-1, DE.AE-1, DE.CM-7



#### 2526 4.2.4 Architecture Map of Where Solution was Implemented

8.6.3g

Virtual Machine...

1 ...

#### 2528 **4.2.5** Installation Instructions and Configurations

2529	Open-AudIT Setup Steps
2530	Prerequisites:
2531	<ul> <li>Identify if physical hardware or virtual machine will be used</li> </ul>
2532	• Requirements from Opmantek who developed "Open-AudIT" indicate the specification required
2533	are low. Please see this link for exact details provided by the vendor link.
2534	Instruction:
2535	Download:
2536	1. Download and save <b>Opmantek Virtual Appliance</b> from Opmantek website. <sup>10</sup>

# Opmantek Virtual Appliance

Experience the power of the complete Opmantek suite in one easy-toinstall Virtual Appliance. This package includes NMIS8, Open-AudIT, and all downloadable commercial modules. This package is created by Opmantek and is the easiest way to try out all our apps without the bother of setting up a dedicated server.

Virtual Appliance Release Notes Installation Guide

- 2537
- 2538 2. Once download has completed **".ova"** file will need to be extracted to view the contents and
- 2539 move to the next step (any tool supporting extracting .ova and .gz can be used).
- **3.** Open the folder where the files were extracted too. There should be a total of four files.
- 4. Next, extract the two files with extension (.vmdk.gz) since this file is still compressed. Once completed two files with the same extension (.vmdk) should now exist.
- S. Now two files just extracted need to be convert to "VHDX" format so we can run these disk in
  a Hyper-V environment. See this link for instruction and additional information useful for
  converting virtual drive format.
- 6. Once both drives have been converted to **"VHDX"** format proceed to next section.
- 2547 Virtual Machine Setup:
- 1. On the virtual server host open **"Hyper-V Manager"** and then right click on server

# 2549 name selecting New → Virtual Machine

2550 2. Now type in the name you going to give this server.

New

<sup>&</sup>lt;sup>10</sup> Opmantek Intelligent Network Management Software <u>https://opmantek.com/</u>

2551	3. Place a check in the box <b>"Store the virtual machine in a different location"</b> click next.					
	You can create a folder or use an existing folder to store the virtual machine. If you don't select a folder, the virtual machine is stored in the default folder configured for this server.					
	Store the virtual machine in a different location					
2552	Location: D:\Hyper-V\ Browse					
2553	4. The step above will place the configuration and hard drive files for the newly create Virtual					
2554	Machine in D:\Hyper-V\NewServerBuild (See Screenshot)					
2555	5. Leave <b>Generation 1</b> selected and click Next. This machine doesn't require additional features					
2556	provided from Generation 2.					
2557	6. Now assign how much memory your new machine will be given for use. For our environment we					
2558	are using <b>"2048"</b> Click next to continue.					
2559	7 Select the network this virtual machine will be using and click Next					
2560	<ul> <li>8 Now select "Attach a virtual disk later" and click</li> </ul>					
2500	Attach a virtual hard disk later					
0561	Use this option to skip this step now and attach an existing virtual hard disk later.					
2561	next.					
2562	<ol> <li>Now a screen appears displaying a configuration summary, click Finish to Description:</li> </ol>					
	Name: NewServerBuild					
	Generation: Generation 1 Memory: 2048 MB					
	Network: Not Connected					
	Hard Disk: None "V					
2563	To create the virtual machine and close the wizard, click Finish.					
2564	10. Next, anon Windows Explorer and pavigate to the location of your newly created virtual					
2565	machine and create a new folder labeled "Virtual Hard					
2303	Virtual Hard Disks 3/1/2018 2:02 PM File folder					
2566	Disk" Virtual Machines 3/1/2018 1:59 PM File folder					
2567	11. Now moves the hard drive files converted earlier to this new folder location just					
	📔 D:\Hyper-V\NewServerBuild\Virtual Hard Disks 🗸 🗸 🖒					
	Name Date modified Type Size					
2569	Opmantek/M-disk1.vhdx     3/1/2018 2:12 PM     Hard Disk Image F     7,180,288 KB     2/29/2018 11:19 AM     Hard Disk Image F     1,708,032 KB					
2508	12. Open Users V/Managers and winkt aliable in Vintual Machine instances and ealerst (Cetting V					
2569	12. Open Hyper-V Manager and right click on Virtual Machine just created and select "Setting"					
	Connect					
	Settings					
	Start					
	Checkpoint					
	Mo <u>v</u> e					
	Export					
Rena <u>me</u>						
	Enable Replication					
2570 2571	13. Memory should be configured for <b>"2048"</b>					
2371						

- 2572 14. Virtual Processor "2"
- 15. Click on **"IDE Controller 0"** then click on **"Add"** button to attach a virtual hard.
- 2574 16. Click browse button and select the first virtual drive that was moved earlier, click

2374	16. Click browse button and select the first virtual drive that was moved earlier, click
	Controller: Location:
	Media You can compact, convert, expand, merge, reconnect or shrink a virtual hard disk by editing the associated file. Specify the full path to the file.
	Virtual hard disk:
	D:\Hyper-V\NewServerBuild\Virtual Hard Disks\OpmantekVM-disk1.vhdx
2575	Apply
2575	appry. 17 New click on <b>(IDE Controllor Of casin and click "Add</b> " button to attach a virtual band
2370	17. Now click on <b>IDE Controller U</b> again and click <b>Add</b> button to attach a virtual hard.
2577	18. Click browse button and select the second virtual drive that was moved earlier, click
	IDE Controller 0 V 1 (in use) V
	Media
	by editing the esterior of the full path to the file.
	Wirtual hard disk:
	D:\Hyper-V\New5erverBuild\Virtual Hard Disks\OpmantekVM-disk2.vhdx
2578	New Edit Inspect Browse
2570	appiy.
2519	19. Now, select Network adapter and click the drop down and select <b>vswitch_restBed_tan</b> or
2580	what you have labeled your
	Memory vswitch_TestBed_LAN V
	Processor
	1 Virtual processor
	The VLAN identifier specifies the virtual LAN that this virtual machine w     Hard Drive
	OpmantekVM-disk1.vhdx
	Hard Drive     Opmantek/M-disk2.vbdx
	Bandwidth Management
	DVD Drive     Enable bandwidth management
	SCSI Controller  Specify how this network adapter utilizes network bandwidth. Both Min Bandwidth and Maximum Bandwidth are measured in Menabits per seco
2581	network dapter
2582	20. Click on Name and make sure to add some descriptive information that will allow other to easily
2583	see this information without having to login into machine
2584	21 Select Integration Service and remove check from <b>"Time Synchronization"</b> Time will be
2585	sync using internal NTP server via DNS pointer. Click "Apply" and
2000	Services
	✓ Operating system shutdown
	☐ Time synchronization ✓ Data Exchange
2586	then "OK"
2500	Configure Virtual Machine Networking:
2301	

- 2588 1. Open Hyper-V Manager and then right click on newly created machine and select start.
- 2589 2. Double click on machine being configured to open a Console window.
- 2590 3. Now type in **"root"** and then hit enter. Now type in Password provided from documentation.
- 2591 Once logged in make sure to change password from default. Additional information for default login 2592 credentials can be found <u>here</u>.

- 2593 4. Now type this command without the quotes to copy a static configuration for
- 2594 "cp ifcfg-eth0.static /etc/sysconfig/network-scripts/ifcfg-eth0" if prompted to networking. 2595 overwrite file type "Yes"
- 2596 5. Now type this command without the quotes "sudo nano /etc/sysconfig/network-scripts/ifcfg-2597 eth0"
- 2598 6. Now use the arrow keys to change the highlighted fields to your desired network

DEVICE="eth0"
NM_CONTROLLED="yes"
ONBOOT=yes
TYPE=Ethernet
BOOTPROTO=static
IPADDR=192.168.1.7
NETMASK=255.255.255.0
BROADCAST=192.168.1.255
GATEWAY=192.168.1.1
IPV4_FAILURE_FATAL=yes
IPV6INIT=yes
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_PEERDNS=yes
IPV6_PEERROUTES=yes
IPV6_FAILURE_FATAL=yes
NAME=eth0

- 2599 configuration. 2600 7. Once all fields have been updated use Ctrl + O "^O" to write the file and then Ctrl + X "^X" to
- 2601

2601	exit.					
2602	∼G Get Help ∼X Exit	°O WriteOut <mark>^J</mark> Justify	^R Read File ^₩ Where Is	<sup>^</sup> Y Prev Page <sup>^</sup> U Next Page	<sup>^</sup> K Cut Text <sup>^</sup> U UnCut Text	<sup>°C</sup> Cur Pos <sup>°T</sup> To Spell
2603						

- 2604 8. Now type "service network restart" This restarts networking services with the newly configured
- 2605 settings.

#### 2606 **Complete Additional Setup via Web Browser:**

- 2607 1. Now with any web browser navigate to "IP Configured Earlier" example would
- 2608 be "10.100.0.177"
- 2609 2. If prompted to proceed to untrusted site, select "Yes". This error is produced since SSL has not
- 2610 been configured and Open-AudIT redirects HTTP sessions over to HTTPS.

- 2611 3. Once this page opens you'll see lots of different options this tool provides. We're using "**Open-**
- 2612 AudIT Enterprise" This version allows for up to 20 nodes to be audited / monitored for

**Opmantek Documentation and Community** 

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

**Open-AudIT V2 Dashboard** 

**Open-AudIT Documentation and Community** 

#### 2613 free.

- 4. You'll now be prompted for login with username and password. This default information is
   provided above "username / password".
- 2616 5. Once logged in we need to make some required changes to allow this produce to function in our
- 2617 environment.
- 2618
   6. Click on "Admin → LDAP Server → Create LDAP Servers" This will allow integration with Active
   2619
   Directory using LDAP authentication for logging into this

5	e Licenses 👻 Admin 👻	Help 🗕 🥾 User: nr
	Enterprise	
	Community	>
	Collectors	·
	Database	Not Coop for 20
	LDAP Servers	List LDAP Servers
	Tasks	Create LDAP Servers
	Logs	

2620

application.

#### 2621 7. Required setting for LDAP server connection. Screen shot provide for 2622 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	?
Туре	Active Directory	?
Base DN	CN=Users,DC=lan,DC=lab	?

- Base DN
- 2624 a. Name - TestConnection 2625

2623

2627

2628

2629

2630

2634

2635

2636

- b. Description -- Documentation
- 2626 c. Domain – LAN.LAB
  - d. Host 10.100.0.17
  - e. Use LDAP Roles -- Yes (Additional configuration is required in AD Groups. See section
  - below in this document for additional steps.
    - f. Base DN "cn=user,dc=lan,DC=lab"
- 2631 8. Click "Submit" once all information has been entered.

#### 2632 **Active Directory Groups for LDAP Integration:**

- 2633 1. Groups listed below are required for integration to work with Open-AudIT and Active Directory.
  - a. Admin "open-audit\_roles\_admin"
  - b. org\_admin "open-audit\_roles\_org\_admin"
    - c. reporter "open-audit\_roles\_reporter"
- 2637 d. user "open-audit\_roles\_user"

- e. Default Organization "open-audit\_orgs\_default\_organisation"
- 2639 2. Create each group listed within quotes in your Active Directory. Each group should be created 2640 with Group Scope (**Global**) Group Type (**Security**)
- 3. Once each group has been created and the appropriate users add you can now login with yourActive Directory credentials.
- 2643 Discover Credentials and Discover Scans

#### 2644 1. From the home screen click on Discover button $\rightarrow$ Credentials $\rightarrow$ Create

- Discover 
  Report 
  Manage 
  Credentials
  List Credentials
  Discoveries
  Create Credentials
- 2645 Credentials. Discoveries
- 2646 2. Now enter in the requested information.
- a. Name Name of the Credentials being used. Example (SSH)
- 2648b. Organization Default Organization is selected. Pickup another if your configuring more2649the one organization.
- 2650 c. Description Description of item being added.
- 2651 d. Type Select which type of credentials will be used. (SNMP (v1 / v2), SNMP v3, SSH,

SNMP (v1 / v2)
SNMP v3
SSH
SSH Key
Windows

#### 2652SSH Key, or Windows)

- e. Credentials enter the appropriate credentials for the select type from above.
- f. Click submit to save this entry.

#### 2655 **Discovered Scan**:

2656 1. Click Discover button  $\rightarrow$  Discoveries  $\rightarrow$ Create



- 2658 2. Name The name for this scan which should be unique.
- 2659 3. Subnet The network discovery will be performed on.
- 2660 4. Click submit to save and return to main discovery screen.
- 2661 5. Main discovery screen allows you to start a scan at any time. Scans can also be configured to2662 run on a schedule interval.
- 2663 2664

2657

Useful information and links:

Discoveries.

- 26651. Default password were not changed, so remember to change all default password before this is2666put into production. (THIS IS VERY IMPORTANT)
- 2667 2. Software Vendor webpage.  $\rightarrow$  <u>https://opmantek.com</u>
- 2668 3. Community forums.  $\rightarrow$  <u>https://community.opmantek.com</u>

- 26694. Software is Open Source. Your able to use Professional Edition for up to 20 machines after that2670there is a cost which is relatively inexpensive.
- 2671 5. Comparison

below.

2672

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

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

2678

6. Ability to perform baseline scan on devices is provided by Enterprise edition. This could be very

useful for determining changes over time.

#### 2679 **Open-AudIT Configuration steps within CRS once system has been installed**

- 2680 Initial Configuration:
- Login via web portal
- Navigate to  $\rightarrow$  Discovery  $\rightarrow$  Credentials  $\rightarrow$  Create Credentials

Discover -	Report <del>-</del>	Manage <del>-</del>
Credentials	;	List Credentials
Discoveries		Create Credentials

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

ID		?
Name	CRS Scans	?
Organisation	Default Organisation	?
Description	Perform Linux Scans	?
Туре	SSH •	?
Username	icsuser01	
Password	•••••	٩
Password Edited By	nmis	(j) ?
Password Edited By Edited Date	•••••• nmis 2018-09-26 13:56:53	ⓐ ? ?

2691

2683

### 2692 **Organization Groups Creation:**

2693 • Click on Manage → Orgs → Create Orgs Manage -

Applications	-	
Attributes	-	
Baselines	>	
Connections		
Dashboards	-	
Devices		
Fields		
Groups		
Licenses		
Locations		
Maps		
Networks		
Queries		
Orgs	- 1	List Orgs
Roles	$\rightarrow$	Create Orgs
Summaries	×.	Import Orgs from CSV
Users		
Widgets	-	

2695	٠	Now enter Name: Description: and click submit at the bottom of the page to save.
		Name         CRS Machines         ?
		Description Robotics Machines within Work Cell ?
		Parent ID     Default Organisation
2696		Type Organisation · ?
2697	•	If you have multiple machines / equipment in different locations you can make
2698		Organizational groups based on business units, or related task.
2699	Config	gure Discovery Scan:
2700	•	Now click on Discover $\rightarrow$ Discoveries $\rightarrow$ Create Discoveries
		Discover - Report - Manage -
		Credentials
		Discoveries List Discoveries
2701		Files Create Discoveries
2701 2702	•	Enter a meaningful name for discover being created
0700		Name CRS Scans ?
2703	•	Next, enter the subnet that'll be used for performing this scan. This scan is using
2705		192 168 0 0/23 <sup>subnet</sup> <sup>192.168.0.0/23</sup> ? Search online for additional
2706		subnetting information / calculators if you'd like to learn more.
2707	•	<b>Network address:</b> should already be defaulted to Open-AudIT installed location, if this
2708		is not true, click the drop-down arrow and select your installed location.
2709	•	Now, click on the advanced button to see more options.
2710	•	Once <b>Advanced</b> has been expaned you'll have additional options to select if desired.
2711		These options are Org, Type, Devices Assigned to Org, and Devices Assigned to
2712		Location. These options aren't required, but allow you to place found devices into
2713		different Organzations groups.
2714	•	Once all selection have been made click on <b>Submit</b> button to continue.
2715	Disco	veries:
2716	•	Once the steps above have been completed clicking on <b>Submit</b> button you'll be taken to
2717		a new webpage that'll allow you to run discovery process created in the previous step.
2718	•	To start discovering devices click on green arrow button. If you need to verify details for
2719		this scan click on the button that looks like an eye: finally, if you need to delete this scan
2720		click on the <b>trash</b> can icon to the right. See screen shot for details.
0701		Collaborative Robotics Collaborative Robotics System subnet Subnet - 2018-09-19 ✔ (512 of 512)
2721		

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

#### 2726 Lesson Learned:

2727 Ensure default passwords are changed

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

2730 When configuring SNMP make sure to use SNMP V3 if possible.

#### 2731 **4.2.6** Highlighted Performance Impacts

- Two performance measurement experiments were performed for the Open-AudIT tool while the manufacturing system was operational:
- 1. <u>CL007.1</u> A discovery scan was performed.
- 2735 2. <u>CL007.2</u> A discovery scan with credentials was performed.

#### 2736 **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).

- 2748 No components of the CRS showed any measurable performance impact from the discovery
- scans beyond the anticipated increase in network traffic.

#### CSF MFG PROFILE LOW SEC LVL EXAMPLE IG DISCRETE-BASED MFG SYSTEM USE CASE

OpenAudIT Traffic on the CRS Network (CL007.1) 150 100 kilobits per second 50 0 0 1000 2000 200 400 600 800 1200 1400 1600 1800 experiment time (seconds)

2750

2755

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.







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.

#### 2758 **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).

2764 Credentials were provided to Open-AudIT, which gave the tool access to the following CRS

2765 hosts: the engineering workstation (POLARIS), the robot driver (MINTAKA), the robot

2766 controllers (vController1, vController2), and the machining stations. The Open-AudIT logs

2767 reported scanning was active for each IP address range for 5 minutes 17 seconds, 6 minutes 18
2768 seconds, and 7 minutes 24 seconds, respectively. Notes taken by the researchers while the

2769 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).





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

2779 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

2781 baseline value of approximately 2% to 8%. The cause of this increase is unknown at the time of

2782 publishing. CPU utilization for vController2 increased to an approximate average of 32% with a

2783 peak of 58% during the scan period (see Figure 4-8).

#### CSF MFG PROFILE LOW SEC LVL EXAMPLE IG DISCRETE-BASED MFG SYSTEM USE CASE



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



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

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



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

#### 2796 **4.2.7** Link to Entire Performance Measurement Data Set

- 2797 CL007.1-OpenAudITNetworkScan.zip
- 2798 <u>CL007.2-OpenAudITAuthenticatedNetworkScan.zip</u>

#### 2799 **4.3 CSET**

2793

### 2800 **4.3.1 Technical Solution Overview**

2801 Cyber Security Evaluation Tool (CSET) is a tool provide by Department of Homeland Security 2802 for performing Cybersecurity evaluation against an organization. This evaluation is completely 2803 manual process of answering multiple questions to determine organizational security posture in 2804 regard to implemented current cybersecurity practices against current security status. This 2805 evaluation will help identify area within the organization that required more attention and 2806 resources.

- 2807 **4.3.2** Technical Capabilities Provided by Solution
- 2808 CSET provides components of the following Technical Capabilities described in Section 6 of2809 Volume 1:
- Network Architecture Documentation
- Risk Assessment

### 2812 **4.3.3** Subcategories Addressed by Implementing Solution

2813 ID.RA-1

#### 2814 **4.3.4** Architecture Map of Where Solution was Implemented



#### 2816 **4.3.5** Installation Instructions and Configurations

2817 CSET Installation and Configuration

#### 2818 **Download and Installation Instructions: Provided by DHS**

2819

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

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

- Decompressing the File Open the file using any one of the newer compression utility software programs.
- 2828
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   2829
   <li
- Burning the file to CD this method uses CD-burn software and the ISO file to burn the
   files onto your own CD to create a physical disk identical to the CSET original.
- 2832 These methods require separate software utilities. There are a variety of both free and purchased

2833 utility programs available through the Internet that will work with the ISO file format. As DHS

2834 does not recommend any specific application or vendor, it will be necessary for you to find a

2835 product that provides the necessary functionality. Step by step instructions for each method are

2836 provided below:

#### 2837 **Decompressing the File**

- CLICK the "Download CSET" link at the bottom of this page and complete the requested information to download the ISO file.
- 2840
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841
  2841</l
- 2842
  3. OPEN the ISO file with a compression utility program and SAVE the files to your hard drive of choice maintaining the original names and file extensions.
- 2844 4. COMPLETE the *Installing the CSET Program* instructions below.

#### 2845 Mounting the File

- 28461. CLICK the "Download CSET" link at the bottom of this page and complete the requested2847information to download the ISO file.
- 2848
  2848
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849
  2849</l
- RUN your ISO-specific utility program that is capable of mounting the file. COMPLETE
   the instructions within the utility software to create a virtual drive using the ISO file. If

- 2852 you do not have an ISO utility application, you will need to find and install one before 2853 continuing with these instructions.
- 2854 4. COMPLETE the *Installing the CSET Program* instructions below.

#### 2855 **Burning the file to CD**

- CLICK the "Download CSET" link at the bottom of this page and complete the requested information to download the ISO file.
- 285828. SAVE the file to the hard drive on your computer maintaining the filename and extension (.iso).
- 2860 3. INSERT a blank, writable CD into the computer's CD drive.
- 4. RUN your CD-burn utility program. COMPLETE the instructions on your utility
  program to burn the ISO image to your DVD. (If you do not have an application that can do this, then you will need to find and install one before continuing with these instructions.)
- 2865 5. COMPLETE the *Installing CSET Program* instructions below.

#### 2866 Installing the CSET Program

- FIND the CSET\_Setup.exe file in the folder, virtual drive, or CD containing the CSET
   files.
- 2869
   2. DOUBLE-CLICK the CSET\_Setup.exe file to execute. This will initiate the installer program.
- 2871 3. COMPLETE the instructions in the installation wizard to install the CSET program.
- 2872 4. READ the material within the ReadMe document for a summary explanation of how to
- use the tool. Help is also available through the User Guide, screen guidance text,and video tutorials.

#### 2875 Video Tutorials

- 2876 A number of video tutorials are available to help you better understand how to use this tool. They
- are designed to play within YouTube, therefore, you must have an active internet connection to
- 2878 view them. You can access these videos by navigating to the CSET YouTube channel
- 2879 (<u>https://www.youtube.com/c/CSETCyberSecurityEvaluationTool</u>).
- 2880 To view close captioning in YouTube, click on the "cc" icon on the video window.

#### 2881 System Requirements

- 2882 In order to execute CSET, the following minimum system hardware and software is required:
- Pentium dual core 2.2 GHz processor (Intel x86 compatible)
- CD-ROM drive if creating a physical CD
- 5 GB free disk space
- 2886 3 GB of RAM

- Microsoft Windows 7\* or higher
- A Microsoft Office compatible (.docx) document reader is required to view reports in .docx format
- A Portable Document Format (PDF) reader such as Adobe Reader is required to view supporting documentation. The latest free version of Adobe Reader may be downloaded from <u>http://get.adobe.com/reader/</u>
- Microsoft .NET Framework 4.6 Runtime (included in CSET installation)
- SQL Server 2012 Express LocalDB (included in CSET installation)
- 2895 NOTE: For all platforms, we recommend that you upgrade to the latest Windows Service Pack
  2896 and install critical updates available from the Windows Update website to ensure the best
  2897 compatibility and security.
- 2898 **CSET Hash Values**
- 2899 SHA-256:
- 2900 B7061B169E3461A298E58B99FADC9978D9F6CE22A0747669A538BDAF39C214ED
- 2901 MD5: 53f2f71eb6e3bb54471e75318eaa64ee
- 2902 SHA-1: f2b020e3a73db9b72ff85bd9b5e158449f6c003a
- 2903 To download CSET, select the following link:
- 2904 **Download CSET**
- If you are unable to download or install CSET from the link, you may request a copy be shipped.
  To request a copy, please send an email to: <u>cset@hq.dhs.gov</u>. Please insert "CSET" in the subject
- 2907 line and include the following in your email request:
- Your name
- Organization name
- Complete street address (no P.O. boxes)
- Telephone number
- The error or installation issue you encountered when attempting the download
- 2913
- 2914 **Running CSET for First time:**
- 2915
  1. Once install of CSET has been completed find the application just installed and double click to run. CICK to run.
- 2917 2. Once program has launched you will see the home screen.
- 2918 3. Click on File and select "New Assetment" New Assessment Ctrl+N

any highlight

2919 4. Now, click on Start Here button in the lower right corner of program. Start Here  $\gg$ 

#### 2920 5. Next, enter all required information.

	Assessment Name		Assessment Date			
	Collaborative Robotics		<mark>4/23/2019</mark>	芀		
	Facility Name					
	Alpha Manufacturing	Alpha Manufacturing				
	City or Site Name			_		
	Gaithersburg					
	State, Province, or Region					
	Maryland					
	Assessor Name	Assessor Email	Assessor Telephone			
	John Doe					
6. 7	Click continue to pro	oceed.	propriate choice	es Change		
/.	options required	own menu and select the up	propriate enoice	.s. Change		
	Sector					
	Sector					
	Critical Manufacturing Sector	¥				
	Industry					
	Machinery Manufacturing	•				
	What is the gross value	of the assets you are trying to p	rotect?			
	<mark>&lt; \$1,000,000</mark>	•				

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.

Wy organization uses industrial control systems (ICS).

- 2926 8. Click continue to proceed.
  - 9. If you want to create a network diagram click the button, otherwise click "Continue".
    - 10. Change Mode Selection to "Advanced" and "Cybersecurity Frame-based Approach"

O 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	sel	ecting which cybersecurity standards your assessment is based on, please choose one of the following options.
	0	Questions-based Approach The questions-based approach uses simple questions and allows for partial credit.
	0	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.
	0	Cybersecurity Framework-based Approach
		The cybersecurity framework-based approach uses allows you to define a custom profile based on the Cybersecurity Framework.

2929

2925

2927

2928

2921 2922

2923

- 2930 11. Click continue.
- 2931 12. Click continue to use default profile or create a new profile.
- 2932 13. Click continue again.
- 2933 14. Now answer the questions as they appear.
- 2934 15. Complete all questions and generate a final report.

- 2935 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.

# 29402941 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).

#### 2944 **4.3.7** Link to Entire Performance Measurement Data Set

2945 N/A

#### 2947 **4.4 GRASSMARLIN**

#### 2948 **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
- 2955 Points to consider:<sup>11</sup>
- Passive IP network mapping tool
- Hardware agnostic portable Java based tool
- Can only see and map hosts where you are capturing data from.
- 2959 **4.4.2** Technical Capabilities Provided by Solution
- GRASSMARLIN provides components of the following Technical Capabilities described inSection 6 of Volume 1:
- Network Architecture Documentation
- Baseline Establishment
- Map Data Flows
- 2965

#### 2966 **4.4.3** Subcategories Addressed by Implementing Solution

2967 ID.AM-3, ID.AM-4, PR.AC-5, PR.IP-1, PR.IP-3, PR.MA-1, DE.AE-1, DE.CM-7

<sup>&</sup>lt;sup>11</sup> GRASSMARLIN Briefing Powerpoint 2017: <u>https://github.com/nsacyber/GRASSMARLIN /blob/master/GRASSMARLIN</u> <u>Briefing\_20170210.pptx</u>





#### 2970 **4.4.5** Installation Instructions and Configurations

2971 Details of the solution implemented:

Name	Version
GRASSMARLIN	3.2.1

2973	Setup
------	-------

- GRASSMARLIN is supported on the following platforms<sup>12</sup>
- 2975 Microsoft Windows (64bit, 7 8 and 10)
- 2976 Fedora Linux
- 2977 Ubuntu (14.04 ,15.10)
- 2978 Kali Linux 2.0
- 2979CentOS (6,7)2980Debian (8)
- 2980 2981
- 2982 Download GRASSMARLIN from <u>https://github.com/nsacyber/GRASSMARLIN/releases</u> as 2983 per the OS version of your system. Upon download, run the installer. The installer will install 2984 additional programs such as Java and Wireshark during the setup.
- GRASSMARLIN can operate in a real time passive mode by sniffing the live traffic or by
   importing a recorded pcap file. Data in GRASSMARLIN is stored in a Session. The Session
   contains imported files and visual state information.
- GRASSMARLIN was installed on the Cybersecurity Scanning Laptop running Windows 10.
- 2989 Using the Software:
- A captured pcap file from the CRS system was imported in GRASSMARLIN to generate a network baseline. The pcap was captured by the running the tcpdump command on a Linux system which had a network connection from a Network aggregator device. This
   Aggregator was configured with mirror port connections in coming from the different network segments such as Supervisory LAN and Control LAN.
- 2996 tcpdump -i <mirror-port interface> -w mypcap.pcap 2997
- 2998 **For example**: tcpdump -i eth1 -w /home/icssec/robotics.pcap
- 2999 Where eth1 is our mirror port connection
- 3000

<sup>&</sup>lt;sup>12</sup> GRASSMARLIN User Guide: <u>https://github.com/nsacyber/GRASSMARLIN</u>

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



#### 3008 • Click on Add Files. Browse to the PCAP

😽 GrassMar	lin 3.2.1 [New Session]						-	
File Vie	w Packet Capture Tools Help							
		Import Pending Impo	orts			3		Start 🛛 Stop
			File Name	Size Type	Timesta	,		
					16:37:37.284	Unable to load user Fingerprints		
					16:37:37.177	Unable to load manufacturer database		
					16:37:37.263	Unable to initialize JNetPCap; packet c		
					16:37:37.179	Unable to create application directorie		
					16:37:36.613	This session cannot be logged to disk:		
					16:37:37.093	Loading Geold -> Name Mapping fron		
			No content in table		16:37:36.627	Loading Cidr -> Geold Mapping from:		
			No content in table		16:37:37.95	Loaded plugin 'ladgov.svgexport'		
					16:37:37.949	Loaded plugin 'iadgov.offlinepcap'		
					16:37:37.094	Geold -> Name Mapping load comple		
					16:37:37.088	Cidr -> Geold Mapping load complete		
					16:37:37.263	Cannot locate Wireshark: please verify		
Timesta▼		Add Files	Load Quicklist Save Quicklist	Import Selected	<(	,		
16:37:37.284	Unable to load user Fingerprints	Running and	Completed Imports					
16:37:37.177	Unable to load manufacturer database from Wireshar	Prograce	File	Cino				
16:37:37.263	Unable to initialize JNetPCap; packet capture function	riogress	rite	3126				
16:37:37.179	Unable to create application directories: C\\Program P							
16:37:36.613	This session cannot be logged to disk: C:\Program File							
16:37:37.093	Loading Geold -> Name Mapping from: C:\Program F			No content in table				
16:37:36.627	Loading Gidr -> Geold Mapping from: C:\Program File							
	8 MB / 45 MB							
	e 📄 🥵 🦛 💻	M 🐠					へ 幅 (1)) 腎	4:42 PM 4/19/2019

- The Pcap will now show up under Pending Imports. Select the file and click on "Import 3011
   Selected". Hit the Close button at the bottom of the page. The Import process can take
- 3012 several minutes to **hours** depending on the size of the pcap file.

Import

File Name	Size	Туре	Timesta▼	
E:\capture.pcap	299.5 MB	Pcap	16:37:37.284	Unable to load user Fingerprints
			16:37:37.177	Unable to load manufacturer database
			16:37:37.263	Unable to initialize JNetPCap; packet o
			16:37:37.179	Unable to create application directorie
			16:37:36.613	This session cannot be logged to disk:
			16:37:37.093	Loading Geold -> Name Mapping from
			16:37:36.627	Loading Cidr -> Geold Mapping from:
			16:37:37.95	Loaded plugin 'iadgov.svgexport'
			16:37:37.949	Loaded plugin 'iadgov.offlinepcap'
			16:37:37.094	Geold -> Name Mapping load comple
			16:37:37.088	Cidr -> Geold Mapping load complete
			16:37:37.263	Cannot locate Wireshark; please verify

3013

Once complete, the screen will display a Logical Graph of the network topology. ٠

3014 3015



3019Take a moment to review the logical graph. Any public IP address will be highlighted with3020their respective Country's flag. This can be useful in finding out information about any3021external IP's that your network is communicating with.

- 3022 3023
- Right-click on any external node IP address in question >> View Details for <IP address>
- 3024



3025 3026

- To Generate a list of all nodes in the Logical Graph, click on View (Top Menu) >> Logical
   Nodes Report. By default, only a single column (IP) is present, although additional columns
   can be added with any Property present in the set of Nodes.
- 3031 To add a column, select the Property Name from the drop-down and click the Add button.
| Logical Node R   | leports            |                         |   |     |        | $\times$ |
|--|--------------------|-------------------------|---|-----|--------|----------|
| <ul> <li>All</li> <li>Source</li> <li>Destination</li> <li>Source and D</li> </ul> | Destination        | ICSProtocol             | • | Add | Export | CSV      |
| IP   | MODBUS.ICSProtocol | MODBUS.Role             |   |     |        |          |
| 192.168.1.101  | MODBUS (4)         | SLAVE (4)               |   |     |        |          |
| 192.168.0.30   | MODBUS (4)         | MASTER (4)<br>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  |                    |                         |   |     |        |          |

- Click on View >> Logical Connections Report to view a summary of all connections captured by the pcap file.
- 3036



- 3037 3038
- 3038
- To view all the logical communications for a specific host for capturing a baseline, Rightclick on a Node >> View Frames. This opens a new screen as shown below displaying all the different IP addresses including ports and protocol information that the selected node is communicating with. You may click further on "Export CSV" button to export this data to a csv file.
- 3044

Action	Media Clipboard Vi D 🕑 🔢 🕪 📷 ssMarlin 3.2.1 [New	ew Help う ふ / み Connections	involving	🖪 Termir	al - icssec@sec	.u					
		Connections involving 192.168.0.20 + 🗆 🗙									
ile Vie	w Packet Capt	Export CSV									
4		Timestam	p	Source IP	Source Port	Destination IP	Destination P	PCAP File			
₩ 10.10	0.0.0/24 (2 item[s	2018-04-04T17:46:36.836Z		192.168.1.4	22	192.168.0.20	51024	robotics.pc			
192.1	68.0.0/24 (6 item[	2018-04-04T17:46:36.836Z 2018-04-04T17:46:36.836Z		192.168.1.4	22	192.168.0.20	51024	robotics.pc			
▶ 192.168	8.0.2			192.168.1.4	22	192.168.0.20	51024	robotics.pc			
▶ 192.168	8.0.11	2018-04-04T17:46:36.836Z		192.168.1.4	22	192.168.0.20	51024	robotics.pc;			
2018-04-04T17:46			36.836Z	192.168.1.4	52807	192.168.0.20	59598	robotics.pc			
▶ 192.1	Select All Instance	es of 192.168.0.20	6.836Z	192.168.1.4	52807	192.168.0.20	59598	robotics.pc			
192.1	View Details for	192.168.0.20	7.603Z	192.168.1.4	22	192.168.0.20	51024	robotics.pc			
192.1	Center in View		7.603Z	192.168.1.4	22	192.168.0.20	51024	robotics.pc			
₩ 192	View Frames		7.604Z	192.168.1.4	52807	192.168.0.20	59598	robotics.pc			
	Expand All Crour		7.604Z	192.168.1.4	52807	192.168.0.20	59598	robotics.pc			
	Colleges All C		7.604Z	192.168.1.4	22	192.168.0.20	51024	robotics.pc			
_	Collapse All Grou	ips	7.604Z	192.168.1.4	22	192.168.0.20	51024	robotics.pc			
		2018-04-04T17:46	37.604Z	192.168.1.4	22	192.168.0.20	51024	robotics.pc			
		2018-04-04T17:46	37.604Z	192.168.1.4	22	192.168.0.20	51024	robotics.pci~			

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

3047 3048

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

### CSF MFG PROFILE LOW SEC LVL EXAMPLE IG DISCRETE-BASED MFG SYSTEM USE CASE





# **4.4.6 Highlighted Performance Impacts**

- 3062 No performance measurement experiments were performed for the use of GRASSMARLIN due 3063 to its installation location and how it was used (i.e., the software performed offline analysis of
- 3064 PCAP files captured by other software).

### 3065 **4.4.7** Link to Entire Performance Measurement Data Set

- 3066 N/A
- 3067

### 3068 4.5 Wireshark

### 3069 4.5.1 Technical Solution Overview

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

### 3074 **4.5.2** Technical Capabilities Provided by Solution

- 3075 Wireshark provides components of the following Technical Capabilities described in Section 6 3076 of Volume 1:
- Network Architecture Documentation
- Baseline Establishment
- Map Data Flows
- **3080** Forensics

### 3081 **4.5.3** Subcategories Addressed by Implementing Solution

- 3082 ID.AM-3, ID.AM-4, PR.AC-5, PR.IP-1, PR.IP-3, PR.MA-1, DE.AE-1, DE.AE-2,
- 3083 DE.CM-7, RS.AN-3

### 3085 **4.5.4** Architecture Map of Where Solution was Implemented



# 3087 **4.5.5** Installation Instructions and Configurations

3088		Steps for installing Wireshark
3089		Download and Installation instructions:
3090		
3091	1.	Only download Wireshark from <u>https://www.wireshark.org</u> (Select 32bit or 64 bit)
3092	2.	Once download has completed locate the executable just downloaded and double click to
3093		start install process. C:\Users\johndoe\Downloads\Wireshark-win64-3.0.1.exe
3094	3.	If prompted for password enter administrator account on local machine.
3095	4.	When first Screen appears click "NEXT"
		🖌 Wireshark 3.0.1 64-bit Setup - 🗆 🗙
		Welcome to Wireshark 3.0.1 64-bit Setup

	Welcome to Wireshark 3.0.1 64-bit Setup
	This wizard will guide you through the installation of Wireshark.
	Before starting the installation, make sure Wireshark is not running.
	Click 'Next' to continue.
R	

- 3096
- 3097 5. Click "**Agree**" to continue.
- 30986. Leave default selected and click "Next" five times to continue install. (Make changes ifall features aren't required. This will be uncommon)

<u>N</u>ext >

Cancel

- 3100 7. When prompted for Npcap install click **"I Agree"** to continue.
- 3101 8. Leave default and click "Install".
- 5101 8. Leave default and click "Install".
- 3102 9. Now click "Next and Finish" to start process.
- 3103 10. Click next and then select "Reboot Now" or "I want to manually reboot later"
- 3104 11. Click "Finish" to complete.
- 3105

### 3106 Running Wireshark and configure

- 3107 1. Click start button and find program labeled "Wireshark".
- 3108 2. Once Wireshark is found right click on icon and select More→Run as Administrator
- 3109 (Windows 10) Older operating system can just hold down "Shift + Right Click" menu
  3110 will appear for run as, select administrator to continue.
- 31113. Wireshark requires administrative privileges to be fully functional, otherwise there willbe undesired results.

3113 4. Once Wireshark is running the initial interface will appear that the screen shot provided.

	) 🖡 🔠 🗶 🖸 🔍 🖷 🖷 🔮 🛫 🛄 📕 🍳 Q, Q, X	
Apply a displa	ay filter <ctrl-></ctrl->	Expre
	Welcome to Wireshark	
	Capture	
	using this filter:	✓ All interfaces shown ▼
	Noran Loophark Adanter	
	Ethernet 3	
	Local Area Connection* 10	
	Ethernet A	
	Local Area Connection* 7	
	Local Area Connection* 6	
	Local Area Connection* 8	
	LURITIES 4	
	Learn	
	User's Guide Wiki Questions and Answers Mailing Lists	
	You are running Wireshark 3.0.1 (v3.0.1-0-gea351cd8). You receive automatic updates.	

3115 5. Select the interface to be monitored.

3114

3116 Wireshark provide lots of information and can be hard to decipher https://www.wireshark.org

3117 provides documentation along with searches for additional command syntax.

### 3118 **Capturing Network Baseline using Wireshark**

- Launch Wireshark. Click **Open** to load a previously captured pcap file or run a "**Start Capture**" as explained in the previous section to record traffic.
- 3121 2. Upon loading the pcap or capturing live traffic; click on **Statistics** >> **Conversations**
- 3. This will generate a window similar to the one below which will list all the different types of communications happening between all endpoints in your traffic. Click **COPY**
- 3124 >> **as Csv** to save this data as a Csv file for further analysis.

### CSF MFG PROFILE LOW SEC LVL EXAMPLE IG DISCRETE-BASED MFG SYSTEM USE CASE

Ethernet · 95	IPv4 · 75	IPv6 • 22	ТСР	• 853 UDP • 6	70								
ddress A	Address B	Packets	Bytes	$Packets\;A\toB$	Bytes A → B	$Packets \: B \to A$	Bytes $B \rightarrow A$	Rel Start	Duration	$Bits/s \: A \to B$	Bits/s B $\rightarrow$ /	4	^
.100.0.16	224.0.0.251	2	174	2	174	0		0109.13388	3600.1009	0		0	
.100.0.17	172.16.1.4	342	33 k	171	17 k	171	16	9235.241245	5111.8544	27		25	
100.0.17	172.16.3.10	349	81 k	163	34 k	186	47	341.621642	4829.8745	57		77	
100.0.17	172.16.2.4	1,097	305 k	484	123 k	613	181	9360.223089	4796.3020	206		303	
100.0.17	10.100.0.255	74	9571	74	9571	0	(	9391.429714	4801.4406	15		0	
100.0.17	224.0.0.252	4	264	4	264	0	(	9475.946375	3600.5112	0		0	
100.0.17	172.16.2.14	1,106	332 k	511	123 k	595	209	9529.909699	4587.6312	214		366	
100.0.17	172.16.2.5	2,534	298 k	1,260	170 k	1,274	128	9656.383446	4381.4873	311		234	
100.0.17	172.16.2.3	688	203 k	295	78 k	393	125	9773.279386	4514.4789	139		221	
100.0.17	172.16.1.5	228	45 k	102	18 k	126	27	0868.02465	1285.4367	114		170	
100.0.18	10.100.0.255	13	2456	13	2456	0	(	9272.279839	4581.1734	4		0	
100.0.18	224.0.0.252	4	264	4	264	0	(	9272.280802	3600.5087	0		0	
100.0.19	224.0.0.251	1	87	1	87	0	(	1365.30458	0.0000	_		_	
100.0.27	10.100.0.255	114	10 k	114	10 k	0	(	9271.772421	5102.5099	16		0	
.100.0.27	224.0.0.252	2	132	2	132	0	(	0 1061.46345	0.4104	2572		0	
.100.0.28	224.0.0.251	1	87	1	87	0	(	1828.86474	0.0000	_		_	
.100.0.33	224.0.0.251	1	81	1	81	0	(	) 1229.03123	0.0000	_		_	
.100.0.101	224.0.0.252	47	3248	47	3248	0	(	2215.07204	1624.9433	15		0	
.100.0.101	239.255.255.250	77	16 k	77	16 k	0	(	2215.69742	2163.4997	61		0	
.100.0.101	224.0.0.251	6	492	6	492	0	(	2219.20341	3.0087	1308		0	
100.0.101	10.100.0.255	116	13 k	116	13 k	0	(	2223.70201	1964.5661	55		0	
100.0.234	239.255.255.250	311	62 k	311	62 k	0	(	9213.476484	5163.1292	96		0	
100.0.234	224.0.0.252	6	394	6	394	0	(	0471.43449	3172.9687	0		0	
100.0.234	10.100.0.255	6	552	6	552	0	(	0591.45248	3054.4517	1		0	
.100.1.4	172.16.2.14	9,390	638 k	6,252	406 k	3,138	232	9213.771229	5185.1215	626		357	
.205.214.21	172.16.3.10	39	2522	0	0	39	2522	2536.51692	1523.2062	0		13	~
Name resolut	ion 🗌 I	Limit to displa	ay filter	Absol	ute start time						[	Conversation Type	is 🔻
						Copy	/ <b>T</b>	llow Stream	Gra	iph	Close	Help	
2 16 2 10	2				172 16 3 10	26	CSV				555 [TC	P Retransmis	ie
2.16.2.5	2				172.16.14	,	VALA				60 652	27 → 50005 F4	ACK
16 2 5					172 16 1 4	as	TAIVIL				60 ETC		10

3125

3126 3127 3128

3129

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

opic / Item	~	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start			^
~	UDP	244				0.0000	100.00%	0.0100	577.838			1
	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			
>	ТСР	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			1
aplay filter: E	Enter a display fi	lter									Apply	

3131

### 3132 **4.5.6** Highlighted Performance Impacts

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

that is attached to the network only during maintenance and engineering activities).

# **4.5.7** Link to Entire Performance Measurement Data Set

- 3138 N/A
- 3139

### 3140 **4.6 Veeam Backup and Replication**

### 3141 **4.6.1 Technical Solution Overview**

- 3142 Veeam Backup and Replication is a proprietary backup and incident recovery software
- developed by Veeam for virtual environments. It is built on VMware vSphere and Microsoft
- 3144 Hyper-V hypervisors. The software provides backup, restore and replication functionality for
- 3145 virtual machines. Veeam® Backup and Replication suite delivers availability for all workloads -
- 3146 virtual, physical, cloud (including VMware vSphere and Microsoft Hyper-V) -from a single
- 3147 management console. It provides fast, flexible and reliable recovery of your applications and 3148 data, and brings backup and replication together into a single software solution [1].
- 5146 uata, and orings backup and replication together into a single software solution [1].
- 3149 The Veeam Backup Free Edition lets you back up your VMs on the fly and provides you with
- 3150 flexible storage options, including file-based (NFS) primary storage, for easy archiving and
- 3151 quick recovery. Veeam also has products such as "Veeam agent for Windows" and "Veeam
- agent for Linux" for backing up physical Windows and Linux servers respectively.
- 3153 Points to consider:
- Free backup edition available for virtual and physical servers.
- Support for file level backups as well as system image type of backups.
  - Backups can be run without having to shut down the system. This can be very critical in ICS/SCADA environments.
  - Tech support available for Free edition users.
- Easy to setup and use. Lot of documentation available online to get started.
- 3160

3156

3157

3158

# 3161 **4.6.2** Technical Capabilities Provided by Solution

- Veeam Backup and Replication provides components of the following Technical Capabilitiesdescribed in Section 6 of Volume 1:
- Data Backup
- 3165 Data Replication

# 3166 **4.6.3** Subcategories Addressed by Implementing Solution

3167 PR.IP-4

### 3168 **4.6.4** Architecture Map of Where Solution was Implemented



#### 3170 4.6.5 Installation Instructions and Configurations

- Setup 3171
- 3172 The following products from Veeam were implemented •
- 3173

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

3174

3175 A Windows 2012 R2 Virtual Machine was setup in the Cybersecurity LAN for installing • 3176 Veeam Backup and Replication Server. Around 4TB of storage was allocated to this VM for 3177 backup storage.

3178 The Free Edition of Veeam Backup and Replication lets you manage virtual machine • 3179 backups from the Central Veeam BandR Console. However, any physical servers configured 3180 for backup using the Veeam agent cannot be managed from the Central console in the Free 3181 edition. These need to be managed locally on the endpoint or client system itself.

A NFS share folder was setup on the same 4TB drive for saving backups. This NFS directory 3182 • 3183 would then be mounted on the Linux clients of the Robotics system. NFS Shares can be hosted on Windows 2012 by installing the Role/Feature "Server for NFS" under "File and 3184 **iSCSI Services**" as shown below 3185

Select server ro	oles	DESTINATION SERVE stwinnfs0
Before You Begin Installation Type	Select one or more roles to install on the selected server.	Description
Server Selection Server Roles Features Confirmation Reputs	DNS Server Fax Server File And Storage Services (Installed) File and iSCSI Services File Server BranchCache for Network Files Data Deduplication DFS Namespaces DFS Replication File Server Resource Manager File Server VSS Agent Service iSCSI Target Server iSCSI Target Storage Provider (VDS and VSS) Server for NISS	Server for NFS enables this computer to share files with UNIX- based computers and other computers that use the network file system (NFS) protocol.
	< Previous Ne	ext > Install Cancel
Add features that You cannot install Serv or features are also ins	are required for Server for NFS? er for NFS unless the following role services talled. Services	
<ul> <li>▲ File And Storage S</li> <li>▲ File and iSCSI S</li> <li>File Server</li> <li>▲ Remote Server Act</li> <li>▲ Role Administr</li> <li>▲ File Service</li> </ul>	Services Iministration Tools ration Tools	
<ul> <li>File And Storage S</li> <li>File and iSCSI</li> <li>File Server</li> <li>Remote Server Ac</li> <li>Role Administr</li> <li>File Service</li> <li>[Tools]</li> </ul>	Services Iministration Tools ration Tools is Tools Services for Network File System Management	

- Next, a directory named **linux-backups** was created. The below two images shows the NFS
- share permissions configured on this directory. The IP address 10.100.0.20 is the NAT IP
  address of the traffic coming out of Robotics Systems. Ensure to not select "Allow Root"
- 3194 access" for security reasons.
- 3195 Right-click on the Directory >> Select NFS-Sharing tab >> Manage NFS Sharing
- 3196



NFS Share Path: Name:	F:Ninux-backups		
10.100.0.11	Read-Write	ANSI	Root Access Disallowed
ALL MACHINES	Read-Write Read-Only	ANSI ANSI	Root Access Disallowed Root Access Disallowed
Type of access:	Read-Write	• □	Add Remove
Encoding:	ANSI	•	
			OK Cancel

# 3202 Configuring Backups

- All Linux systems in Collaborative Robotics system were configured for Backup using
   Veeam Agent for Linux [2].
- The Offline Mode of Agent installation was followed using the below instructions as the
   Linux systems did not have internet connectivity
- 3207 <u>https://helpcenter.veeam.com/docs/agentforlinux/userguide/installation\_offline.html?ver=30</u>
- Network connectivity between the Linux clients and the Veeam server was verified using
   telnet for NFS ports. If using NFS to connect to Veeam server, ensure to test if the NFS
   mount folders can be accessed and written to from the Linux client.
- A backup or restore operation needs to be initiated from the client system. Once the agent is
   installed, run a sudo veeam command to launch the Veeam Control Panel utility. The initial
   screen will look as shown below. Accept the End User Agreement and click on Continue.
- Under **Recovery ISO** You can either select "**Patch Veeam Recovery media ISO**" and
- 3215 "Download and patch ISO" if the Linux system has internet connectivity else both of these
  3216 options can be unchecked and proceed. The Veeam Recovery Media for Linux can also be
  3217 downloaded manually from the Veeam website.
  - Veeam Agent for Linux [ graylog ] Custom Recovery Media Agreements Recovery ISO Add drivers from this machine into Veeam Recovery ISO, > It might be required for a successful bare-metal restore: License Patch Veeam Recovery Media ISO [ ] EFI system (X) Download and patch ISO ( ) Patch local ISO from https://repository.veeam.com, 100 MB Save patched ISO to: [Browse] [Prev] [Next] [Cancel] Enter Next Backspace Back Esc Cancel

3221 3222 3223

3220

#### 3225 •

### 3226

3224



Veeam Agent for Linux [ graylog ] Provide license file for Veeam Agent for Linux File location: Agreements Recovery ISO [Browse] > License Choose agent edition to use on this computer: (X) Workstation ( ) Server If you do not have a license, then just click [Finish] and the product will operate in Free Edition mode. [Prev] [Finish] [Cancel]

3227 3228

- 3229 3230
  - Press "C" to Configure a new backup job.
- 3231

Veeam Agent for Linux
Thank you for installing our product!
As the first step, you will need to configure a backup job. You can choose between backing up the entire computer, individual volumes or select files an directories only. In any case, we will create an image-level backup containing the selected data. Press [C] to create your first backup job now.
If you already have any type of backup created and want to perform a restore of individual files, press [R] now. To restore the entire computer or an individual volume, you will need to boot from Veeam Recovery Media first.
Need help? We will be glad to assist you on Veeam Agent for Linux forum at
https://forums.veeam.com
C Configure R Recover Files M Misc Esc Exit

3232 3233

3234 Enter an appropriate Job name. Hit Next button •



		Veeam Agent for Linux	[ polaris ]	
	Please specif	y backup job name		
>	Name Backup mode Destination Network Advanced Schedule Summary	Job name: Full-weekly		
			[Next]	[Cancel]
	Ente	r Next	Esc Cancel	

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



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



8	192.168.0.20 - PuTTY	X
	Veeam Agent for Linux [ polaris ]	^
Choose	here you want to back up your data to	
Name Backup > Destin	() Local ode Back up to a locally attached storage device.	
Networ Advanc Schedu	(X) Shared Folder Back up to a network location (SMB or NFS).	
Summar	( ) Veeam Backup & Replication Back up to a Veeam repository (9.5 U4 or later).	
	( ) Veeam Cloud Connect repository Back up to a cloud repository managed by Veeam Cloud Connect Provider (9.5 U4 or later).	
	[Prev] [Next] [Cancel]	≡
Ente	Next Backspace Back Esc Cancel	~

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

P		192.168.0.20 -	PuTTY			_	x
	Veeam Age	ent for Linu	ıx [polar	is]			^
Specify a ne	twork location	to backup t	:0				
Name Backup mode	(X) NFS () SMB						
<pre>&gt; Network Advanced Schedule Summary</pre>	Path:	10.100.	0.10	/ <mark>linux</mark>	-backup	os/pol	
	Restore poin	ts: <mark>60</mark>					
			[Pre	v] [Ne	xt] [C	Cancel]	
Enter Nex	t	Backspace	Back	1	sc Can	icel	~

• Under Advanced, Enable the options as required. For security purposes, Enable the

# 3254 "Backup Encryption"

# 3255



- 3256 3257
- Under Schedule, you can either configure an automated job to run daily/weekly or uncheck
  "Run the job automatically" option to run a onetime manual backup.
- 3260

Choose when you want backup job to be started automatically Name Backup mode [X] Run the job automatically Destination Daily at: 06:00 Location Advanced [X] Monday Schedule [X] Saturday [X] Tuesday [X] Sunday Summary [X] Wednesday [X] Thursday [X] Friday

- Verify the settings on the Summary Screen and hit Next to kick off the job. Hit FINISH when done.
- 3265 **Note**: The free edition allows to schedule only one Backup job at a time. To change the
- backup mode, delete any existing job and re-run the configure wizard.
- 3267 **Recovery:**

- A Restore operation is also initiated from the client and requires the Veeam Recovery Media
   to begin with. This media is available for download on the Veeam <u>website</u>
- Download the ISO and boot the server off it. The initial screen(s) will look like this:
- 3271

Veeam Recovery Media	
Accept license agreement	
You must accept the license terms to proceed	
IXI I accept Veeam End User Software License	
https://www.ueeam.com/eula.html	
Local path: /usr/share/doc/ueeam/EllLA	
[X] I accept the terms of the following 3rd party	
software components license agreements:	
Local path: /usr/share/doc/veeam/3rd_party	
[Continue] [Shutdown] [Reboot]	
Contraction	
Ree Delevat	
INST REDOOT	
Veeam Recovery Media	
MAIN MENU	
Restore volumes	
Restore files	
Switch to compand line	
Switch to Command line Report	
Shutdown	
onucuown	
Enter Select Un Down Manager	te
Uncer Derect Op, Down Haorga	

3275

3274

• If restoring from a Network drive (NFS or SMB), select the option "**Configure Network**" to 3277 first assign an IP address to the system. The Media supports both Static and DHCP method for obtaining an IP address as shown below. Once done, Hit **ESC** to go Back. Click on

3279 "**Restore Volumes**" to proceed.

3280



• 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
- 3289 set to connect to Veeam backup server using NFS.

	Ų	leeam Recove	ry Media		
		MOUNT SHARE	D FOLDER		
C C	O NFS O SMB				
Pat	th: 10.	100.0.10	∕ <mark>linux-ba</mark>	ckups/p	
Enter Connect		Backspace	Back	Esc Ma	in menu

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

	Veeam Recov	Jery neala	
IM	PORTED BACKUPS		RESTORE POINTS
Job name	Hostname	Points	Created at
graylog BackupJob1	graylog	1	20:19 12-04-2019
I Import backup	R	escan	Esc Main menu

- The wizard will then display a comparison of the filesystem layout that's currently on the
- Linux server versus to what it currently has on that Backup Restore point. Select the
- Appropriate volume/disk to Restore and hit **Enter**. This will confirm your selection
- 3303

COMENT STOLE			IN BACKU	IP
Device Restore sda1 sda2 sda5 (lum) free sdb free sdb1 free graylog-ug root swap_1	Size 243.0M 19.29G 5.97G 25.00G 1007K 20.00G 5.00G 19.29G 15.29G 15.29G 4.00G	Device sda1 sda2 sda5 (lum) sdb sdb1 graylog-ug root swap_1	Size 243.0M 19.29G 25.00G 20.00G 19.29G 15.29G 4.00G	Usage /boot (ext2) (LVM2_mem /uar/opt/ / (ext4) (swap)

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

		Veeam Rec	overy Media		
CURF	ENT SYSTEM		Ĩ	IN BACK	JP
Device	Restore	Size	Device	Size	Usage
<pre>sda (boot)    sda1    sda2    sda5 (lum)    free    sdb    free    sdb1    free    graylog-vg    root    swap_1</pre>	Resto Resto Delet Close Table Bootl Size:	sda re whole di re bootload e partition type: mbr oader: Grub 25.50G	(boot) sk from ler from table	<b>G</b> <b>M</b> G G G G G G G	<pre>/boot (ext2) (LVM2_mem /var/opt/ / (ext4) (swap)</pre>
Ente	r Select			Esc 🕻	ancel

- The next screen lets you choose the disk from backup to restore from. Select the appropriate disk and hit Enter.
- 3312

ada (ba	Diek	ada (bast) 2E E00		
sda (b)	DISK.	Sua (DUDI) 25.50G		t (ext
sda2 sda5	Select disk	in backup to restore	: from:	2 mem.
free	Device	Usage	Size	
sdb				/opt/.
free cdb1	sda (boot)	ext2	25.50G	x+4)
free	sda2	EXIL	19 296	n)
graylog	sda5 (lum)	LVM2 member	19.29G	P
root	sdb	_	25.00G	
swap_1	sdb1	ext4	20.00G	
1.000	graylog-vg		19.29G	
	root	ext4	15.296	
	Swap_1	swap	4.000	
L		i i i i i i i i i i i i i i i i i i i		

3313 3314 3315

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

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 (ext
sda5 (lum)		19.29G	sda5 (lum)	19.29G	(LVM2_mem.
free		5.97G	sdb	25.00G	
sdb		25.00G	sdb1	20.00G	/uar/opt/.
free		1007K	graylog-vg	19.29G	( ( much A )
free		5 006	ruut suan 1	4 006	(Swan)
maulog-ug		19.296	Swup_r	1.000	Cowepy
root	root (/)	15.29G			
swap_1	swap_1 (s	4.00G			

- Next the Recovery Summary screen will confirm the filesystem changes. Hit Enter to start
   the Recovery
- The restore process will now run and show a success message once complete. Eject the
   Veeam Recovery Media once restore completes and Reboot the server.
- 3322

	and the second sec					
Veean Recovery Media						
Restore	26× S	itatus: <b>R</b> u				
Tine	Action	Durati				
19:50:06 19:50:06	Job started at 2017-06-21 19:50:06 UTC Starting volume restore					
19:50:10 19:50:13	Applying changes to disks configuration Restoring bootloader on /dev/sda	00:00:00 00:00:00				
19:50:14 19:50:19	sdal restored 285 MB at 55.5 MB/s sda5 272 GB at 3.9 GB/s (95%)	00:00:0 00:01:0				
	S Stop restore					

# 3324 Changing backup job type:

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

3327	sudo veeamconfig job list
3328	sudo veeamconfig job delete name <job name=""></job>
3329	sudo veeamconfig job delete id < id >

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

### 3333 **References:**

- 3334 [1] Veeam Backup and Replication <u>https://www.veeam.com/vm-backup-recovery-replication-</u>
   3335 <u>software.html</u>
- 3336 [2] Veeam agent for Linux Free edition <u>https://www.veeam.com/linux-backup-free.html</u>

### **3337 4.6.6 Highlighted Performance Impacts**

- Three performance measurement experiments were performed for the Veeam tool while the manufacturing system was operational:
- 1. <u>CL004.1</u> Veeam agent is installed and running on predetermined CRS hosts.
- 3341 2. <u>CL004.2</u> A full image backup is performed on CRS hosts.
- 3342 3. <u>CL004.3</u> A directory backup (i.e., incremental backup) is performed on CRS hosts.

### 3343 **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 3361 vControllers are not shown in this plot.

3362 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.



3369Figure 4-12 - Stem plot displaying the inter-packet delays (greater than or equal to 1.10 seconds) of Modbus3370TCP traffic between the HMI and Station 1, as measured during the baseline CL001.2 and experiment3371CL004.2. Note the large inter-packet delays measured between experiment time 400 to 1000 sec., resulting in3372multiple HMI loss-of-view events of over 15 seconds, and the largest event over 130 seconds in length.

- 3373 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.).
- 3376 Measurements of the packet path delay (shown in Figure 4-14) show a similar increase,
- 3377 suggesting that one or more of the CRS network devices may have been overloaded while
- 3378 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).





- 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
- 3388 measured while the Veeam tool was imaging the two 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.

### 3398 4.6.6.3 Experiment CL004.3

3389

- 3399 A directory backup of the /opt/ directory on the Engineering Workstation (POLARIS) host was
- 3400 performed for this experiment. The backup was performed from 347 sec. to 1052 sec.
- 3401 (experiment time), and all data was transferred over the CRS network. The network traffic
- 3402 generated by the backup is shown in Figure 4-17.

Veeam Traffic on the CRS Network (CL004.3)



3403

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.

3406 Loss-of-view events with Station 3 and Station 4 were observed on the HMI multiple times

3407 during the experiment. Large inter-packet delay measurements between the HMI and Station 1

3408 are shown in Figure 4-18. The longest loss-of-view event occurred over 9 sec. in length. Based

3409 on the large inter-packet delay measurements, it is hypothesized that the loss-of-view events can

3410 also be classified as loss-of-control incidents, although this was not tested during the experiment.

3411 All the observed incidents occurred while the Veeam tool was actively backing up POLARIS.



3413Figure 4-18 - Stem plot showing the inter-packet delays (greater than or equal to 1.10 seconds) of Modbus3414TCP traffic between the HMI and Station 1, as measured during the baseline CL001.2 and experiment3415CL004.3. Note the large inter-packet delays measured between experiment time 370 to 700 sec., resulting in3416multiple HMI loss-of-view events of over 2 seconds, and the largest event over 9 seconds in length.

- 3417 The loss-of-view events were likely caused by the large round-trip (RTT) times (shown in Figure
- 3418 4-19) observed between the HMI and Station 1 while the Veeam tool was active, which were
- 3419 larger than the configured connection timeout value on the HMI (100 msec.). Measurements of
- 3420 the packet path delay (shown in Figure 4-20) show a similar increase, suggesting that one or
- 3421 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.



3426Figure 4-20 - Time-series plots showing the measured packet path delay Modbus TCP packets sent from the<br/>34273427HMI to Station 1 (left) and sent from Station 1 to the HMI (right) during the experiment. Note the large path<br/>delay of over 600 msec. around 350 sec., followed by consistent delays of around 20 msec. until around 700<br/>sec.



### CSF MFG PROFILE LOW SEC LVL EXAMPLE IG DISCRETE-BASED MFG SYSTEM USE CASE



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.

### 3435 **4.6.7** Link to Entire Performance Measurement Data Set

3436 • CL004.1-HostBackups.zip

- 3437 CL004.2-FullImageBackup.zip
- 3438 CL004.3-DirectoryBackup.zip

### **3439 4.7 TeamViewer**

### 3440 **4.7.1 Technical Solution Overview**

3441 TeamViewer is a Remote Desktop sharing tool. TeamViewer provides Secure Remote Access

- 3442 and Support Solutions for Entrepreneurs, Small Businesses, and Large Enterprises. Some of its
- 3443 features include Cross Platform Support Access such as PC-PC, PC-Mobile, Mobile-Mobile, etc.
- 3444 Multi User Support Sessions and Remote Device Control [1]
- 3445 **4.7.2** Technical Capabilities Provided by Solution
- 3446 TeamViewer provides components of the following Technical Capabilities described in Section3447 6 of Volume 1:
- Secure Remote Access
- 3449 Secure Remote Access
- 3450 **4.7.3** Subcategories Addressed by Implementing Solution
- 3451 PR.MA-2, PR.AC-5



# 3452 4.7.4 Architecture Map of Where Solution was Implemented
### 3454 **4.7.5** Installation Instructions and Configurations

- 3455 <u>Setup for Robotics System:</u>
- Secure Remote Access was setup for the CRS system using TeamViewer. The Cybersecurity
   scanning laptop was used a jump box for installing TeamViewer and connecting remotely to
   the Work Cell network within.
- 3460 Configuration:
- TeamViewer v14 was downloaded and installed on the Cybersecurity scanning laptop. The
   person connecting remotely needs to have Team viewer installed on their system too.
- The scanning laptop had internet access via wireless and at the same time access to the Work
   cell network by connecting a physical Ethernet connection coming from the core switch. A
   Static IP was assigned to the system on the Ethernet interface.
- The person connecting remotely needs to know your ID and password to punch in. Both of these are displayed on the TeamViewer panel itself.
- 3471

3468

3459

3461

3464



3472 3473 3474

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

- 3477 Once the connection was established, the HMI Panel was accessed off a browser on the
- 3478 Cybersecurity Scanning laptop to perform maintenance on the HMI.
- 3479 3480



3483 Two factor authentication was configured by using the procedure mentioned here: • 3484 https://community.teamviewer.com/t5/Knowledge-Base/Two-factor-authentication-Activation-and-Deactivation/ta-p/66 3485

3486 3487 References:

3488

- 3489 [1] Team Viewer: https://www.teamviewer.com
- 3490

#### 3491 4.7.6 Highlighted Performance Impacts

- 3492 No performance measurement experiments were performed for the use of Team Viewer due to 3493 its intended usage (i.e., Team Viewer was installed on a laptop that is attached to the network 3494 only during maintenance and engineering activities).
- 4.7.7 Link to Entire Performance Measurement Data Set 3495
- 3496 N/A

### 3497 **4.8 Microsoft Active Directory**

### 3498 **4.8.1 Technical Solution Overview**

3499 Active Directory (AD) is a directory service developed by Microsoft for Windows 3500 domain networks. A directory is a hierarchical structure that stores information about objects on 3501 the network. A directory service, such as Active Directory Domain Services (AD DS), provides 3502 the methods for storing directory data and making this data available to network users and 3503 administrators. For example, AD DS stores information about user accounts, such as names, 3504 passwords, phone numbers, and so on, and enables other authorized users on the same network to 3505 access this information. A server running Active Directory Domain Services (AD DS) is called 3506 a domain controller [1]. It authenticates and authorizes all users and computers in a Windows 3507 domain type network—assigning and enforcing security policies for all computers and installing or updating software. Active Directory uses Lightweight Directory Access Protocol (LDAP) 3508 versions 2 and 3. Microsoft's version of Kerberos and DNS.<sup>13</sup> 3509

- 3510 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.
- 3514 **4.8.2** Technical Capabilities Provided by Solution
- 3515 Microsoft Active Directory provides components of the following Technical Capabilities 3516 described in Section 6 of Volume 1:
- Credential Management
- Authentication and Authorization

#### 3519 **4.8.3** Subcategories Addressed by Implementing Solution

3520 PR.AC-1, PR.MA-1, PR.MA-2, PR-PT-3, PR.PT-4, DE.CM-3

<sup>&</sup>lt;sup>13</sup> <u>https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview</u>

### 3522 **4.8.4** Architecture Map of Where Solution was Implemented



### 3524 **4.8.5** Installation Instructions and Configurations

#### 3525 Setup:

- 3526 The setup consists of two virtual machines running Active Directory services in the
- 3527 Cybersecurity LAN. The server "LAN-AD" is the Primary DC and DNS server while "LAN-
- 3528 **AD-02**" one is the backup DC and DNS server.

#### 3529 Details of the AD-servers

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

3530

### 3531 Installation:

- Below are high level instructions for installing Active Directory services (ADDS) on a
   Windows 2012 R2 server.
- It is recommended to have 2 servers running AD for redundancy. Ensure the servers are up to
   date with patches and have meaningful hostnames as per their role. Begin by configuring a
   static IP address on the network interface of your server. Since the server will also act as
- 3537 DNS server, for DNS server field you can use local host address 127.0.0.1

Internet Protocol Version	4 (TCP/IPv4) Properties
General	
You can get IP settings assigned auton this capability. Otherwise, you need to for the appropriate IP settings.	natically if your network supports ask your network administrator
Obtain an IP address automatical	ly
• Use the following IP address:	
IP address:	10 . 100 . 0 . 17
Subnet mask:	255.255.255.0
Default gateway:	10 . 100 . 0 . 1
Obtain DNS server address auton	natically
Use the following DNS server add	resses:
Preferred DNS server:	127.0.0.1
Alternate DNS server:	
Ualidate settings upon exit	Advanced
	OK Cancel

- Launch "Server Manager" and click on "Add Roles and Features"
- 3540

<b>a</b>	Serv	er Manager 📃 🗖	x
💮 🕘 🕌 🕶 Dashb	oard	🕶 🇭   🚩 Manage Tools View H	lelp
Dashboard	WELCOME TO SEF	RVER MANAGER	
Local Server			
■ All Servers File and Storage Services ▷		<ol> <li>Configure this local server</li> </ol>	
- 2	QUICK START		
		2 Add roles and features	
		3 Add other servers to manage	
	WHAT'S NEW	4 Create a server group	
		5 Connect this server to cloud servi	ic
		Hide	e

### 3541 3542

3543 • Click "Next" at the first page

<b>a</b>	Add Roles and Features Wizard	-		x
Before you begin	DESTIN	NATION SymTe	V SERV Ist.lan.l	'ER lab
Before You Begin Installation Type Server Selection Server Roles Features Confirmation Results	<ul> <li>This wizard helps you install roles, role services, or features. You determine which roles, rol features to install based on the computing needs of your organization, such as sharing do hosting a website.</li> <li>To remove roles, role services, or features:</li> <li>Start the Remove Roles and Features Wizard</li> <li>Before you continue, verify that the following tasks have been completed: <ul> <li>The Administrator account has a strong password</li> <li>Network settings, such as static IP addresses, are configured</li> <li>The most current security updates from Windows Update are installed</li> </ul> </li> <li>If you must verify that any of the preceding prerequisites have been completed, close the complete the steps, and then run the wizard again.</li> <li>To continue, click Next.</li> </ul> <li>Skip this page by default</li>	vizar	vices, c	or r
	< Previous Next > Install	0	ance	

# • Select "Role Based or Feature Based Installation" under Installation Type

	Add Roles and Features Wizard	
Select installation	on type	DESTINATION SERV SymTest.lan.
Before You Begin	Select the installation type. You can install roles and features on a running machine, or on an offline virtual hard disk (VHD).	physical computer or virtu
Installation Type	Role-based or feature-based installation	
Server Selection	Configure a single server by adding roles, role services, and features.	
Server Roles		
Features	Remote Desktop Services installation	
	Install required role services for Virtual Desktop Infrastructure (VDI) to cr or session-based desktop deployment.	eate a virtual machine-ba

- 3549 3550
- Select "Active Directory Domain Services" and "DNS Server" to install. Click Next

#### CSF MFG PROFILE LOW SEC LVL EXAMPLE IG DISCRETE-BASED MFG SYSTEM USE CASE

	Add Roles and Features Wizard	_ <b>D</b> X
Before You Begin Installation Type Server Selection Server Roles Features AD DS DNS Server Confirmation Results	Add Roles and Peatures Wizard         Select one or more roles to install on the selected server.         Roles         Active Directory Certificate Services         Active Directory Domain Services         Active Directory Pederation Services         Active Directory Lightweight Directory Services         Active Directory Rights Management Services         Active Directory Rights Management Services         Application Server         DHCP Server         ØDNS Server         Fax Server         Image: File and Storage Services (1 of 12 installed)         Hyper-V         Network Policy and Access Services         Print and Document Services         Remote Access	<ul> <li>DESTINATION SERVER SymTestlan.lab</li> <li>Description</li> <li>Active Directory Domain Services (AD DS) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process.</li> </ul>
		v
	< Previous N	lext > Install Cancel

3552

3554

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

	Add Roles and Features Wizard	
Select features	Select one or more features to install on the selected sen	DESTINATION SERVER SymTest.lan.lab
Before You Begin	Select one of more reactives to install on the selected selected	vei.
Installation Type	Features	Description
Server Selection	NET Framework 3.5 Features	<ul> <li>.NET Framework 3.5 combines the</li> </ul>
Server Roles	NET Framework 4.5 Features (2 of 7 installed)	power of the .NET Framework 2.0
Features	Background Intelligent Transfer Service (BITS)	≡ building applications that offer
AD DS	BitLocker Drive Encryption	appealing user interfaces, protect
DNS Server	BitLocker Network Unlock	your customers' personal identity
Confirmation	BranchCache	secure communication, and provide
	Client for NFS	the ability to model a range of
	Data Center Bridging	business processes.
	Direct Play	
	Enhanced Storage	
	Failover Clustering	
	✓ Group Policy Management	

3558

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

<b>a</b>	Add Roles and Features Wizard	_ 🗆 X
Active Directory Before You Begin Installation Type Server Selection Server Roles Features DNS Server Confirmation Results	<ul> <li>Domain Services</li> <li>Active Directory Domain Services (AD DS) stores information about users, on the network. AD DS helps administrators securely manage this inform sharing and collaboration between users. AD DS is also required for direct such as Microsoft Exchange Server and for other Windows Server technology.</li> <li>Things to note: <ul> <li>To help ensure that users can still log on to the network in the case of a minimum of two domain controllers for a domain.</li> <li>AD DS requires a DNS server to be installed on the network. If you do the installed, you will be prompted to install the DNS Server role on this material services and the prospecies.</li> <li>Installing AD DS will also install the DFS Namespaces, DFS Replication, a which are required by AD DS.</li> </ul> </li> </ul>	DESTINATION SERVER SymTest.lan.lab computers, and other devices ation and facilitates resource tory-enabled applications ogies such as Group Policy. a server outage, install a not have a DNS server achine. and File Replication services
	< Previous Next >	Install Cancel

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



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

<b>a</b>	Add Roles and Features Wizard	- X
Installation progr	ESS DESTINATION S	ERVER AN-AD
Before You Begin	View installation progress	
	i Feature installation	
	Configuration required. Installation succeeded on LAN-AD.	
Features	Active Directory Domain Services	^
AD DS	Additional steps are required to make this machine a domain controller.	
	Promote this server to a domain controller	
	DNS Server	_
Results	Group Policy Management	=
	Role Administration Tools	
	AD DS and AD LDS Tools	
	Active Directory module for Windows PowerShell	
	AD DS Tools	
	Active Directory Administrative Center	~
	You can close this wizard without interrupting running tasks. View task progress or open to page again by clicking Notifications in the command bar, and then Task Details. Export configuration settings	his
	< Previous Next > Close Car	ncel

3561

3562 > Launch "Server Manager" again and click on "Promote this server to a domain
 3563 controller"



3564

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

3570

à	Active Directory Domain Services Configuration Wizard	_ 🗆 🗙
Deploym	ent Configuration	TARGET SERVER LAN-AD
Deployment C Domain Cont DNS Optic Additional Op Paths Boview Optic	Configuration       Select the deployment operation         roller Options       Add a domain controller to an existing domain         ons       Add a new domain to an existing forest         otions       Add a new forest         Specify the domain information for this operation	
Review Option Prerequisites Installation Results	Check Root domain name: LAN.LAB	
	More about deployment configurations	
	< Previous Next > Instal	Cancel

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

<b>b</b>	Active Directory Domain Service	s Configuration Wizard	_ <b>_</b> ×
Domain Controlle	er Options		TARGET SERVER LAN-AD
Deployment Configuration	Select functional level of the new fore	est and root domain	
Domain Controller Options	Forest functional level:	Windows Server 2012 R2	•
Additional Options	Domain functional level:	Windows Server 2012 R2	-
Paths	Specify domain controller capabilities	5	
Review Options	Domain Name System (DNS) serv	er	
Prerequisites Check	Prerequisites Check I Global Catalog (GC)		
Installation	Read only domain controller (ROI	DC)	
Results	Type the Directory Services Restore N	Iode (DSRM) password	
	Password:	•••••	
	Confirm password:	•••••	

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

a di seconda di second	Active Directory Domain Services Configuration Wizard	
DNS Options		TARGET SERVER LAN-AL
A delegation for this DN	S server cannot be created because the authoritative parent zone cannot be found	Show more X
Deployment Configuratio Domain Controller Option DNS Options	n Specify DNS delegation options	
Additional Options Paths		

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

<b>a</b>	Active Directory Domain Services (	Configuration Wizard	_ <b>D</b> X
Additional Option Deployment Configuration Domain Controller Options DNS Options Additional Options Paths Review Options Prerequisites Check Installation Results	IS Verify the NetBIOS name assigned to th The NetBIOS domain name:	e domain and change it if necessary LAN	TARGET SERVER LAN-AD

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



3576

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

2	Active Directory Domain Services Configuration Wizard	X
Review Options Deployment Configuration Domain Controller Options DNS Options Additional Options Paths Review Options Prerequisites Check Installation Results	TARGET : Review your selections: Configure this server as the first Active Directory domain controller in a new forest. The new domain name is "LAN.LAB". This is also the name of the new forest. The NetBIOS name of the domain: LAN Forest Functional Level: Windows Server 2012 R2 Domain Functional Level: Windows Server 2012 R2 Additional Options: Global catalog: Yes	SERVER AN-AD
	DNS Server: Yes Create DNS Delegation: No These settings can be exported to a Windows PowerShell script to automate additional installations View sc More about installation options	ript ncel

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

Prerequisites Che	CK TARGET SERVI
All prerequisite checks pass	sed successfully. Click 'Install' to begin installation.
Deployment Configuration Domain Controller Options	Prerequisites need to be validated before Active Directory Domain Services is installed on this computer
DNS Options	Rerun prerequisites check
Additional Options	
Paths	<ul> <li>View results</li> </ul>
Review Options Prerequisites Check	Windows Server 2012 R2 domain controllers have a default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security channel sessions.
Installation Results	For more information about this setting, see Knowledge Base article 942564 (http://go.microsoft.com/fwlink/?Linkld=104751).
	A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found or it does not run Windows DNS server. If you are integrating with an existing DNS infrastructure, you should manually create a delegation to this DNS server in the parent zone to ensure reliable name resolution from outside the domain "LAN.LAB". Otherwise, no action is required.
	1 If you click Install, the server automatically reboots at the end of the promotion operation.

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

Installation	TARGET SERV LAN-/
Deployment Configuration	Progress
Domain Controller Options	Securing machine\software\microsoft\enterprisecertificates
DNS Options	<ul> <li>View detailed operation results</li> </ul>
Additional Options	Windows Server 2012 R2 domain controllers have a default for the security setting named     "Allow contemportations compatible with Windows NT 4.0" that prove the security setting reasons
Paths	cryptography algorithms when establishing security channel sessions.
Review Options	For more information about this setting, see Knowledge Page acticle 042564 (http://
Prerequisites Check	go.microsoft.com/fwlink/?Linkld=104751).
Installation	A delegation for this DNS server cannot be created because the authoritative parent zone
Results	cannot be found or it does not run Windows DNS server. If you are integrating with an existing DNS infrastructure, you should manually create a delegation to this DNS server in the parent zone to ensure reliable name resolution from outside the domain "I AN I AR"

3583

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

B	Server	Manager	
🔶 🔿 – 🖪 📢 Dashba	oard	• 🗊   🚩 Manage	Tools View Help
Ċ			Active Directory Administrative Center
	WELCOME TO SERVE		Active Directory Domains and Trusts
Dashboard	WELCOWE TO SERVE	ER MANAGER	Active Directory Module for Windows PowerShell
Local Server			Active Directory Sites and Services
All Servers			Active Directory Users and Computers
AD DS		Conligure this i	ADSI Edit
	OLIICK START		Component Services
	QUICKSTART	2 Add roles and fe	Computer Management
■ File and Storage Services ▷		2 Add toles and to	Defragment and Optimize Drives
		3 Add other serve	TS DNS
			Event Viewer
	WHAT'S NEW	A Croate a corver	ar Group Policy Management

### 3587 **Configuration:**

- All of the Linux systems from the Robotics System were joined to the AD domain lan.lab
   using Centrify Express [2]. The initial domain join process is a onetime task and involves a
   system restart.
- The procedure to join Ubuntu Linux Systems to Active Directory domain using Centrify can
   be found in the section below "CentrifyDC Installation"
- In addition, DNS records for each Linux host were manually created on the Active Directory server.
- 3597

3586

3591

3594

#### 3598 CentrifyDC Express Installation

- 3599 <u>Pre-requisites</u>: Connectivity between your Linux server and AD server.
- Ensure you can ping the AD Domain Controller from your Linux host. Configure the DNS
  settings on its network interface to point to the IP address of the AD server and set the search
  domain to whatever domain name you have created in your AD. Once done, you can verify the
- 3603 DNS-settings by checking the /etc/resolv.conf file of your Linux server.
- 3604
- The free Centrify Express (Centrifydc) package can be downloaded either from
   <u>https://launchpad.net</u> or <u>https://www.centrify.com/express/linux/download/</u>. Ensure to select
   the correct OS version and CPU architecture that matches your Linux host.
- Upload the downloaded file to any Ubuntu Linux server which you want to join to AD.
- Run the command "dpkg -i <package\_name> "to install it. It may prompt you to install some dependencies. Ensure the dependencies have been installed prior.

	root@rigel:/home/icssec# dpkg -i /media/CDROM/centrifydc_5.1.1-831-0ubuntu1_amdd 4.deb Selecting previously unselected package centrifydc. (Reading database 270726 files and directories currently installed.) Unpacking centrifydc (from/centrifydc_5.1.1-831-0ubuntu1_amd64.deb) Setting up centrifydc (5.1.1-831-0ubuntu1) Processing triggers for man-db Processing triggers for ureadahead Processing triggers for libc-bin Idconfin deferred processing now taking place
3612 3613	root@rigel:/home/icssec#
3614 •	Run the command "adlicenseexpress" to activate the free express mode.
3015	<pre>root@rigel:/home/icssec# adlicenseexpress The mode is express. root@rigel:/home/icssec#</pre>
3616 3617	
3618 • 3619 3620	Next run the " <b>adjoin –workstation domain-name</b> " command. This will prompt you to enter the Domain Administrator password.
	<pre>     root@rigel:/home/icssec  root@rigel:/home/icssec# adjoinworkstation lab.local </pre>
3621	If the above star completes successfully, my "adiafe" command to verify the domain isin
3622       •         3623       3624	status as follows
	😣 🚍 🗊 root@rigel: /home/icssec
	root@rigel:/home/icssec# adinfo Local host name: rigel Joined to domain: lan.lab Joined as: rigel.lan.lab Pre-win2K name: rigel Current DC: lan-ad.lan.lab Preferred site: default-first-site-name Zone: Auto Zone Last password set: 2017-06-22 10:28:38 EDT CentrifyDC mode: connected Licensed Features: Disabled
3625 3626	root@rigel:/home/icssec#

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

3628 • For example: ssh <u>username.domain-name@hostname.domain-name</u>

```
3629
```

• OR directly via Desktop as shown below: Domain-Name\Username



3630

# **• Enabling sudo for administrators**

3632 3633 3634	To make an AD Domain Group a sudoer; edit the file /etc/sudoers file (using the command visudo) and add the following line:			
3635	%adgroup ALL=(ALL) ALL			
3636 3637 3638 3639	Where, <b>adgroup</b> , is a group from your active directory. The group names from active directory are transformed into all lower case letters with underscores replacing spaces, so you can use %domain_admins for the Domain Admins group.			
3640 3641	4.8.6 Highlighted Performance Impacts			
3642 3643	One performance measurement experiment was performed for the Active Directory service while the manufacturing system was operational:			

- 1. <u>CL002.1</u> The Active Directory service is installed and running on CRS hosts.
- 3645 **4.8.6.1 Experiment CL002.1**
- 3646 No performance impact to the manufacturing process was measured during the experiment.

#### CSF MFG PROFILE LOW SEC LVL EXAMPLE IG DISCRETE-BASED MFG SYSTEM USE CASE



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.

#### 3650 **4.8.7** Link to Entire Performance Measurement Data Set

3651 • <u>CL002.1-ActiveDir.zip</u>

### 3652 **4.9 Symantec Endpoint Protection**

#### 3653 4.9.1 Technical Solution Overview

#### 3654 Symantec Endpoint Protection:

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

- 3661 learning, behavior analysis and exploit prevention with proven protection capabilities like
- 3662 intrusion prevention, reputation analysis and more.<sup>14</sup>
- 3663 Points to Consider:
- Next Generation Antivirus / Endpoint protection solution to prevent against virus attacks and emerging cyber threats such as zero-day attacks, ransomware etc.
- OS Platform independent: The endpoint agents are supported on Windows and Linux.
- Comes with a lightweight agent and virus definition sets that require minimal network
   bandwidth.
- Diverse Feature set: Core capabilities include Antivirus, Host Firewall, Intrusion Prevention,
   Host Integrity, System lockdown, Application White listing and USB Device Control.
- Centralized Management: All endpoints, rule sets, policies can be centrally managed from
   the Symantec Endpoint Manager console.
- The Symantec Manager component is supported only on Windows OS.
- The Linux agent requires the OS kernel on Linux systems to be at a certain level for
   installation. In addition, the Linux agent is a 32-bit installer. If installing on a 64-bit Linux
   system, it requires certain 32-bit packages/libraries to be installed as a pre-requisite. This
   may conflict with some of the existing packages on the system.
- The endpoint agent on each system by default needs to communicate outbound with a range of public IP addresses for its Reputation analysis and Global Threat intelligence feature. It is recommended to allow this traffic from your firewall to leverage the advanced features of the product.
- Important: System reboot is required to complete the installation process on clients/endpoints. Plan ahead of time.

 $<sup>{}^{14} \</sup> Symantec \ Endpoint \ Protection: \ \underline{https://www.symantec.com/content/dam/symantec/docs/data-sheets/endpoint-protection-14-en.pdf}$ 

## 3684 **4.9.2** Technical Capabilities Provided by Solution

- 3685 Symantec Endpoint Protection provides components of the following Technical Capabilities 3686 described in Section 6 of Volume 1:
- Anti-virus/malware
- 3688 **4.9.3** Subcategories Addressed by Implementing Solution
- 3689 PR.AC-1, DE.CM-3, DE.CM-4



### 3690 **4.9.4** Architecture Map of Where Solution was Implemented

3691

# 3692 **4.9.5** Installation Instructions and Configurations

3693 Setup Overview:

- 3694 Setup consists of a single Symantec Endpoint Protection Manager (SEPM) instance in the
- 3695 Cybersecurity LAN network. This central instance communicates with all the endpoint agents
- 3696 deployed on to the Process Control systems. Likewise, all endpoints report their status to the
- 3697 Manager server. The communication ports required to be opened are different for Windows
- 3698 clients as compared to Mac/Linux clients. Detailed list of firewall ports can be obtained from
- 3699 Symantec website. The SEP Manager server downloads its daily signature updates from the 3700 Symantec cloud servers, so this necessary traffic was allowed to pass thru the Manufacturing
- 5700 Symantec cloud servers, so this necessary traffic was allowed to pass thru the Manufa 2701 System Eiropeal
- 3701 System Firewall.

## 3702 Details of the software used

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

3703

# 3704 Installation of SEP Manager:

0

- SEPM is supported only on Windows server platforms. A Windows Server 2012 R2 virtual
   machine was setup in the Cybersecurity LAN to install the SEPM component.
- Upon purchase, there will be a license file emailed to you along with the link to download
   the install binaries. Download the zip bundle from the Symantec website. Extract the zip
   file which will be like the one below depending on whatever is the latest version available.
- 3710 3711

Symantec\_Endpoint\_Protection\_14.2.0\_Full\_Installation\_EN.exe

- Open the extracted folder and run the Setup.exe file. Mid-way during the setup, the install
   wizard will prompt to select a password for the admin user. Enter a strong password and hit
   Next.
- On the Backed Database selection page, there are two options "Embedded" and "MS
   SQL Server". Choose the Embedded database if you do not have a MS SQL Server.
   Follow the on-screen instructions and complete the installation wizard. Reboot the server
   once done.
- Launch the SEP Manager console and login with the admin user created earlier.
- 3720

0	Symantec Endpoi	nt Protectio	n Manager		_ □	X
			demo			
			• Syman	nec.		
	Endpoint P	rotection M	anager			
	User name: admin					
	Password:					
	Server: SymantecMgrV	M:8443	~			
	Forgot your pas	sword?				
	Log On	Exit	Options >>			
	Copyright © 2018 Symantec Corpo	pration. All rights res	served.			
	This Symantec product may conta that are subject to a separate lice	in open source and nse.	other third party materials			
	- '					

3726

3727

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

### 3731 Custom Configuration of SEPM server

- The following client groups were created to group devices from each of the systems.
   Upon installing the AV agent on the endpoints, the devices were moved to their
   respective groups.
- 3736

0		Symantec Endp	oint Prote	ection Manager			
🛡 s	ymantec Endpoint Prote	ction Manager			Lates	st Alerts Refres	sh Help LogOff
	Clients My Company — Default Group — DMZ	Process Contro Clients Policies D	)	ll Packages	Policy serial r	umber: D575-11/29	/2018 15:33:34 712
Monitors	LAN Network     Process Control     Debation	View: Client status	~	All users a	nd computers		Filter
Reports	RUDUICS	Name	Health State	Logon User or Computer	IP Address	<b>Client Version</b>	Last Time Sta
		FGS-47631EHH	Online	Administrator	172.16.3.10	14.2.758.0000	April 23, 2019 1
1		FGS-47631LHH	Online	cheet	172.16.2.4	14.2.758.0000	April 23, 2019 1
Policies		FGS-61338CH	Online	cheet	172.16.1.5	14.2.758.0000	April 23, 2019 1
я		FGS-61338HH	Online	cheet	172.16.1.4	14.2.758.0000	April 23, 2019 1
		FGS-613380SH	Online	cheet	172.16.2.5	14.2.758.0000	April 23, 2019 1
Clients	Tasks	GS-61338PSH	Online	cheet	172.16.2.3	14.2.758.0000	April 23, 2019 1
{ô} dmin Cļoud	Instal a client	WIN-FPVTDCDEUCR	Online	Administrator	172.16.2.14	14.2.758.0000	April 23, 2019 1

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

🛡 s	ymantec Endpoint Protection	Manager	🔔 Latest News Refresh Help Log Off
	Servers ■ Servers ■- 品 Local Site (Site SymantecMgrVM)  - ■ SymantecMgrVM	Server Properties for Symanted           File Fingerprint Update         Full Definitions Download           General         Email Server         Directory Servers	Proxy Server
Monitors	L 👼 locanusi	Directory Servers Name Type Properties	
Eeports			Edit
Policies		Synchronized Directory Settings	
Clients	Tasks         ✓       Edit the server properties         ※       Delete Selected Server         ④       Manage Server Certificate         ✓       Configure Securit Authentication         ♦       Import Server Properties         ►       Export Server Properties	Synchronize with Directory Servers  Auto-schedule (occurs every 24 hours)  Synchronize every: hours	
C	Administrators Se Domains Se Servers Se Install Packages Licenses	OK ptember 27, 2017 11:10:42 AM EDT: Retry timestamp is over the maximum re ptember 27, 2017 11:00:42 AM EDT: LiveUpdate retry failed. Will try again. [ ptember 27, 2017 11:00:42 AM EDT: LUALL.EXE finished running. [Site: Site ptember 27, 2017 11:00:42 AM EDT: LiveUpdate encountered one or more er	Cancel Help try window, switching to regular schedule run. [S • Site: Site SymantecMgrVM] [Server: SymantecMgr SymantecMgrVM] [Server: SymantecMgrVM] rors. Return code = 4. [Site: Site SymantecMgrVM •

- 3744 3745
  - Similarly, Email server can be configured by clicking on the "Email Server" tab.

#### 3746 Getting started with Endpoint installs

#### 3747 High level steps:

- 3748 Create a deployment package specific for a client group
  3749 Deploy the package from the SEPM server to the endpoint using Network Deployment
- options or manually copy over the package to the endpoint for installation.
- Restart the endpoint. Verify the device shows up in the SEPM console.

### 3752 Creating a deployment package:

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

V	Client Deployment Wizard
\$	Select Deployment Type Symantec.
,	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:
	New Package Deployment
	Select packages from the server and specify client group and features.
	O Existing Package Deployment
	Choose from previously exported packages that are located on your hard drive.
	Browse
	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 Protect Information Manager, or to convert an unmanaged client to a managed client.
	🔘 Create a package for Symantec Endpoint Protection clients that run on Windows. 🦓
	O Create a package for Symantec Endpoint Protection clients that run on Mac. 🗯
	< Back Next > Cancel

- 3762
- 5702
- Click "Next" >> Choose the appropriate OS Platform as per the endpoint OS, from the dropdown list of Install Packages. You will notice the Group Name is already pre populated. This ensure the client will be placed directly in that group upon install. Under
   Content Options; Select "Include virus definitions in the client installation package"
   [optional]. Click Next.

0	Client Deployment Wizard	X
Select Group a	nd Install Feature Sets 🛛 🗹	Symantec.
Install Packages:	Windows - Symantec Endpoint Protection version 14.2.758.0000 - English         Windows - Symantec Endpoint Protection version 14.2.758.0000 - English         Linux - Symantec Endpoint Protection version 14.2.758.0000 - English         Windows - Symantec Endpoint Protection version 14.2.758.0000 - English         Windows - Symantec Endpoint Protection version 14.2.758.0000 - English         Mac - Symantec Endpoint Protection version 14.0.3929.1200 - English         Mac - Symantec Endpoint Protection version 14.0.3929.1200 - English         Mac - Symantec Endpoint Protection version 14.0.3929.1200 - English         Mindows - Symantec Endpoint Protection version 14.0.3929.1200 - English         Windows - Symantec Endpoint Protection version 14.0.3929.1200 - English         Windows - Symantec Endpoint Protection version 14.0.3929.1200 - English         Windows - Symantec Endpoint Protection version 14.0.3929.1200 - English         Windows - Symantec Endpoint Protection version 14.0.3929.1200 - English         Windows - Symantec Endpoint Protection version 14.0.3929.1200 - English         Windows - Symantec Endpoint Protection version 14.0.3929.1200 - English	
Group:	My Company\Process Control	Browse
Install Feature Sets:	Full Protection for Clients Recommended for laptops and desktops - Includes all protection technologies. Some security features are not supported on some platforms. Please refer to product documentation for details.	
Install Settings:	Default Standard client installation settings for Windows	Options
Content Options:	Include virus definitions in the client installation package. Uncheck this option to create a smaller client installation package that does not include virus definitions but does i other content. After the client is installed, run LiveUpdate immediately on the clients to download the virus definition	nclude all ins.
	< Back Next >	Cancel

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

choose your preferri	o installation method.	
<ul> <li>Save Package</li> </ul>		
Creates ar	executable installation package, but does not distribute protection software to remote computers.	
O Remote Push		
Creates a	lient installation package and pushes the package onto client computers. The package installs auto	omatically on the computers.
Prepar	ng for Remote Push Installation	
O Web Link and E	nail	
Creates a	lient installation package and an email template so you can send an email notification with downloa	ad instructions to users.

# 3775 Installing the AV on Robotics Systems

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

D	Client Deployment Wizard					
Select Group	and Install Feature Sets	Symantec.				
Install Packages:	<ul> <li>Linux - Symantec Endpoint Protection version 14.2.758.0000 - English</li> <li>Windows - Symantec Endpoint Protection version 14.2.758.0000 - English</li> <li>Linux - Symantec Endpoint Protection version 14.2.758.0000 - English</li> <li>Linux - Symantec Endpoint Protection version 14.2.758.0000 - English</li> <li>Windows - Symantec Endpoint Protection version 14.0.3929.1200 - English</li> <li>Mac - Symantec Endpoint Protection version 14.0.3929.1200 - English</li> <li>Linux - Symantec Endpoint Protection version 14.0.3929.1200 - English</li> <li>Linux - Symantec Endpoint Protection version 14.0.3929.1200 - English</li> <li>Windows - Symantec Endpoint Protection version 14.0.3822.1101 - English</li> <li>Windows - Symantec Endpoint Protection version 14.0.3876.1100 - English</li> <li>LINUXDPKG: Linux - Symantec Endpoint Protection version 14.2.758.0000 - English (6/19/18)</li> </ul>					
Group:	My Company\Robotics	Browse				

Symantec AV on Linux requires the below 32-bit packages to be installed as a pre-3783 requisite<sup>15</sup>. A Full backup of all Linux systems in Robotics was taken prior to installing 3784 3785 these. 3786 o libc6:i386 3787 o libx11-6:i386 3788 libncurses5:i386  $\circ$  libstdc++6:i386 3789 3790 3791 • If installing it on a 64-bit server, ensure to enable/check if multi-architecture mode is 3792 enabled as follows, prior to installing those 32-bit libraries. For instance, on a Debian 3793 /Ubuntu system; run the following commands. 3794 Verify if the system has 64-bit architecture by running dpkg --print-architecture 3795 3796 If the output is something like the one shown below, it means you are okay amd64 3797 Verify that you have multi-arch mode enabled by running the following command. 3798 3799 Multi-architecture mode lets us install 32-bit packages on a 64-bit system. Type: dpkg --print-foreign-architectures The output is: i386 If you don't have multi-arch support you have to enable it. 3800 3801 Run this command to enable multi-arch support: sudo dpkg --add-architecture i386 3802 3803 This will allow us to install those 32-bit packages.

<sup>&</sup>lt;sup>15</sup> <u>https://support.symantec.com/en\_US/article.TECH228118.html</u>

3804		sudo apt-get install libc6:i386 libx11-6:i386 libncurses5:i386 libstdc++6:i386
3805 3806 3807 3808	•	The zip file containing the .deb package was extracted on the Linux client. The following command was run to grant execute permissions to the "install.sh" file found in the extracted folder.
3809		chmod u+x install.sh
3810 3811 3812 3813	•	Next, the install.sh script was run as sudo ./install.sh -i
3814 3815	•	Upon successful install, it showed an output like the one below
		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 definitions 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
3816	_	The log files for installation of Symantec Endpoint Protection for Linux are under ~/: sepfl-install.log sepap-install.log sepui-install.log sepfl-kbuild.log youbot@vSaiph:/var/sepfiles\$

- The client was rebooted, and its status was verified to be green ONLINE in the SEPM console. The process was repeated for all other Linux machines.
- 3820 Additional Configuration
- An "Exceptions" policy was created for excluding the /sys and /proc directories from scanning. Click on Policies >> Exceptions >> Default policy or create your own >>
   Exceptions >> Click Add to add folders to exclude from scanning.
- 3824

0	Linux exceptions policy							X
Exceptions Policy								
Overview Exceptions	Exceptions							
Client Restrictions	Exceptions Configure exceptions for scan You can only edit Symantec En	Exceptions Configure exceptions for scans and Tamper Protection, as applicable. You can only edit Symantec Endpoint Protection Manager console exceptions.						
	Exception Item	Platform	Exception Type		Acti	Action		
	/sys	∆ Linux	Security Risk Folder		Igno	Ignore		
	/proc	∆ Linux	Security Risk Fr	older	Igno	re		
				Add 🔻	Edit	Delete	Сору	Paste
	Exception Details							
	Exception item: /sys							•
	•							•
						ОК	Cancel	Help

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

ion Policy
Intrusion Prevention
Intrusion Prevention Network Intrusion Prevention automatically detects and blocks network attacks. Browser Intrusion Prevention automatically detects and
Excluded Hosts
Host List         Hosts to exclude from Intrusion Prevention:         Enabled       Group Name       Content         Image: Pladdress:192.168.0.12       Image: Pladdress:192.168.0.12       Image: Pladdress:192.168.0.11         Image: Pladdress:192.168.0.11       Image: Pladdress:192.168.0.11       Image: Pladdress:192.168.0.11         Image: Pladdress: Pladdress: Pladdress       Image: Pladdress: Pladdress       Image: Pladdress         Image: Pladdress       Image: Pladdress       Image: Pladdress         Image: Pladdres       Image: Pladdress       Image:

- alongside their 64bit counterparts. This can cause issues/conflicts with some of existing
   packages such as python libraries especially if you are on older versions of Linux such as
   Ubuntu 12.04.
- On newer versions of Linux, ensure "Multiarch" mode is enabled to allow 32bit apps to
   install on 64bit systems.<sup>17</sup> On our Ubuntu 12.04 servers, wherein we couldn't get the agent to
   install due to these package conflicts, we ended up applying other compensating controls.
- 3847

<sup>&</sup>lt;sup>16</sup> <u>https://support.symantec.com/en\_US/article.TECH228118.html</u>

<sup>&</sup>lt;sup>17</sup> https://wiki.debian.org/Multiarch/HOWTO

#### 3848 **4.9.6** Highlighted Performance Impacts

- 3849 Two performance measurement experiments were performed for the Symantec tool while the 3850 manufacturing system was operational:
- 3851 1. <u>CL005.1</u> Symantec agent is installed, and real-time scanning is enabled on CRS hosts.
- 3852 2. <u>CL005.2</u> A full system scan is performed on predetermined CRS hosts.
- 3853 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.
- 3856 CPU utilization increased from around 2% to 7% on vController1 during the experiment (see
- 3857 Figure 4-23). However, this CPU increase was not observed on vController2 (see Figure 4-24),
- 3858 which performs all of the same functions as vController1. At the time of publishing, it is
- 3859 unknown if this CPU increase on vController1 was caused by the Symantec agent.



3861Figure 4-23 - Time series plots showing the CPU utilization ratio for vController1 during the CL005.13862experiment and CL001.2 baseline (left), and during the period of measured impact (right).

#### CSF MFG PROFILE LOW SEC LVL EXAMPLE IG DISCRETE-BASED MFG SYSTEM USE CASE



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 isnot 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.

#### 3871 4.9.6.2 Experiment CL005.2

3872	A full system sca	n of the robot driver (	(MINTAKA), robot	controller vController1	. and robot
					,

- 3873 controller vController2 were initiated at 106 sec., 140 sec., and 309 sec. experiment time,
- 3874 respectively. The tool did not report when the scanning ended, so it was not recorded. The host
- 3875 MINTAKA does not run a performance logger, so data from this host is not available.

- 3876 The CPU utilization increased during the scan period on both vController1 and vController2.
- 3877 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
- 3879 vController2 (see Figure 4-27) increased from 2% to 26% while the scan was executing (from
- 3880 300 sec. to 920 sec. experiment time), with a peak of 33%.





#### CSF MFG PROFILE LOW SEC LVL EXAMPLE IG DISCRETE-BASED MFG SYSTEM USE CASE



3885Figure 4-27 - Time series plots showing the CPU utilization ratio for vController2 during the CL005.23886experiment and the CL001.2 baseline (left), and during the period of measured impact (right).

3887 Network activity increased for a short time on both vController1 and vController2 while the scan

3888 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

3891 (from 335 sec. to 365 sec. experiment time). Sustained network bitrates over 2 Mbps for around

3892 30 seconds total were measured on both vControllers.



3893 3894

3894Figure 4-28 - Time series plots showing the quantity of network traffic received by vController1 during the<br/>experiment (left), and during the period of measured impact (right). The peak in traffic shown between 720<br/>sec. to 750 sec. occurred while the scan was active.


3897

3898<br/>3899Figure 4-29 - Time series plots showing the quantity of network traffic received by vController2 during the<br/>experiment (left), and during the period of measured impact (right). The peak in traffic shown between 330<br/>sec. to 365 sec. occurred while the scan was active.



3901 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.

3905

3902

#### 3906 **4.9.7** Link to Entire Performance Measurement Data Set

- 3907 <u>CL005.1-AntivirusRealTimeScan.zip</u>
- 3908 CL005.2-AntivirusFullScan.zip

#### **4.10 Tenable Nessus**

#### 3910 **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.<sup>18</sup> It supports both authenticated and
unauthenticated scans.

- 3917 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.
- 3927

# 3928 **4.10.2 Technical Capabilities Provided by Solution**

- 3929 Tenable Nessus provides components of the following Technical Capabilities described in3930 Section 6 of Volume 1:
- Vulnerability Scanning
- 3932•Vulnerability Management

# 3933 **4.10.3 Subcategories Addressed by Implementing Solution**

3934 ID.AM-3, ID.AM-4, ID.RA-1, DE.CM-4, DE.CM-8

<sup>&</sup>lt;sup>18</sup> Nessus Professional: <u>http://info.tenable.com/rs/934-XQB-568/images/NessusPro\_DS\_EN\_v8.pdf</u>



# 3936 4.10.4 Architecture Map of Where Solution was Implemented

#### 3938 **4.10.5** Installation Instructions and Configurations

3939 Details of the solutions implemented:

Name	Version
Nessus Professional	7.2.0

3940

# 3941 Setup Overview:

- The Robotics systems being behind a firewall (NAT) cannot be reached directly from the Cybersecurity LAN network. To work around this, a dedicated laptop was setup to assume the role of Nessus server and Nessus Professional 7.x was installed on it.<sup>19</sup> This laptop would be used on-demand to perform scans. A temporary network connection from the Supervisory LAN would be arranged as required and the system was assigned a static IP address.
- 3947
- During the setup, the wizard will prompt for registration. The Registration process and updates can be configured either in online or offline mode. An online mode is suitable for environments where Nessus server is connected to the internet while an offline mode is for air-gapped environments. Detailed instructions for registering Nessus offline can be found in the product guide. Upon completion, Nessus can be accessed via
   https://clB address of Nessus server :8834
- 3953 https://<IP address of Nessus server>:8834
- The Nessus server needs to have network connectivity from whichever networks or subnets
   that are intended to be scanned. In addition, if performing authenticated scans then
   appropriate firewall rules should be in place to allow SSH, WMI or SNMP traffic depending
   on the type of hosts. If performing unauthenticated scan, the firewall should be allowed for
   any-any communication between the Nessus server and target network.
- 3960

- 3961 Configuration for Robotics System:
- Ensure to allow firewall rules for Nessus scanning. Port 22 was allowed on our firewall
   between the Nessus system and Supervisory, Control LAN networks.
- 3964
- It is important to not change the IP address on the Nessus server once setup is done, as it causes errors. This is because Nessus installer records all network settings during the install process. Any hardware change made post install is not recognized by Nessus.
- 3968

<sup>&</sup>lt;sup>19</sup>Nessus Official Documentation: <u>https://docs.tenable.com/nessus/Content/GettingStarted.htm</u>

- A new policy was created specific to the assets in Robotics and linked to a scan job. The scan was scheduled to be On-Demand. The figure below shows the Policy configured Robotics
   System
- 3972



- The figure below shows the corresponding scan job settings which has the
- 3976 **"Robotics\_Enclave\_II**" policy assigned to it under **Policy**.

Nessus Professional / Scan	ns / Edit × +			
$\leftrightarrow$ $\rightarrow$ C $\blacktriangle$ Not se	cure   https://localhost:8834/#/	/scans/reports/55/config/settir	ıgs/basic/general	☆ 🔒
		A new version of Nessus is a	vailable and ready to install. Learn more or apply it now.	
Nessus 🔊	Scans Settings			🐥 admin
FOLDERS	Robotics_Enclave /	′ Configuration		
My Scans				
LAN-Measurement	Settings			
Process Control	BASIC			
Robotics	. Conoral	General Settings		
Transportation		Name	Robotics_Enclave	
All Scans	Schedule			
🛍 Trash	Notifications	Description	Using Advanced Scan Policy template	
Resources				
Policies		Folder	Robotics	
Plugin Rules			Polatics Enclove II	
Customized Reports		Policy	KODOTICS_ETICIAVE_IT	
Scanners 🖤		Targets	192.168.0.0/24 192.168.1.3-192.168.1.104	
		, , , , , , , , , , , , , , , , , , ,		
		Upload Targets	Add File	

- 3978 3979
- To kick-off a manual on-demand scan, click on the launch button next to the scan.
- 3981

#### **4.10.6 Highlighted Performance Impacts**

3983 Two performance measurement experiments were performed for the Nessus tool while the3984 manufacturing system was operational:

- 3985 1. <u>CL006.1</u> A host discovery scan was performed on the CRS network.
- 3986 2. <u>CL006.2</u> Credentialed checks were performed on predetermined CRS hosts.

#### 3987 4.10.6.1 Experiment CL006.1

- 3988 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).

3991 Multiple performance impacts were observed while the Nessus tool was actively scanning the

- 3992 HMI and machining stations. Loss-of-view events likely occurred (but were not directly
- 3993 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
- 3996 Station 1.

Nessus Network Traffic on the CRS Network



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





3997



4004Figure 4-32 - Stem plot displaying the inter-packet delays (greater than or equal to 1.10 seconds) of Modbus4005TCP traffic between the HMI and Station 1, as measured during the baseline CL001.2 and experiment4006CL006.1. Note the large inter-packet delays between experiment time 600 to 800, resulting in HMI loss-of-view4007for over 5 seconds.

- 4008 Performance impacts to the supervisory PLC task execution time were observed while the
- 4009 Nessus tool was actively scanning. Relatively large fluctuations of the average task execution
- 4010 time and the maximum task execution time were observed from 800 to 1000 seconds experiment

- 4011 time. The largest maximum task execution time was observed at 930 seconds with a value of
- 4012 2088 microseconds (a threefold increase above the average). Impacts to the measured inter-
- 4013 packet delay between the PLC and Station 2 were also observed during this period. Further
- 4014 analysis revealed Nessus was actively scanning the machining stations while these PLC impacts 4015 were observed. It is hypothesized that the impacts were caused by interruptions to Modbus TCP
- 4016 communications between the supervisory PLC and the machining stations, likely due to
- 4017 increased resource utilization on the machining stations.



4019

4020Figure 4-33 - Plots showing the maximum PLC task execution time during the experiment (left) and during4021the period of measured impact (right). While the Nessus tool was active, the PLC experienced periods of4022fluctuating and increased task execution time.

4023 A slight increase of the part production time mean and variance were observed during this 4024 experiment, but they are not statistically significant.





4028

#### 4029 **4.10.6.2 Experiment CL006.2**

- 4030 "Credentialed checks" were performed on the two CRS networks: Supervisory LAN
- 4031 (192.168.0.0/24) and Control LAN (192.168.1.0/24). The credentials gave Nessus access to the
- 4032 following hosts and ICS devices: the engineering workstation (POLARIS), the robot driver
- 4033 (MINTAKA), the robot controller vController1, and the robot controller vController2, and the
- 4034 four machining stations.
- 4035 The Nessus GUI reported scanning was active between 200 to 1500 seconds (experiment time).





4037<br/>4038Figure 4-35 - Time series plot showing the quantity of network traffic transmitted and received by the Nessus<br/>tool during the experiment, with the most prominent activity from 200 to 600 seconds.



4040
 4041
 4041
 4041
 4042
 4042
 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.

- 4043 Multiple performance impacts were observed while the Nessus tool was actively scanning the
  4044 HMI and machining stations. Loss-of-view events likely occurred (but were not directly
  4045 observed) on the HMI multiple times during the experiment, as evident by the large inter-packet
- 4046 delay measurements between the HMI and Station 1 shown in Figure 4-37. Two large round-trip

4047 time transients (over 500 milliseconds) were observed on TCP traffic between the HMI and4048 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.

4053 Performance impacts to the supervisory PLC task execution time were observed while the
 4054 Nessus tool was actively scanning. Relatively large fluctuations of the average task execution

4054 The substant tool was actively scanning. Relatively large fluctuations of the average task execution 4055 time and the maximum task execution time were observed from 250 to 600 seconds experiment

time and the maximum task execution time were observed from 250 to 000 seconds experime

time (see Figure 4-38). Impacts to the measured inter-packet delay between the PLC and Station

4057 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

4060 PLC and the machining stations, likely due to increased resource utilization on the machining

4061 stations.



4064Figure 4-38 - Plots showing the maximum (top) and average (bottom) PLC task execution time during the4065experiment (left) and during the period of measured impact (right). While the Nessus tool was active, the PLC4066experienced periods of fluctuating and increased task execution time.

4067 Since Nessus was configured to perform an authenticated scan, vController1 and vController2
4068 both hosts experienced increased utilization of resources (i.e., CPU, disk, memory).





4071 4072 4073 4074 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.

4075 A slight increase of the part production time variance was observed during this experiment, but it 4076 is not statistically significant.

4077



4080

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.

#### 4084 **4.10.7** Link to Entire Performance Measurement Data Set

- 4085 CL006.1-NessusNetworkScan.zip
- 4086 CL006.2-NessusAuthenticatedScan.zip

#### 4087 **4.11 NamicSoft**

#### 4088 **4.11.1 Technical Solution Overview**

- 4089 NamicSoft Scan Report Assistant, a parser and reporting tool for Nessus, Burp, Nexpose
   4090 OpenVAS and NCATS.<sup>20</sup>
- 4091 **4.11.2 Technical Capabilities Provided by Solution**
- 4092 NamicSoft provides components of the following Technical Capabilities described in Section 64093 of Volume 1:
- Vulnerability Management

#### 4095 **4.11.3 Subcategories Addressed by Implementing Solution**

4096 ID.RA-1, DE.CM-4, RS.MI-3

<sup>&</sup>lt;sup>20</sup> Namicsoft <u>https://www.namicsoft.com/</u>



## 4097 **4.11.4** Architecture Map of Where Solution was Implemented

# 4099 **4.11.5** Installation Instructions and Configurations

4100 Details of the solutions implemented:

Name	Version
NamicSoft Scan Report Assistant	3.5.0

4101

4102 <u>Setup:</u>

Download NamicSoft from <u>https://www.namicsoft.com</u> and run the installer on a Windows
PC. NamicSoft is currently supported on 64-bit Windows with .Net Framework 4.5 installed
The installation is tied to a user account. Any changes made by a user would not be visible to a different user logging in to the same system.

4107 • If using for the first time, the installation will prompt for a license file. If a license is not entered, it runs in free mode. The free mode is limited to five hosts.

• NamicSoft was installed on the Scanning laptop used for Nessus scanning.

## 4110 <u>Configuration for reporting Nessus scans:</u>

- Export a Scan Report of Nessus format from the Nessus web interface.
- 4112 Launch NamicSoft Report Assistant. Click Import on left-side explorer, select Nessus
- 4113 Click on **Choose** button to import files

4			NamicSoft Scan Report Assistant	_ 🗆 X
		File Settings Tools	About	
8	Dashboard	Import		
	Overview	Tool	Nessus	•
	Vulnerability age	Description	Import your Nessus scan results to using Nessus export to XML (.nessus format). Nessus file format v2 supported.	
		Choose file(s) to import	Choose 📾	
윪	Hosts	Number of files to read	1	
		Files read	0	
⊞	Vulnerabilities	Import vulnerabilities	with the following severities	~
		Informational		
Ð	Import	Low 🗹		
	_	Medium 🔽		
G	Export	High 🔽		
	·			
1	Report	Status		
		Elapsed time 0		
٩	Actions	Status		
		Job Id File	File size (kB) Time to import Status Hosts Vulnerabilities	
				Import
Versi	on 3.0.5.0			mport

- 4115
- 4116
- 4117
- Browse to the Nessus scan report. Under Import Vulnerabilities with following
- 4119 vulnerabilities, Check / Un-check whichever severity of vulnerabilities you wish to be
  4120 included in the report. Click Import
- 4121 The below image shows "Informational" type being excluded. When the Import finishes, the
  4122 Status bar should display All files read
- 4123

-			NamicSoft Scan Report Assistant	_ 🗆 🗙
	Dashboard	File Settings Tools	About	
	Dashboard	Import		
	Overview	Tool	Nessus	•
	Vulnerability age	Description	Import your Nessus scan results to using Nessus export to XML (.nessus format). Nessus file format v2 supported.	
		Choose file(s) to import	Choose 🕋	
윩	5 Hosts	Number of files to read	1	
		Files read	1	
•	Vulnerabilities	Import vulnerabilities	; with the following severities	^
5	Import	Informational		
		Low 🔽		
	Export	High		
	• Export	Critical 🔽		
E	Report	Status		
		Elapsed time 7		
٩	Actions	Status All files r	ead	
		Job Id File	File size (kB) Time to import Status Hosts Vulnerabilities	
Vers	ion 3.0.5.0			Import

4125 Upon completion of Import, go to Hosts page to view all the hosts level summary. Similarly, clicking on Vulnerabilities page shows all the vulnerabilities

4				NamicSoft Scan Repo	rt Assistant				
		File Settings Tool	s About						
:	Dashboard	Name	IP	Operating System	MAC	NetBIOS	FQDN	System Type	Report Na
	Overview	machining-station-4	192.168.1.104	Linux Kernel 4.4.54-ti-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 <sup>↑</sup>
	Vulnerability age	machining station 2	102 168 1 102	Linux Kornel 4.4 E4 ti c02 on Dahing 8.7	P0-D5-00-F4-74-42	machining station 2	station? Ion Joh		Dehatias E
윪	Hosts	machining-station-o	192.100.1.103	Linux Kentel 4.4.54-1195 on Debian 6.7	B0:D5:CC:FA:7A:45 B0:D5:CC:FA:7A:45 B0:D5:CC:FA:7A:48	macriming-station-3	stauono.ian.iau	general-purpose	RODUICS_E
		machining-station-2	192.168.1.102	Linux Kernel 4.4.54-ti-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
Ħ	Vulnerabilities	machining-station-1	192.168.1.101	Linux Kernel 4.4.54-ti-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
Ð	Import	192.168.1.10	192.168.1.10						Robotics_E
G	Export	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
A	Report	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-netgearsw.lan.lab	192.168.0.239	Linux Kernel 2.4	A0:63:91:70:D5:6F A0:63:91:70:D5:71		crs-netgearsw.lan.lab	general-purpose	Robotics_E
٩	Actions	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 ↓
Vers	ion 3.0.5.0	Total: 18 Selected: 0							100

4128

*				NamicSoft S	Scan Report Assistant			_ 🗆 X
		File Settings To	ools About					
-	Dashboard						Optimize colums f	or ALL 🔻
	Overview	Host name	Host Name	Synposis	Description	Solution	Severity	Severity Number
	Vulnerability age	machining-stat ^	station4.lan.lat	The remote Debian host is missing	Hubert Kario discovered that GnuTL	Upgrade the gnutis28 packages.	Medium	2 *
		machining-stat	station4.lan.lat	The remote Debian host is missing	Joern Schneeweisz discovered that	Upgrade the git packages.	Medium	2
ᇮ	Hosts	machining-stat	station4.lan.lat	The remote Debian host is missing	Several vulnerabilities have been for	Upgrade the apache2 packages.	High	1
		machining-stat	station4.lan.lat	The remote Debian host is missing	Two vulnerabilities were discovered	Upgrade the curl packages.	Medium	2
▦	Vulnerabilities	192.168.1.10	station4.lan.lat	The remote Debian host is missing	It was discovered that an integer ov	Upgrade the icu packages.	Medium	2
		mintaka	station4.lan.lat	The remote Debian host is missing	It was discovered that libXcursor, a	Upgrade the libxcursor packages.	Medium	2
Ð	Import	vController2	station4.lan.lat	The remote Debian host is missing	Jeffrey Altman, Viktor Duchovni anc	Upgrade the samba packages.	Medium	2
		vController1	station4.lan.lat	The remote Debian host is missing	Jayakrishna Menon and Christophe	Upgrade the affected packages.	High	1
Ŀ.	Export	crs-netgearsw.	station4.lan.lat	The remote Debian host is missing	An information disclosure vulnerabi	Upgrade the bluez packages.	Low	3
	LAPOIT	192.168.0.120	station4.lan.lat	The remote Debian host is missing	Several vulnerabilities were discove	Upgrade the libxml2 packages.	Critical	0
	<b>.</b> .	hmi.lan.lab	station4.lan.lat	The remote Debian host is missing	CVE-2018-5740 The 'deny-answer-a	Upgrade the affected packages.	High	1
h	Report	192.168.0.60	station4.lan.lat	The remote Debian host is missing	Multiple vulnerabilities have been di	Upgrade the jasper packages.	Medium	2
		plc-robotics.lar	station4.lan.lat	The remote Debian host is missing	Several vulnerabilities have been dis	Upgrade the linux packages.	High	1
*	Actions	polaris	station4.lan.lat	The remote Debian host is missing	Felix Wilhelm, Fermin J. Serna, Gabi	Upgrade the dnsmasq packages.	High	1
_		192.168.0.12	station4.lan.lat	The remote Debian host is missing	The cPanel Security Team reported	Upgrade the perl packages.	Medium	2
		NessusVM,Ian. 🗸	<del>«</del>					*
Versi	on 3.0.5.0	Total: 857 Displaye	ed: 120 Selected	0				

4129

• To mark a Vulnerability as Fixed, select the Vulnerability >> Right Click >> Fixed.

4				Namics	Soft Scan Report Assistant				_ □
		File Settings 1	Tools About						
8	Dashboard							Optimize colums for	ALL
	Overview	Host name	Host Name	Synposis	Description		Solution	Severity	Severity Numb
	Vulnerability age	machining-stat ^	station4.lan.lat	The remote Debian host is n		nuTL	Upgrade the gnutIs28 packages.	Medium	2
		machining-stat station4.lan.lat The remote Debia		The remote Debian host is n	n Edit		Upgrade the git packages.	Medium	2
緣	Hosts	machining-stat	station4.lan.lat	The remote Debian host is n	Delete In for U		Upgrade the apache2 packages.	High	1
	_	machining-stat	station4.lan.lat	The remote Debian host is n	Vulnerability fixed	ered	Upgrade the curl packages.	Medium	2
	Vulnerabilities	192.168.1.10	station4.lan.lat	The remote Debian host is miss	ing It was discovered that an inte	ger ov	Upgrade the icu packages.	Medium	2
		mintaka	station4.lan.lat	The remote Debian host is miss	ing It was discovered that libXcur	sor, a	Upgrade the libxcursor packages.	Medium	2
Ð	Import	vController2	station4.lan.lat	The remote Debian host is miss	ing Jeffrey Altman, Viktor Duchov	ni and	Upgrade the samba packages.	Medium	2
		vController1	station4.lan.lat	The remote Debian host is miss	ing Jayakrishna Menon and Chris	tophe	Upgrade the affected packages.	High	1

4132 4133

- Under Actions, click on Save Workspace. Ensure to Save your workspace after every
   change made. When running NamicSoft the next time, you can load this saved workspace
   file.
- 4137
- To generate a Report, click on **Report.** You can select one of the default reporting templates from the list or create a custom one. To use a default template, select one from the list >>
   Create Report.



4142 • To view the Report, click **Open Report.** 

4				1	NamicSoft	Scan Report A	Assistant			_ 🗆 X
::	Dashboard	File Settings Tools About Word Report								
	Overview	Create Word Report Other Se	ettings							
	Vulnerability age	Load default 🗃 Browse 🗁 C:\Program Files (x86)\NamicSoft Scan Report Assistant\templates								9 Ø
		Host summary table with e.	Exam	ple outpu	it					ICS-LAB-Host summa
쁆	Hosts	ICS-LAB-Host summary		NamicSoft Sca	n Report Assistant	Report SQL template Exc	mple – <u>http://www.nar</u>	micsoft.com		Author: NamicSoft/Michael Petters A summary table of each host's vulnerabilities. The total CVSS
⊞	Vulnerabilities	One table per vulnerability v	One table per vulnerability v This is an example template from Namiciant. This template presents an overview of the xamming result for each host. The total CVSS score is also presented for each host.							
		Remediations with affected		You need to enter desi about how to enter de	gn mode to edit th sign mode.	is template. See <u>https://</u>	www.namicsoft.com/dc	oc/enter-design-mode-micro	soft-word/ for information	Version: 1.0 News in this version:
Ð	Import	Repeat information for eacl		NamicSoft will populat https://www.namicsof content controls.	e data into this ter t.com/doc/conten	nplate by SQL queries de t-controls/ for more info	ined in the content cor mation about available	trois below. See content controls in Namic5	oft and how to edit the	- Settings
ŀ	Export	Vulnerabilities with highest		IP 192.168.0.105 192.168.0.107 192.168.0.109 192.168.0.110 192.168.1.14	Low 7 1 1 1 0	Medium 16 0 0 0 1	High 6 0 0 0 0 0	Critical 9 2 0 0 0	Total CVSS 224.1 23.2 3.2 3.2 3.2 5	New line after table rows: True
8	Report	Plugin overview (see the setting: Active Pre-hooks: 0 Active Post-hooks: 0	s tab for m	nore informatio	in) ———					
۹	Actions	- Status	t saved in	C:\Users\Adm	inistrator\D	ownloads\Hos	t Summary.do	cx		
		Time to create report Omin and 5	s							
Versi	on 3.0.5.0									Open Report Create Report

4143

To create a custom template, copy one of the template files located under C:\Program
 Files(x86)\NamicSoft Scan Report Assistant\templates and save it to a different folder.
 Open the copied file in MS Word to begin editing. The image below shows a customized
 template file created for CRS system. This report generates a summary of hosts and their

4148 respective vulnerabilities based on the Severity level.

	U.S. Department	t of Commerce	Robotics System Vulnerability Assessment Report					
		Robotics	System Vulne	erability Scan S	Summary			
D	Hostname	low	Medium	High	Critical	Zotal CV/SS		
r DummyValue	DummyValue	DummyValue	DummyValue	DummyValue	DummyValue	DummyValue		
ELECT DISTINCT : JueryTable y WHI	x.ip, x.hostname, (S ERE severitynumber	ELECT COUNT(*) FR r=2 AND y.ip=x.ip),(\$	OM queryTable y WHI SELECT COUNT(*) FRO	ERE severitynumber=3 M queryTable y WHER	AND y.ip=x.ip), (SELEC E severitynumber=1 A	T COUNT(*) FROM ND y.ip=x.ip), (SELECT		
SELECT DISTINCT queryTable y WHI COUNT(*) FROM r.ip=x.ip) FROM q	x.ip, x.hostname, (S ERE severitynumber queryTable y WHER µueryTable x ORDER	ELECT COUNT(*) FR r=2 AND y.ip=x.ip),(\$ E severitynumber=( BY ipSortValue	OM queryTable y WHI SELECT COUNT(*) FRO D AND y.ip=x.ip), (SELE	ERE severitynumber=3 M queryTable y WHER CT ROUND(SUM(cvssB	AND y.ip=x.ip), (SELEC E severitynumber=1 A aseScore),1) FROM qu	T COUNT(*) FROM ND y.ip=x.ip), (SELECT eryTable y WHERE		
ELECT DISTINCT : jueryTable y WHI :OUNT(*) FROM q :.ip=x.ip) FROM q	x.ip, x.hostname, (S ERE severitynumber queryTable y WHER ueryTable x ORDER of each host's vulne	ELECT COUNT(*) FR (=2 AND y.ip=x.ip),(t (E severitynumber=( BY ipSortValue erabilities. The total	OM queryTable y WHI SELECT COUNT(*) FRO D AND y.ip=x.ip), (SELE CVSS base score is also	ERE severitynumber=3 M queryTable y WHER CT ROUND(SUM(cvssB o presented for each h	AND y.ip=x.ip), (SELEC E severitynumber=1 A aseScore),1) FROM qu ost.	T COUNT(*) FROM ND y.ip=x.ip), (SELECT eryTable y WHERE		
ELECT DISTINCT : jueryTable y WHI :OUNT(*) FROM ( :ip=x.ip) FROM q : summary table .0	x.ip, x.hostname, (S ERE severitynumber queryTable y WHER ueryTable x ORDER of each host's vulne	ELECT COUNT(*) FR (=2 AND y.jp=x.jp),(5 (E severitynumber=( BY jpSortValue erabilities. The total	OM queryTable y WHi SELECT COUNT(*) FRO D AND y.ip=x.ip), (SELE CVSS base score is also	ERE severitynumber=3 M queryTable y WHER CT ROUND(SUM(cvssB o presented for each h	AND y.ip=x.ip), (SELEC E severitynumber=1 A aseScore),1) FROM qu iost.	T COUNT(*) FROM ND y.ip=x.ip), (SELECT eryTable y WHERE		
SELECT DISTINCT : yueryTable y WHI COUNT(*) FROM ( r.ip=x.ip) FROM ( summary table 0 JamicSoft/Micha	x.ip, x.hostname, (S ERE severitynumber queryTable y WHER ueryTable x ORDER of each host's vulne el Pettersson Soluti	ELECT COUNT(*) FR (=2 AND y.jp=x.jp),(* (E severitynumber=( BY jpSortValue erabilities. The total	OM queryTable y WHI SELECT COUNT(*) FRO D AND y.ip=x.ip), (SELE CVSS base score is also	ERE severitynumber=3 M queryTable y WHER CT ROUND(SUM(cvssB o presented for each h	AND y.ip=x.ip), (SELEC E severitynumber=1 A aseScore),1) FROM qu rost.	T COUNT(*) FROM ND y.ip=x.ip), (SELECT eryTable y WHERE		

- 4151
- Detailed instructions for creating custom reports are available on the NamicSoft website
   under <a href="https://www.namicsoft.com/doc/content-controls/">https://www.namicsoft.com/doc/content-controls/</a>
- Save your changes and give the file a suitable name. Copy this file back to the "Templates"
- 4155 directory. For instance, the below image shows our customized file ICS LAB Host
- 4156 **Summary** copied back to the templates folder.

i I 💽 🚺 = I	t	emplates			D X
File Home Shar	e View				~ (
🕣 💿 🔹 🕇 📕 « I	.ocal Disk (C:)	Scan Report Assistant	▶ templates ∨ C	Search templates	,
☆ Favorites	Name	Date modified	Туре	Size	
Desktop	퉲 images	4/11/2019 3:20 PM	File folder		
📜 Downloads	Content control bar_chart	8/19/2017 8:55 PM	Office Open XML Document	55 KB	
🔛 Recent places	Content control pie_chart	8/19/2017 9:01 PM	Office Open XML Document	54 KB	
sec_550	Content control raw_table_columns	8/19/2017 9:03 PM	Office Open XML Document	36 KB	
	Content control raw_table_rows	8/19/2017 9:06 PM	Office Open XML Document	37 KB	
🖳 This PC	Content control raw_table_rows_v2 (mult	8/19/2017 9:09 PM	Office Open XML Document	38 KB	
C on PN108214	Content control repeat	8/19/2017 9:12 PM	Office Open XML Document	35 KB	
hesktop	Dashboard	10/28/2017 11:44	Office Open XML Document	44 KB	
Documents	Five most vulnerable hosts	8/19/2017 9:19 PM	Office Open XML Document	38 KB	
🐌 Downloads	Five most vulnerable Linux operating syst	8/19/2017 9:24 PM	Office Open XML Document	39 KB	
Music	Host compliance report	8/8/2017 9:00 PM	Office Open XML Document	37 KB	
E Pictures	Host information table	8/19/2017 9:27 PM	Office Open XML Document	36 KB	
Videos	Host summary table with exploitable vul	8/20/2017 8:46 PM	Office Open XML Document	36 KB	
🏭 Local Disk (C:)	Host summary table	8/19/2017 9:33 PM	Office Open XML Document	35 KB	
	Host table with affected vulnerabilities	8/19/2017 9:54 PM	Office Open XML Document	39 KB	
🗣 Network	CS-LAB-Host summary	9/18/2018 10:59 AM	Office Open XML Document	47 KB	
	One multi-column table per vulnerability	8/19/2017 9:52 PM	Office Open XML Document	38 KB	
	One table per vulnerability with affected	8/19/2017 9:38 PM	Office Open XML Document	37 KB	
	Dpen ports	12/9/2017 8:46 PM	Office Open XML Document	37 KB	
	Remediations with affected hosts	12/27/2017 8:28 PM	Office Open XML Document	40 KB	

4158

4159 Launch NamicSoft again. The custom report should now appear under the list. Select it and click on Create Report.

4				NamicSof	t Scan Report .	Assistant			_ 🗆 X
::	Dashboard	File Settings Tools About Word Report							
	Overview	Create Word Report Other Se	ettings						
	Vulnerability age	Load default 🖨 🛛 Brows	9 Ø						
		Host summary table with e	Example o	utput					ICS-LAB-Host summa
쁆	Hosts	ICS-LAB-Host summary	A Na	nicSoft Scan Report Assista	nt Report SQL template Ex	ample – <u>http://www.na</u>	micsoft.com	L	Author: NamicSoft/Michael Petters A summary table of each host's vulnerabilities. The total CVSS
⊞	Vulnerabilities	One table per vulnerability v	This is an er also calcula	ample template from Nam ed per host.	icSoft. This template prese	nts an overview of the :	scanning result for each host	. The total CVSS score is	base score is also presented for each host.
		Remediations with affected	You need to about how	enter design mode to edit o enter design mode.	this template. See <u>https://</u>	www.namicsoft.com/d	loc/enter-design-mode-micro	soft-word/ for information	Version: 1.0 News in this version:
Ð	Import	Repeat information for eacl	NamicSoft https://www content con	III populate data into this wnamicsoft.com/doc/cont trols.	emplate by SQL queries de ent-controls/ for more info	fined in the content co rmation about available	ntrois below. See e content controls in Namic5	oft and how to edit the	- Settings
G	Export	Vulnerabilities with highest	192.168.0. 192.168.0. 192.168.0. 192.168.0. 192.168.0. 192.168.1.4	Low 05 7 07 1 09 1 10 1 4 0	Medium 16 0 0 1	High 6 0 0 0 0 0	Critical 9 2 0 0 0	Total CVSS 234.1 23.2 3.2 3.2 3.2 5	New line after table rows: True
•	Report	Plugin overview (see the setting Active Pre-hooks: 0 Active Post-hooks: 0	s tab for more info	rmation) —					
۹	Actions	Status Done, repo	rt saved in C:\User	s\Administrator	Downloads\Ho	st Summary.do	ocx		
		Time to create report 0min and 5	s						
Versi	on 3.0.5.0								Open Report Create Report

- 4161
- The output should appear as per your changes.

	Standards and Te U.S. Department of C	Commerce Robotic	Robotics System Vulnerability Assessment Report Robotics System Vulnerability Scan Summary			
IP	Hostname	Low	Medium	High	Critical	Total CVS
192.168.0.2	192.168.0.2	0	7	0	0	38.6
192.168.0.11	NessusVM.lan.lab	2	4	0	0	28
192.168.0.12	192.168.0.12	2	9	1	0	59.8
192.168.0.20	polaris	2	6	9	2	118.9
192.168.0.30	plc- robotics.lan.lab	0	1	1	0	12.5
192.168.0.60	192.168.0.60	0	4	1	0	27.5
192.168.0.239	crs- netgearsw.lan.lab	0	2	1	0	18.3
192.168.1.3	vController1	4	63	49	8	718.4
192.168.1.4	vController2	4	63	49	8	718.4
192.168.1.5	mintaka	3	23	40	6	477.6
192.168.1.101	machining- station-1	3	63	50	5	660.5
192.168.1.102	machining- station-2	3	63	50	5	660.5
192.168.1.103	machining- station-3	3	63	50	5	660.5
192.168.1.104	machining- station-4	3	62	50	5	653.7

- To report on Vulnerabilities remediated based off the previous vulnerability scans, use the
- 4166 "Compare Workspaces" feature under Action Menu
- 4167
  4167
  4168
  4168
  4169
  Load Nessus result from your previous scan. Save as a workspace.
  Clear the workspace in the GUI (or restart NamicSoft)
  Load Nessus results from the latest scan
- 4170
   Open Actions --> Compare workspaces. Choose Compare with current workspace
   4171
   o Open Actions --> Compare workspaces. Choose Compare with current workspace
   and point Workspace 2 to your workspace saved earlier.
- 4172 Choose Excel output file (target)
- 4173 O Click "Compare Workspaces"

4175

# 4176 **4.11.6 Highlighted Performance Impacts**

- 4177 Two performance measurement experiments were performed for the vulnerability management4178 technical capability while the manufacturing system was operational:
- 4179 1. <u>CL011.1</u> Patches are installed on network hardware.
- 4180 2. <u>CL011.2</u> Patches are installed on servers and ICS devices (e.g., PLC).
- 4181
- 4182 **4.11.6.1 Experiment CL011.1**
- 4183 The firmware and operating systems for all three of the networking devices in the CRS (one
- 4184 router, two switches) were updated and patched to the most current versions. The firmware was
- 4185 updated while the CRS system was not operational.
- 4186 A slight increase of the part production time mean was observed during this experiment but is4187 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.

4191

4188

# 4192 **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.

4198 A decrease in the average inter-packet delay (IPD) was observed on the PLC Modbus TCP

4199 communications to Station 2. Further analysis revealed that the performance impact also showed

4200 a relatively unstable IPD, as compared to the baseline (see Figure 4-42). These new performance

4201 characteristics were consistent throughout the experiment. An increase in the average IPD was

4202 also observed on the Modbus TCP communications between Robot 2 and the PLC. Again,

4203 further analysis revealed that the performance impact showed a relatively unstable IPD, as 4204 compared to the baseline (see Figure 4-43).



4206Figure 4-42 - Time series plot displaying the inter-packet delay of Modbus TCP traffic between the PLC and4207Station 2, as measured during the baseline CL001.2 and experiment CL011.2. Note the relatively constant4208baseline average delay of around 0.050 sec., while the experimental delay is decreased to an average of 0.0424209sec. with large deviations.



4210

4211 Figure 4-43 - Stem plot displaying the inter-packet delay of Modbus TCP traffic between Robot 2 and the PLC,

4212 as measured during the baseline CL001.2 and experiment CL011.2. Note the relatively constant baseline 4213 average delay of around 0.016 sec., while the experimental delay is increased to an average of 0.019 sec. and 4214 relatively unstable.

- 4215 A small increase in the average robot job actuation time was observed on Robot 1 for Job 103
- 4216 (see Figure 4-44). No other increases were observed for any of the other jobs. This added
- 4217 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.

4222 Performance impacts to the supervisory PLC task execution time were observed after the PLC

4223 operating system was updated. The task execution time increased from an average of around 330

4224 µsec. during the baseline to around 690 µsec., with the maximum task execution time now

4225 consistently exceeding 2000 µsec. (see Figure 4-45).

4226 CPU utilization on vController2 also increased from an average of around 2% during the

4227 baseline to an average of around 7% during the experiment (consistent with the increase

4228 vController1 had experienced in previous experiments). This CPU increase was observed for all

4229 the experiments performed after CL011.2 but was not consistent with vController1, which

4230 measured a consistent average of 2% CPU utilization for CL011.2 and all subsequent

4231 experiments.

4232



4235 Figure 4-45 - Plots showing the maximum (top) and average (bottom) PLC task execution time during the 4236 4237 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.



4239 Figure 4-46 - Time series plots showing the CPU utilization ratio for vController2 during the CL011.2 4240 experiment and the CL001.2 baseline (left), and a detailed view of the same data (right).

- 4241 A slight increase of the part production time mean was observed during this experiment, but it is
- 4242 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.

- 4246 **4.11.7** Link to Entire Performance Measurement Data Set
- 4247 CL011.1-PatchesNetworkHardware.zip
- 4248 CL011.2-PatchesServersICSDevices.zip

#### 4249 **4.12 GTB Inspector**

#### 4250 **4.12.1 Technical Solution Overview**

4251 GTB Inspector by GTB Technologies is a DLP solution that has been evaluated in our lab 4252 environment for low baseline manufacturing profile. GTB Inspector's built in ability to detect, 4253 log, and block network traffic trying to leave premise. Inspector detects and blocks FTP, Email, HTTP, HTTPS (SSL/TLS), Finger Printed files, USB protection, and other configured 4254 4255 exfiltration methods. GTB Inspector is the main component that analyzes all network traffic and 4256 depending on the configuration Bridge (In-Line), Monitoring (OOL), TAP, Transparent Proxy 4257 (TPROXY), and Load Balancing if required. GTB Central Console which is the device Inspector 4258 reports back to, so there is always a log of violation that occurred. Central Console allows for 4259 groups and escalation paths depending on the alerting required.

- 4260 GTB is configured within the corporate network. This option was chosen to ensure we could get 4261 the best protection for the entire environment.
- 4262 All DLP products have a high cost to implement, but GTB Technologies provides a product that 4263 can grow as your company does.
- 4264 Once installed and configured system requires little maintenance.
- Install time within the lab was approximately 16 hours for configuration, but for simple datacapture setup took about an hour.

#### 4267 **4.12.2 Technical Capabilities Provided by Solution**

- 4268 GTB Inspector provides components of the following Technical Capabilities described in4269 Section 6 of Volume 1:
- Data Loss Prevention

#### 4271 **4.12.3** Subcategories Addressed by Implementing Solution

4272 PR.DS-5

#### 4273 **4.12.4** Architecture Map of Where Solution was Implemented









# 4288 Hyper-V Install Configuration

• Create two virtual machines (See below for current specification of our environment)

4290	• GTB Inspector
4291	<ul> <li>VHDX D:\Hyper-V\GTB InspectorVirtual Hard Disks\GTB Inspector.vhdx</li> </ul>
4292	<ul> <li>Memory – 16GB (16384MB)</li> </ul>
4293	<ul> <li>Processor – 4 CPU</li> </ul>
4294	<ul> <li>Network Adapter</li> </ul>
4295	<ul> <li>"vswitch_TestBed_LAN" Management Port</li> </ul>
4296	• Management port IP is (10.100.0.175)
4297	• "Eth2 for GTB Inspector" Connects to Monitor Port 1 on Tap
4298	Device
4299	• "Eth3 for GTB Inspector" Connects to Monitor Port 2 on Tap
4300	Device
4301	• GTB Central Console
4302	<ul> <li>VHDX D:\Hyper-V\GTB Central Console\Virtual Hard Disks\GTB Central Console.vhdx</li> </ul>
	239

4303	<ul> <li>Memory – 16GB (16384MB)</li> </ul>
4304	Processor – 4 CPU
4305	<ul> <li>Network Adapter</li> </ul>
4306	• "vswitch TestBed LAN" Management Port / Connection
4307	• Management Port / Connection IP is (10.100.0.176)
4308	Install Instructions for Each Virtual Machine and any additional configuration
4309	• Inspector
4310	• See install guide for most updated instructions, or attachment below. Changes
4311	made within our environment are included below.
4312	• Each network connection was installed and rebooted to ensure they were assigned
4313	correct name / location, and if not, this command can be used to rename the
4314	network to reflect and needed changes. /usr/local/gtb/libexec/manage_nics -i ethX -o ethX
4315	(This syntax is included within installation guide)
4316	• IP Address (10.100.0.175)
4317	• Hostname = gtbinspector / gtpinspector.lan.lab
4318	• Created DNS A record for "gtbinspector" along with reverse lookup
4319	• Configured LDAP integration with Active Directory (10.100.0.17)
4320	• UPN is required for username
4321	• Configured email
4322	<ul> <li>SMTP Server Hostname (postmark.nist.gov)</li> </ul>
4323	<ul> <li>Send email from (<u>GTBInspector@nist.gov</u>)</li> </ul>
4324	<ul> <li>SMTP Server Port (25)</li> </ul>
4325	• Check and ensure LAN and WAN interfaces are configured for eth2 (WAN) eth3
4326	(LAN)
4327	<ul> <li>Configuration tab, Network, #-3 and #-4</li> </ul>
	<b>2</b>
	GTB Inspector
4328	O Installation Guide.pdf
4329	Central Control
4330	• See install guide for most updated instructions or attachment below. Changes
4331	made within our environment are included below.
4332	• IP Address (10.100.0.176)
4333	• Hostname = gtbcc / gtbcc.lan.lab
4334	<ul> <li>Created DNS A record for "gtbcc" along with reverse lookup</li> </ul>
4335	• Configured LDAP integration with Active Directory (10.100.0.17)
4336	• UPN is required for username
4337	• Configured email
4338	<ul> <li>SMTP Server Hostname (postmark.nist.gov)</li> </ul>
4339	<ul> <li>Send email from (<u>GTBInspector@nist.gov</u>)</li> </ul>
4340	<ul> <li>SMTP Server Port (25)</li> </ul>



4341	O Installation Guide.pdf
4342	Install information for VMware
4343	• Install
4344	<ul> <li>Installed a separate physical machine with vSphere (10.100.0.180) for</li> </ul>
4345	testing since problems were observed with Hyper-V ability to block rule
4346	violations with HTTP/HTTPS traffic.
4347	<ul> <li>Configured two network cards in vSphere for pass thru access. This was</li> </ul>
4348	completed to give the virtual machine access to physical network cards to
4349	eliminating possible configuration issues being observed in Hyper-V.
4350	(Will try to confirm if possible still exist with Hyper-V since new release
4351	from GTB has been released)
4352	<ul> <li>GTB's Inspector (10.100.0.181) is currently at release 15.4 and contains</li> </ul>
4353	an options under <b>"Configuration → Network "labeled</b> (Failover Mode).
4354	In our environment this option is set to "NO" since we don't have a
4355	bypass card installed. This setting allows all web traffic to be filter via
4356	scanning engine.
4357	14     Failover mode     No     Select "Yes" to enable failover mode of the Bypass Network Card in Bridge and TPROXY. Select "No" to enable fail closed mode.
4358	<ul> <li>Email filtering is designed to use "MTA" from Inspector and then</li> </ul>
4359	forward along to intended recipient after been scanning for any rule
4360	violations.
4361	<ul> <li>Added GTTB Certificate to "Default Domain Policy" so any machine</li> </ul>
4362	within the domain will update with the required Trusted Certificate
4363	Authority so as not to get a warning message. (Confirmed working)
4364	
4365	<ul> <li>Lesson learned:</li> </ul>
4366	<ul> <li>Microsoft Hyper-V solution detects and logs traffic, however even</li> </ul>
4367	when configured for blocking, only detection occurs. Support has
4368	indicated that this is since we're not using a bypass network card
4369	stated earlier with a physical box.
4370	
43/1	Performance Impact:
4372	I his tool has not been configured and ran against ICS enclaves
43/3	currently, so there has been no performance impact that were
43/4	aware of.
4375	
4376	
4377	

- 4378 Specific configuration steps for GTB's Inspector and Central Console
- 4379 within Testbed environment
- 4380 This document contains information for configuration within our environment. If scanning email
- 4381 for content violation, you'll need to configure email clients to point SMTP to 10.100.0.175
- 4382 (Inspector MTA) for email scanning. For additional configuration information please see
- 4383 vendors Administrator Guides which are included in download package from vendor.

## 4384 Inspector

4385 Generating and applying License: 4386 • Generating o Click on middle top web page once logged into Inspector 4387 License expires in 349 days 4388 You will now be directed to a page that allows you to download, email, or 4389 4390 upload a license file. 4391 • License files should be emailed to support@gttb.com . Support will reply 4392 with an updated file to be uploaded. When to generate a new license file 4393 • Anytime a network change effects the MAC (Media Access Control) address for 4394 0 4395 Inspector you'll need to generate a new license key an email support@gttb.com. Before emailing change the extension from ".dat" to ".txt". Example: Inspector 4396 4397 - "7-31-2018-sysinfo\_inspector.dat to 7-31-2018-sysinfo\_inspector.txt". This 4398 change may be required if your email provider blocks ".dat" file extension 4399 0 4400 **Configuration Setting** • • Login into GTB Inspector web page and click "Configuration" tab. 4401 Rule Viewer Quarantine Configuration Logs Statistics Administration Events 4402 4403 • All setting are accessible via "Groups" located on left side of webpage. 4404 • Central Console = "gtbcc.lan.lab"

Network

#### CSF MFG PROFILE LOW SEC LVL EXAMPLE IG DISCRETE-BASED MFG SYSTEM USE CASE

4405

# • Network = Screenshot below

1	Inspector location	GTBInspector.lan.lab	The location or hostname the Inspector appliance.
2	Deployment mode	TPROXY	Deployment mode of the Inspector: "OOL" for Out-of-Line, "BRIDGE" for Inline, "TAP" for a Tap connection, "TPROXY" for Transparent Proxy.
3	LAN interface	eth2	LAN interface (ie. eth0, eth1, eth2, or eth3) where the network traffic is coming from. It is being used in all Inspector modes.
4	WAN interface	eth3	WAN interface (ie. eth0, eth1, eth2, or eth3) where the network traffic is coming to. It is being used in TAP, BRIDGE, and TPROXY modes.
5	OOL LAN	10.100.0.0/24, 172.16.3.0/24	List of source IP addresses, subnets or MAC addresses separated by commas which are inspected in the OOL mode.
6	OOL WAN		List of destination IP addresses, subnets or MAC addresses separated by commas which are inspected in the OOL mode. An empty entry accepts all WAN packets.
7	TPROXY LAN	10.100.0.0/20,192.168.0.0 /20,172.16.0.0/20	List of source IP addresses or subnets separated by commas which HTTP/HTTPS traffic is being inspected in the TPROXY mode.
8	TPROXY source exceptions	10.100.0.14, 10.100.0.11	List of source IP addresses or subnets which are not inspected in the TPROXY mode. Each object is delimited by comma or new line.
9	TPROXY destined exceptions		List of destination IP addresses or subnets which are not inspected in the TPROXY mode. Each object is delimited by comma or new line.
10	TPROXY IP address	10.100.0.175	IP address of TPROXY NIC device.
11	TPROXY netmask	255.255.255.0	Subnet mask of TPROXY NIC device.
12	TPROXY gateway	10.100.0.1	Default gateway of TPROXY NIC device.
13	TPROXY routing	10.100.0.0/24 via 10.100.0.1 dev eth0 192.168.0.0/20 via 10.100.0.1 dev eth0 172.16.0.0/20 via 10.100.0.1 dev eth0	Static routing rules each on a separate line. Example: 192.168.0.0/24 via 191.168.0.1 dev eth0. Where 192.168.0.0/24 is destination host/subnet, 191.168.0.1 is a gateway, eth0 is a NIC device of the Inspector.
14	Failover mode	No	Select "Yes" to enable failover mode of the Bypass Network Card in Bridge and TPROXY. Select "No" to enable fail closed mode.
15	OOL/TAP blocking	Yes	Select "Yes" to enable blocking in OOL/TAP modes.
16	Blocking interface	eth2	Network interface name for sending TCP Reset or FIN packets in "TAP" mode (ie. eth0, eth1, eth2, or eth3).
17	DNS servers	10.100.0.17, 10.100.0.13	DNS servers IP addresses separated by commas.
18	Network Overload Protection	No	Enable skipping stream inspection (BRIDGE mode only) due to excessive network traffic.
19	Network MTU	9000	The maximum transmission unit size for inspection ports (LAN and WAN), this can be up to 16110.
20	CRC checking	No	Select "Yes" to perform a CRC check of every network packet. Normally, should be set to "No".

4406

# 4407

#### **Emails Alerts = Screenshot below** 0 Email Alerts

1 Security Respondents wesley.downard@nist.gov,neeraj.shah Default Security Respondents - list of email addresses separated by commas.

		@nist.gov	
2	Special Case Security Respondents		Format: [Policy: list of email addresses separated by commas]. Example: PCI: demo@gttb.com
3	MD5 Recipients		Email address receiving MD5 of triggered events.
4	System Administrator Email	wesley.downard@nist.gov,neeraj.shah @nist.gov	System Administrator email address(es) separated by commas.
5	Notify about system errors by email	Yes	Select "Yes" to notify System Administrator about system errors by email.
6	Send Emails From	GTBInspector-ICSLab-220- A230@nist.gov	Email address, appears as the source of the email notification.
7	SMTP Server Hostname	postmark.nist.gov	The IP address or domain name (FQDN) of the SMTP server. This address is required in order for the Inspector to send email notifications.
8	SMTP Server Port	25	The SMTP server port number. Typically, it is port 25.
9	Use SSL/TLS	No	Select "Yes" to use SSL/TLS encrypted connection.
10	Email Username		Authenticated Email Username.
11	Email Password		Authenticated Email Password.
12	Time between Alerts	60	Minimum interval in seconds, between alert emails.
13	Enable HTTP Block Response	Yes	Select "Yes" to return an alert page to a web browser when HTTP request is blocked.
14	HTTP Response Message	http://testpage.gtbtechnologies.com:	Response message in HTML or redirect URL returned when the HTTP session is blocked.

4408 4409

#### LDAP Intergration = Screenshot below 0 LDAP Integration

1	LDAP Server Hostname	10.100.0.17	IP address or hostname of the corporate LDAP server.
2	LDAP Server Port	389	LDAP server port.
3	LDAP Username (bind DN)	gttbldap@lan.lab	Example: Domain\Username (for MS Active Directory), cn=Admin,o=MyOrganization (for Novell eDirectory or OpenLDAP).
4	LDAP Password	*****	LDAP password.
5	LDAP SSL	No	Select "Yes" to use SSL connection to the LDAP server.
6	LDAP Cache Refresh Period	1800	Period in seconds used for LDAP objects cache periodic refreshes. Zero means no periodic refreshes.
7	Hostnames Cache Refresh Period	3600	Period in seconds used for hostnames cache periodic refreshes. Zero means no periodic refreshes.
8	NRH UDP Port	2222	UDP port for receiving reports from Name Resolution Helpers (the device acts as server).
9	Cache Persistence Timeout	450	User names cache persistence timeout in seconds. If the system is stopped for more than timeout specified, cache becomes obsolete and is dropped. Zero means "never obsoleted".
#### CSF MFG PROFILE LOW SEC LVL EXAMPLE IG DISCRETE-BASED MFG SYSTEM USE CASE

4411

## • Mail Transfer Agent = Screenshot below Mail Transfer Agent

1	List Of Allowed Hosts	*		Allowed hosts for email processing. Insert hostnames or IP addresses in separate rows. Insert * to accept emails from any host. A blank field means emails are rejected from any host.
2	Route Emails	Yes		Select "Yes" to have MTA route all emails to the next email hops listed in the "Domain Routing Rules" field.
3	Email Username			Authenticated next email hop Username. Example: demo@gttb.com.
4	Email Password			Authenticated next email hop User Password.
5	Domain Routing Rules	* 129.6.16	5.94	This entry contains routing rules per email domain on separate lines. Each rule consists of a domain pattern and a list of hostnames to which MTA will attempt to relay emails for this pattern. Use a colon to separate hostnames. Use double colon to specify a port number. Example: *.com 192.168.0.1:192.168.0.100, *.net 192.168.1.1:2525
6	Excluded domains			Emails destined to these domains will be passed without inspection. Domains should be colon delimited and without spaces. Example: gmail.com:gttb.com
7	Bcc domain inspection			List of email domains for inspection only (without routing). Domains should be colon delimited and without spaces. Example: gmail.com:gttb.com
8	MTA Listening Ports			List of listening TCP port numbers separated with colons. Default is 25. Example: 25:465
9	Email Size Limit	20		Maximum allowed email size in MBytes which is accepted for delivery and inspection. Value "0" means unlimited size.
10	Alert on Queue Above	4		System will alert Administrator hourly, when the number of email messages in the MTA queue is above this value. Set 0 to disable it.
11	Backup Emails	None		Enable email backup system.
12	Reject Email on fail	No		Select "Yes" to enable email rejection when inspection fails.
SI	EM = Scree	nsho	t below	
SIE	EM			
1	SIEM Receiver Host	name	10 100 0 27	IP address or bostname of the corporate SIEM receivers separated by commas

4412 4413

1	SIEM Receiver Hostname	10.100.0.27	IP address or hostname of the corporate SIEM receivers separated by commas.
2	Log Content	Yes	Select "Yes" to include security events triggers into the SIEM message.
3	Arcsight CEF	Yes	Select "Yes" to use Arcsight Common Event Format in the SIEM messages.

SSI Provu

4415

## • SSL Proxy = Screeshot below

General		
Enable SSL Proxy	Yes  No O	Select "Yes" to enable SSL Proxy.
Proxy Port	3128	SSL Proxy listening port.
Transparent Proxy HTTP Ports	80	List of HTTP ports separated by commas for transparent proxy. Works only in the TPROXY mode. Example 80, 81, 82.
Transparent Proxy HTTPS Ports	443	List of ports separated by commas for which HTTPS decryption is preformed transparently. Works only in TPROXY mode.
Transparent Proxy Source IP	Yes (I) No ()	Select "Yes" to enable source IP address in TPROXY mode (allows user client IP to the firewall).
Enable RESPMOD	Yes No	Enables server response inspection.
RESPMOD for internal servers		Inspects responses of external requests to internal servers such as OWA, WEB-Servers, etc. Make sure traffic is forwarded on the same port to the Inspector Example: 192.168.0.10:444, owa.gttb.com:445.
RESPMOD for internal users	Ŀ	List of IP addresses or subnets for which responses inspection is enabled. Example: 192.168.0.0/24, ws12.local
Bypass inspection on failure	Yes  No	Select "Yes" to bypass on failure and forwards traffic without inspection.
Proxy Server Identity	gtbinspector	The Inspector name, which is shown in user browsers in case of SSL Proxy errors.
System Administrator		Email address of System Administrator shown in SSL Proxy errors.
Append domain name		Appends local domain name to hostnames without any dots in them. Must begin with a period. Example: .foo.net
Access Control		
Restricted Sources		List of source IP address or subnets which are restricted to use the SSL Proxy. Example: 192.168.1.10, 192.168.2.0/24.
Restricted Destinations		List of destined domains which are basically blocked by SSL Proxy. Example: foo.net, www.bar.net.
Allowed ports		List of ports which are allowed SSL Proxy to connect to. Example: 21,80,443
SSL Decryption		
Current Certificate	Issued to: www.gttb.com CA Issued by: www.gttb.com CA Valid from 06.15.2012 to 05.28.2024	Detailed information about the certificate used for the HTTPS decryption.
Download Certificate	Public certificate Key and certificate	Save and view the certificate used for HTTPS decryption.
Upload Certificate	Browse No file selected.	Customer defined SSL Certificate in PEM format to be used for HTTPS decryption. The file should include both RSA private key and public certificate in plain text.
Block Invalid Sites	Yes O No 🖲	Select "Yes" to block destined domains with invalid certificates.
Exception Source List	Ŀ	List of source IP addresses, subnets, or domains for which HTTPS decryption is disabled. Example: 192.168.1.10, 192.168.2.0/24.
Exception Source List file (Upload empty file to clear list)	Browse No file selected.	List of source IP addresses, subnets, or domains for which HTTPS decryption is disabled. Upload empty file to clear it. Each sourse should be on a separate line no other separators are needed. Example: 192.168.1.10 192.168.2.0/24 foo.net www.bar.net
Exception Source List Download	Source exceptions file was not uploaded.	List of sources IP and domain addresses file download.
Exception Destinations List		List of destined IP addresses, subnets, or domains for which HTTPS decryption is disabled. Example: www.bar.net, .foo.net, , 192.168.1.10,192.168.0.1/24.
Exception Destinations List File (Upload empty file to clear list)	Browse No file selected.	List of destined IP addresses, subnets, or domains for which HTTPS decryption is disabled. Upload empty file to clear it. Each source should be on a separate line no other separators are needed. Example: 192.168.1.10 192.168.2.0/24 .foo.net www.bar.net
Exception Destinations List Download	Destination exceptions file was not uploaded.	List of destination IP and domains address file download.
Enable SSLv2	Yes O No 🖲	Select "Yes" to enable SSLv2.
Enable SSLv3	Yes O No 🖲	Select "Yes" to enable SSLv3.
Enable TLSv1.0	Yes  No	Select "Yes" to enable TLSv1.0.
Enable TLSv1.1	Yes • No O	Select "Yes" to enable TLSv1.1.
Enable TI Sv1 2	Yes No	Select "Yes" to enable TI Sv1 2
LINDIC ILUTIA		
	Apply Settings Discard Setting	5

## 4416 4417

4422

## Administration setting

Events	Rule Viewer	Quarantine	Configuration	Logs	Statistics	Administration	
<ul> <li>Licen</li> </ul>	sing = Used t	for download	ing and uploa	ding license	information.		
<ul> <li>Healt</li> </ul>	h Check = $Al$	oility to perfo	orm <b>"Self-Tes</b>	t" to check I	nspector insta	ull health.	

• Account Manager = Used to add new personal who will be administrating Inspector or responding to alerts for further investigation.

4423	0	System Time =	= Screenshot	below		
		System Time				
		Edit Date/Time:	08/02/2018 11:	30:10		Apply
		Edit NTP Server:	10.100.0.15			Apply
		Select Timezone:	(GMT-05:00)	Eastern Time (US & Canada)		
4424		Select fillezone.	(0111 05.00)			Abbiy
4425	<u>Central Cons</u>	sole				
4426	Genera	ating and applyin	ng License:			
4427	• Gener	ating				
4428	0	Click on middle	e top web pa	ge once logged into Cen	tral Console	
		Pleas	e acquire Endpoi	int licenses (support@gttb.com)		
4429		•	11			.1
4430		• You will	ll now be all	to a page that will	allow you to down	noad, eman,
4451			files should	lle.	sttle some Summant	4
4432		• License	mes snould	to be upleaded	<u>gub.com</u> . Support	t will reply
4433	• When	with an	upuateu me			
4454 1125	• when	Anytime a netu	vork change	ie offects the MAC (Modie	a Access Control)	address for
4435	0	Central Consol	e vou'll need	to generate a new licen	se key and email it	t to
4437		support@gtth.c	om Before e	mailing change the exte	se key and emain it	. to " tyt"
4438		Example: Cent	ral Console	- 7-31-2018-sysinfo cc	dat to 7-31-2018-	
4439		sysinfo cc.txt	This change	may be required if your	email provider blo	ocks ".dat"
4440		file extension	11115 011011-80			
4441	0					
4442	• Syster	m settings				
	•			DLP Setup		
4443	0	Click on "DLP	Setup" tab			
4444	0	Network (Loca		ategories)	1 /	
4445		Enter re     Parameter	quirea inform	Nation. See below for sc	reensnot	
		This Consol	e's IP or Domain nam	ne: 10 100 0 176	E @	
4446		DNS Server	IP:	10.100.0.17.10.100.0.13		Test Connection
4446		Click sa	we to continu	10	U	
1118	0			uc.		
1110 1110	0	• Enter in	formation fo	r screenshot below. This	s user has been cre	ated and
4450		only has	s Domain He	er right Check for pass	word in database	
UCFI				er fight. Check for pass	a ora in aatabase.	
4451				Port Is Forest ? Domain\Username 389 gttbidap@an.lab	Password	Use SSL Refresh, Hrs
4452		• User na	me = gttblab	@lan.lab		

4453	•	Password = chee	ck database			
4454	•	LDAP Server =	10.100.0.17			
4455	o <b>Email</b>	and alerts				
4456	•	Enter information	on from screenshot below			
		Parameter	Value			
		Email Server:	10.100.0.175	<u>+</u>	(i) Send Test Email	
		Email Port:	25		<b>(i)</b>	
		Email User Name:			•	
		Email Password:		٩	<b>(i)</b>	
		Email Originator:	GTBCC-ICSLab-220-A230@nist.go	)V	<b>(i)</b>	
		Encryption:	None	~	<b>(i)</b>	
		Alert manager:	Network (SMTP only)		<b>(i)</b>	
			Save Cance	el		
4457		F 10	10 100 0 175			
4458	•	Email Server =	10.100.0.175			
4459	•	Email Originato	$\mathbf{r} = \mathbf{GTBCC} \cdot \mathbf{ICSLab} \cdot 220 \cdot \mathbf{A}$	<u>A230@nis</u>	<u>t.gov</u>	
4460	•	Click save				
4461	o Data a	and Time				
4462	•	NTP Server $= 10$	0.100.0.15 (Click set time t	o sync)		
4463	•	Time Zone = Ea	stern Time (US and Canad	a) (Click	Apply to save)	
4464	•	Click Save				
1101	-	Chex Buve				
4465	Other settings under l	DLP Setup → Sy	stem aren't currently conf	igured. Th	ese setting will	be
4466	updated an included v	when these feature	es are enabled.			
4467	Lesson learned: If int	egrating with Act	tive Directory using LDAP	it's recon	nmended to use	
4468	Secure LDAP to ensu	re user name and	password are not sent in p	laintext.		
4469						
4470	II.	ACI mulas ana a	wasted for use with CTD			
4470	HOW	ACL rules are c	reated for use with GIB.	DLP Insp	ector.	
<i>AA</i> 71	GTR DLP Inspector	· views data as it	nasses thru the device an	d respon	ds based on	
AA72	configured rules	views data as it	passes that the device an	u respon	us based on	
4472	configured rules.					
4473	GTB Central Conso	le is the portal w	vere all policy rules and o	ther setti	ngs are configu	red.
		<b>F</b>			-88-	
4474	ACL Rules:					
4475	<ul> <li>Login into to</li> </ul>	Central Console	via web browser (E.g. 10.1	00.0.176)		
4476	<ul> <li>Now click on</li> </ul>	DLP-Setup→N	etwork DLP to access rule	s.		
	Dashboard All Events	Network Events Discovery Events	Cloud Events Endpoint Events Reports Network	Status Accounts	lanager DLP Setup	
4477	Network DLP Discove	ry Endpoint & Device Control A	pp Control IRM Policy Management Inspection	System		
4478	• Now, look to	the left of windo	w under categories and sele	ect your Ir	spector installa	tion.

# Categories

- GTBInspector.lan.lab
- Once selected you will see on the right current ACL Rules being applied.
- Click Add button. +Add
  - A new window will appear titled "Add New ACL Rule"

ule lame*: Protocol*:					
lame*: Protocol*:					
Protocol*:					
	Any				
ource:	Any				
Destination:	Any				
ile type:	None				
ile size:	Any				
Enforcement: + Add   X Delete		1			
Policy/Sets		Action	Alerts	File capture	
		Log			î 🕆 🖶

4483 4484

4488 4489

4492

4493

- Now type in a name for the new rule being created.
- Change Protocol to desire setting. This can be left to "ANY" which will look at all protocols passes thru the Inspector (*This may cause a performance impact on you Inspector installation depending on the number of clients within your organization*).
  - Source: Choices are → Any, IP Address, Hostname, Hostname (Custom), and Group (User/Computer).
- 4490 Destination: Choices are → Any, IP Address, Hostname, Hostname (Custom), and
   4491 Group (User/Computer).
  - File type: Choices are → None, All Files, Encrypted, and Extension.
    - File Size: Choices are  $\rightarrow$  Any, and Not more than.

4479

4480

• **Comments:** Give a description of the rule being applied then click **Add** button.

lame*:	CRS				E
Protocol*:	Any				
ource:	Any				
estination:	Any				
ile type:	None				
ile size:	Any				
Enforcement	This rule app	lies to Collaborative F	lobotics System		
enforcement:	This rule app	Action	Abotics System	File capture	
Enforcement + Add > > 0 Policy/Sets All	This rule app	Action Block	Alerts Security	File capture	<b>↑</b>
iomment: Enforcement + Add X 0 Policy/Sets All	This rule app	Action Block	Alerts Security	File capture	<b>↑</b>
omment: Enforcement + Add >> D Policy/Sets All	This rule app	Action Block	Alerts Security	File capture	Î.↓

- 4496 • Once Add has been clicked you'll have an option to select a "**Policy/Sets**" to enforce. Default policies that are enforce are (Credit Card Number CCN and Social Security 4497 4498 Numbers SSN). 4499 • Next, select the action to be taken. There are four choices, Log, Block, S-Block, and 4500 Pass. 4501 • Now select if you would like additional personal to be notification upon rule violations. • Finally, place a check in **File Capture** if you want to retain a copy of the offending data. 4502 • Click **Save** to complete. 4503 4504 Last step is to click on **Deploy all** button. This sends newly created policy to Inspector. ٠ 4505 This button will have a red blinking box around it is indicating required action. 🛃 Deploy all 4506 4507 4508 **Useful Information:** • Once a new rule has been created double click on that rule to adjust the ordering from top 4509 to bottom by click the **UP** or **Down** arrows towards the right.  $\uparrow \downarrow \downarrow$ 4510 • Remember rules work from  $Top \rightarrow Down$ , so think about ordering process. If unsure 4511 move the rule all the way to the top and then click **Deploy all** again. 4512 4513 4514
- 4515 How to Fingerprint Files using GTB Security Manager for DLP Protection

#### 4516 **Download:**

4517 First download "GTB Security Manager" by clicking on Help tab within Central • 4518 Console server web portal then select "GTB Security Manager" link to start download. Dashboard All Events Network Events Discovery Events Cloud Events Endpoint Events Reports Network Status Accounts Manager DLP Setup Maintenance Logs Help 4519 GTB Security Manager (19 MB) - Fingerprinting Management System 4520 • Select location to save file being downloaded. 4521 Double click to start install for "GTBSecurityManager 15.3.0.msi" from location 4522 • where file was saved to (version number might be different than one listed above). 4523 4524 Once first screen appears click on "Next" to continue. • GTB Security Manager Setup × Welcome to the GTB Security Manager Setup Wizard The Setup Wizard allows you to change the way GTB Security Manager features are installed on your computer or to remove it from your computer. Click Next to continue or Cancel to exit the Setup Wizard. TB Technologies Data Loss Back Next Cancel 4525 Select Yes to License Aggreement and click "Next" to continue. 4526 • GTB Security Manager Setup × End-User License Agreement  $\odot$ Please read the following license agreement carefully GTB Technologies, Inc. End User License and Warranty Terms & Conditions For: GTB's Information Leak Prevention Product(s); IMPORTANT - READ CAREFULLY: This End User License and Warranty Terms 8 IMPORTANT - READ CAREFULLY: This End User License and Warranty Terms & Conditions (this "Agreement") is a legal agreement between you, a purchaser and/or any end user, either an individual or an entity ("You" or "Your") and GTB Technologies ("GTB") for the license of one or mote of the software products listed above (the "Software") either embedded in the GTB hardware device (the "Hardware") or not embedded, and for the warranties for such Software and Hardware. The Software and Hardware are collectively referred to as, the "Product". By breaking the seal on the envelope containing the Software or accessing, installing, copying or otherwise using the Software or Hardware, You agree to be bound by the terms of this Agreement. If You do not agree to the terms of this Agreement, GTB is unvaling to license the Product to You. In such event, You may not access, use or copy the Product and ↓ I accept the terms in the License Agreement Print Back Next Cancel

• Leave Destination Folder as default and Click "Next"

GTB Security Manager Setup		-		×
Destination Folder				
Click Next to install to the default folder or	click Change to choose and	other.	(	8
Install GTB Security Manager to:				
C:\Program Files (x86)\GTB Technologies\	Security Manager\			-
Change	, ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,			
<u>Change</u>				
	Back N	ext	Can	cel
	Dack	ext	Cali	cei

- 4529 4530
  - Click "Install" to continue.

GTB Security Manager Setup			-	×
Ready to install GTB Security Manage	er			3
Click Install to begin the Installation. Click B settings. Click Cancel to exit the wizard.	Back to review	v or change any o	of your instal	lation
	Back	Install		Cancel

4531

4537

- When prompted by User Access Control (UAC) enter administrator password to continue install.
- If prompted to close Open Applications, select either option. Reboot is required if second option is selected.
- Click **"OK"** to continue.
  - Once install has completed click "Finish" to complete install.
- 4538
   If prompted to reboot, select "Yes". MAKE SURE TO SAVE ALL OPEN FILES
   4539
   BEFORE SELECTING "YES"

뤻 GTB Se	curity Manager Setup		$\times$
i	You must restart your syst made to GTB Security Man restart now or No if you pl	em for the configuration changes ager to take effect. Click Yes to an to manually restart later.	
	<u>Y</u> es	No	

- 4541
  Once machine has completed rebooting open "GTB Security Manager" by right click and selecting "Run as administrator"
- When prompted enter administrator password for application to start.

- Once "GTB Security Manager" has opened, click on setting button on menu bar.
- 4545 File Profiles View Command Settings Window Help
- Now enter the IP Address of where "Central Console" is installed. Login and password are already populated with default credentials from vendor. Both can be changed. See foot notes for additonal steps required to change Fingerprint Inspections login an

9	
Co	nnection Advanced Network
	Device Connection
1	Database IP Address 10 · 100 · 0 · 175 : 17023 🔷
١,	
ľ	Login (Customer Code) myingerprints
F	Password
	OK Cancel

4549 password.

4552

- Once IP Address has been enter click "**OK**" to save changes.
- 4551 Now, click on **File** from menu bar and select **New → New File Profile**

ile	Profiles	View	С	omm	and	Settings	Window
	New		۲	١	New	File Profi	le
)	Open Prof	ile		19	New	Ouerv Pr	ofile

- A new window will appear allowing the ability to select files to be added. Files can be
   copied to Local Machine, or accessed from a Network Share, Subversion
   Repositories, or SharePoint Respositories.
- 4556
   Select the folder, or files that need fingerprinting. Once a folder is selected all files within selected folder will recive a check mark indicating which files will be fingerprinted.



- 4559 Now click on floppy disk icon to save.
- Select location to save newly created profile.

- Now the profile has been saved click the **padlock** icon to start fingerprinting process
- 4562 (Depending on the number of files being fingerprinted this can take a few minutes).
  - To view the process see the Output screen that will display what files have been processed and there status. Once completed click **Close**

Fingerprinting				
1	Processed 570 Fingerprinti	Skipped 140 ing : 100,00 %	Total 570	
	Close	Stop		

- Now look to the right side window for a tab labeled "Profiles" if this is missing click on
  "View" from menu bar and select "Profiles Window". Click on Profile tab and a slide
  out appears show all the Profiles that can be monitored.
- 4569 Now select the Profile that was created earlier and right click, then select Start
   4570 Monitoring.
  - Once monitoring is enabled it'll appears under "Currently Monitoring" under help.
     Currently Monitoring

ProjectsFromCRS.prf

- Files that were included in fingerprinting profile will now have ACL rules applied from
   Network DLP section from Central Console.
- 4575 Login to Central Console and navigate to Account Manager Tab and click Refesh
   4576 Polices.

 Dashboard
 All Events
 Network Events
 Discovery Events
 Cloud Events
 Endpoint Events
 Reports
 Network Status
 Accounts Manager

 4577
 4578
 You'll see a message indicating Fingerprint polices successfully synchronized.



4579

4563 4564

4565

4571

- 4580 How to add policy to GTB Central Console for detecting fingerprinted files
- Login to Central Console
- 4582 Click on DLP Setup tab. DLP Setup
- Now select Policy Management tab. Policy Management
- Now double click on Default to launch a new window.
- Click Add Policy. + Add Policy
- Click drop down and select File. File

• Now click save button for setting to be applied.

All fingerprinted files from above steps will automatically be added to default Network DLP
policy applied ACL. New Default values are "SSN, CCN, and File"

4590

4609

## 4591 Additional Information for Fingerprinting:

- 4592 Recommended to configured GTB Security Manager to connect to IP address of DLP
   4593 Inspector.
- Fingerprint only allows for one active Profile at a time. If another profile is set to Start
   Monitoring you'll receive a warning asking if you'd like to disable the active profile.

8,		0	0
Profile			$\times$
GTB Security Manager is currently monito clicking Yes, monitoring will stop for C:\U Information\Finger Printing\ProjectsFrom profile. Do you wish to continue?	ring files from anothe sers\wnd1\Document iCRS.prf profile and sta	r profile. By s\GTB art for currer	nt
	Yes	<u>N</u> o	

- 4596
  4597 O Recommendation would be to install GTB Security Manager on a machine that
  4598 can be the central repositoiry for all fingerprinted files. Creating a large folder
  4599 were the files can placed into for fingerprinting. Files don't have to remain in
  4600 saved location once the profile has been fingerprinted and uploaded to Central
  4601 Console. Access to fingerprinted files is only required when changes are made to
  4602 profile containing said files.
- Although only one profile is able to monitored at a time you are able to define multiple
   Polices within that profile. This is useful since when a fingerprint violation is triggered it
   will be tagged with the Defined Policy name, which allows for easier usability.
- 4606 Fingerprinted files follow **ACL Rules:** created within **Central Console** under **DLP Setup** →
- 4607 Network DLP. Rules are processed in order from top to bottom. This means the first rule with a4608 matching violation takes precedence over rules below.

0		1							
Dashboard All Events N	etwork Events Discove	ery Events Cloud	d Events Endpoint Event	ts Reports Net	work Status Acc	ounts Manager	DLP Setup	Maintenance	Logs
Network DLP Discovery	Endpoint & Device Co	ontrol App Cont	trol IRM Policy Mana	gement Inspectio	n System				
Categories	ACL Rules: GTBInspect	tor.lan.lab							
Inspectors (1)	🕂 Add 🛛 🗙 Delete	📄 🯦 Load 📄	🛓 Save all 🔰 🛃 Deploy all						
GTBInspector.lan.lab	Name F	Protocol Source	Destination	Files	Policy/Sets	Action	Alerts	Files capt	
	Any A	Any Any	Any		All	Block	Security	m 1	t 🕹 🦯 🗙

## 4610 **4.12.6 Highlighted Performance Impacts**

4611 No performance measurement experiments were performed for the installation of GTB into the

4612 CRS due to its location within the network topology. No workcell components involved with

4613 controlling the manufacturing process communicate across the boundary on a regular basis while

the system is operational.

## 4615 **4.12.7** Link to Entire Performance Measurement Data Set

4616 N/A

## 4618 **4.13 Graylog**

## 4619 **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 realtime 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

- 4626 trends in one central location.<sup>21</sup>
- 4627 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).

## 4634 **4.13.2 Technical Capabilities Provided by Solution**

- 4635 Graylog provides components of the following Technical Capabilities described in Section 6 of4636 Volume 1:
- Network Monitoring
- Event Logging
- Forensics

## 4640 **4.13.3 Subcategories Addressed by Implementing Solution**

4641 PR.DS-4, PR.PT-1, DE.AE-2, DE.AE-3, DE.CM-1, DE.CM-6, DE.DP-3, RS.AN-3

<sup>&</sup>lt;sup>21</sup> Graylog Documentation <u>http://docs.graylog.org/en/3.0/</u>

## 4642 **4.13.4** Architecture Map of Where Solution was Implemented



## 4644 **4.13.5 Installation Instructions and Configurations**

4645 Details of the solutions implemented:

Name	Version	Daily volume of logs	Server
Graylog Enterprise	2.4.6	< 5GB per day	Ubuntu 14

#### 4646

#### 4647 **Setup:**

Download the installation package from the Graylog website (<u>https://www.graylog.org/</u>).
 Graylog can be installed on any flavor of Linux. In addition, Graylog also provides a
 preconfigured virtual machine for **non-production** environments. This virtual machine
 template (OVA) file was used in our environment.

- The OVA file was deployed on a Microsoft Hyper-V host server in our Cybersecurity LAN network.
- The Graylog server receives all syslog traffic by default on UDP port 514, accordingly UDP
   514 was permitted in the firewall rules. Additional ports are required to be allowed if
   utilizing other features of Graylog as described in the <u>documentation</u>.
- Upon deploying the OVA file, the virtual machine will default to a DHCP IP address. Login to the system to assign it a static IP address as per below shown instructions.

## 4659

## Assign a static IP

Per default the appliance make use of DHCP to setup the network. If you want to access Graylog under a static IP please follow these instructions:

\$ sudo ifdown eth0

Edit the file /etc/network/interfaces like this (just the important lines):

```
auto eth0
iface eth0 inet static
address <static IP address>
netmask <netmask>
gateway <default gateway>
pre-up sleep 2
```

Activate the new IP and reconfigure Graylog to make use of it:

```
$ sudo ifup eth0
$ sudo graylog-ctl reconfigure
```

Wait some time until all services are restarted and running again. Afterwards you should be able to access Graylog with the new IP.

٠	Login to	the Web Interface using the default credentials and change the admin password.
٠	Active I	Directory (AD)-integration is supported in Graylog. To configure, on the Top Menu
	Bar Clic	k on <b>System</b> >> <b>Authentication</b> . On the Authentication Management page, click on
	LDAP /	Active Directory and fill out the AD server details. Detailed instructions can be
	found in	product documentation. <sup>22</sup>
	0	Note: Any AD domain user that's added is assigned "Reader" access by default. This
	С	an be changed by configuring Group Mapping options in the same page. Change
	t	he Default User Role depending on your requirement. Adding permissions can be
	а	ssigning by clicking on LDAP Group Mapping button on the same page
	•	<ul> <li>Login to</li> <li>Active E Bar Clic LDAP / found in</li> <li>N c ti a</li> </ul>

## 4. Group Mapping (optional)



4677 <u>Syslog on Linux servers:</u>

4675

<sup>&</sup>lt;sup>22</sup> Configuring External Authentication in Graylog

http://docs.graylog.org/en/2.3/pages/users\_and\_roles/external\_auth.html?highlight=ldap

- The "rsyslog" package on Linux was leveraged to forward logs out of all Linux hosts in the Robotics system to the Graylog server. Rsyslog is by default present in all Linux distributions. Configure the /etc/rsyslog.conf file to enable forwarding the logs to the IP address of the Graylog server. Detailed instructions can be found here:
   https://marketplace.graylog.org/addons/a47beb3b-0bd9-4792-a56a-33b27b567856
- Below is a snippet of a /etc/rsyslog.conf file from one of the Linux servers. Restart the
   rsyslog service once the rsyslog.conf file is modified.
- 4686

<b>#</b> C	Graylog	configuration
*.*	010.10	0.0.14:514;RSYSLOG_SyslogProtocol23Format
roc	ot@gitla	b:/home/icssec#

- You should now begin to receive syslog data in Graylog from this client. Login to the
  Graylog Web UI and search for the asset / server name in the dashboard to view these logs.
  The corresponding Linux device will also be listed under "Sources" page when its actively
  forwarding the data.
- 4693 <u>Syslog on the Boundary Firewall (RuggedCom):</u>
- Most of the firewall devices available today support syslog capabilities. This can be configured by either by setting it up from command line via SSH or from the Web Interface of the Firewall device. Ensure UDP 514 is allowed between the firewall and Graylog server.
   Similarly, the RuggedCom boundary router/firewall device in Robotics system was configured to send syslog traffic to Graylog. Below screenshots reference the syslog setting on the RX1510 appliance where 10.100.0.14 is the IP address of our Graylog server. The log
- 4701 level was set to "**Informational and above**".
- 4702 Detailed instructions can be found in the product manual.<sup>23</sup>

<sup>&</sup>lt;sup>23</sup> <u>http://www.plcsystems.ru/catalog/ruggedcom/doc/ROXII\_RX1500\_User-Guide\_WebUI\_EN.pdf</u>

SIEMENS					RUGGEDCON
Configure Running Tool	s Log	gout from ruggedcom		_	
View   Edit Private   Edit Exc	clusive				
<ul> <li>admin</li> <li>chassis</li> <li>global</li> <li>interface</li> <li>interfaces</li> <li>switch</li> <li>tunnel</li> <li>jp</li> </ul>		alarms alarm-config dns logging users snmp authentication software-upgrade	-	diagnostics secure-remote-syslog <u>server</u>	10.100.0.14
			/admin/loggi	ng/server	
Damata Samar					

4705

Syslog on the Network Switches: 4706

4707 • Both the network switches (Netgear and Siemens i800) were configured to log to the Graylog server. The below image shows Syslog server configuration on the Netgear SW pointing to 4708 the IP address of the Graylog server. 4709

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help Index
Ports   Logs	Mirroring						
> Memory Log		Server	Log				
> FLASH Log > Server Log		Serve	er Log Config	uration			()
> Trap Logs		Admin St	tatus		Disab	e 🖲 Enable	
> Event Logs		Local UD	P Port		514		(1 to 65535)
		Message	s Received		1386		
		Message	s Relayed		83		
		Message	s Ignored		0		
		Serve	er Configurat	ion			(?)
		IP /	Address Type	Host Address	State	is Port	Severity Filter
			•				▼
		IPv4	1	10.100.0.14	Activ	e 514	Informational

- 4711
- 4712

## 4713 Configuring Email Notifications for Alert conditions:

- 4714 You can create email alerts for any custom events, alert condition as per your requirement.
   4715 Below process show how our Graylog was configured to send out email notifications, for any
   4716 Veeam backup events that it received from the Linux machines. Follow this process to
   4717 define your custom alert conditions
- 4718 There are multiple configuration settings required for email notification to work Creating a 4719 stream, adding an alert condition and creating a notification.
- To create a stream, click on Streams on the Top-Menu >> Create a Stream >> Enter Title,
   Description, and Index Set which should default to "Default index set"
- 4722 Click **Save** to save the changes
- 4723

		~
	Title	
	Backup Notifications	
	Description	
	Backup Messages	
	Index Set	
	Default 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	9
•	Cancel       Save         Next, click on "Alerts" options on the top menu >> Click on Manage conditions >       on         Add new condition       to define a condition.         Click drop menu under "Alert on Stream" and select the stream created earlier. Cli         "Condition Tupe" menu drop down and select "Message Count Alert Condition"	> C
•	Cancel       Save         Next, click on "Alerts" options on the top menu >> Click on Manage conditions >       on         Add new condition       to define a condition.         Click drop menu under "Alert on Stream" and select the stream created earlier. Cli       "Condition Type" menu drop down and select "Message Count Alert Condition"	e > ( ck
•	Cancel       Save         Next, click on "Alerts" options on the top menu >> Click on Manage conditions >       on         Add new condition       to define a condition.         Click drop menu under "Alert on Stream" and select the stream created earlier. Cli       "Condition Type" menu drop down and select "Message Count Alert Condition"         Condition       Define the condition to evaluate when triggering a new alert.	≥ ( ck
•	Cancel       Save         Next, click on "Alerts" options on the top menu >> Click on Manage conditions >       on         Add new condition       to define a condition.         Click drop menu under "Alert on Stream" and select the stream created earlier. Cli       "Condition Type" menu drop down and select "Message Count Alert Condition"         Condition       Define the condition to evaluate when triggering a new alert.         Alert on stream	e > (
•	Cancel       Save         Next, click on "Alerts" options on the top menu >> Click on Manage conditions >       on         Add new condition       to define a condition.         Click drop menu under "Alert on Stream" and select the stream created earlier. Cli       "Condition Type" menu drop down and select "Message Count Alert Condition"         Condition       Define the condition to evaluate when triggering a new alert.         Alert on stream       Backup Notifications	) ck
•	Cancel       Save         Next, click on "Alerts" options on the top menu >> Click on Manage conditions >       on         Add new condition       to define a condition.         Click drop menu under "Alert on Stream" and select the stream created earlier. Cli       "Condition Type" menu drop down and select "Message Count Alert Condition"         Define the condition to evaluate when triggering a new alert.       Alert on stream         Backup Notifications       Select the stream that the condition will use to trigger alerts.	= > ( ck
•	Cancel       Save         Next, click on "Alerts" options on the top menu >> Click on Manage conditions >       on         Add new condition       to define a condition.         Click drop menu under "Alert on Stream" and select the stream created earlier. Cli       "Condition Type" menu drop down and select "Message Count Alert Condition"         Condition       Define the condition to evaluate when triggering a new alert.         Alert on stream         Backup Notifications         Select the stream that the condition will use to trigger alerts.         Condition type	e ) > ( ,
•	Cancel       Save         Next, click on "Alerts" options on the top menu >> Click on Manage conditions >       on         Add new condition       to define a condition.         Click drop menu under "Alert on Stream" and select the stream created earlier. Cli       "Condition Type" menu drop down and select "Message Count Alert Condition"         Condition       Define the condition to evaluate when triggering a new alert.         Alert on stream       Backup Notifications         Select the stream that the condition will use to trigger alerts.         Condition type         Message Count Alert Condition	> C ck

- Click "Add Alert Condition". Once window appears fill out the required information.
- 4732

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

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	
Veeam Backup Alerts	
The alert condition title	
Time Range	
2	\$
Evaluate the condition for all messages received in the given number of minutes	
Threshold Type	
more than	$\sim$
Select condition to trigger alert: when there are more or less messages than the threshold	
Threshold	
0	\$
Value which triggers an alert if crossed	
Grace Period	
1	\$
Number of minutes to wait after an alert is resolved, to trigger another alert	
Message Backlog	
1	-
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 satisfier regardless of its state.	d
Cancol	Save

## • Now create a **notification**.

4739	• Click on "Manage notifications" blue button in upper right-hand corner.
4740	<ul> <li>Click green button for "Add new notification"</li> </ul>
4741	• Under "Notify on Stream" select notification created earlier from drop down
4742	menu.
4743	• Under "Notification type" select "Email Alert Callback" from drop down
4744	menu.
4745	<ul> <li>Click "Add alert notification" button</li> </ul>
4746	• Title: "Veeam Backup Alerts"

4747	• Email Subject: "Successful Veeam Backup source: \${foreach backlog
4748	message}\${message.source}\${end}" without the quotes, see below for screen
4749	shot of current callback wording.
4750	• Sender: < sender address >
4751	• E-mail Body: "This can be adjusted as required"
4752	
4753	Alert Description: \${check_result.resultDescription}
4754	Date: \${check_result.triggeredAt}
4755	Stream ID: \${stream.id}
4756	Stream title: \${stream.title}
4757	Stream description: \${stream.description}
4758	Alert Condition Title: \${alertCondition.title}
4759	
4760	\${if backlog}Last messages accounting for this alert:
4761	<pre>\${foreach backlog message}\${message}</pre>
4762	
4763	\${end}\${else} <no backlog=""></no>
4764	\${end}
4765	
4766	• User Receivers: "Select a Graylog user if desired"
4767	• Email Receivers: "Enter email address for individuals receiving these
4768	alerts"
4769	• Click Save
4770	
4771	• Test new Streams / Alerts / Notifications to ensure they are configured correctly.
4772	
4773	4.13.6 Highlighted Performance Impacts
4774	Two performance measurement experiments were performed for the Graylog tool while the

- 4775 manufacturing system was operational:
- 47761. CL003.1 Syslog service was installed and running on CRS network hosts, and all<br/>generated syslog messages were forwarded from CRS hosts to Graylog server.
- 4778 2. <u>CL003.2</u> Syslog forwarding to Graylog was configured on CRS networking devices.

## 4779 **4.13.6.1 Experiment CL003.1**

- 4780 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).

#### CSF MFG PROFILE LOW SEC LVL EXAMPLE IG DISCRETE-BASED MFG SYSTEM USE CASE

Syslog Traffic on the CRS Network (CL003.1)





4787

4784 Figure 4-48 - Time series plot showing the rate of syslog network traffic (in packets per second) transmitted 4785 during the CL003.1 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.

## 4790 **4.13.6.2 Experiment CL003.2**

- 4791 The rsyslog service was installed and configured on CRS networking devices to forward all
- 4792 syslog messages to the Graylog server. A total of 28 syslog packets were transmitted during the
- 4793 experiment by the rsyslog service from CRS hosts and networking devices (see Figure 4-50).

#### CSF MFG PROFILE LOW SEC LVL EXAMPLE IG DISCRETE-BASED MFG SYSTEM USE CASE

Syslog Traffic on the CRS Network (CL003.1)



4794

4795 Figure 4-50 - Time series plot showing the rate of syslog network traffic (in packets per second) transmitted
 4796 during the CL003.2 experiment.



4797 No performance impact to the manufacturing process was measured during the experiment.



4799 Figure 4-51 - Bihistograms showing the part production time (left) and estimated mean production time using 4800 the bootstrap method (right) using the measurements from baseline CL001.1 and experiment CL003.2.



- 4802 <u>CL003.1-Syslog.zip</u>
- 4803 <u>CL003.2-Syslog.zip</u>
- 4804

## 4805 **4.14 DBAN**

## 4806 **4.14.1 Technical Solution Overview**

4807 DBAN is a free open source data wiping utility allowing the ability to sanitize hard drives to
4808 ensure data is not left behind when drives are beginning decommissioned and prepared for
4809 removal from on premise. DBAN and other hard drive sanitization tools only work with spinning
4810 hard drives, SSD hard drives and other flash media refer to vendors for specific directions for
4811 sanitizing media before removing from company control.

4812

## 4813 **4.14.2 Technical Capabilities Provided by Solution**

4814 DBAN provides components of the following Technical Capabilities described in Section 6 of4815 Volume 1:

4816 • Media Sanitization

## 4817 **4.14.3** Subcategories Addressed by Implementing Solution

4818 PR.DS-3, PR.IP-6





4821		
4822	4.14.5 Instal	lation Instructions and Configurations
4823		Instructions for installing DBAN and use
4824	Down	load:
4825	DBAN	V can be downloaded from <u>https://dban.org</u>
4826	Click	download link which redirects the page and a pop will appear to start download
4827	proces	s for ISO image file "dban-2.3.0_i586.iso".
4828	Down	load ISO file and burn to CD/DVD, or USB drive using widely available ISO
4829	bootat	ble utilities.
4830	<b>T</b> (	
4831	Instru	
4832	1.	Once ISO has been burned to bootable media go to device requiring sanitization.
4833	2.	Power on machine and boot from USB or CD/DVD depending on the install option
4834		from earlier steps above. (Change Boot order in BIOS if no option for Boot
4835		Menu is available during machine power-up)
4836	3.	Once machine has booted from media select desire option for media sanitization.
		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/
		<ul> <li>* Press the F2 key to learn about DBAN.</li> <li>* Press the F3 key for a list of quick commands.</li> <li>* Press the F4 key for troubleshooting hints.</li> <li>* Press the ENTER key to start DBAN in interactive mode.</li> <li>* Enter autonuke at this prompt to start DBAN in automatic mode.</li> </ul>
		boot: _
4837		
4838	4.	Select option to continue. Default sanitization mode is "short DoD 5520.22-M",
4839		but this can be changed depending on the level your security program indicates.
4840	5.	Follow menu options to start wiping process.

4841 6. Once wipe had completed you will see a screen like the image below.



484348447. Once sanitization has completed, remove hard drive from device and label wiped ready for disposal.

## 4845 **Lesson Learned and thing to know:**

4846 Not all hard drives are able to be wiped clean using this sanitization method. Media that is either
4847 SSD or flash memory is written differently than spinning drives, so follow SSD/Flash media

4848 vendors' recommendations for proper media sanitization for all non-spinning hard drives.

## 4849 **4.14.6 Highlighted Performance Impacts**

- 4850 No performance measurement experiments were performed for the use of DBAN due to its
- 4851 typical installation and usage location.

## 4852 **4.14.7** Link to Entire Performance Measurement Data Set

4853 N/A

## 4855 **4.15** Network Segmentation and Segregation

## 4856 **4.15.1 Technical Solution Overview**

- 4857 Network segmentation and segregation solutions enable a manufacturer to separate the
- 4858 manufacturing system network from other networks (e.g., corporate networks, guest networks),
- 4859 segment the internal manufacturing system network into smaller networks, and control the
- 4860 communication between specific hosts and services.
- 4861 Each Router's native capabilities were leveraged to implemented network segmentation.

## 4862 **4.15.2 Technical Capabilities Provided by Solution**

- 4863 Network Segmentation and Segregation provides components of the following Technical
- 4864 Capabilities described in Section 6 of Volume 1:
- Network Segmentation and Segregation

## 4866 **4.15.3 Subcategories Addressed by Implementing Solution**

4867 PR.AC-5

## 4868 **4.15.4** Architecture Map of Where Solution was Implemented



## 4870 **4.15.5** Installation Instructions and Configurations

4871 The following devices were involved in implementing Network Segmentation

Device	Details	Location
Cisco-ASA 5512	NGFW, running Firepower Services FTD 6.2.3	Manufacturing System
RuggedCom RX1510	Firewall, Router	Work cell

4872

## 4873 • Segmentation in the Cybersecurity LAN:

- 4874 Following is a list of interfaces created on the Boundary Router/Firewall Cisco ASA of the
- 4875 Cybersecurity LAN network

Interface	IP address of Interface	Subnet	Description
GE 0/0	129.6.66.x	129.x.x.x/x	Uplink to Corporate
GE 0/1	10.100.0.1	10.100.1.0/24	Cybersecurity LAN
GE 0/2	129.6.1.x	129.x.x.x/x	VPN users
GE 0/3	10.100.2.1	10.100.2.0/24	Management LAN
GE 0/4	10.100.1.1	10.100.0.0/24	Manufacturing DMZ LAN

4876

## 4877 • Segmentation in the Work Cell:

4878 4879

## • The Work Cell consists of the following network devices.

4880

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

- Network segmentation was implemented using the RuggedCom firewall. The firewall has the
- 4883 following interfaces defined. There were two subnets created as listed in the below table.

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

4885

4886

- 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).
- 4891
- 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)
- 4896 **4.15.6 Highlighted Performance Impacts**
- 4897 No performance measurement experiments were performed for network segmentation due to it4898 being implemented on the CRS before the Manufacturing Profile implementation was initiated.
- 4899 **4.15.7** Link to Entire Performance Measurement Data Set
- 4900 N/A

## 4902 **4.16 Network Boundary Protection**

## 4903 **4.16.1 Technical Solution Overview**

4904 Boundary Protection devices are implemented to monitor and control connections and

4905 communications at the external boundary and key internal boundaries within the organization.
4906 Boundary protection mechanisms include for example, Routers, Firewalls, Gateways, Data

4907 diodes separating system components into logically separate networks and sub networks.

## 4908 **4.16.2 Technical Capabilities Provided by Solution**

4909 Network Boundary Protection provides components of the following Technical Capabilities4910 described in Section 6 of Volume 1:

• Network Boundary Protection

## 4912 **4.16.3 Subcategories Addressed by Implementing Solution**

4913 PR.AC-5, PR.PT-4, DE.CM-1

## 4914 **4.16.4** Architecture Map of Where Solution was Implemented



## 4916 **4.16.5** Installation Instructions and Configurations

- 4917 **Setup:**
- 4918 The following devices were implemented for Boundary protection in the CRS System

Device	Details	Location
Cisco-ASA 5512	NGFW, running Firepower Services FTD 6.2.3	Manufacturing System
RuggedCom RX1510	Firewall + Router running ROS 2.12.2	Work cell
GTB Inspector	Data Loss Prevention (DLP) virtual appliance	Cybersecurity LAN

4919

## 4920 • Configuration on Cisco-ASA:

- 4921 The following features, settings were enabled on the ASA firewall
- 4922 Network Segmentation
- 4923 ACL Rules
- 4924 NAT policy for Internet access
- 4925 Snort Inspection
- 4926 DMZ network
- 4927 Network Segmentation
- 4928 Separate network interfaces were configured for the different network segments as listed below
- 4929 Inside Interface (Network: 10.100.0.0/24)
- 4930 DMZ Interface (Network: 10.100.1.0/24)
- Outside Interface (Uplink to NIST Corporate for Internet)
- 4932 Management interface (out of scope)
- 4933 Access Control List (ACL) rules
- 4934 The following ACL rules were put in place on the ASA with a default Action to Block all4935 traffic.

4936

4937

Source	Source Port	Destination	Dest Ports	Protocol	Action
10.100.0.0/24,	Any	DMZ network	SSH,RDP,ICMP	ТСР	Trust
DMZ Historian	TCP_High _Ports	PCS-Historian	5450	ТСР	Trust
CRS-NAT (10.100.0.20)	TCP_High _Ports	DMZ-Historian	5450, 5460, 5671, 5672	ТСР	Trust
DMZ Historian	TCP_High _Ports	CRS-NAT (10.100.0.20)	5457, 5450	ТСР	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	ТСР	Trust
Hyper-V Host Servers, Esxi Host Server	Any	Veeam Server	ICMP, 2500- 5000	ТСР	Trust
inside_interface	Any	outside_interface	Any	Any	Allow
DMZ Historian	Any	Symantec Server	SMB (445), HTTPS	ТСР	Trust
Symantec Server	Any	DMZ Historian	HTTP, HTTPS, 8014	ТСР	Trust
DMZ Historian	Any	Graylog Server	514	UDP	Trust
#### CSF MFG PROFILE LOW SEC LVL EXAMPLE IG DISCRETE-BASED MFG SYSTEM USE CASE

Ove	rview Analysis Policies Devices Objects	AMP Intelligen	ce ors Correlation	Actions v									Deplo	iy 📀 System Help 🔻	admin 🔻
	-Policy Access Control Policy	, Application Detect	and the second se											Save (	🔀 Cancel
refil Rul	ter Policy: <u>Default Prefilter Policy</u>	ging Advanced	SSL Policy: None		Ide	entity Policy: )	None						📑 Inhe	ritance Settings   🖳 Policy Assi	gnments (1)
尙	Filter by Device								l	Show Rule Conflicts 😣	O Add	Category	🔾 Add Rule	earch Rules	X
#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicat	Source Ports	Dest Ports	URLs	ISE/S	Action	V 🗅 🔒 🕁 🏾 🛡	
<b>•</b> 1	Mandatory - AC-Policy (1-13)														-
1	Allow-SSH-RDP-DMZ	Any	Any	Testbed-LAN-Networ	DMZ-Network	Any	Any	Any	Any	x <sup>®</sup> ICMP (1)	Any	Any	⇒ Trust	Ū 🗅 🔒 🖄 Ū Ū	d 🕄
2	PI-To-PI	Any	Any	RCS-Historian	👼 PI-Server-DMZ	Any	Any	Any	TCP_high_ports	🤌 PI-to-PI	Any	Any	⇒ Trust	V 🗅 🔒 💼 🖉 o	0
3	PI-to-PI-PCS	Any	Any	PI-Server-DMZ	🚍 PCS-Historian	Any	Any	Any	/ TCP_high_ports	🎤 PI-to-PI	Any	Any	⇒ Trust	00,8650	/ 8
4	CRS-PI-PI	Any	Any	CRS-NAT-IP	PI-Server-DMZ	Any	Any	Any	/P TCP_high_ports	2 TCP (6):5671 TCP (6):5672 PI-Connector PI-DCM	Any	Any	⇒ Trust	0020000	0
5	CRS-PI-To-PI-2	Any	Any	PI-Server-DMZ	💼 CRS-NAT-IP	Any	Any	Any	TCP_high_ports	x <sup>®</sup> TCP (6):5457	Any	Any	⇒ Trust	00.2600	/ 0
6	Allow-DNS-DMZ	Any	Any	DMZ-Network	💂 LAN-AD01-DNS-Sen	w Any	Any	Any	Апу	DNS_over_UDP	Any	Any	🖌 Allow	002600	/ 8
7	Veeam-Mgmt-Hosts	Any	Any	💭 Veeam	Hyper-VServers Esxi-Host.mgmt	Any	Any	Any	Απγ	<pre># ICMP (1)     TCP_high_ports     Veeam-channel-ports     NetBIOS-TCP     (4 more)</pre>	Any	Any	⇒ Trust	V 6 2 6 C •	0
8	HyperV-Hosts-Veeam	Any	Any	Esxi-Host.mgmt Hyper-VServers	👼 Veeam	Any	Any	Any	Απγ	☆ ICMP (1) → Veeam-channel-ports	Any	Any	⇒ Trust	002600	/ 6
9	Internet-Access	🚓 inside	🚓 outside	Any	Any	Any	Any	Any	Any	Any	Any	Any	🖌 Allow	😈 🗅 🔏 🖄 🖉 o	/ 8
10	Symantec-DMZ-1	Any	Any	SymantecMgr	PI-Server-DMZ	Any	Any	Any	Any	☆ TCP (6):445 > SMB-Windows > HTTPS	Any	Any	🖋 Allow	0 1 <b>6 6</b> 7 V	0
11	Symantec-DMZ-2	Any	Any	PI-Server-DMZ	SymantecMgr	Any	Any	Any	Any	<ul> <li>HTTPS</li> <li>HTTP</li> <li>Symantec</li> </ul>	Any	Any	🖋 Allow	U D 2 6 D 0	/ 5
12	DMZ-Syslog	Any	Any	💂 PI-Server-DMZ	💂 Graylog	Any	Any	Any	Апу	🎤 SYSLOG	Any	Any	🖌 Allow	00,8650	6
												Die	playing 1 - 13 of 13	rules 1/ / Page 1 of 1	•
												513	,, 1 10 01 10		alulu

4942

# 4943 NAT Policy

• A Dynamic NAT policy was configured to allow internet access.

Type of NAT rule	Auto NAT [1]
Source Interface	inside
Destination Interface	outside
Original sources	10.100.0.0/8
Translated Source	Destination Interface IP
Options	Translate DNS Replies that match this Rule: False

Edit NAT Rule							?
NAT Rule:	Auto NAT Rule	×					
Туре:	Dynamic	•	🖉 Enable				
nterface Objects	Translation	PAT Pool	Advanced				
Original Packet					Translated Packet		
Original Source:* Original Port:	IPv4-Priva	te-10.0.0.0-8		▼ ○	Translated Source:	Destination Interface IP The values selected for Destination Interface Objects in 'Interface Objects' tab will be use	ve ved
					Translated Port:		

## 4947 Snort Inspection

# 4948 • Snort Inspection was enabled on the following ACL rules

Name of the ACL	Intrusion Policy
Internet- Access rule	Balanced connectivity and security

Name Internet-Access   Action Allow     Zones Networks   VLAN Tags Users   Applications Ports   URLs SGT/ISE   SGT/ISE Inspection   Logging Comment   Intrusion Policy Variable Set   Balanced Security and Connectivity Default Set	Editin	ng Ru	ile - Intern	et-Access								
Action Allow	Name	e Int	ernet-Access				🗹 Ena	abled	Move			
Zones       Networks       VLAN Tags       Applications       Ports       URLs       SGT/ISE Attributes       Inspection       Logging       Comme         Intrusion Policy       Variable Set       Variable Set<	Action	n 🖌	Allow			R 🗇 💟 💌	in 📘					
Intrusion Policy Variable Set Balanced Security and Connectivity File Policy None	Zon	nes	Networks	VLAN Tags	🛆 Users	Applications	Ports	🛆 URLs	SGT/ISE Attributes	Inspectio	on Logging	Commer
Balanced Security and Connectivity	Intrusi	ion Po	licy						Variable Set			
File Policy None	Baland	nced S	ecurity and Con	nectivity				*	Default Set			~
	None											

## 4955 DMZ Network

- 4956 A Separate interface was setup for the Manufacturing DMZ LAN Network for hosting the DMZ
- 4957 **Historian** server.

Overvie	w Analy	sis Policie	es Device	es Obje	ects AMP	Intel	ligence			Deploy	0	System
Device I	Manageme	nt NAT	VPN <b>•</b>	QoS	Platform Sett	tings	FlexConfig	Certificates				
Cisco ASA	-ASA 5512-X Threa	at Defense										<b>E</b> 5
Device	Routing	Interfaces	Inline Sets	DHCP								
									🔍 dmz	>	<u>چ</u> ]	Sync Device
Inte	rface	Logical N	lame	Тур	be :	Security	y Zones	MAC Addr.	IP Addr	ess		
<b>(</b>	GigabitEthern	let dmz		Phy	sical	dmz			10.100.1	L.1/24(Statio	c)	

4958

## 4959 **2. Configuration on RuggedCom Firewall**:

- 4960 The following features, settings were enabled on this firewall
- 4961 Network Segmentation
- 4962 ACL Rules
- 4963 Masquerading (NAT) rules

#### 4964 Network Segmentation

- 4965 Separate network interfaces were configured for the different network segments as listed below
- Supervisory LAN Interface (Network: 192.168.0.0/24)
- 4967 Control LAN Interface (Network: 192.168.1.1/24)
- LAN Interface (IP: 10.100.0.20, Uplink to Cybersecurity LAN)
- 4969 Access Control List (ACL) rules
- 4970 The following zones were created:
- WAN Zone for internet-bound / uplink connections to Cybersecurity LAN.
- 4972 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)
- 49754976 The following firewall policies were created:
- 4977 Allow traffic between firewall and WAN.

- 4978 Allow traffic between firewall and MGMT.
- Allow traffic between firewall and CTRL.
- 4980 Allow traffic between firewall and Supervisory.
- 4981 All other traffic is DROPPED.
- 4982
- 4983 The following firewall rules were created

4984	1) ALLOW: POLARIS:ANY -> 192.168.1.0/24,10.100.0.0/24:22 (TCP)
4985	2) ALLOW: vCONTROLLER1, vCONTROLLER2: ANY -> PLC:502 (TCP)
4986	3) ALLOW: STATION1,STATION2,STATION3,STATION4:ANY -> PLC,HMI:502 (TCP)
4987	4) ALLOW: STATION4:ANY -> PLC:502 (TCP)
4988	5) ALLOW: HISTORIAN:ANY -> STATION1,STATION2,STATION3,STATION4,PLC:502 (TCP)
4989	6) ALLOW: MINTAKA, vCONTROLLER1, vCONTROLLER2: ANY -> POLARIS: 11311 (TCP)
4990	7) ALLOW: vCONTROLLER1,vCONTROLLER2:ANY -> POLARIS:115,2049 (TCP)
4991	8) ALLOW: vCONTROLLER1,vCONTROLLER2:ANY -> POLARIS:115,2049 (UDP)
4992	9) ALLOW: ANY:ANY -> ANY:ANY (ICMP)
4993	10) ALLOW: PLC,HMI:ANY -> STATION1,STATION2,STATION3,STATION4:502 (TCP)
4994	11) ALLOW: PLC:ANY -> vCONTROLLER1,vCONTROLLER2:502 (TCP)
4995	12) ALLOW: POLARIS:32678-65535 -> MINTAKA,vCONTROLLER1,vCONTROLLER2:32768-
4996	65535 (TCP)
4997	13) ALLOW: POLARIS:ANY -> I800Switch-Management-UI:80,443 (TCP)
4998	14) ALLOW: NESSUS/OPEN-AUDIT:ANY -> 192.168.1.0/24:22 (TCP)
4999	15) ALLOW: VCONTROLLER1,VCONTROLLER2:32768-65535 -> POLARIS:32768:65535 (UDP)
5000	

Rule Name	IP Type	Action	Source Zone Hosts	Destination Zone Hosts	Log Level	Protocol	Source Po
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
/lodbusRule4	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
/lodbusRule5	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	
VFSudp	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	32678:655
800MgmtUI	ipv4	accept	192.168.0.20	192.168.1.10	none	tcp	none
lessusSSH	ipv4	accept	192.168.0.11,192.168.0.12	192.168.1.0/24	none	tcp	none
Vountd	ipv4	accept	192.168.1.3,192.168.1.4	192.168.0.20	none	udp	32768:65

----

	~ .
50	$\Omega A$
30	04

5006

- 5007 NAT Policy:
- Two Masquerading rules were created (one for each LAN segment) to NAT all traffic going
- 5009 outbound from the Work Cell to the Cybersecurity LAN network. Masquerading is a form of
- 5010 Dynamic NAT. Both hide a single subnetwork behind a single IP address
- 5011

Rule #	Outgoing Interface	Source Network	NAT IP address
1	Ge-3-2 (Uplink interface to Cybersecurity LAN)	192.168.1.0/20	10.100.0.20
2	Ge-3-2 (Uplink interface to Cybersecurity LAN)	192.168.0.0/20	10.100.0.20

#### 5012

iew   Edit Private   Ed	dit Exclusive								
by fwconfig		5 fw1		fwzone		📄 snat			
🛅 fwhost 📄 snat2									
im fwinterface									
twpolicy									
				fwrule					
				fwnat					
				<u>fwmasq</u>					
/security/firewall/fwconfig{fw1}/fwmasg									
Masqueradings									
Masquerade Entry Name	IP Туре	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		
10	inud	de-3-2	not found	disabled	192 168 0 0/24	10 100 0 20	not found		

- 5014 **3. Configuration on GTB Inspector**:
- 5015 Refer to section 4.12.5

#### 4.16.6 Highlighted Performance Impacts 5016

- 5017 Two performance measurement experiments were performed for network boundary protection 5018 while the manufacturing system was operational:
- 5019 3. <u>CL009.1</u> - Firewall rules and Access control list (ACL) rules are implemented at the CRS 5020 boundary router.
- 5021 4. CL012.1 - Firewall and ACL rules are implemented on an upgraded boundary router.
- 5022 These two experiments were performed chronologically after the experiment CL011.2 where the
- 5023 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 5024 and CL012.1) are not included in those sections.
- 5025

#### 5026 4.16.6.1 Experiment CL009.1

- 5027 Firewall rules and access control list (ACL) rules were implemented at the CRS boundary router.
- 5028 All authorized connections were verified to be allowed by the firewall before the manufacturing
- 5029 process was operational.

5032

5030 A small increase in the average robot job actuation time was observed on Robot 2 for Job 203 5031 (see Figure 4-52). No other increases were observed for any of the other jobs.



#### 5033 Figure 4-52 - Time-series (left) and boxplot (right) showing the job actuation times for Job 203 during the 5034 CL001.2 baseline and CL009.1 experiment.

5035 A slight increase of the part production time mean was observed during this experiment but is 5036 not statistically significant.

#### CSF MFG PROFILE LOW SEC LVL EXAMPLE IG DISCRETE-BASED MFG SYSTEM USE CASE



5037

5038 Figure 4-53 - Bihistograms showing the part production time (left) and estimated mean production time using 5039 the bootstrap method (right) using the measurements from baseline CL001.2 and experiment CL009.1.

#### 5040 **4.16.6.2 Experiment CL012.1**

5041 The CRS boundary router was replaced with a Cisco ASA-5506, and the same firewall rules and 5042 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.



5047 Figure 4-54 - Bihistograms showing the part production time (left) and estimated mean production time using 5048 the bootstrap method (right) using the measurements from baseline CL001.2 and experiment CL012.1.

5049

#### 5050 **4.16.7** Link to Entire Performance Measurement Data Set

- 5051 CL009.1-BoundaryFirewall.zip
- 5052 <u>CL012.1-CiscoASA5506.zip</u>

## 5053 **4.17 Managed Network Interfaces**

### 5054 **4.17.1 Technical Solution Overview**

5055 Managing network interfaces controls what network devices are plugged into switches within 5056 manufacturing system, along with physical labeling connections to help with system 5057 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 5058 5059 the corresponding network cable for easy identification. All cable should be labeled/identified at 5060 the switch and at the opposite end of the network cable. Switch Port Security should be 5061 configured to restrict access to only allowed preconfigured Media Access Control (MAC) addresses devices. 5062

- 5063 Minimal cost for labeling. Effort of implement is high, but not difficult. The effort will be spent 5064 taking the required time to accurately identify cabling connections.
- 5065 Most switches have built in Port security. Since this technical control is built into switches there 5066 is no additional cost for implementation. Configuration for Port security is well documented and 5067 easily configured.

## 5068 **4.17.2 Technical Capabilities Provided by Solution**

- 5069 Managed Network Interfaces provides components of the following Technical Capabilities5070 described in Section 6 of Volume 1:
- Managed Network Interfaces

#### 5072 **4.17.3 Subcategories Addressed by Implementing Solution**

5073 PR.AC-5

#### 5074 **4.17.4** Architecture Map of Where Solution was Implemented



5070	-
<u>ה/ נור</u>	
2010	

5077	4 17 5 Installation Instructions and Configurations
3011	$-\tau$ . $\tau$ . $\tau$ . $\tau$

#### Managing Network Interface Instructions

5079 **Overview:** 

5080 Port labeling provides ability for others to understand and know what network devices belong
5081 where. Managing your switches with correct labeling and classification makes troubleshooting
5082 simpler along with improving cybersecurity.

- 5083 Labeling ports within switch:
- 5084 Switches within CRS:
- 5085 Siemens RuggedCom RX1510 (Router) 192.168.0.2
- 5086 Siemens RuggedCom i800 (Switch) 192.168.1.10
- 5087 Netgear GS724T (Switch) 192.168.0.239
- 5088
- 5089 Siemens RuggedCom RX1510
- Interface labels can't be changed from defaults.
- 5091 Siemens RuggedCom i800
- Login to switch via web browser. <u>https://192.168.1.10</u>
- Click on **Ethernet →Ports-Configure Port Parameters**.
- Click desired port number for renaming.

• Type in Name to identify port and click apply.

		• 1	• • • • •
		Port:	1
		Name:	STA1
		Media:	100TX
		State:	Disabled: O Enabled: •
		AutoN:	On:  Off:  O
		Speed	Auto ~
		Dupx	Auto ~
		FlowCtrl:	On: ○ Off: ●
		LFI:	Off: 💿
		Alarm:	On:  Off:  O
		Act on LinkDown:	Do nothing: <ul> <li>Admin Disable: O</li> </ul>
			Apply Reload
5006			Changes saved
5096			5
5097	Netgear		
5098		• Login to switch v	ia web browser. <u>https://192.168.0.239</u>
5099		• Click on Tab labe	eled "Switching"
5100		System Switching	Routing QoS Security Monitoring Maintenance Help Index
5101		• Select port that w	ill be labeled.
5102		Enter Description     Port Description     g1     CTRL SYS I	AN UPLINK
5103			AN UPLINK
5104		• Finally click appl	y button in lower right-hand corner.
5105			CANCEL
5106	Overview:		

5107 Port security prevents unauthorized devices from being plugged into a network switch while
5108 trying to obtaining sensitive information, which could be used for mapping out network
5109 connections for possible data exfiltration. When an unauthorized device is plugged into a
5110 protected port a warning message is logged and sent to a syslog server if supported by switch

5111 vendor.

5113 **Collaborative Robotics Enclave:** 5114 • This enclave contains three different switches/routers. 5115 • Siemens RuggedCom RX1510 (Can function as Router/Firewall/Switch) 5116 • Siemens RuggedCom i800 (Switch) • NETGEAR GS724Tv4 (Switch) 5117 5118 **RuggedCom RX 1510:** Has multiple ports which are individual configurable depending on 5119 desired network topology. 5120 • Ports LM1/1 and LM1/2 = disabled 5121 • Ports LM2/1 (Switchport = False, port is configured for routing), LM2/2 (Switchport = 5122 True, port is configured for mirroring) 5123 • Ports LM3/1 and LM3/2 (Switchport = False, ports are configured for routing) 5124 • Ports LM4/1 and LM4/2 = disabled 5125 • Only port security being applied to RuggedCom RX 1510 is LM1/1, LM4/1, LM4/2 which are disabled. 5126 5127 **RuggedCom i800:** Layer 2 switch that allows for all ports for switching or mirroring. 5128 • Ports 1 to 7 are all configured for switching. 5129 • Port **8** is configured for mirroring. NETGEAR GS724Tv4: Layer 2, Layer 2+ along with Layer 3 Lite features. All ports on this 5130 5131 switch in our environment are configured for switching only. 5132 • Ports 2, 4, 6, 8, 9, 10, 12, 14, 16, 17, 18, 20, 21, 22, 25, 26 are disabled (If any device is 5133 plugged into any of these ports there will be no link light). 5134 • Ports 1, 3, 5, 7, 11, 13, 15, 19 are all enabled and labeled (Each port has Port Security 5135 enabled). • Port 23 is used for management with no Port Security enabled (Used for accessing 5136 5137 switch with any network device). 5138 • Port 24 is mirror port connect to RA3. This port is configured for Probe. 5139 **Port Security Configuration for NETGEAR and i800:** 5140 **NETGEAR:** 

> **Port-Security** interface g1 dot1x port-control mac-based description 'CTRL SYS LAN UPLINK' Port Security port-security max-dynamic 0 port-security max-static 3

port-security mac-address 00:0C:29:CE:7F:94 1 port-security mac-address 94:B8:C5:0E:E1:01 1 port-security mac-address 94:B8:C5:0E:E1:9F1 interface g3 dot1x port-control mac-based description 'Beckhoff Automation GmbH' port-security port-security max-dynamic 0 port-security max-static 1 port-security mac-address 00:01:05:17:DB:08 1 interface g5 dot1x port-control mac-based description 'Polaris (DELL)' port-security port-security max-dynamic 0 port-security max-static 1 port-security mac-address F8:B1:56:BA:09:A8 1 interface g7 dot1x port-control mac-based description 'PROBE1-A' port-security port-security max-dynamic 0 port-security max-static 1 port-security mac-address 00:05:E4:03:7C:3B 1 dot1x port-control mac-based description 'Wago Kontakttechnik Gmbh' port-security port-security max-dynamic 0 port-security max-static 1 port-security mac-address 00:30:DE:00:C4:3C 1 interface g13 dot1x port-control mac-based description 'Robotics Hyper-V / Open AudIT' port-security port-security max-dynamic 0 port-security max-static 3

port-security mac-address 00:15:5D:02:0A:07 1 port-security mac-address 00:15:5D:02:0A:0E 1 port-security mac-address 00:15:5D:02:0A:43 1 interface g15 dot1x port-control mac-based description 'Laptop on CRS Desk' port-security port-security max-dynamic 0 port-security max-static 1 port-security mac-address 34:E6:D7:22:C3:ED 1 interface g19 dot1x port-control mac-based description 'HyperV' port-security port-security max-dynamic 0 port-security max-static 3 port-security mac-address 00:10:18:B8:19:10 1 port-security mac-address 00:10:18:B8:19:11 1 port-security mac-address 00:15:5D:16:AC:07 1

#### 5141

5142

#### 5143 **i800**:

MAC Address	Attached Machine	VID	Port	Туре	CoS
00-15-5D-16-AC-02	vController1	1	6	Static	N/A
00-15-5D-16-AC-03	vController2	1	6	Static	N/A
94-B8-C5-0E-E1-9F	Uplink	1	5	Static	N/A
A0-CE-C8-1F-BD-99	MINTAKA	1	7	Static	N/A
B0-D5-CC-F4-26-EC	Station 4	1	4	Static	N/A

B0-D5-CC-FA-70-C9	Station 1	1	1	Static	N/A
B0-D5-CC-FA-7A-43	Station 3	1	3	Static	N/A
B0-D5-CC-FE-6E-B1	Station 2	1	2	Static	N/A
C8-1F-66-C8-6A-ED	MINTAKA	1	7	Static	N/A
C8-1F-66-CA-26-C0	Robotics VH	1	6	Static	N/A
C8-1F-66-CA-26-C2	Robotics VH	1	6	Static	N/A

#### 5145 **4.17.6 Highlighted Performance Impacts**

5146 Two performance measurement experiments were performed for the Managed Network

5147 Interfaces technology implementation while the manufacturing system was operational:

- 5148 1. <u>CL010.1</u> Alerts are generated on new physical network connections (via syslog).
- 5149 2. <u>CL010.2</u> MAC address filtering is enabled and configured on CRS network devices,
- and unused physical network ports are disabled on CRS network devices.

#### 5151 **4.17.6.1 Experiment CL010.1**

5152 No performance impact to the manufacturing process was measured during the experiment.







#### 5156 **4.17.6.2 Experiment CL010.2**

- 5157 An increase in the robot job execution time was observed on Robot 1 for Job 103 (see Figure
- 5158 4-56), with two relatively large increases for parts 3 and 24. No other increases were observed 5159 for any of the other jobs.





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



5166 Figure 4-57 - Bihistograms showing the part production time (left) and estimated mean production time using 5167 the bootstrap method (right) using the measurements from baseline CL001.1 and experiment CL010.2.

#### 5168 **4.17.7** Link to Entire Performance Measurement Data Set

- 5169 <u>CL010.1-NetworkPhysicalConnections.zip</u>
- 5170 CL010.2-NetworkMACFiltering.zip

#### 5171 **4.18 Time Synchronization**

#### 5172 **4.18.1 Technical Solution Overview**

- 5173 Ability to have all devices sync from a reliable time source. Time synchronization is vital for
- 5174 system logins, event tracking and all other time sensitive events occurring with a manufacturing 5175 system.
- 5176 No additional cost since services are included.
- 5177 Ease of use simple
- 5178 Effort and time required = minimal

#### 5179 **4.18.2 Technical Capabilities Provided by Solution**

- 5180 Time Synchronization provides components of the following Technical Capabilities described in 5181 Section 6 of Volume 1:
- Time Synchronization

#### 5183 **4.18.3 Subcategories Addressed by Implementing Solution**

5184 PR.PT-1

#### 5185 **4.18.4** Architecture Map of Where Solution was Implemented



5187	4.18.5 Installation Instructions and Configurations
5188	<b>Collaborative Robotics System Time Synchronization</b>
5189	
5190	Computers:
5191 5192	<b>Linux Machines:</b> Directions below work for all Linux machine within manufacturing system environment.
5193 5194 5195 5196 5197 5198	<ul> <li>Login to desired system using SSH client.</li> <li>Once logged on open a terminal window.</li> <li>Navigate to /etc</li> <li>open "ntp.conf" using text editor. (Make sure to type "sudo" before command for required write permissions)</li> <li>Edit the location for NTP Server setting. Save the file and exit.</li> </ul>
5199	<pre># 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</pre>
5200 5201 5202 5203 5204	<ul> <li>Now type this command to restart NTP "sudo service ntp restart "</li> <li>Provide password for sudo when prompted.</li> <li>Type "ntpq -p" to verify ntp is getting time from correct source.</li> </ul>
5205	Domain Controller: Is not providing time for this environment.
5206	Other Devices:
5207	Router:
5208	Siemens RuggedCom RX 1510: Device connects to Meinberg at 10.100.0.15 for time.
5209	• Login into RuggedCom RX 1510 via web browser. <u>https://192.168.1.2</u>

• Click on "Edit Private" to put into configuration mode.

?

?

3

0

?

?

5211 Click on Services  $\rightarrow$  time  $\rightarrow$  ntp  $\rightarrow$  server. • time <u>time</u> htp <u>ntp</u> istatus <Add server> vrrp 💮 ntp-status 10.100.0.15 dhcpserver berver 📩 dhcpserver6 broadcast ddns 📄 restrict 📄 nhrp in key conn-sync netflow 5212 • Click on Add server or select existing to edit. 5213 Enter server IP address for device providing time service and click Add button. 5214 • Metwork Time Protocol (NTP) Servers Key settings **NTP Server** Enable 3 10.100.0.15 Enabled Peer

Image: Per

Image: Per
</t

Prefer

Key

Enabled

- 5215
- Make sure to enable newly created entry. See screen shot to right side above.
- 5217 Switches:
- 5218 Siemens i800:
- Login via web browser. <u>http://192.168.1.10</u>
- 5220 Once logged in click on "Administration → System Time Manager → Configure
- 5221 NTP → Configure NTP Servers"

• Now Select primary or back and make the required changes.

	Server:	Primary	
	IP Address:	192.168.1.2	E
	Reachable:	Yes	
	Update Period:	60 min	
	Apply	Reload	
•	Click Apply to save	e changes.	

5225 • Log out

5223 5224

## 5226 Netgear GS724T:

- Login via web browser portal. <u>https://192.168.0.239</u>
- Once logged in click on  $\rightarrow$  **Time** button.

×.	System Information
×.	IP Configuration
×.	IPv6 Network
	Configuration
s.	IPv6 Network Neighbor
2	Time
×.	Denial of Service
×.	DNS
×.	Green Ethernet

- Enter required information to configure NTP time on this switch.
- 5231

5229

Lesson Learned: The master time reference selected should be as close to your physical locationas possible. This should reduce the Off Set.

- 5234 **4.18.6 Highlighted Performance Impacts**
- 5235 No performance measurement experiments were performed for time synchronization due to its 5236 installation in the system before the Manufacturing Profile implementation was initiated.

#### 5237 4.18.7 Link to Entire Performance Measurement Data Set

- 5238 N/A
- 5239

#### 5240 **4.19 System Use Monitoring**

#### 5241 **4.19.1 Technical Solution Overview**

- 5242 System use monitor is accomplished by multiple tools to protect manufacturing system
- environment from harmful actives using data loss protection, system hardening and syslog serverfor monitoring, store and auditing. Each tool provides a different level required to protect the
- 5245 manufacturing system.
- 5246 Implementation effort is moderate requiring understand of Linux systems, along with virtual
- 5247 machine experience. Time required to install and configure all components 20 to 30 hours
- 5248 depending on skill level.

#### 5249 **4.19.2** Technical Capabilities Provided by Solution

- 5250 System Use Monitoring was provided by GTB Inspector, Ports and Services Lockdown, and
- 5251 Graylog.

#### 5252 **4.19.3 Subcategories Addressed by Implementing Solution**

5253 PR.AC-1, PR.DS-5, PR.MA-2, DE.CM-3

#### 5254 **4.19.4** Architecture Map of Where Solution was Implemented

5255 DLP Solution:



## 5257 Graylog Solution:

5258



#### 5260 **4.19.5** Installation Instructions and Configurations

- 5261 System use monitoring was implemented using a combination of tools such as GTB Inspector,
- 5262 Graylog and native Linux OS capabilities such as enabling rsyslog, hardening of permissions.
- 5263 GTB Inspector: See Section 4.12.5 for instructions.
- 5264
- 5265 Graylog: See Section 4.13.5 for instructions.
- 5266 Permissions on user home directories changed from 755 to 700 to protect data from authorized5267 access using chmod.

#### 5268 **4.19.6 Highlighted Performance Impacts**

- 5269 Due to the specific implementation of "System Use Monitoring" performed in the CRS, the
- 5270 performance impacts relating to this technical capability can be found in the following sections:
- 5271 GTB Inspector Section 4.12.6
- 5272 Graylog Section 4.13.6
- 5273 **4.19.7** Link to Entire Performance Measurement Data Set
- 5274 N/A
- 5275

### 5276 **4.20** Ports and Services Lockdown

### 5277 4.20.1 Technical Solution Overview

5278 Ports and services lockdown solutions enable a manufacturer to discover and disable 5279 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 5280 5281 identifying what ports it must send traffic to. Hackers use port scanners and vulnerability 5282 scanners to identify open ports on servers. By revealing which ports are open, the hacker can 5283 identify what kind of services are running and the type of system. Closing down unnecessary 5284 ports by uninstalling un-necessary programs considerably reduces the attack surface. These 5285 actions need to be performed manually.

5286

Native OS capabilities, Open-AudIT and Nessus scanner were leveraged to inventory list of ports
and applications currently running on each device of the plant.

## 5290 **4.20.2** Technical Capabilities Provided by Solution

5291 Ports and Services Lockdown provides components of the following Technical Capabilities 5292 described in Section 6 of Volume 1:

- 5293
- Ports and Services Lockdown

#### 5295 **4.20.3 Subcategories Addressed by Implementing Solution**

5296 PR.IP-1, PR.PT-3



#### 5298 **4.20.4** Architecture Map of Where Solution was Implemented

- 5300 **4.20.5** Installation Instructions and Configurations
- 5301 The following steps were performed
- 5302 On the Linux hosts:
- A software inventory of each Linux system was performed using Open-AudIT. The
   inventory reports were reviewed, and a list of unwanted packages were identified. This
   includes software that comes with the OS by default such as Remina, vino, Thunderbird etc.
   These programs were then uninstalled.
- Hardened /etc/exports file on the NFS-server to export nfs-shares to specific client IP
   addresses with Read only permissions
- Disabled the **dnsmasq** service and socket on machining stations, as they are not required for normal operations
- Disabled services such as mongodb, modem-manager from Robot Driver server and
   Engineering Workstation.
- Restricted SSH access to select users in the /etc/ssh/sshd\_config file.
- 5315 On the HMI:
- Ports 21 161 which were detected as open by Open-AudIT were disabled.
- Modified the HMI program to disable the option to "restart" a machining station and to "clear the part counter" of a station if the station is NOT in the STOP mode.
- 5321 1. On the PLC:
- 5322

5314

- Ports 23, 80, 139, 443, 445, 5120, and 8080 were closed by disabling services.
- Services disabled: HTTP server, Telnet, web proxy, SMB, SNMP. This was performed by modifying Windows CE registry entries, as described on p.40 in the "Document about IPC Security" from Beckhoff. These actions required the PLC to be rebooted.
- Remaining open TCP ports: 21, 987. FTP is used by current work cell operations
- SMB and SNMP services were disabled. The SNMP service was disabled by modifying
   Windows CE registry entries.
- 5330 2. On the Network devices:
- 5331
- Changed the SNMP community string from the default **public** to something private.
- 5333
- 5334
- 5335

#### 5336 **4.20.6 Highlighted Performance Impacts**

- 5337 One performance measurement experiment was performed for the Ports and Services Lockdown
- technology implementation while the manufacturing system was operational:
- 5339 1. <u>CL008.1</u> The concept of least privilege is implemented on CRS hosts.

#### 5340 **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.



5344 Figure 4-58 - Bihistograms showing the part production time (left) and estimated mean production time using 5345 the bootstrap method (right) using the measurements from baseline CL001.1 and experiment CL008.1

- 5346 **4.20.7** Link to Entire Performance Measurement Data Set
- 5347 CL008.1-LeastPrivilege.zip

#### 5348 **4.21 VeraCrypt**

#### 5349 **4.21.1 Technical Solution Overview**

- VeraCrypt is a free open source disk encryption software for Windows, Mac OSX and Linux<sup>24</sup>.
   VeraCrypt main features:
- Creates a virtual encrypted disk within a file and mounts it as a real disk.
- Encrypts an **entire partition or storage device** such as USB flash drive or hard drive.
- Encrypts a **partition or drive where Windows is installed** (pre-boot authentication).
- Encryption is <u>automatic</u>, <u>real-time(on-the-fly)</u> and <u>transparent</u>.
- <u>Parallelization</u> and <u>pipelining</u> allow data to be read and written as fast as if the drive was not encrypted.
- Encryption can be <u>hardware-accelerated</u> on modern processors.
- 5359 **4.21.2 Technical Capabilities Provided by Solution**
- 5360 VeraCrypt provides components of the following Technical Capabilities described in Section 65361 of Volume 1:
- Encryption

#### 5363 **4.21.3 Subcategories Addressed by Implementation**

5364 PR.DS-5

<sup>&</sup>lt;sup>24</sup> VeraCrypt: <u>https://www.veracrypt.fr/en/Home.html</u>





# 5367 **4.21.5** Installation Instructions and Configurations

5368 Details of the Program used

Name	Version	Location
VeraCrypt	1.23	Work-Cell Supervisory LAN

5369

## 5370 Setup Overview:

5371 VeraCrypt was installed on the Engineering Workstation (running Ubuntu Linux) to encrypt a5372 directory containing confidential documents and code files.

#### 5373 Installation:

5374 5375 5376 5377 5378	•	VeraCrypt can be downloaded from <u>https://www.veracrypt.fr</u> . Download the version specific to the Operating System of the Computer you intend to encrypt data on. To install VeraCrypt on Ubuntu, download the .tar.bz2 bundle and extract it on the Linux system. Once done, run the setup script (x86 or x64 version) using the following command:
5379 5380		sudo ./veracrypt-1.23-setup-gui-x64 (File name varies depending on the version used)
5381 5382 5383	•	Once installed, launch it from the Unity Dash or your preferred application launcher. It is important to understand basics of volume-types that can be created using VeraCrypt. As per official documentation <sup>25</sup> , there are two types of VeraCrypt volumes:
5384 5385		<ul> <li>File-hosted (container)</li> <li>Partition/device-hosted (non-system)</li> </ul>
5386 5387 5388		A VeraCrypt file-hosted volume is a normal file, which can reside on any type of storage device. It contains (hosts) a completely independent encrypted virtual disk device.
5389 5390 5391		A VeraCrypt partition is a hard disk partition encrypted using VeraCrypt. You can also encrypt entire hard disks, USB hard disks, USB memory sticks, and other types of storage devices.
5392 5393		The following procedure shows how to configure encrypted volumes of <b>Container</b> type using <b>cli</b> (command line).

<sup>&</sup>lt;sup>25</sup> <u>https://www.veracrypt.fr/en/Documentation.html</u>

- The first thing you need to do is create an encrypted volume where you will store all
- 5396folders/files you'd like to protect. Run the following command(s) and follow the interactive5397menu

5398 sudo veracrypt -t -c

5399

website Terminal
youbot@polaris:/\$ sudo veracrypt -t -c
Volume type:
1) Normal
2) Hidden
Select [1]:

5400 5401

Select 1 for Normal (Standard) Volume. Next, you need to create a file for your encrypted volume. Enter the complete path of the mapper file and select a size. This file will act as the virtual container of your encrypted data so, plan the path and volume size accordingly.

5405

😣 🖨 🗊 Terminal
2) Hidden Select [1]:
Enter volume path: /home/youbot/veracrypt-mapper
Enter volume size (sizeK/size[M]/sizeG): 4096M
Next, select an Encryption algorithm followed by Hashing algorithm from the list

5408 5409 •

😣 🖨 💷 🛛 Terminal
Encryption Algorithm:
1) AES
2) Serpent
5) Kuznvechik
6) AES(Twofish)
7) AES(Twofish(Serpent))
8) Camellia(Kuznyechik)
9) Camellia(Serpent)
10) Kuznyechik(AES)
11) Kuznyechik(Serpent(Camellia)) 12) Kuznyechik(Twefich)
12) KUZHYECHIK(TWOTISH) 13) Serpent(AES)
14) Serpent(Twofish(AES))
15) Twofish(Serpent)
Select [1]:
Hash algorithm:
1) SHA-512
4) Streeboa
Select [1]:

• Select a Filesystem type depending on the OS of the computer. FAT works on all Operating systems.



5414

Enter a password for the virtual container file. For the other options such as Enter PIM and
 Enter Keyfile path, hit Enter to leave them blank or configure one if required. Next the
 wizard will prompt you to type in 320 random characters. This helps to increase the
 cryptographic strength of the encryption keys. Punch in 320 characters randomly and the
 process should move forward. Next, the virtual container for our directory will be created and
 a success message will be shown once it's completed.

5424

5426 5427

5428 5429

5430

5431

5432

5433

5435 5436

😣 🗐 🗊 🖉 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. 5423 Create a directory on which you would want to mount this virtual container on. In our example, a /encrypted directory was created to mount the container on. Next run the 5425 following command to mount sudo veracrypt <path of the container mapper file> <directory to mount on> Enter the password configured earlier and hit Enter for PIM and keyfile if left blank earlier. Choose NO for Protect hidden volume since there wasn't any created. 🗴 🗐 🗊 🖉 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]: If the above command completes successfully, you should have your directory mounted 5434 • successfully. Run df -kh to verify the mount

	P 192.168.0.20 - PuTTY − □ ×
5437	<pre>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:~\$</pre>
<ul> <li>5438</li> <li>5439</li> <li>5440</li> <li>5441</li> <li>5442</li> <li>5443</li> <li>5444</li> <li>5445</li> <li>5446</li> <li>5447</li> <li>5448</li> <li>5449</li> </ul>	<ul> <li>By default, other system users would only have <b>Read</b> access to this directory. To allow other users to write files, configure the permissions or owner as required. You can use this encrypted volume just like any other partition on your hard drive. Data saved in this directory is accessible only as long as the virtual container is mounted. An encrypted volume is just like a file and can be deleted. Ensure to take regular backups of the mapper file to avoid losing data incase if the volume gets deleted</li> <li>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.</li> </ul>
5450	4.21.6 Highlighted Performance Impacts
5451 5452 5453	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).
5454	4.21.7 Link to Entire Performance Measurement Data Set
5455	N/A
5456	
#### 5458 **4.22 Media Protection**

### 5459 4.22.1 Technical Solution Overview

Port locks provide a low-cost solution for protecting USB ports. Implementation and ease of use
provide for quick install and easy removal. USB Port locks provide a simple yet effective
solution to restrict USB use. Once USB Port lock has been inserted and engaged there is no way
of removing lock device without damaging USB port unless key is used. Each USB Port lock can
block up to two ports. These ports are the inserted port, and the port directly to either side
depending on the blocking plate direction. USB Port Lock can be purchased with a collar that
protects attached USB Mice and Keyboards from removal without prior approval.

### 5467 **4.22.2 Technical Capabilities Provided by Solution**

5468 Media Protection provides components of the following Technical Capabilities described in 5469 Section 6 of Volume 1:

- 5469 5470
- 347
- Media Protection

## 5472 **4.22.3 Subcategories Addressed by Implementation**

- 5473 PR.PT-2
- 5474

## 5475 **4.22.4** Architecture Map of Where Solution was Implemented



5476

5477	4.22.5 Installation Instructions and Configurations						
5478	Product / Tools selected to be implemented in testbed:						
5479	<ul> <li>Kensington USB Port Locks (Protects Linux Machines)</li> </ul>						
5480	<ul> <li>Symantec Endpoint Protection (USB Policy Enforcement - Protects Windows</li> </ul>						
5481	Machines)						
5482	<ul> <li>Group Policy (GPO) Active Directory (Protects Windows Machines)</li> </ul>						
5483	Products Overview:						
5484	• USB Port locks from Kensington provide an alternative for small manufactures						
5485	that don't have the resources or primarily run Linux machines within their						
5486	environment to have a solution that protections from rogue USB devices being						
5487	used without approval.						
5488	<ul> <li>Pros: Quick solution, Hardware only solution, inexpensive</li> </ul>						
5489	<ul> <li>Cons: Feels like having to force device into USB Port first few times</li> </ul>						
5490	Insert USB Port lock then push locking button in to secure. Kensington provides inserts to block						
5491	multiple ports including locks designed for securing USB Keyboards and Mice.						
5492	Lessons learned:						
5493	Patience is required when using this product so as not to inadvertently damage USB port						
5494	4.22.6 Highlighted Performance Impacts						
5495 5496	No performance measurement experiments were performed for the USB port locks due to their implementation method (i.e., physically restricting access to USB ports).						
5497	4.22.7 Link to Entire Performance Measurement Data Set						

5498 N/A

## 5499 Appendix A - Acronyms and Abbreviations

- 5500 Selected acronyms and abbreviations used in this document are defined below.
- 5501 **CSF** Cybersecurity Framework
- 5502 **FIPS** Federal Information Processing Standards
- 5503 HMI Human Machine Interface
- 5504 ICS Industrial Control System
- 5505 ICS-CERT Industrial Control Systems Cyber Emergency Response Team
- 5506 **ISA** The International Society of Automation
- 5507 **IT** Information Technology
- 5508 LAN Local Area Network
- 5509 NCCIC National Cybersecurity and Communications Integration Center
- 5510 NIST National Institute of Standards and Technology
- 5511 **NVD** National Vulnerability Database
- 5512 **OT** Operational Technology
- 5513 PLC Programmable Logic Controller
- 5514 US-CERT United States Computer Emergency Readiness Team
- 5515 **VPN** Virtual Private Network

5516 Appendix B - Glossary

5517	Selected	terms	used	in	this	document	are	defined	helow
5517	Sciected	unis	uscu	111	uns	uocument	arc	ucinicu	UC10 W

- 5518 Business/Mission Objectives Broad expression of business goals. Specified target outcome
   5519 for business operations.
   5520
- 5521 **Capacity Planning -** Systematic determination of resource requirements for the
- 5522 projected output, over a specific period. [businessdictionary.com] 5523
- 5524 **Category -** The subdivision of a Function into groups of cybersecurity outcomes closely tied to 5525 programmatic needs and particular activities.
- 5527 **Critical Infrastructure -** Essential services and related assets that underpin American society 5528 and serve as the backbone of the nation's economy, security, and health. [DHS]
- 5529

5526

- 5530 Criticality Reviews A determination of the ranking and priority of manufacturing system
   5531 components, services, processes, and inputs in order to establish operational thresholds and
   5532 recovery objectives.
   5533
- 5534 **Critical Services -** The subset of mission essential services required to conduct manufacturing 5535 operations. Function or capability that is required to maintain health, safety, the environment and 5536 availability for the equipment under control. [62443]
- 5538 **Cyber Risk** Risk of financial loss, operational disruption, or damage, from the failure of the 5539 digital technologies employed for informational and/or operational functions introduced to a 5540 manufacturing system via electronic means from the unauthorized access, use, disclosure, 5541 disruption, modification, or destruction of the manufacturing system.
- 5542

5537

- 5543 Cybersecurity The process of protecting information by preventing, detecting, and responding
   5544 to attacks. [CSF]
- 5545
- 5546 Defense-in-depth The application of multiple countermeasures in a layered or stepwise manner
  5547 to achieve security objectives. The methodology involves layering heterogeneous security
  5548 technologies in the common attack vectors to ensure that attacks missed by one technology are
  5549 caught by another. [62443 1-1]
- 5550
- 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]
- 5554
- 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]
- 5558

5559 Framework - The Cybersecurity Framework developed for defining protection of critical 5560 infrastructure. It provides a common language for understanding, managing, and expressing cybersecurity risk both internally and externally. Includes activities to achieve specific 5561 5562 cybersecurity outcomes, and references examples of guidance to achieve those outcomes. 5563 5564 Function - Primary unit within the Cybersecurity Framework. Exhibits basic cybersecurity 5565 activities at their highest level. 5566 5567 **Incident** - An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or 5568 availability of an information system or the information the system processes, stores, or transmits 5569 or that constitutes a violation or imminent threat of violation of security policies, security 5570 procedures, or acceptable use policies. [CSF] 5571 5572 Integrator - A value-added engineering organization that focuses on industrial control and 5573 information systems, manufacturing execution systems, and plant automation, that has 5574 application knowledge and technical expertise, and provides an integrated solution to an 5575 engineering problem. This solution includes final project engineering, documentation, procurement of hardware, development of custom software, installation, testing, and 5576 5577 commissioning. [CSIA.com] 5578 5579 Manufacturing Operations - Activities concerning the facility operation, system processes, 5580 materials input/output, maintenance, supply and distribution, health, and safety, emergency 5581 response, human resources, security, information technology and other contributing measures to 5582 the manufacturing enterprise. 5583 5584 **Network Access** - any access a network connection in lieu of local access (i.e., user being 5585 physically present at the device). 5586 5587 **Operational technology** - Hardware and software that detects or causes a change through the 5588 direct monitoring and/or control of physical devices, processes and events in the enterprise. 5589 [Gartner.com] 5590 5591 **Programmable Logic Controller** - A solid-state control system that has a user-programmable 5592 memory for storing instructions for the purpose of implementing specific functions such as I/O 5593 control, logic, timing, counting, three mode (PID) control, communication, arithmetic, and data 5594 and file processing. [800-82] 5595 5596 Profile - A representation of the outcomes that a particular system or organization has selected 5597 from the Framework Categories and Subcategories. [CSF] 5598 Target Profile - the desired outcome or 'to be' state of cybersecurity implementation \_ 5599 Current Profile – the 'as is' state of system cybersecurity 5600 5601 **Protocol** - A set of rules (i.e., formats and procedures) to implement and control some type of 5602 association (e.g., communication) between systems. [800-82] 5603

- **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]
  5607
- 5608 **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]

- 5617 **Risk Tolerance** The level of risk that the Manufacturer is willing to accept in pursuit of
  5618 strategic goals and objectives. [800-53]
  5619
- **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]
- 5633 **Supporting Services -** Providers of external system services to the manufacturer through a 5634 variety of consumer-producer relationships including but not limited to: joint ventures; business 5635 partnerships; outsourcing arrangements (i.e., through contracts, interagency agreements, lines of 5636 business arrangements); licensing agreements; and/or supply chain exchanges. Supporting 5637 services include, for example, Telecommunications, engineering services, power, water, 5638 software, tech support, and security. [800-53]
- 5639

5610

5616

5627

5632

- 5640 Switch A device that channels incoming data from any of multiple input ports to the specific5641 output port that will take the data toward its intended destination. [Whatis.com]
- 5642
- 5643 **System Categorization** The characterization of a manufacturing system, its components, and 5644 operations, based on an assessment of the potential impact that a loss of availability, integrity, or 5645 confidentiality would have on organizational operations, organizational assets, or individuals. 5646 [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.
- 5654
- 5655 **Thresholds -** Values used to establish concrete decision points and operational control limits to 5656 trigger management action and response escalation.

# 5657 Appendix C - References

5658 5659 5660 5661 5662	1.	Executive Order no. 13636, Improving Critical Infrastructure Cybersecurity, DCPD-201300091, February 12, 2013. <u>https://www.govinfo.gov/app/details/FR-2013-02-19/2013-03915</u>
5663	2.	National Institute of Standards and Technology (2014) Framework for Improving Critical
5664		Infrastructure Cybersecurity, Version 1.0. (National Institute of Standards and
5665		Technology, Gaithersburg, MD), February 12, 2014.
5666		https://doi.org/10.6028/NIST.CSWP.02122014
5667		
5668	3.	Stouffer KA, Lightman S, Pillitteri VY, Abrams M, Hahn A (2015) Guide to Industrial
5669		Control Systems (ICS) Security. (National Institute of Standards and Technology,
5670		Gaithersburg, MD), NIST Special Publication (SP) 800-82, Rev. 2.
5671		https://doi.org/10.6028/NIST.SP.800-82r2
5672		
5673	4.	Stouffer K, Zimmerman T, Tang CY, Lubell J, Cichonski J, McCarthy J (2017)
5674		Cybersecurity Framework Manufacturing Profile. (National Institute of Standards and
30/3 5676		rechnology, Galhersburg, MD), NIST Internal Report (NISTIR) 8185, Includes updates
5677		as of May 20, 2019. <u>https://doi.org/10.0028/NIS1.IK.8185</u>
5678	5	Federal Motor Vehicle Safety Standards 49 C F R & 571 2011
5679	5.	rederar Wotor Venicle Safety Standards, 47 C.I. K § 571, 2011.
5680	6	Zimmerman T (2017) Metrics and Key Performance Indicators for Robotic Cybersecurity
5681	0.	Performance Analysis. (National Institute of Standards and Technology, Gaithersburg,
5682		MD). NIST Internal Report (NISTIR) 8177. Includes updates as of May 21, 2019.
5683		https://doi.org/10.6028/NIST.IR.8177
5684		
5685	7.	Zimmerman T (2019) Manufacturing Profile Implementation Methodology for a Robotic
5686		Workcell. (National Institute of Standards and Technology, Gaithersburg, MD), NIST
5687		Internal Report (NISTIR) 8227. https://doi.org/10.6028/NIST.IR.8227