NIST Cybersecurity White Paper
NIST CSWP 28

Security Segmentation in a Small Manufacturing Environment

Dr. Michael Powell
National Cybersecurity Center of Excellence
National Institute of Standards and Technology

John Hoyt
Aslam Sherule
Dr. Lynette Wilcox
The MITRE Corporation

This publication is available free of charge from:

https://doi.org/10.6028/NIST.CSWP.28

April 6, 2023

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Technical Series Policies

Publication History

Approved by the NIST Editorial Review Board on 2023-03-30

How to Cite this NIST Technical Series Publication:

Powell M, Hoyt J, Sherule A, Wilcox L (2023) Security Segmentation in a Small Manufacturing Environment. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 28. https://doi.org/10.6028/NIST.CSWP.28

Author ORCID iDs

Dr. Michael Powell: 0000-0002-3922-7435
John Hoyt: 0000-0002-0783-7036
Aslam Sherule: 0000-0002-2003-3817
Dr. Lynette Wilcox: 0000-0003-1246-6505

Contact Information

manufacturing_nccoe@nist.gov

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

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

Abstract

Manufacturers are increasingly targeted in cyber-attacks. Small manufacturers are particularly vulnerable due to limitations in staff and resources to operate facilities and manage cybersecurity. Security segmentation is a cost-effective and efficient security design approach for protecting cyber assets by grouping them based on both their communication and security requirements. This paper outlines a six-step approach that manufacturers can follow to implement security segmentation and mitigate cyber vulnerabilities in their manufacturing environments. The security architecture resulting from the security segmentation design activities is a foundational preparation step for additional security strategies like Zero Trust.

Keywords

Assets; cyber risk mitigation; industrial control systems; manufacturing; security architecture; security controls; security requirements; security segmentation; security strategy.

Audience

The intended audience is managers of information technology and operational technology (IT/OT) systems at small manufacturing organizations. This may include roles of company owner, operations manager, and, if technical resources are present, network and security architect or even the Chief Information Officer/Chief Information Security Officer (CIO/CISO). This paper is intended for those who are interested in implementing a cost-effective and efficient mitigation for cyber vulnerabilities in small manufacturing environments.

Table of Contents

1. Introduction 1
2. Why should I implement Security Segmentation? 2
3. Security Segmentation Overview 3
4. Building Blocks of Security Segmentation 3
4.1. Security Zones 3
4.1.1. Sample Security Zones and Assets 3
4.2. Security Controls 4
4.2.1. Security Control Templates 5
4.3. Trusted Communication 6
5. A Six-Step Approach to Security Segmentation and Typical Deliverables 6
5.1. Step 1: Identify List of Assets 6
5.2. Step 2: Assess Risk and Create Security Zones 7
5.3. Step 3: Determine the Risk Level for the Security Zones 10
5.4. Step 4: Map Communication between the Security Zones 11
5.5. Step 5: Determine Security Controls for the Security Zones 12
5.6. Step 6: Create Logical Security Architecture Diagram 15
6. Next Steps 15
7. Conclusion 16
References 17
Appendix A. Selected Bibliography 18
Appendix B. List of Symbols, Abbreviations, and Acronyms 20

List of Tables

Table 1. How Security Segmentation Addresses Common Weaknesses 2
Table 2. Sample Cybersecurity Practices from the CSF. 5
Table 3. Security Control Template 6
Table 4. Business Impact to Security Zone Risk Level Mapping 10
Table 5. Security Zones and Cyber Risk 11
Table 6. Technical Cybersecurity Practices from the CSF 13

List of Figures

Fig. 1. Representative Example of a Company's Assets and Network. 1
Fig. 2. Manufacturing Applications Security Zone 4
Fig. 3. Industrial Control Systems Security Zone 4
Fig. 4. Business Applications Example. 8
Fig. 5. Administrative Systems Example. 8
Fig. 6. Connectivity Services Example. 8
Fig. 7. Manufacturing Applications Example 9

Fig. 8. Industrial Control Systems Example 9
Fig. 9. Mapping of Communication between Security Zones.....12
Fig. 10. Logical Security Architecture.....15

Acknowledgments

National Institute of Standards and Technology (NIST) and the National Cybersecurity Center of Excellence (NCCoE) would like to thank Celia Paulsen of the NIST Manufacturing Extension Partnership and Suzanne Lightman of NIST Information Technology Laboratory for their contributions to this paper.

1. Introduction

Small manufacturers tend to operate facilities with limited staff and limited resources often causing cybersecurity to fall by the wayside as something that takes too much time or cost. The resulting lack of cybersecurity leaves small manufacturers vulnerable to cyber-attack. The objective of this paper is to introduce security segmentation as a cost-effective and efficient approach to mitigate cyber vulnerabilities for small manufacturing environments.

Some information technology (IT) and operational technology (OT) assets used by a manufacturing company need more cyber protection than other assets. Typical examples of assets in a manufacturing environment are computing infrastructure, networking infrastructure, control system components, and sensitive information. Of these, assets that are involved in the direct operation of the assembly line or plant may require more protection than other assets.

Security segmentation is the grouping of assets into security zones according to the cyber protection they need and placing appropriate safeguards around these security zones. Security segmentation builds on the concept of network segmentation, which is grouping assets based on the communication requirements between these assets. These concepts are explained in the subsequent sections of this whitepaper.

Throughout this paper, a fictional small manufacturer that operates a facility is used as an example. Figure 1 below shows a fictional company's assets and network. This diagram is representative of what may be found in a small manufacturing environment. In reality, manufacturing environments vary in complexity from this example.

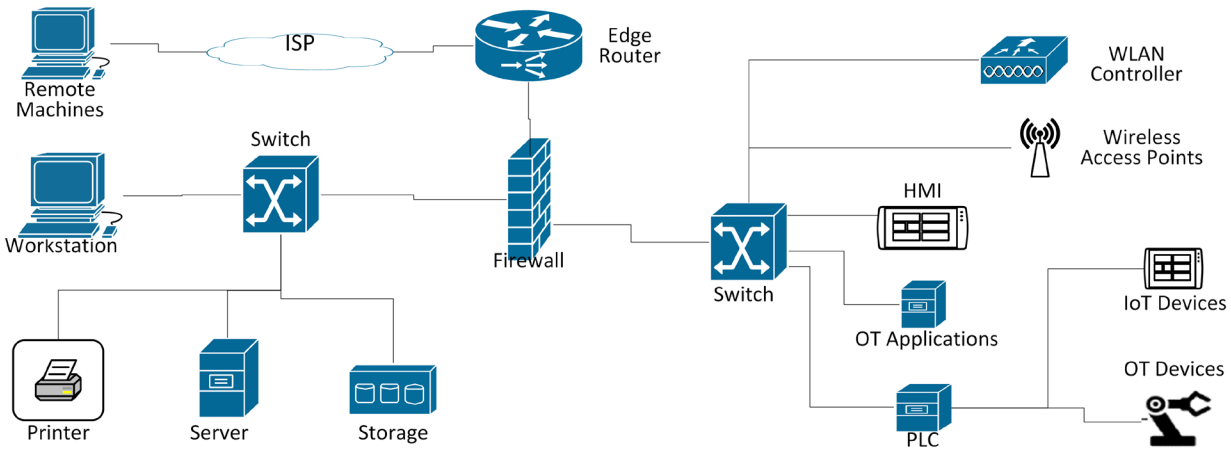

Fig. 1. Representative Example of a Company's Assets and Network.

The activities presented in this paper lay the foundation for an effective and efficient cybersecurity strategy for your company. This paper provides an overview of security segmentation, and then presents an example of a security segmentation design using the following six-step approach:

1) identify a list of assets
2) assess risk and create security zones
3) determine the risk level for the security zones

4) map communications between the security zones
5) determine security controls for the security zones
6) create a logical security architecture diagram

2. Why should I implement Security Segmentation?

Table 1 shows how security segmentation helps address some common cybersecurity weaknesses that most small manufacturing environments face.

Table 1. How Security Segmentation Addresses Common Weaknesses

Common Weakness	Security Segmentation
Incomplete or nonexistent asset inventory: without an asset inventory, it is difficult to identify vulnerabilities or to mitigate them in devices and on the network.	Security segmentation identifies assets and groups them into security zones, which can help with inventory management. Asset inventory is an intrinsic part of security segmentation.
Poor visibility of assets and network traffic: without real-time visibility of assets and network traffic, it is difficult to detect new devices, nefarious activities, or a device going offline.	Security segmentation facilitates implementing network visibility tools through creation of security zones. Security zones break down assets into small groups, so it is easier to set up monitoring tools and analyze results.
Lack of isolation: absence of isolation between different parts of the network enables an attacker to easily move from one system to another.	Grouping assets into security zones can make it easy to identify where to use isolation.
Undefined separation of duties: without the capability to implement separation of duties, a single person may have the ability to change the way systems operate without any oversight or approval. This could allow an attacker who compromises that user's account to make changes without anyone else noticing.	Security segmentation can help clarify who should be able to make changes to systems and who should approve those changes, which can simplify implementation of role-based or rule-based authentication.
Absence of least privilege: in a system that does not limit privileges, individuals may have the ability to perform actions they are not authorized to perform. Additionally, this means anyone with an account on a system can do whatever they want. This means an actor with access to one account can do more damage than if the account had limited privileges.	The application of security segmentation can make implementation of least privilege easier as each security zone has a well-defined function. For example, administrative functions are placed into a separate security zone, and access to that security zone is limited. This makes it easier to determine who should have what privileges and limits access to privileged functions.
Unmanaged remote access (RA) to plant environment: unsecured and unmanaged RA provides an easy attack vector.	Security segmentation can make it easier to identify where RA is needed and to implement a secure RA solution. Some security zones, for example, might not allow RA at all and others can be limited to only certain personnel for specific functions.

In addition, security segmentation provides a standardized way of designing a scalable and consistent security architecture, which can provide benefits such as:

- **Adaptable configurations**: allowing for quick and secure changing of configurations within a security zone to support flexible manufacturing requirements.
- **Increased network resiliency**: helping to provide and maintain an acceptable level of service availability in the face of misconfiguration and faults.

- **Strengthened technological advancements**: enabling secure implementation of automation and technologies associated with Industry 4.0 [1].
- **Support for various security requirements**: a cost-effective approach to separate sensitive product lines for manufacturers with multiple security requirements.

3. Security Segmentation Overview

Security segmentation is an approach for protecting assets by grouping them based on both their communication and security requirements. Security segmentation is accomplished through creating security zones, which are groupings of assets that have similar security requirements, and then applying security controls to the security zones. Securing assets in groups rather than individually makes security easier to implement and manage.

Security zone-based architecture provides a standardized way of designing a scalable and consistent security architecture. It offers increased network resiliency, meaning it helps keep communications working in the face of misconfiguration and faults. Security segmentation can help mitigate the vulnerabilities listed above and should be part of a comprehensive cybersecurity plan.

4. Building Blocks of Security Segmentation

The fundamental building blocks of security segmentation are security zones, security controls, and trusted communications. Each is explained in turn, below.

4.1. Security Zones

A security zone is a group of assets that have similar operational function and criticality; they share common cybersecurity requirements. Assets that have similar operational function often have similar system attributes and need similar protections; they may directly interact with each other and with the surrounding systems in a similar manner. The assets within the security zone have trusted communications with each other. Communication from inside a security zone to outside of the security zone is considered untrusted and subject to security controls. Security zones need to have physical or virtual boundaries to separate them from other security zones. A set of security practices that meets common security requirements is applied either at the security zone edge or within the security zone or both.

4.1.1. Sample Security Zones and Assets

Some possible security zones and sample assets within each security zone are listed below. A facility may not have all of these assets and some assets may be owned by the property manager, internet service provider (ISP), or other vendor. More security zone examples can be found in the six-step approach later in the document.

4.1.1.1. Manufacturing Applications

A security zone can be composed of applications that are involved in the manufacturing operation but are not required for the operation of the assembly line. Examples include the engineering workstation, manufacturing execution systems (MES), data historian, and plant scheduler.

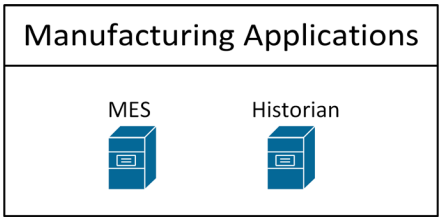

Fig. 2. Manufacturing Applications Security Zone

4.1.1.2. Industrial Control Systems (ICS)

This security zone includes systems that are directly involved in running the production line. Examples include programmable logic controllers (PLC), computer numerical controls (CNC) machines, robot controllers, and human machine interfaces (HMIs).

In some plants with critical manufacturing processes that have people or environmental safety implications, the safety instrumented systems (SIS) would be grouped into a separate security zone because of its criticality for safety-related functions. Plants may also have multiple ICS zones to separate different production lines or have sections of a production line that are more critical than others.

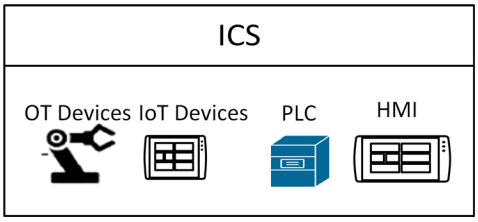

Fig. 3. Industrial Control Systems Security Zone

4.2. Security Controls

Security controls are cybersecurity practices used to safeguard and protect the confidentiality, integrity, and availability of the information and systems of an organization. Security controls can be technical, policy-based, or procedural. Technical security controls are technology solutions like firewalls, antivirus software, or virtual private network (VPN) that increase security of systems. Policy-based security controls are rules that must be followed as part of conducting business operations, e.g., password policy. Procedures are the steps to be followed in executing a task, e.g., procedures to determine necessary access for new employees. Technical, policy, and procedural security controls work in concert with each other to improve security. For

example, a policy requiring use of a VPN for RA does not work without having a VPN (technical practice) in place.

This document uses the NIST Cybersecurity Framework (CSF) [2], and the related NISTIR 8183 Rev. 1 Cybersecurity Framework Version 1.1 Manufacturing Profile ("CSF Manufacturing Profile") [3], as a framework for systematically evaluating what cybersecurity practices are needed for each security zone. The CSF can be used to manage and reduce cybersecurity risks in an organization's environment. The CSF manufacturing profile gives guidance on which practices should be higher priority based on the mission or focus of the OT systems which it separates into five areas: Maintain Human Safety, Maintain Environmental Safety, Maintain Quality of Product, Maintain Production Goals, and Maintain Trade Secrets.

The cybersecurity practices in the CSF and the CSF Manufacturing Profile are organized into five high-level functions (Identify, Protect, Detect, Respond, Recover); each function has one or more categories, and each category has one or more cybersecurity practices. Informative references are also included to show how the CSF maps to various standards or best practices that a business may follow and to provide more context. The following is a sample of cybersecurity practices from the CSF:

Table 2. Sample Cybersecurity Practices from the CSF.

CSF Function	CSF Category	Cybersecurity Practices	CSF Subcategory
Protect	Identity Management, Authentication and Access Control	Manage issuing, verifying, revoking, and auditing identities and credentials for authorized devices, users, and processes.	PR.AC-1
		Manage and control physical access to assets.	PR.AC-2
		Manage RA.	PR.AC-3
		Manage access permissions and authorizations incorporating the principles of least privilege and separation of duties.	PR.AC-4
		Authenticate users, devices, and other assets commensurate with the risk of the transaction (e.g., consider multi-factor authentication for RA).	PR.AC-7

4.2.1. Security Control Templates

Security control templates are organizing mechanisms by which cybersecurity practices can be systematically applied to security zones and assets within them based on their risk level. An organization can establish security control templates for each risk level in an environment by determining what cybersecurity practices should be required for each risk level. Organizations may have multiple security zones of the same risk level. A given security template can be applied to all security zones that share the same risk level.

For this example, "low", "moderate", and "high" risk levels are used for IT assets and "ICS risk" is used for OT assets, as seen in Table 3. After the number of templates are determined, a set of cybersecurity practices are assigned for each security control template indicated by an "X" in Table 3. A higher risk-level security template will include all the security controls of the lower risk-level as well as the additional cybersecurity practices specified for that risk-level. Although Table 3 contains all four risk levels in one table, organizations can use multiple tables, typically one table for each risk level.

The relevant cybersecurity practices depend on the nature of the business and the cyber risks that are being mitigated. Each organization should choose risk levels based on their needs and preferences. Guidelines for assigning the risk level to the security zone and completing the security template are explained later in Sec. 5: A Six-Step Approach to Security Segmentation.

Table 3. Security Control Template

CSF ID	Cybersecurity Practice Description	Applies to Security Zones that are			
		Low Risk	Moderate Risk	High Risk	ICS Risk
PR.AC-3	Manage RA.	X	X	X	X
PR.AC-7	Authenticate Users, devices, and other assets commensurate with the risk of the transaction.				
	Single-factor authentication	X	X		X
	Multi-factor authentication			X	

4.3. Trusted Communication

In the context of security segmentation, *trusted communication* is the principle that the assets within a security zone trust each other and will accept communication originating from any asset within that security zone but will not trust communication from a different security zone. In other words, *intra*-zone communication is trusted, but *inter*-zone communication is considered untrusted and must be well understood, defined, configured, and managed. Furthermore, communications between security zones of the same risk level require less protection than communications between security zones of differing risk levels.

To establish and configure trusted communication between security zones, the communication dependencies between assets must be determined. This can be identified from the documentation of existing traffic flows between all the assets, or it can be determined using a network monitoring tool. Once the communication pattern between the assets is determined and documented, this can be used to determine the communication dependencies between security zones.

5. A Six-Step Approach to Security Segmentation and Typical Deliverables

This section lays out the six steps for doing security segmentation. The fictional small manufacturing environment is used as an example. The examples given in this section should give a high-level, tangible feel for the steps with an example output of the step.

5.1. Step 1: Identify List of Assets

The first step in the security segmentation process is to inventory the hardware, software, and sensitive data or information assets involved in the operation of the business. Hardware assets include IT (e.g., office computers, workstations, servers, phones, tablets) and OT (e.g., cobots, sensors, PLCs). Software includes operating systems, and off-the-shelf or custom code used by your hardware devices. Data or information assets include sensitive business, product, or customer information typically stored in hardware assets and accessed by software assets.

The asset inventory should contain attributes such as device identification number, manufacturer, model number, version number, license or warranty information, and date created or installed. It is also good to include the location of the asset, although location information may change after completing a security segmentation exercise.

For many small manufacturers, it may be more valuable to identify where assets—especially information assets—*should* be located as opposed to where they currently reside.

- For hardware assets, location may be a physical location (e.g., room number) or location on a network map.
- For software assets, location may be what hardware asset the software is installed on.
- For data at rest, location may be what hardware the data resides on and what software applications have access to the data.

If you do not have a complete and accurate inventory, make a best effort to identify as many assets and attributes as possible. The inventory can be created manually or with the help of an asset discovery tool. The inventory will be used for identifying the risk level of assets. It can also be useful for identifying process inefficiencies and keeping track of what assets need updating/upgrading. A more accurate and detailed asset inventory will allow for more precise and cost-effective cyber protections.

5.2. Step 2: Assess Risk and Create Security Zones

This step involves conducting an informal assessment of the risk associated with hardware assets. Assets that have similar operational functions, mission criticality levels, or data sensitivity levels generally also share common cybersecurity requirements. The manufacturer can use these operational similarities to group their assets and these groups of assets become security zones. The business should use criteria for grouping assets based on their specific environment.

For example, consider the primary operational function of an asset. Some potential operational functions are real-time monitoring, controlling a machine or process, planning, scheduling of machines, business operation, administrative systems, and communication devices. Based on these criteria, assets identified in step 1 during the asset inventory can be classified into the operational function zones. An example grouping is below.

Business Applications

This zone consists of applications and devices used for day-to-day business operation. Examples include financial applications, office applications (Word®, Excel®), manufacturing resource planning (MRP), enterprise resource planning (ERP), AutoCAD, printers, plotters, and scanners.

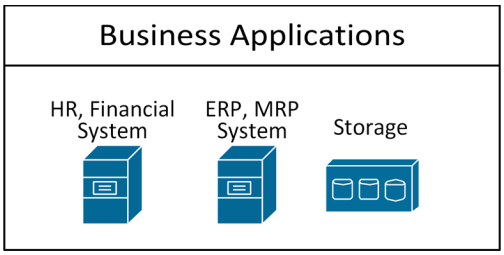

Fig. 4. Business Applications Example.

Administrative Systems

This zone consists of systems and applications used for configuring, patching, administering, and monitoring the computing and networking devices in the business. Typical assets to include in this group are the domain controller, active directory (AD), and applications used to administer network, security, and computer systems.

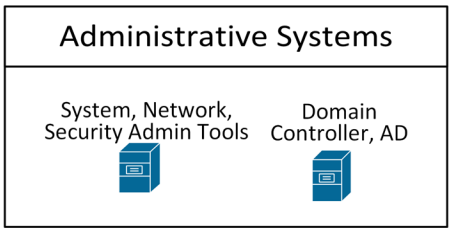

Fig. 5. Administrative Systems Example.

Connectivity Services

This zone consists of networking systems that connect everything else together. Examples include routers, firewalls, wireless access points and controllers, and VPN appliance. Note that switches that are used to connect the assets within a group belong to that group.

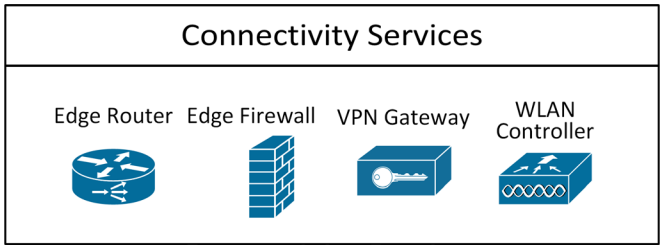

Fig. 6. Connectivity Services Example.

Manufacturing Applications

This zone consists of assets that are involved in the manufacturing operation but are not required for the operation of the assembly line. Examples include engineering workstation, MES, data historian, and plant scheduler.

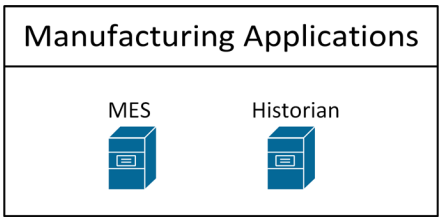

Fig. 7. Manufacturing Applications Example

Industrial Control System (ICS)

This zone consists of assets that are directly involved in running the manufacturing process. Examples include PLCs, robot controllers, and HMIs.

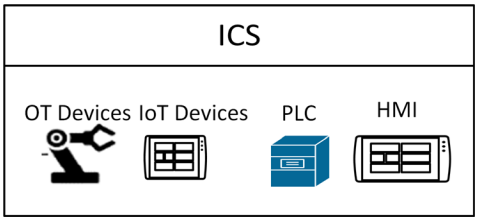

Fig. 8. Industrial Control Systems Example

Once the assets are grouped based on operational function, further refinement into security zones can be done based on the criticality and sensitivity of the assets. As you group assets into security zones, you may choose to refine the grouping of assets. For example, if you have two product lines, one for off-the-shelf items and one for custom items, you may separate each of your operational zones into two separate zones based on the assets that support each product line. As you refine your zones, it may be appropriate to create "sub-zones", where a small number of assets have a higher security requirement than other assets that they might otherwise be grouped with. For example, in a group of manufacturing applications, all but a single machine may have redundant systems. The single machine could be placed in a sub-zone of the ICS Zone with extra protection to reduce the chance of downtime due to a cyber-attack.

Some example questions to consider related to mission criticality and data sensitivity include:

- If a setting on the asset is changed without authorization, could it have a direct impact on safety?
- If the asset becomes unusable (e.g., as a result of a cyber-attack), would that directly and immediately impact production?
- If the asset becomes unusable (e.g., as a result of a cyber-attack), would that directly and immediately impact sales?
- How long can the business afford to have the asset down?
- Does the asset contain or use sensitive data or information?

The questions help identify devices that should be in a security zone and help determine the level of cyber protection various assets need. For example, if the systems contain personally identifiable information (PII), customer information, or strategic information then these systems may need enhanced protection from cyber-attacks.

At this point, the question arises about how many security zones are appropriate for a business environment. There are no formal rules dictating this decision. However, practical implementation requires that the number of security zones should balance minimizing the complexity and operational impact of changes against maximizing the risk mitigation. More security zones lead to reduced risk, while fewer security zones are easier to implement and manage. Organizations should think about their own capabilities and what is easiest for them to manage effectively and securely.

5.3. Step 3: Determine the Risk Level for the Security Zones

Next, a risk level must be determined for each security zone. The more risk associated with the assets in a security zone, as found in step 2, the higher the protection needed. Each business must determine their own categories of risk with definitions for each; the example in this document uses the categories of Low, Moderate, High, and ICS based on the following definitions:

- **Low Risk (L)**: Loss of devices causes little impact.
- **Medium Risk (M)**: Loss of devices causes some impact or significant impact but is easily recoverable.
- **High Risk (H)**: Loss of devices causes severe impact.
- **ICS Risk (ICS)**: High-risk manufacturing assets that may not be able to implement traditional high-risk security controls.

Table 4 gives an example mapping of potential impact to business to the risk level that can be assigned to the security zone. If one or more assets in a security zone were made unavailable or altered due to cyber incident, it could result in one of the impacts listed in the first column. The corresponding risk level to be assigned to the security zone due to these impacts is listed in the second column.

Table 4. Business Impact to Security Zone Risk Level Mapping

Impact of Non-availability of Assets Results in:	Risk Assignment for Security Zone
Risk to safety or the environment	ICS Risk
Low or no loss of production	Low Risk
Production loss, but there is an existing workaround already	Low Risk
Significant degradation of business operation	Moderate Risk
Loss of customer information, Intellectual Property, loss of sales, or impact to company reputation	Moderate or High Risk
Total production halt or significant financial losses	High Risk for IT assets, ICS Risk for ICS assets

For the example in this document, the risk level and the rationale for assigning the risk level are summarized in Table 5.

Table 5. Security Zones and Cyber Risk

Security Zone	Rationale for Assigning the Risk Level	Security Zone Risk			
		Low Risk	Moderate Risk	High Risk	ICS Risk
Administrative	Cyberattack could result in loss of production			H	
Business Applications	Cyberattack could result in significant degradation of business operation.		M		
Manufacturing Applications	Based on the specific business, cyberattack could result in significant degradation of manufacturing operation.			H	
ICS	Cyberattack could result in loss of production				ICS
Connectivity Services	Cyberattack could result in significant degradation of business operation.		M		

5.4. Step 4: Map Communication between the Security Zones

To understand and configure the trusted communication between security zones, the communication requirements between assets must be determined based on a deep understanding of the existing traffic flows between all the assets in the plant or using a network monitoring tool. The traffic flows identified need to be validated for accuracy to detect any spurious traffic that may exist in the environment. A network monitoring tool typically gives a more accurate picture of the actual communication pattern between the assets that exists in the environment. Additionally, incorporating a network monitoring tool as part of the business and plant operation provides continuous visibility into assets, vulnerabilities in those assets, and network traffic. This helps mitigate the "Poor Visibility of assets and network traffic" vulnerability that typically exists in the small manufacturing environment.

Once the communication pattern between the assets is determined and documented, this can be aggregated at the security zone level to determine the inter-zone communication requirement. It is important to distinguish between communications among assets in the same security zone and communications that are between assets in different security zones. Use this information to configure the firewalls or other devices used to isolate the security zones in order to permit or deny the traffic between zones. It is a good practice to deny all traffic between zones except the traffic necessary for operation.

For the example under consideration, the expected communication pattern between the security zones is depicted in the diagram below. Business applications such as ERP and MRP may interact with the MES applications and the Data Historian. Therefore, traffic between the Business Applications zone and the Manufacturing Application zone may be permitted for specific data based on the need.

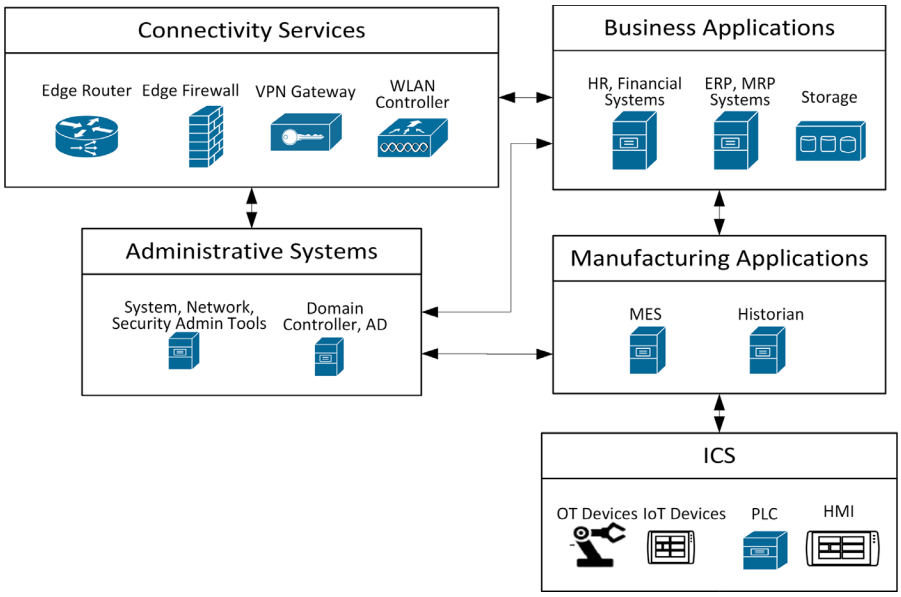

Fig. 9. Mapping of Communication between Security Zones.

In this example, the Manufacturing Applications Security Zone interacts with the ICS Security Zone, but the Business Applications Security Zone does not directly interact with the ICS Security Zone. Therefore, traffic from the Manufacturing Applications Security Zone may be permitted to the ICS Security Zone while Business Applications traffic would be blocked from reaching the ICS Security Zone.

5.5. Step 5: Determine Security Controls for the Security Zones

Once assets are classified and grouped into security zones, risk levels have been assigned to the security zones, and communication requirements between these security zones have been identified, the next step is to determine and apply security controls.

> **Compensating Security Controls**
> Because many of the OT assets use embedded controllers, have limited processing power, or have tight time constraints some of the security controls applicable for IT systems cannot be applied to OT systems. However, compensating controls, which are indirect cybersecurity practices, can be applied to protect the OT assets, e.g., a firewall can be used around devices where endpoint detection and response (EDR) cannot be implemented. To improve the cybersecurity posture, multiple security controls can be implemented. This is also known as a defense-in-depth security strategy.

To start, a template for each risk level must be completed. NIST IR 8183 Rev. 1 Cybersecurity Framework Version 1.1 Manufacturing Profile (CSF Manufacturing Profile) [3] can help determine what cybersecurity practices are needed based on the business goals combined with the impact of a cyber incident. Engineers and operators can then refine the templates for the specific manufacturing environment.

Table 6 shows an example of a selection of security controls and how they map to the security zones that have been identified earlier in the example. Each row of Table 6 contains the cybersecurity practices from the CSF including the subcategory and a description. Lastly, there is an indication of what security zones will need the security control implemented. The columns containing the security zone are colored based on the corresponding risk level.

For some controls, there may be different levels of implementation for different security zones based on their level of risk. For example, users can login with just a password (single-factor authentication), or they can use a pin and a code generated by a security token (two-factor authentication).

Cybersecurity solutions that can be used to implement the security controls are also listed in Table 6 for each control. The solutions considered in this example are:

- RA - Remote Access.
- AAC- Authentication and Access Control
- BkUp – Back up
- FW-Firewall
- VM- Vulnerability Management
- BAD-Behavior Anomaly Detection
- EDR- Endpoint Detection and Response

Table 6. Technical Cybersecurity Practices from the CSF

CSF subcategory	Security Control Description	Solu-tions	Security Zone				
			Connectivity Services (M)	Business Applications (M)	Administrative Systems (H)	Manufacturing Applications (H)	ICS (ICS)
PR.AC-3	Manage remote access.	RA	X	X	X	X	X
PR.AC-7	Authenticate users, devices, other assets commensurate with the risk of the transaction.	AAC					
	Single-factor authentication		X	X			X
	Multi-factor authentication				X	X	
PR.IP-4	Conduct backups of information	BkUp	X	X	X	X	X
PR.PT-3	Configure systems to provide only essential capabilities required to function. Disable functionalities that are not used.				X	X	X
PR.PT-4	Protect communications and control networks	FW	X	X	X	X	X

CSF subcategory	Security Control Description	Solu-tions	Security Zone				
			Connectivity Services (M)	Business Applications (M)	Administrative Systems (H)	Manufacturing Applications (H)	ICS (ICS)
DE.CM-1	Monitor the network to detect potential cybersecurity events.	BAD, EDR	X	X	X	X	X
DE.CM-3	Monitor personnel activity to detect potential cybersecurity events.		X	X	X	X	X
DE.CM-7	Monitor for unauthorized personnel, connections, devices, and software.		X	X	X	X	X
DE.CM-8	Perform vulnerability scans.	VM	X	X	X	X	

For a full list of cybersecurity practices relevant for manufacturing environment, refer to NIST IR 8183 Rev. 1 Cybersecurity Framework Version 1.1 Manufacturing Profile (CSF Manufacturing Profile) [3]. Implementing all cybersecurity practices listed in the CSF Manufacturing Profile is probably not needed nor economically feasible for all manufacturing organizations. Each organization will need to determine the target profile and the cybersecurity practices needed to attain the target profile based on the desired organizational risk reduction.

5.6. Step 6: Create Logical Security Architecture Diagram

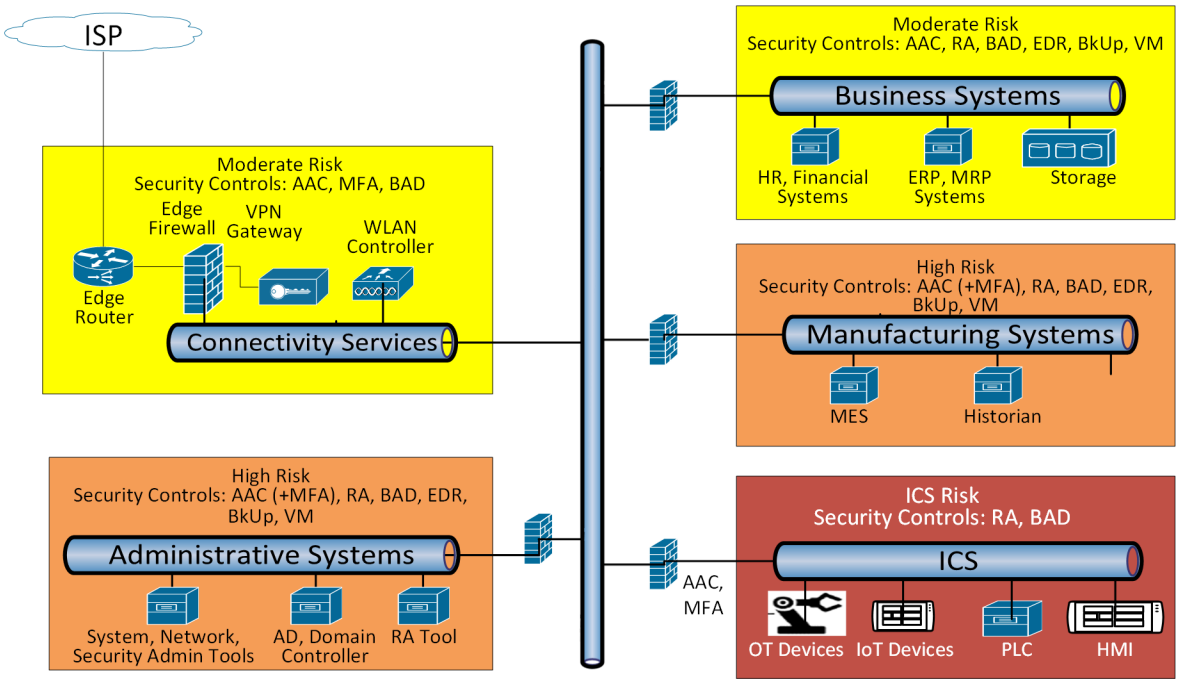

Fig. 10. Logical Security Architecture

When you apply these building blocks of the security segmentation to the target environment, it results in a logical security architecture. For the network and systems under consideration in this example, a logical security architecture is shown in **Fig. 10.** Logical Security Architecture. This shows the security zones, inter-zone communication requirements, color indicating the risk level, and notations for security solutions that are implemented inside each zone.

6. Next Steps

Once the security segmentation design is completed, the next phase is implementing this logical security architecture. This requires a detailed design, which involves the following tasks:

- Write policies for the company and for each security zone, including identifying users and permissions required.
- Write detailed procedures where needed. Include steps for executing each policy.
- Add technical security controls to the network and devices.
    - Determine and implement appropriate settings on devices in the environment.
    - Select and purchase security solutions as needed to meet security goals.
    - Configure security solutions and products.

7. Conclusion

Security segmentation is an approach to mitigate cyber vulnerabilities for small manufacturing environments through use of security zones. Implementing security controls and improving the cybersecurity posture are part of a journey not a one-time task. Each step on that journey makes a facility more secure and less vulnerable to a cyber attack. To facilitate the difficult task of implementing security controls, a limited initial set of security controls are presented as an example to begin the cyber risk mitigation journey. Additional cybersecurity practices can be selected from NISTIR 8183 Rev. 1 [3] as needed by the business. The security architecture design activities presented in this paper are foundational and will prepare the organization for additional security strategies like Zero Trust.

References

[1] Jeff Winter, What Is Industry 4.0?, https://blog.isa.org/what-is-industry-40

[2] National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 6. https://doi.org/10.6028/NIST.CSWP.6

[3] Stouffer KA, Zimmerman T, Tang C, Pease M, Lubell J, Cichonski J, McCarthy J (2020) Cybersecurity Framework Version 1.1 Manufacturing Profile. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Internal Report (IR) 8183 Rev. 1, https://doi.org/10.6028/NIST.IR.8183r1

Appendix A. Selected Bibliography

Framework for Improving Critical Infrastructure Cybersecurity, Ver 1.1, April 16, 2018
Also known as the Cybersecurity Framework or CSF, lists a set of cybersecurity practices that an organization can use to guide their activities for mitigating cyber-risk in their environment. The cybersecurity practices are organized into five high-level functions (Identify, Protect, Detect, Respond, Recover); each function has one or more categories, and each category has one or more cybersecurity practices. Informative references are also included to show how the CSF maps to various standards or best practices that a business may follow and to provide more context.

NIST IR 8183, Cybersecurity Framework Manufacturing Profile
The CSF manufacturing profile further identifies the cybersecurity practices based on the mission or focus of the systems in the OT environment that may fall in to one of the five mission objectives: Maintain Human Safety, Maintain Environmental Safety, Maintain Quality of Product, Maintain Production Goals, and Maintain Trade Secrets.

NIST IR 8183, A Cybersecurity Framework Manufacturing Profile Low Impact Level Example Implementations Guide
This guide provides general implementation guidance (Volume 1) and example proof-of-concept solutions (Volume 2 and 3) demonstrating how available open-source and commercial off-the-shelf (COTS) products could be implemented in manufacturing environments to satisfy the requirements in the CSF Manufacturing Profile Low Impact Level.

NIST SP 1800-23 Energy Sector Asset Management for Electric Utilities, Oil & Gas Industry
This publication focuses on OT asset management, namely devices used to control, monitor, and maintain generation, transmission, and distribution of various forms of energy. These devices include PLCs, IEDs, engineering workstations, historians, and human-machine interfaces (HMIs). The solution covered in this publication is designed to deliver an automated OT asset inventory that provides asset information in real or near real time and focuses on OT asset management from a cybersecurity perspective. This publication addresses the following characteristics of asset management: asset discovery, asset identification, asset visibility, asset disposition, alerting capabilities.

NIST SP 800-82 Rev 3 (Draft), Guide to Operational Technology (OT) Security
This document provides guidance on how to secure systems in the OT environment (ICS, SCADA), while addressing their unique performance, reliability, and safety requirements. This third revision of SP 800-82 provides an overview of OT and typical system topologies, identifies typical threats to organizational mission and business functions supported by OT, describes typical vulnerabilities in OT, and provides recommended security safeguards and countermeasures to manage the associated risks.

NIST SP 800-30 Rev 1, Guide for Conducting Risk Assessments

This document provides guidance 1.) for conducting risk assessments of organizations from cyber threats 2.) for carrying out each of the steps in the risk assessment process (i.e., preparing for the assessment, conducting the assessment, communicating the results of the assessment, and maintaining the assessment), and 3.) to organizations on identifying specific risk factors to monitor on an ongoing basis.

ISA Global Cybersecurity Alliance (ISAGCA) Quick Start Guide

This document is intended to provide the reader with a detailed overview of the ISA/IEC 62443 Series of standards and technical reports. The ISA/IEC 62443 Series addresses the Security of Industrial Automation and Control Systems (IACS) throughout their lifecycle.
https://gca.isa.org/isagca-quick-start-guide-62443-standards
https://www.youtube.com/watch?v=tCUdZ51oKAg&ab_channel=ISA

ISA/IEC 62443-1-1, Security for industrial automation and control systems: Models and Concepts

ISA/IEC 62443 is a set of standards that addresses the various aspects of cybersecurity for the industrial automation and controls systems. This specific standard (62443-1-1) describes the concepts and models that form the foundation of all documents in this series. It addresses the concepts such as risk-based threat mitigation, defense-in-depth cybersecurity strategy, security, and functional safety. It also provides a model for decomposing the OT environment into security zones based on the system types and its function in the OT environment. It also lists other standards in the ISA/IEC 62443 series and provides a brief description for it.

Appendix B. List of Symbols, Abbreviations, and Acronyms

AAC
Authentication and Access Control

AD
Active Directory

BAD
Behavior Anomaly Detection

BkUp
Back up

CIO
Chief Information Officer

CISO
Chief Information Security Officer

CNC
Computer Numerical Control

COTS
Commercial off-the-shelf

CSF
Cybersecurity Framework

EDR
Endpoint Detection and Response

FW
Firewall

HMI
Human-Machine Interface

ICS
Industrial Control System

IEC
International Electrotechnical Commission

ISA
International Society of Automation

ISP
Internet Service Provider

IT
Information Technology

MES
Manufacturing Execution System

MFA
Multi-Factor Authentication

MRP
Manufacturing Resource Planning

OT
Operational Technology

PII
Personally Identifiable Information

PLC
Programmable Logic Controller

RA
Remote Access

SCADA
Supervisory Control and Data Acquisition

VM
Vulnerability Management

VPN
Virtual Private Network