



IEC 62443

SECURITY ZONE

Edge SDN White Paper

A glance at the creation of Security Zones in production
and mission critical environments

CONTENTS

Introduction	2
Standard IEC 62443	2
Security Zone.....	2
Conduit	2
Reference Architecture.....	2
VLAN	3
Traffic North-South	3
Traffic East-West	3
Layered Protection.....	4
How to create Security Zones	4
Operational steps for creating Security Zones.....	4
Best practice	5
Common errors	6
Segmentation And Segregation	7
Layered Protection Model.....	7
Example Of Protection	7
Layered Protection.....	10
Conclusion	11



INTRODUCTION

This document aims to provide an accessible and understandable introduction to the creation of **Security Zones** according to the guidelines of the **IEC 62443 standard**. Targeting primarily IT and OT professionals, our goal is to offer a clear starting point for those who are approaching this standard for the first time, rather than industry experts.

It is not an exhaustive treatise on detailed **Security Zone design**, but rather a helpful guide to understanding how to tackle the crucial task of defining a cybersecurity perimeter in industrial environments. The document aims to simplify complex concepts to enable readers to grasp a general understanding of the fundamental principles underlying the definition of such perimeters.

Using simplified concepts and practical examples, we aim to provide a clear and accessible overview of the essential concepts of the **IEC 62443** standard, in order to provide a solid foundation for the implementation of Security Zones in industrial infrastructures.

STANDARD IEC 62443

The IEC 62443 standard is an international standard that provides guidelines and requirements for the security of industrial control systems (ICS), including automation and control systems used in sectors such as energy, chemical industry, manufacturing, and other critical sectors. This standard has been developed to protect industrial control systems from cyber threats while ensuring operational continuity and the security of industrial processes.

Security Zones and conduits are fundamental concepts within the IEC 62443 standard.

SECURITY ZONE

Security Zones are logical or physical areas within an industrial control system that are defined based on security requirements and the criticality of processes or resources within them. Each Security Zone may have specific security rules and policies. These zones are designed to restrict unauthorized access and control the flow of information within the system. Security Zones can be created based on criteria such as function, encryption, access level, monitoring, and physical protection.

CONDUIT

Conduits are the communication pathways between different Security Zones within an industrial control system. They can be comprised of physical networks (e.g., wiring, cables) or logical networks (such as virtual networks). Conduits must be designed and implemented in accordance with the security requirements defined by the IEC 62443 standard. Security measures applied to conduits may include data encryption, access control, network segmentation, and other protection techniques to ensure the integrity and confidentiality of communications between different Security Zones.

In summary, the IEC 62443 standard promotes the implementation of Security Zones and conduits as part of a comprehensive strategy to protect industrial control systems from cyber threats and ensure the security of critical industrial processes.

REFERENCE ARCHITECTURE

The structure of a security project for creating Security Zones and Conduits follows simple architectural principles. Industrial networks typically have two types of traffic directions: *North-South traffic*, which



identifies communication between the field and external services, and *East-West traffic*, which defines communication between field devices within the same Security Zone or between different Security Zones.

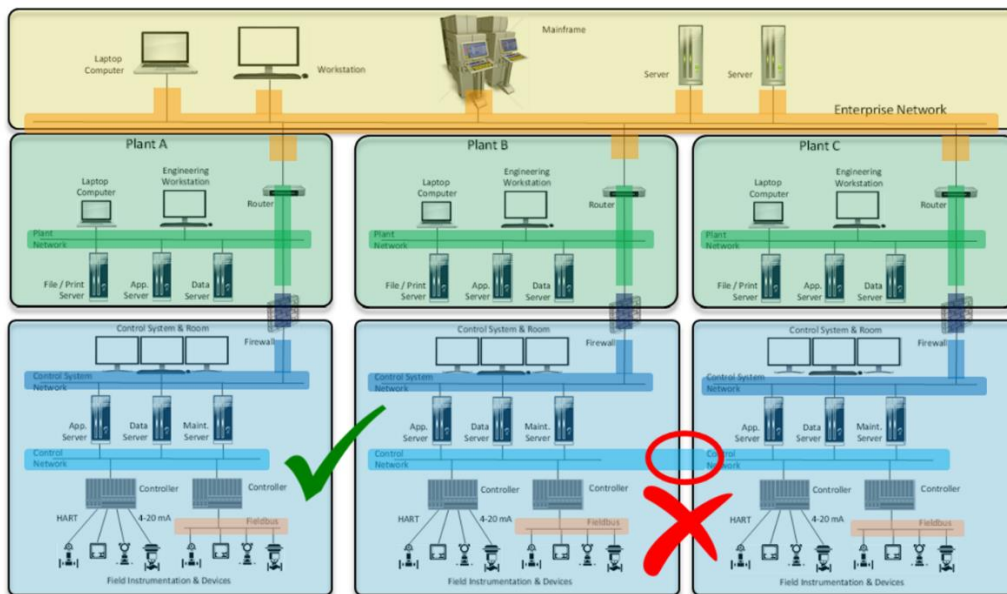


Figure 1 Examples of correct and incorrect configurations (source: <https://gca.isa.org>)

In an industrial telecommunications network, the directions of traffic between devices or services are easily identifiable and must follow two simple principles:

- control North-South traffic
- block or control East-West traffic

VLAN

An industrial network is often segmented with specific VLANs for production environments, defining network domains that serve as the starting point for creating the security architecture.

TRAFFIC NORTH-SOUTH

North-South traffic refers to communication between peripheral devices or systems (such as terminals, sensors, actuators, etc.) and central systems or servers. In other words, it is traffic that flows from the network's edges toward the center and vice versa.

Protecting North-South traffic in an industrial network is crucial to ensure the security and integrity of data transmitted between peripheral devices and central systems. Typically, centralized protection strategies are used for 'vertical' network traffic, such as border firewalls, DMZs, VPNs, and role-based access control (RBAC), which limit unauthorized access and protect data in transit. North-South traffic segregation and segmentation strategies are often combined with intrusion detection and prevention systems (IDS/IPS) and data and communication encryption, ensuring security against suspicious activities and eavesdropping.

TRAFFIC EAST-WEST

East-West traffic refers to communication between devices or systems within the same hierarchical level of the network. This type of traffic is typically horizontal, meaning it flows between peer-level nodes.



East-West traffic is particularly insidious, as it is permitted within the VLAN and is typically used for lateral movement by attackers, promoting privilege escalation and preparing for an attack. To protect East-West traffic in an industrial network, various key strategies are adopted. Internal network segmentation and the use of internal firewalls limit traffic between segments, reducing threat propagation. Intrusion detection and prevention systems (IDS/IPS) and role-based access control (RBAC) ensure rapid detection of suspicious activities and authorized access. Microsegmentation with SDN and encryption of internal traffic enhance the security of data in transit. Vulnerability management and patching reduce the risk of exploits, while security policies and compliance ensure secure behavior. Finally, isolating critical systems and training personnel promote a security-conscious culture and reduce human error.

LAYERED PROTECTION

Layered security in a telecommunications network is based on an approach of concentric segregation layers to protect different parts of the network and the data transmitted through them, creating a structure similar to that of an onion.

This model allows for defining distinct security areas, each with increasingly restrictive rules and controls as one moves closer to the core of the network. The outermost sections of the network may be dedicated to public or non-sensitive traffic, while the innermost areas, accessible only through strictly controlled gateways, are reserved for critical data and services.

For example, the first layer may consist of a perimeter firewall that controls incoming and outgoing network traffic. At a more internal level, VLANs (Virtual LANs) can be implemented to isolate traffic for specific groups or departments, restricting access to certain network resources. Additional layers can include protecting critical servers through network segmentation and using technologies like SDN (Software-Defined Networking) to dynamically monitor and control data flows.

This 'layered' or 'onion' approach offers enhanced protection, as even if an attacker breaches one layer, they must overcome additional security levels to compromise the entire network.

HOW TO CREATE SECURITY ZONES

Creating Security Zones within an industrial network requires a methodical and careful approach, considering specific security requirements and operational needs. Below are outlined the general operational steps for creating Security Zones, along with best practices and common errors to avoid.

OPERATIONAL STEPS FOR CREATING SECURITY ZONES

Establishing Security Zones is as the starting point for an effective strategy to protect industrial assets and hosts.

1. **Identification of Critical Resources:** Identify and classify critical industrial resources and processes within the industrial control system. This may include machinery, automation systems, databases, servers, and other relevant devices or components.
2. **Risk Analysis:** Conduct a risk analysis to identify potential threats and vulnerabilities that may impact critical resources. Evaluate the impact and likelihood of harmful events and determine necessary security measures.
3. **Definition of Security Zones:** Based on the risk analysis, define Security Zones within the industrial network. This may involve dividing the network into logical or physical zones based on function, criticality, and sensitivity of resources.



4. **Development of Security Policies:** Define security policies for each Security Zone, establishing rules and procedures for access control, credential management, activity monitoring, and other security-related tasks.
5. **Implementation of Security Measures:** Implement appropriate security measures within each Security Zone. This may include configuring firewalls, installing intrusion detection systems, applying access controls, and other protective measures.
6. **Testing and Validation:** Test and validate the effectiveness of implemented Security Zones, ensuring that security measures function as expected and critical resources are adequately protected.
7. **Monitoring and Maintenance:** Implement a continuous monitoring and maintenance process for Security Zones to ensure compliance with security policies and timely addressing of any new threats or vulnerabilities.

NOTE: It is essential to identify and protect critical processes and assets, while the remaining ones can be grouped into Security Zones without specific protection needs. However, compromising unprotected processes and assets should not compromise operational continuity or operator safety.

BEST PRACTICE

For a pragmatic approach point of view, for creating Security Zones, it is necessary to apply theory, but it is essential to tailor it to the actual risks and operational processes of the production environments. According to the IEC 62443 standard, Security Zones are defined in layers to ensure a robust and scalable approach to protecting critical infrastructures.

This multi-layered approach allows for the creation of a graduated and multifunctional defense environment that reflects the diverse security needs within an industrial organization. Indeed, Security Zones can be defined for entire production sites down to the specific definition of Security Zones within a single machine or production line. The goal is to adopt an approach based on the principle of "least privilege," limiting access only to the resources necessary to perform work functions while avoiding lateral movement between Security Zones.

- **Grouping computer assets with the same application purposes or the same cybersecurity risk is advisable.** For example, a production line or individual machines constitute a grouping of assets with the same application purposes, while a grouping of energy meters, cameras, or printers represents assets with the same cybersecurity risk.
- **Consideration should be given to the fact that assets of different types, even if part of the same production block, may be subject to different risks.** For example, a PC with control and management software connected to a machine or production line, if not adequately protected, could be considered a separate Security Zone.
- In the case of **communications to the outside**, it may be useful to perimeter and isolate external accesses with an isolated Security Zone.
- Particular attention should be given to those **factory assets that require communication with the outside**, such as gateways that collect data and send it to the cloud. Evaluate the risks associated with external communication and, if necessary, perimeter them in a separate Security Zone.
- **Assets that are not under direct control represent a risk that needs careful evaluation**, i.e., all assets for which updates or computer maintenance cannot be done directly, either because they are under someone else's control (e.g., the supplier) or because they are closed and inaccessible systems.
- Avoid the temptation to design architectures with a **multitude of Security Zones** with excessive layers and details.



- Starting from the risk analysis, **let common sense guide you, considering that each Security Zone is a constituent element of the production process.** If a Security Zone is compromised, only a single element of the production process should be affected, without impacting the operational continuity of the rest. For example, a production line composed of multiple process units can be seen as a single production unit, but if the line can continue to operate even in the presence of a fault on individual machines, then the production line can be divided into essential and optional parts for operational continuity. For example, in a production line, if the palletizer is compromised, it can be isolated, and production can continue by manually palletizing.
- Radio communication, both Wi-Fi and Bluetooth, should always be considered subject to risks and would be best isolated in a separate Security Zone.

Additionally, it is necessary to thoroughly document security policies and operational procedures to ensure effective management of Security Zones.

COMMON ERRORS

In the creation of Security Zones, several errors can compromise the overall effectiveness of the security system. Not fully understanding the specific security needs and criticalities of industrial processes can lead to inadequate design of Security Zones with architectures that are either too rigid or too permissive, which can compromise operational efficiency or system security.

- **Lack of communication and collaboration between IT and OT teams** can compromise the effectiveness of the initial analysis, leading to an inaccurate risk analysis. One of the main errors is not conducting a complete and accurate risk analysis before defining Security Zones. Without a detailed understanding of potential threats and vulnerabilities in the industrial environment, Security Zones may be designed inefficiently or inadequately to protect critical assets.
- **Designing Security Zones solely based on current system vulnerabilities is very dangerous;** segmenting devices only based on identified vulnerabilities often results in a finely segmented architecture that is difficult to maintain. Furthermore, continuous monitoring of vulnerabilities and updates, often intrusive, to the protection architecture are necessary. Vulnerability analysis is a fundamental part of risk analysis, and it must be taken into account, but it should not be the only factor to drive the security architecture.
- **Another common issue is the imprecise definition of Security Zone boundaries.** Without clear and well-defined boundaries, it becomes challenging to properly apply security policies and monitor activities within each zone. Additionally, overlaps or gaps in protection between different Security Zones may occur. This can happen when the production process between different zones is unclear or when there are areas not covered by any Security Zone.
- **Neglecting regular updates and maintenance of Security Zones leaves the system outdated** regarding changes in setup and vulnerable to new threats or vulnerabilities.

Below are some practical examples of common errors in addressing factory segregation.

- **Creating a Security Zone where assets of the same type are placed,** even if machines and production processes are different because they are considered to have equal cybersecurity risk, such as placing all PLCs from one manufacturer together.
- **Not separating IT assets from OT assets;** in a production line, if there are IT computing services present, such as a PC in the corporate domain performing functions other than OT tasks, it is necessary to segregate it.
- **Considering VLANs or IP addressing as Security Zones.** Using logical IP addressing to segregate Security Zones. IP network determines the visibility of services and devices in the network through routing paths that can also be protected by firewalls. IP numbering is often a result of past choices



and can be difficult to change it. Within a single VLAN, multiple IP networks can exist, and a single production process can span across multiple VLANs. Security Zones are logical groupings that define security areas and are often not in line with the logical numbering of the network.

Finally, the lack of user training and awareness can pose a significant risk to the security of Security Zones. Users must be adequately educated on security policies and aware of best practices to protect data and assets within the zones.

SEGMENTATION AND SEGREGATION

A Security Zone is, therefore, a portion of the network in which the devices are segregated and external communications are segmented.

LAYERED PROTECTION MODEL

Layered protection of an industrial network, according to the IEC 62443 standard, is an approach that divides the network into layered Security Zones, each with a specific level of protection. This type of architecture is commonly referred to as the Onion Security Model because, like an onion, protection occurs through multiple concentric layers, each of which shields internal assets from external attacks, with increasingly stringent levels of security as one moves toward the core of the infrastructure. The benefits of applying this model are numerous:

- **Defense in Depth:** Each layer adds an additional level of protection, reducing the likelihood of an attack penetrating to critical systems.
- **Threat Isolation:** In the event of a system or zone compromise, other areas remain protected thanks to the boundaries between layers.
- **Separate Management:** The architecture allows for specific responsibilities to be assigned to manage each layer, enhancing response and operational control. The Onion Security Model offers an effective and scalable approach for protecting industrial networks, ensuring that critical assets remain protected even in the event of an attack or compromise of outer layers

EXAMPLE OF PROTECTION

Below are some practical examples of how to begin defining a segregation architecture based on design criteria. We will show how it is possible to use the existing network infrastructure, based on switches. Again, this is an introductory guide intended solely to help a beginner understand the foundational logic of segregation according to Security Zones. Do not take the following examples as dogmatic, but rather as useful thought prompts.



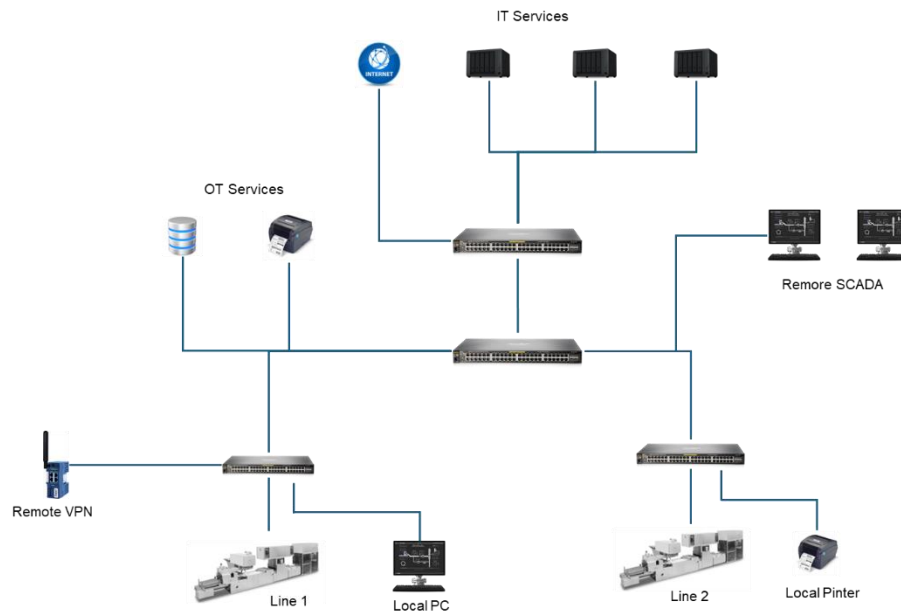


Figure 2 IT/OT network

Using the network shown in Figure 2 as an example, the devices shown belong to the same subnet; communication is open and uncontrolled.

Let's take, for example, the protection of Line1, which communicates with local and remote devices using standard or proprietary applications.

Destitution	Application
Remote VPN	RDP, SSH, HTTP
Local PC	Proprietary protocol
OT service	Printer, Shared Folder, NTP
Remote SCADA	OPC UA, ICMP
IT service	DNS, HTTP

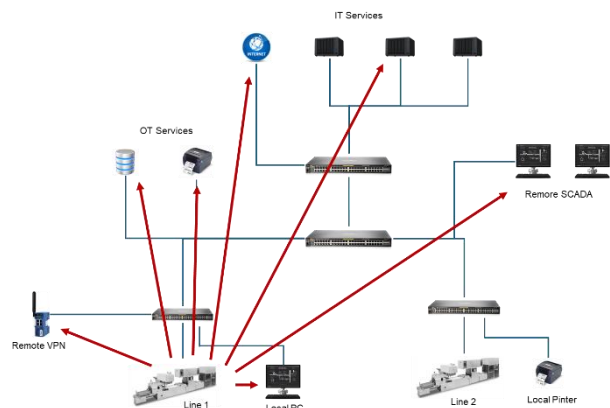


Figure 3 Communication between Line1 and the other devices on the network

Let's start by precisely designing the Security Zones around the areas to be protected.



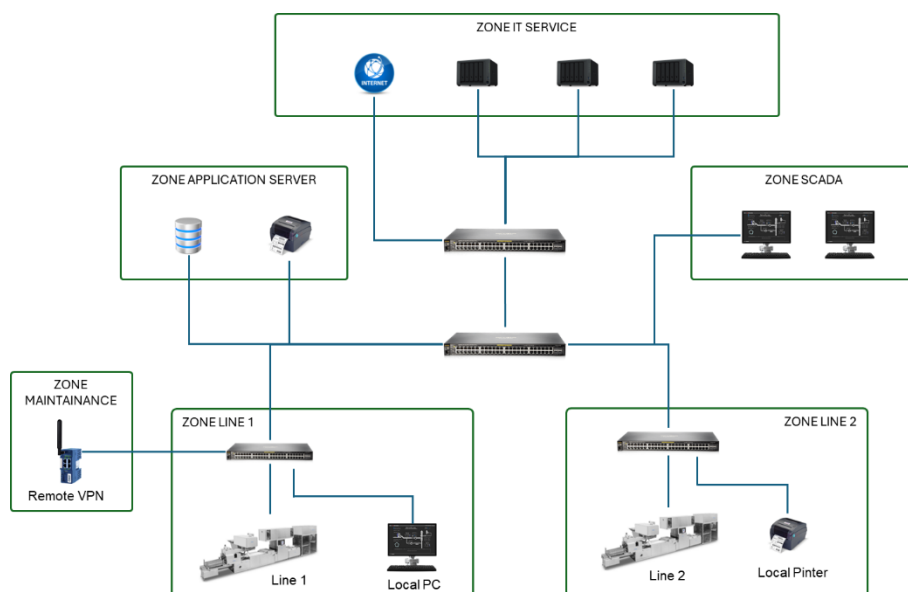


Figure 4 IT and OT Security Zones

In this scenario, we have a communication matrix between zones rather than individual objects; within each Security Zone, traffic is exchanged freely.

As we have designed the zones, in ZONE LINE 1, traffic between Line1 and Local PC has no restrictions, while Table 1 shows the traffic matrix between the zones.

Grouping assets into Security Zones has already led to an initial simplification in describing communication between Line1 and Local PC

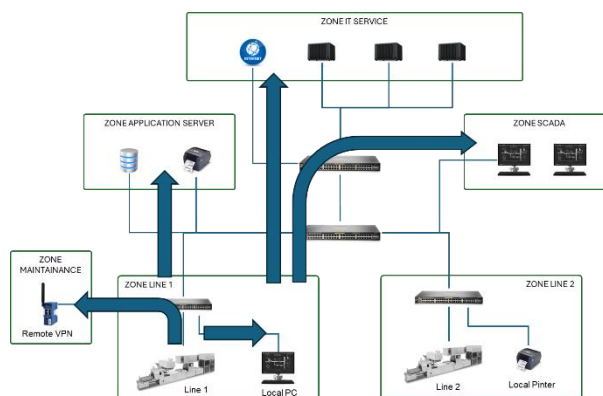


Figure 5 Communication flows between zones

Security Zone	Applications	Security Zone
ZONE LINE 1	RDP, SSH, HTTP	ZONE MAINTAINANCE
ZONE LINE 1	Printer, Shared Folder, NTP	ZONE APPLICATION SERVER
ZONE LINE 1	OPC UA, ICMP	ZONE SCADA
ZONE LINE 1	DNS, HTTP	ZONE IT SERVICE

Table 1 Traffic matrix between zones



This logical segmentation allows us, with great simplicity, to apply segmentation rules to the switches in the network to limit traffic propagation across the network.

Note how the rules applied to the switches enable an information propagation path rather than simple perimeter protection. This means that information exchange follows a defined path.

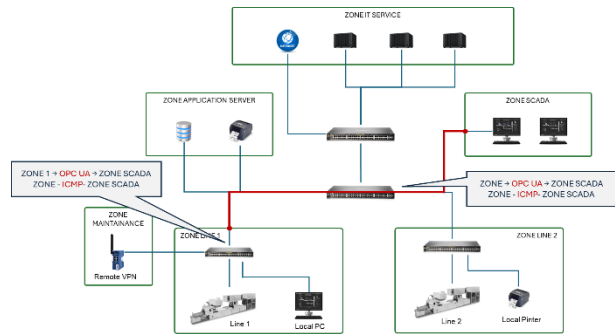


Figure 6 Propagation path between ZONE LINE 1 and SCADA

By broadly applying this methodology, we can achieve controlled and non-bypassable information exchange. In fact, at every point in the network, communication is regulated by the established propagation paths, so the level of communication protection depends solely on the implemented paths and not on operator behavior or device vulnerabilities.

This communication protection, when combined with traffic control, proves extremely effective because it prevents the propagation of information not necessary for production activities.

LAYERED PROTECTION

The Security Zones defined in this way can be further layered to achieve multi-level segmentation of protection. A layered protection architecture is commonly referred to as 'Onion Security'.

We add two additional zones to establish protection for the production lines and the entire plant.

- **ZONE PRODUCTION LINES:** includes the production lines and local services
- **ZONE PLANT:** includes the production lines and all OT services of the plant

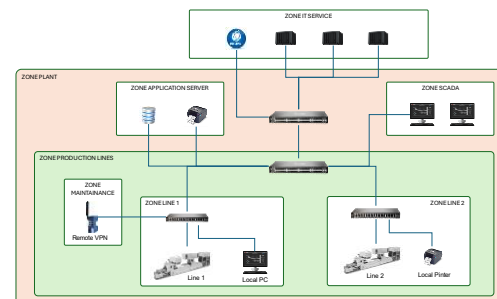


Figure 7 Layering of Security Zones

In this scenario, traffic flows change as we have concentric zones where traffic can be aggregated to create propagation paths.

Communications between the zones are as follows.

➡	ZONE LINE 1 ZONE MAINTAINANCE
➡	ZONE PRODUCTION LINES ZONE APPLICATION SERVER ZONE SCADA
➡	ZONE PLANT ZONE IT SERVICE

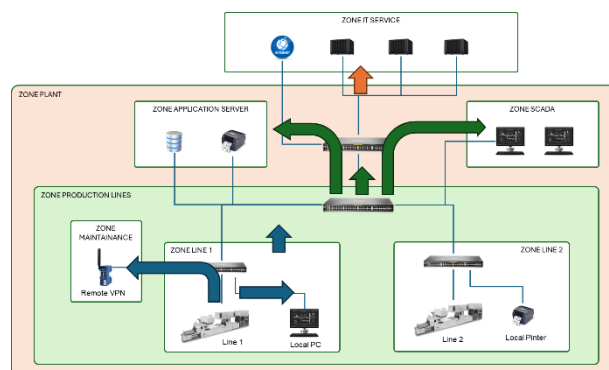


Figure 8 Traffic matrix between zones

Simplifying the traffic matrix among all devices involved in communication, layered protection enables the creation of a system that maintains the level of protection even when combining operational conditions.



Let's look at two simple examples that demonstrate how layered protection can enable business processes.

OBJECTIVE: Temporarily enable communication between all lines and allow remote maintenance.

SOLUTION: Temporarily disable the three security zones ZONE LINE 1, LINE 2, and MAINTENANCE. Communications within ZONE PRODUCTION LINES are thus unrestricted, while external communications remain protected

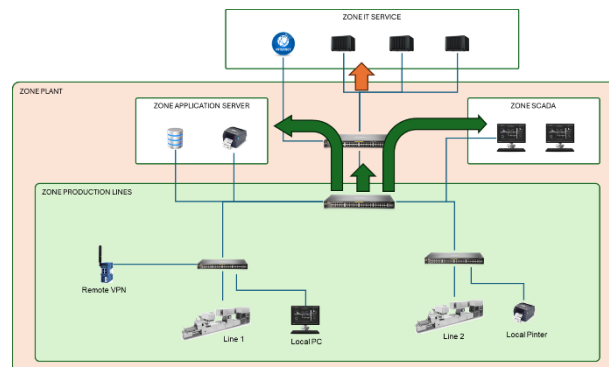


Figure 9 Enabling field communication

OBJECTIVE: Temporarily enable communication between all field devices.

SOLUTION: Temporarily disable all OT security zones. The plant can communicate freely, but external protection remains enabled

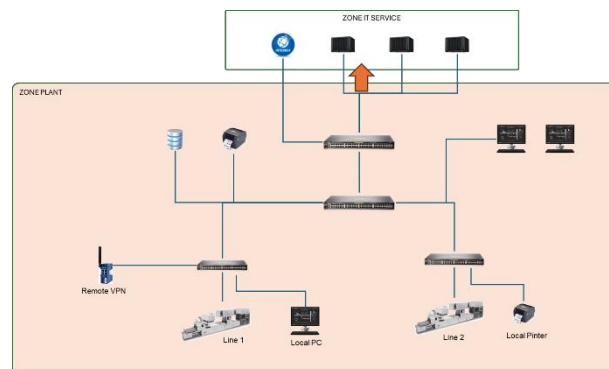


Figure 10 Enabling OT zone

The controlled use of switches can enable and disable the protection of security zones, effectively creating protection under any operating condition.

It is therefore essential to adopt a network segregation solution that can be easily implemented with the existing network and requires minimal effort to adjust segregation conditions.

CONCLUSION

In conclusion, it is important to emphasize that there is no universal approach or rigid methodology for designing Security Zones according to IEC 62443. The definition and implementation of Security Zones depend on various factors, including specific risk analysis, the organization's operational needs, and emerging threats in the industrial context.

It is essential to understand that creating Security Zones must be guided by an accurate assessment of risks and vulnerabilities within the industrial environment. This process requires close collaboration between IT and OT personnel, as well as an in-depth understanding of the organization's operational procedures and security requirements.

Additionally, Security Zones should be viewed as a dynamic and evolving element, subject to review and updates in response to industrial setup changes, evolving threats, and new technologies. It is therefore crucial to implement solid operational procedures and effective monitoring mechanisms to ensure that Security Zones remain appropriate and effective over time.

Edge SDN is a platform designed to integrate with existing network infrastructure, enabling effective protection without the need for radical changes or investments in new equipment. With its advanced traffic segmentation features, centralized management, and support for internationally compliant



security standards, Edge SDN can transform an existing network into a secure and resilient platform. This approach allows for optimizing current resources, enhancing data traffic security, and reducing risks without compromising operational continuity.

Whether using SDN switches or non-SDN switches, Edge SDN can manage both types of network nodes, leveraging the potential of each device type. Thanks to advanced traffic segmentation and centralized management, it is possible to implement layered protection that adapts to the specific needs of the network to be secured.

Moreover, OT (Operational Technology) operators have full control over network security thanks to Edge SDN's intuitive interface, which allows them to independently manage layered protections. This approach reduces reliance on IT and ensures continuous, customized protection adapted to the operational workflow, thereby increasing the efficiency and security of the industrial network





Powered by
stoorm5[®]
Natalino Corazza 7/7
40128, Italy (IT)

www.stoorm5.com

www.edge-sdn.com

Copyright © 2024, Stoorm5 and/or its affiliates. All rights reserved.

This document is provided for information purposes only and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Stoorm5 and Edge SDN are registered trademarks of Stoorm5 and/or its affiliates.