



**UNTERTURKHEIM**

**Segmentation and operational risk containment - Firewall Deployment - assessment**

**About OTORIO**

OTORIO is an Industrial-focused full life-cycle cyber-risk solutions and service provider, founded as a joint venture between experienced Israeli defense professionals, and a leading Austrian plant engineering group. This unique combination incorporates the best of both domains.

OTORIO offers comprehensive cybersecurity solutions and services for established industries.   
Our knowhow is based on years of deep domain expertise in cyber security engineering, and hands-on hacking of operational mission critical systems. The venture with Andritz AG brings over 160 years of industrial engineering and operational technology knowhow for leading industrial customers in a variety of verticals.

In the ever-changing technology landscape, security does more than protect existing systems; It enables businesses to maximize production and utilize opportunities.

OTORIO takes part and assists businesses in driving their operational environment forward in an optimized and secure way.

Guided by strong professional integrity and competence, we offer a comprehensive solution based on a unique formulation of military grade innovative technology and professional services. This supply-chain-centered offering, with OT risk management platform and SOC, threat Intelligence, and Incidence Response (IR) modules, is designed and operated by highly trained cyber-security “special forces”.

OTORIO’s leading experts are engaged throughout the entire security process at different touch points (requirement, specification, development and deployment).

Content

1. Executive summary
2. Introduction to Segmentation
3. Segmentation strategy
4. Threat modeling and segmentation
5. MB’s segmentation plan analysis
6. MB & OTORIO unified Analysis process
7. Recommendation and summary
8. Appendix A – enforcement points locations comparison

# Executive summary

While most IT networks are constantly evolving and adapting to the challenging cyber landscape, OT related production floors topology and architecture is evolving at a much slower pace. This situation provides potential attackers with both the means and the opportunity to unhurriedly develop generic or targeted offensive tools, and operate freely and undetected for long periods of time in the production floor environment.

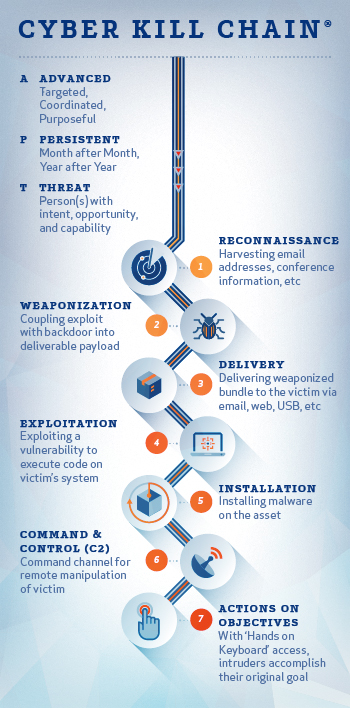
The ongoing penetration of industry 4.0, and the digitalization of the manufacturing plant, has introduced new potential attack vectors to the production process, which the current security paradigm and countermeasures are unprepared to deal with.

Designing and deploying new security mitigation controls in a production floor is a complex task. There are multiple parameters affecting the equilibrium between security and the system manageability, such as: team competence, capacity to efficiently operate more systems, and the ability of plant assets to co-exist with advanced security countermeasures (e.g. EDR for endpoints, strong authentication, segmentation etc).

MB’s shop floor, in general, and Untertürkheim’s hall networks specifically, like most industrial world production floors, were not designed and built over the years to withstand the present and future attack techniques leveraged by the proliferation of IIoT, nor the newly-focused attention of attackers to penetrate OT networks, for a various reasons (i.e. financial gain, espionage, business competition, terror and sabotage).

Cyber-risk management, and its derivative risk assessment, aim to tip the balance in the defenders’ favor by prioritizing and focusing mitigation resources according to several parameters such as: asset identification, visibility and management, impact analysis, digital growth, risk appetite, and others.

Most production floors worldwide vary from one another, creating a need for a tailored risk management plan. An effective and efficient plan must be tailored to the plant characteristics in order to make the implantation successful and the risk management plan effective.

OTORIO’s risk assessment methodology is tailored according to different specifics and context. We have developed a unique approach that focuses on the attack kill chain. It identifies and analyzes the effort required by the attacker to achieve each stage.

OTORIO’s team analyzed the MB “Planning Manual for protecting manufacturing equipment against IT Threats” and “Information implantation SITS 2.0” documents. Fusing the MB concept with OTORIO’s threat modeling methodology, by applying attack vector scenarios in the industrial environment of MB, and prioritizing these scenarios according to the probability of their overcoming the existing security controls, we conclude with a proposal for a network segmentation implementation.

According to our analysis of probable attack vectors, we assume that the majority of the attacks will originate from the IT network (despite its layers of defense), due to a wide range of day-to- day operations in this environment, while the remaining attacks will originate in IT-OT, through unmonitored and unsecured access by MB personal/supply-chain to the production floor, for remote maintenance or conditional monitoring. Due to inability of the hall network to deploy the entire IT security suite (a mismatch of security versus operational technology), the first lines of defense should focus on impact reduction and containment, based on stringent segmentation. PUT GRAPH OF PROBABILTITY ATTACK

Appropriate segmentation can considerably reduce the potential impact of a cyber-attack. Ransomwares, for example, spread by scanning the network for accessible devices, and copy their code to it, thereby expanding and increasing the damage. Restricting movements between zones and assets, or even monitoring it to identify lateral movement, can prevent the ransomware from spreading while generating alerts in real-time.

Different considerations should be made before segmenting the network. A detailed and balanced (operational vs. risk management) strategic plan must be prepared, with the involvement of every stakeholder (IT/Sec teams, production engineers, BISO, etc..). This process, if not handled with the appropriate consideration, could unintentionally create disturbance to legitimate production traffic, which could result in production loss or safety issues on the one hand, and unacceptable risk on the other hand.

This document proposes a four-part segmentation roadmap, designed to complement the MB network segmentation plan:

* The first part presents a methodological process for segmentation planning and implementation.
* The second part offers OTORIO’s approach based on the attacker’s targets analysis. By analyzing the concepts, tools and techniques of a potential attack, we prioritize the segmentation plan in order to balance the mitigation of such attack vectors and manufacturing continuity, with a realistic assessment of the plant capability to implement additional security devices and operate them in a continuous and effective way.
* The third part provides an overview for SITS 2.0 optional segmentation options, with key advantages/disadvantages for each segmentation model
* The fourth part merges OTORIO’s unique segmentation model with the MB SITS 2.0 segmentation design and implementation guide, to provide a tailored implementation design

The last chapter concludes the process, and provides recommendations for Untertürkheim’s segmentation implementation according to these rules:

1. Stringent segmentation for the Production hall’s ingress/egress traffic, deployed in a preventative (continuously preemptive assessment) mode between the IT and OT network (Layer 3.5)
2. Gradual segmentation change for inner hall segmentation traffic, starting with a short learn and adjust period in detection mode, followed by a meticulous transfer to preventive mode
3. Separation between managing traffic that directly effects production level assets (incoming/outgoing as well as inner production level), and non-production traffic, by deploying different gateways

# Introduction to network segmentation

The increase in cyber attacks on the industrial sector is slowly turning into a major concern which needs to be monitored and treated accordingly.

The current security posture of most industrial manufacturing organizations is decoupled from digital growth in the plant, resulting in an expanded attack surface, and the task of identifying and stopping possible attack or a potential incident lags behind.

Attackers can penetrate a network in many ways. Once inside, they perform a silent reconnaissance, map the network and asset vulnerabilities, gather credentials, and the design their attack on the network. Sometimes they will steal and exfiltrate information, and sometimes they prefer to monetize the attack with ransomwares, or cause damage to production.

A stringent defense-in-depth aims to prevent or detect each stage of the attack by a suitable set of security controls.

Network segmentation is one of the most powerful security controls in a successful information security program. It directly addresses the realities of the evolving threat landscape—it is difficult, if not impossible, to prevent a cyber breach, but it is very feasible to isolate one and limit the potential impact.

Network segmentation focuses on separating parts of the network from one another with barriers and\or controls. In some cases, the segmentation is there by design—for example, the manufacturing execution system (MES) is segmented from the sensors and actuators. In other cases, the segmentation will be by data classification—for example critical production equipment is isolated from the users LAN. By implementing network segmentation, manufacturing plants can address the upcoming cyber security challenges far better than with flat networks embedded with other cyber security solutions. Proper ***network segmentation lays the groundwork for controls*** which protect against lateral movement on the network by malicious software and actors, which prevents a potential infection or compromise from spreading across the network. It also allows additional control points across the network, which significantly increases visibility and control over traffic on the network[[1]](#footnote-1).

The rationale for good segmentation is derived from a number of motives and usually varies between plants and verticals. Where one plant decides to create segmentation by geographic or physical layout, another plant can create separation between processes.

***To be effective, network segmentation measures must be carefully planned, robustly enforce and closely and continuously monitored.***

Key advantages of stringent Network Segmentation

* **Improved Security-** Network traffic can be isolated and/or filtered to limit and/or prevent unauthorized or unwanted access between the different segments.
* **Better Access Control -** Allow users or processes to access only specific network resources.
* **Improved and Accurate Monitoring -** the capability to continuously log events, monitor allowed and denied internal connections, and detect suspicious behavior. ***This will be a key asset in network forensics or Incident response activities, to more accurately and promptly identify and mitigate threats***.
* **Improved Performance** – Segmentation also simplifies operational maintenance, in addition to being a cyber-security advantage. With fewer hosts per subnet, local traffic is minimized, allowing network problems to be accurate pinpointed. Broadcast traffic can be isolated to the local subnet, reducing unnecessary traffic.
* **Better containment** -When an incident occurs, its effect are limited to the local segment, thus affecting a smaller proportion of process/ assets, and having a smaller impact. For example, WannaCry spreads by exploiting any reachable network file share (which are opened by default on any Windows machine). Blocking access between segments on that port will prevent WannaCry from infecting devices on other segments.

Usability Considerations

As with any security control, it is important to balance business functionality and constant improvement of production efficiency with the need to secure it. Improved automation and production control require increased access to floor assets, which could oppose the segmentation plan. Segmenting the network is a valuable technique for maintaining operational continuity, and an entirely different way of managing it. In involves going from a flat network – where communications are wide open, and there are no difficulties or obstructions in reaching and/or communicating with hosts – to a network that is divided into zones, both logical with VLAN, or physical with firewalls, switches and routers.

It takes careful planning to achieve the desired balanced manageable result, which is a network that is difficult for attackers to penetrate and operate in without being blocked and detected on the one hand, and one that enables simple and easy operations that support digital growth on the other hand.

**It is important/essential to keep in mind that the more isolated / segmented your network is: PUT GRAPH security vs usability**

* **the harder it can be for an attacker to compromise your critical assets / data/processes.**
* **the more time it takes to design / manage the network access lists**

**the more difficult it can be to manage and ensure that users, processes and systems are able to access all required assets**

# Segmentation Strategy

As mentioned, a balanced segmentation strategy in manufacturing plants is essential and fundamental to ensure efficient risk management. When designing segmentation, most network architects or engineers focus on the larger network zones: DMZ, Datacenter, users LANs, and so on. While this is an important first step, it is not nearly enough to tackle today’s ever-growing security threats. Most opportunistic attacks take advantage of the fact that there is limited or no segmentation inside production floors[[2]](#footnote-2), allowing them to roam around the network without hindrance, and to spreading damage quickly. A complete list of network assets and an understanding of processes are essential in order to better design and implement a stringent inner-zone segmentation that encapsulates processes and assets.

Having a balanced strategy is an important first step, but a strategy is only useful if there is an implementation concept and a detailed program to back it. The implementation concept should be comprehensive enough to provide all the tools that an enterprise/organization requires to protect its critical assets and processes. This section illustrates a segmentation strategy lifecycle that begins by identifying existing resources and onboarding any new asset, process or resource. Each of the steps are discussed in detail in the following sub-sections. This process needs to be repeated and re-assessed once a year, or whenever a change is introduced to the production floor, or a new threat that changes the strategy is identified globally.

Design and implantation of a good segmentation strategy is a long and continuous process, modifying an existing OT networks takes time and should be done in small steps to insure operational safety is kept at all times.

**Figure 1: Segmentation Strategy Steps REPLACE GRAPH WITH SEGEMENTATION PHASES**

**Identification:** Segmentation should be based on the importance/impact of a critical production process, asset or resource, not simply on network boundaries or zones. The first step of an attacker/malware is reconnaissance that maps the network and assets and in advanced attacks the processes. That is essentially what the first step of the segmentation strategy should be: identifying resources (both data and assets) and the attacker’s challenges in their exploitation. This step in necessary to perform risk prioritization.

To protect (or compromise) a network, it is important to gather intelligence about the various weaknesses that may exist. These weaknesses are exploited by attackers to encroach on other resources to the point where the attackers have privileged access to all critical resources. This makes any type of resource, even one that is considered to have low value, extremely valuable if it is used as the entry or next-stage point into the network and leads to a more valuable target. The questions to ask are:

1. What is the impact of a compromised resource?
2. What is the likelihood of a resource being compromised?

These assets, or objects, are primarily digital in nature and can include, but are not limited to:

1. **Hardware:**servers, network devices, workstations, controllers, physical security components, connected peripherals and accessories such as printers, scanners, IP phones, voice and video collaboration tools
2. **Software:** operating systems, server and client applications, firmware
3. **Documentation:** network diagrams, asset information, product designs, employee information, passwords and privileges.

The value of an asset is not based on the business impact it has or may cause if compromised. If an unauthorized change happens in PLC configuration leading to potential defect auto parts, the total value of the loss is not merely the cost of replacing a $500 controller or just reprogramming it.

**Classification:** The result of this stage is a comprehensive view of the resources on the network along with their risk classification and rating. ***Organizations should understand how various resources relate to each other, and not treat them individually***. A low-value target may ultimately provide access to a very high-value target, so the entire chain should be protected with adequate controls. Depending on the size of the organization, this could be one of the most resource-consuming steps. Various methodologies and/or frameworks can be followed to perform a thorough assessment of the resources that exist in the network.

One should now be able to move on to the next steps of creating a segmentation policy that utilizes the value of each asset to determine how it should be protected. For example, if user workstations are treated as a low-value target but are used to compromise a system that is of high value, such as an engineering station, the workstations should also be segmented depending on the resources they are accessing.

**Policy Creation:**Most cybersecurity programs do not explicitly call for a segmentation policy. It is usually mentioned indirectly in various topics within the program, which unfortunately does not place sufficient importance or value on it. For example, an access-control policy may call out how an HR employee should not be able to access MES system. This can be done simply through an access-control list on a firewall along with VLANs, which may protect the resource, but does not necessarily focus on segmentation itself.

A segmentation policy should be built based on data gathered about the resources in the previous steps. This policy should start at a high level, which segregates the various zones through traditional network boundaries, such as DMZ, Datacenter, and hall network then gradually drills into each zone. This process should continue all the way to the application itself, essentially moving up the layers of the OSI model. Once all objects (and even sub-objects) have been discovered, the policy should be developed based on the type and location of those objects and on the users, who are requesting access to various resources hosting or containing data. How deep one goes depends on the criticality of the asset, since in certain cases the cost associated with going through the entire process for a certain asset may not be justified.

**Access control modeling**: Network engineers are most familiar with network-based ACLs, and while they are a good way to control access between the larger zones, it is difficult to make them granular, especially since they are mostly static and become difficult to manage over time. There are several access-control models to choose from. one should pick the one (or a combination of several) that best fit the network requirements and constraints. This includes, but is not limited to:

1. Attribute Based Access Control (ABAC)
2. Role Based Access Control (RBAC)
3. Identity Based Access Control (IBAC)
4. Rules Based Access Control (RuBAC)

**Execution:** Once an access-control model has been defined and the appropriate policies have been mapped in this model, the next step is to implement these controls. This involves thorough planning, which will lead to the procurement, design, and implementation of the relevant technologies. This can be broken down into the following phases:

1. Plan
2. Design
3. Implement/Migrate
4. Monitor

Plan

Design

Implement

Monitor

**Figure 9: Execution Phases**

*Plan:* This phase of execution entails coming up with a list of requirements to satisfy the goals of the segmentation strategy. Once you have an accurate understanding of what to protect and what to protect against, the next step is to determine the tools, techniques, and procedures which are required to provide the ongoing protection. it is important to not start by implementing a all-segmentation strategy across the entire organization. It will require a large pool of resources be costly and achieve a relatively small advantage of a more balanced, granular approach. Based on your data/resource classification and the access-control model, build an implementation plan by prioritizing parts of your organization that handle and store business-critical data. You will not have a fully segmented infrastructure overnight. It is a process that could take months. An adaptive fit from day one strategy will guarantee success in the most cost-effective way. A step by step approach will assist in lessons learned and improving implantation process with feedback changes during the process.

*Design:* In most cases, the organization’s lead architect will oversee the design created by the product vendors. The design, when it comes to segmentation, should focus on the core elements, including:

1. Location: Network location of the resource, and how is it segmented from the rest of the network?
2. Device and Application: Does the resource need access to other resources? And do other resources need access to it? For example, a multi-tier application may have a front-end (web), middleware, or back-end (database). Is each service running in its own container and what are the privileges that each service has for the others? What is the relationship between the services?
3. User: User devices in normal circumstances do not need to communicate directly with each other. How is this being handled? What can the users access? How does the organization certify that a user’s endpoint has the same level of access regardless of the location?

Once the design phase is complete, it is time to start the implementation.

*Implement and Test:* The implementation phase assumes that all the hardware has been tested and is working as expected. Any components that may have failed during the POST tests should have been replaced and be ready for configuration. The implementation should follow a plan that is created based on the design. This includes the detailed configuration that the vendors have already tested and verified in their environments during the design phase.

It is essential to carry out testing to ensure that all is working according to the specifications and expectations for the solution. Testing should follow a proper methodology and should assess both functionality and features that are then recorded. Any issues encountered during testing should be addressed with the vendors and rectified before moving into the implementation phase.

As mentioned earlier, the pilot phase is important to this phase and should be conducted once functional and feature tests are completed. The pilot tests for performance, resiliency, user experience, and interoperability, and addresses any issues that may have been overlooked during the initial phases. The pilot phase should also span across locations, departments, technologies, and resources. This reach ensures that all stakeholders are involved in the process and will work towards a proper resolution of any challenges faced.

**Monitoring:** This step is one that is given very little importance in most enterprises. Based on the understanding that the Digital surface of the production floor will change in time (due to maintenance or other required changes) monitoring is essential as the key to safeguarding the network from intruders and ensuring that systems and networks are performing as per specifications. Monitoring marks the culmination of the whole segmentation strategy and is the glue that brings people, processes, and technologies together to preserve the integrity of the protected resources. Keeping a stringent view of the network not only eases detection of any anomalous activity but also helps in attack surface governance based on identification of any resources, new or existing, that may have been missed during the initial pass. This will determine whether another iteration through the whole segmentation lifecycle is required. The monitoring design phase is one of the most important in the processes of achieving a stringent evolving segmentation.

**4. Threat modeling and segmentation**

Applying the mentioned segmentation strategy will strengthen the network cyber security by forming obstacles that will increase the level of difficulty and potentially will create alerts when an attacker will try to penetrate the network.

Shifting to a more stringent segmentation policy entails both a meticulous planning and adequate deployment abilities, such as: knowledgeable personnel and technological tools.

Many organizations feel overwhelmed when facing such a task and subsequently perform a less then complete analysis, leading into a less then optimal plan and thus not achieving the maximum security possible under the operational limitations.

OTORIO has developed a complementary approach to full segmentation strategy, this method should go hand in hand with the classical approach portrayed earlier, but it could also be used as an initial procedure to assess current or proposed segmentation architecture.

Based upon our intimate knowledge of cyber attack’s tools, techniques and procedures we recommend an advanced layer that incorporates security controls and policies where the attack has more probability to breach the network and propagate unhindered.

The threat modeling produces a prioritized segmentation roadmap which is customized to the plant threat vectors and mitigation controls.

The threat modeling risk assessment takes into considerations several factors when formulating the optimal mitigation plan for the shop floor.

There are three major steps to generate a customized risk assessment that addresses the following questions:

1. **Where are the shop floor’s weak spots?**

The first step in threat modeling is identifying the attack surface and vectors, then we perform attacks scenarios and analyze the current and relevant security controls that mitigate or hinder the attack routes. Based on this procedure, we prioritize the risks.

1. **What needs protection?**

It is crucial to refine the exact definition of our security goal. In most shop floors there are hundreds or thousands of assets with their specific vulnerabilities and mitigation solutions. Will the segmentation address each asset or a focal point of communication? Do we need to consider all the ingress points of data into our shop floor or just some of them? How do we prioritize the granularity of segmentation?

1. **How to design the mitigation controls?**

There are a variety of mitigations solutions, but there is only a select few that matches the plant’s (personnel, process and technology) ability to deploy and operate in an optimal way. OTORIO strongly advocates deploying preventative technology as a priority, but, sometimes due to shop floor’s constraints, detective controls have better likelihood of achieving a cyber maturity progress.

Choosing the right design and deployment model of the segmentation solution must be customized to the plant’s particularities and limitations. An extra care must be taken in understanding the security personnel capacity and experience and avoiding operations and maintenance overwhelming.

The following diagram describes the workflow:

**5. MB’s segmentation plan analysis**

MB’s SITS 2.0 segmentation planning documentation presents clear and secure options for a segmentation deployment. The documents elaborate and provide technical know-how to network and security considerations for each deployment’s selection.

The documents methodology and the analysis align with good cyber engineering practice, additionally the several deployment options presented are covering a wide spectrum of possibilities.

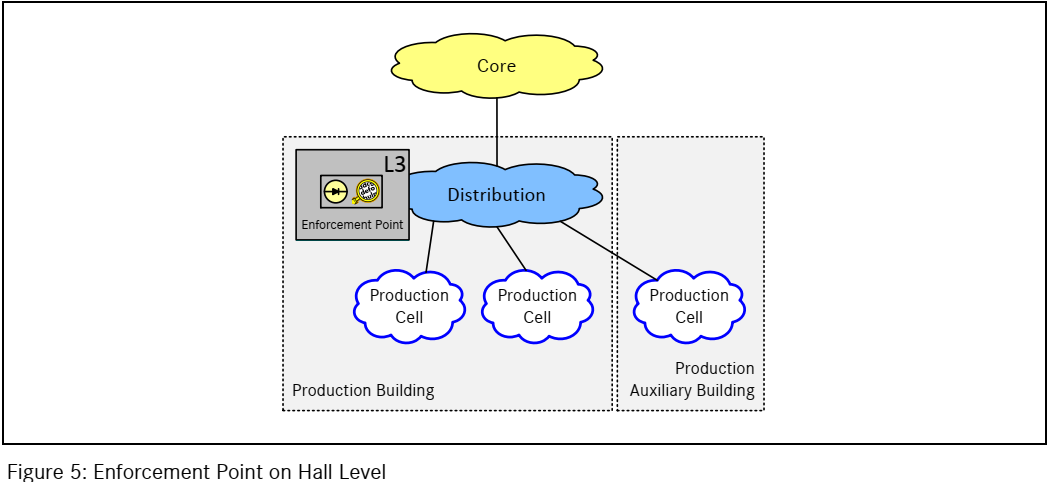
**We suggest adding to the documentation a list of benefits and downsides for each option, including security, safety, cost and maintenance considerations.**

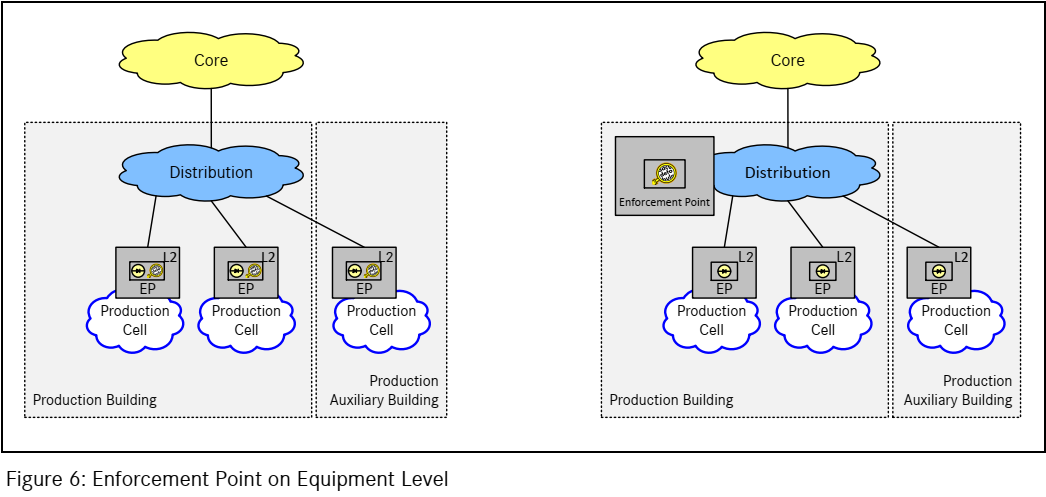
Some options might provide better security but at a large maintenance upkeep, for example.

Such an effort is paramount to the selection of the optimal deployment for Untertürkheim plant. The suggested process should involve all the relevant stakeholder of the segmentation deployment, from network/security team to the BISO and plant manager.

Upon reviewing the documentation, we would like to share the following insights:

1. Deployment of an enforcement point between production level and non-production level (layer 3.5) in preventative mode is a paramount consideration in protecting the production processes and equipment against external threats. As discussed in detail in the next chapter, our threat modeling analysis predicts that the majority of cyber attacks on production equipment will commence from the MB IT network (e.g. DCN or office LANs) or through the DMZ. A Significant attack mitigation control is a stringent, preventative deployment in front of the production level network. SITS 2.0 segmentation plan document present several such deployment possibilities. For example, figures 5 and 6 shows two optional deployment models:





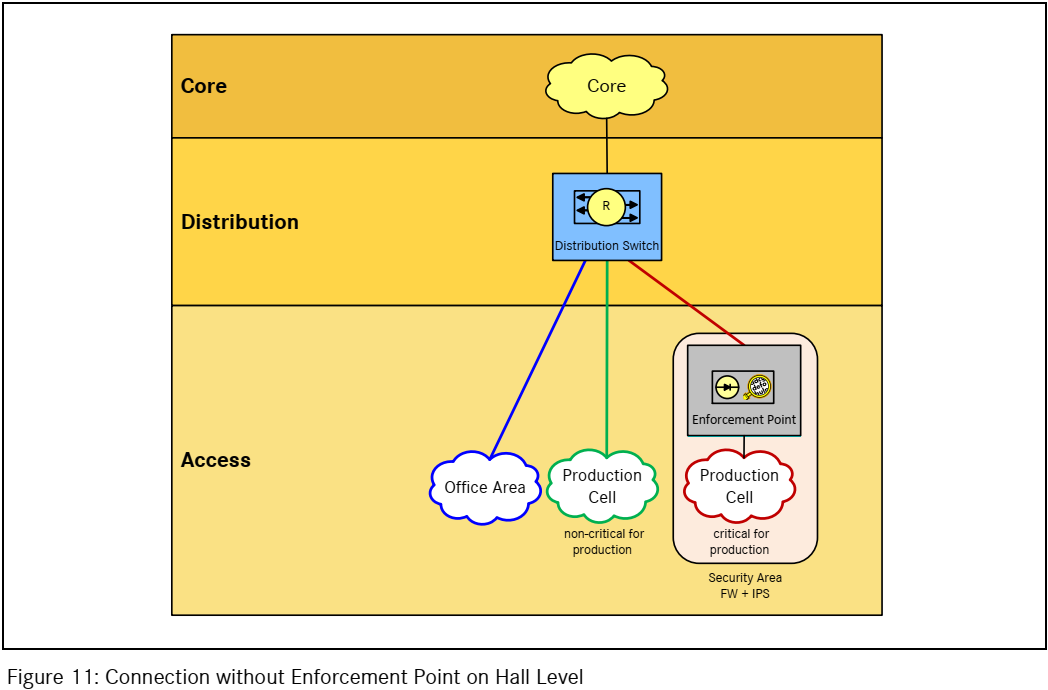
One of the major obstacles in the implementation presented in figure 6 is the amount of time and effort it will take to properly configure and ongoing maintenance of such a large array of gateways even though they are deployed as a layer 2 network devices. In addition, a policy misconfiguration could take a lot of resources to detect and locate.

**It is our recommendation to avoid the design and implementation of such architectures since it degrades security for the reasons mentioned above. The architecture presented in figure 5 has an easier manageability and overall a larger security efficiency, we believe it has higher success of implantation and ongoing maintenance.**

1. All production equipment level must have an enforcement point governing its intra-process communications. This requirement enables an important part in production networks security which is traffic monitoring for detection purposes. Since shaping an “approved traffic only” policy might take time to mature to full enforcement due to the risks in preventing legitimate traffic, a detection and monitoring phase is highly recommended.

**All SITS 2.0 implementation selections that are not supporting complete visibility and enforcement capabilities for the entire traffic in production equipment level should not be chosen**.

For example, figure 11 shows such a “limited” deployment one shouldn’t use.



1. Emergency planning for potential failures of the gateway is an important consideration in implementation design. “Planning Manual for protecting manufacturing equipment against IT Threats”, chapter 6, provides the use cases scenarios and suggests workarounds. The deployment scenarios of the gateway and their respective failure solutions are important for preserving the production processes safety when either the gateway has a malfunction or accidentally a rule policy prevents a legitimate traffic despite a good policy implementation. The ideal solution, in our view, should provide minimum intervention from an administrator/BISO and utilize automated/semi-automated (non-manual) recovery. A High availability gateway cluster offers an automatic failure recovery in case of a single gateway failure (see following diagram for a suggested HA deployment).

A screenshot of a cell phone

Description generated with very high confidence

**Deactivating IPS feature to solve prevention of legitimate traffic increases the plant’s risk, alerts are treated as potentially false positive. Reverting to prevention mode is extremely difficult because of the time and effort it takes to find the root cause analysis of the initial incident that caused the prevention capability.**

**It is advisable to handle those scenarios (degrading to IDS) with high priority and create procedures to mitigate that risk (such as establishing a responsible role for managing the process to research the root cause analysis and the return to IPS mode).**

**6. MB & OTORIO unified Analysis process**

The following section will describe in detail OTORIO’s threat modeling in conjunction with Untertürkheim production halls and MB SITS 2.0 documentation.

The combination of OTORIO model with MB SITS 2.0 provides an effective segmentation plan customized to MB to efficiently counteract an attacker and providing a swift detection of an attack with the means to stop it.

As seen in chapter 3, OTORIO’s model should comply with three questions.

1. **What are the attack surfaces and vectors?**

Untertürkheim plant (like most MB plants) has several attack surfaces and potential attack vectors that enable cyber attackers to breach the shop floor and propagate in the network.

A cyber-attack, whether targeted (i.e. a planned and prepared attack) or opportunistic generic (i.e. exploiting an unsecured attack surface or a generic malware that was introduced to the shop floor unintentionally by an employee) has the potential to cause production failure or interfere with the safety mechanisms resulting in potential financial cost, reputation loss or even human injuries.

**The cornerstone of risk governance by segmentation is identifying the most probable to be exploited attack surfaces and the respectively attack vectors that would offer the least resistance to an attack.**

The following are a potential entry points (with some short examples) of a cyber-attack to the UT hall, prioritized by ease of penetration’s potential (prioritization is based upon our insights of MB shop floors and halls gained by the intimate knowledge we developed over the last months):

1. Untertürkheim offices/datacenter LANs
   1. A malicious email containing undetected malware
   2. Surfing into an infected web site and unintentionally downloading a malware
2. DCN
   1. An infected workstation tries to scan the networks and perform lateral movement
3. DMZ
   1. The AV server (water holing attack or unpatched platform) was breached and used as a staging point
4. Supply chain (as a part of hardware/software)
   1. A production floor asset comes with a preinstalled malware
5. External technician laptop/DVD/USB
   1. Emergency firmware updates via external infected laptop
6. Remote access solution
   1. Through credentials theft or misconfiguration of the remote access solution
7. Daimler’s employee USB/laptop
   1. Ungoverned workstation used to upload materials to the network

The highest risk’s priority is given to the IT network and assets, even though it has a relatively good security control policies and infrastructure it is due to the fact that the entire IT cyber security mindset is focused upon protecting IT infrastructure and not OT infrastructure, which leaves the shop floor vulnerable to any successful breach or OT attack technique from the IT infrastructure.

1. **How to identify and prioritize the plant’s assets’ risks?**

This section deals with defining in clear terms the protection goals. It may seem trivial but focusing the effort in the most probable attacks’ targets or the paths in which the attack propagate in the network can greatly increase the security controls’ effectiveness. The segmentation challenge is in continuously assessment and identification of the part of the network the gateway will have better odds of detecting and preventing the attack. A concise description of the defensive goal can help in designing the solution which will be best suited to the plant.

Initially one has to identify and define the top worst-case scenarios caused by an attack. Each potential threat could cause a substantial impact to the plant such as: financial cost (productivity, intellectual property), safety hazard and even reputation loss. The outcome can be a combination of these examples.

The following table contains the MB’s shop floor prioritized potential threats:

|  |  |
| --- | --- |
| 1. | Disrupting a critical process production |
| 2. | Sabotaging a shop floor asset and decreasing quantity/quality of parts production |
| 3. | Fraudulent SAP/MES communication causing wrong numbers of production parts |
| 4. | Causing Denial of service in remote access operations |

Understanding the motivation of the attacker and his tactics helps in defining the protection’s vision in a more strategic concept.

**TIP**

We suggest a minor rephrasing of the sentence in the Daimler document “**Secure Network Structure within IT and Plant Network**” which states: “Production-critical manufacturing equipment must be protected by firewall and IPS” into a more agile concept enabling a prioritization of the several security deployment designs (SITS 2.0 blue print). Defining the vision as: “**Production-critical manufacturing equipment must have a clear and defined ingress data policy (both for prevention and monitoring) whether it’s direct (e.g. MES) or indirect (e.g. remote access, USB)”.**

**Merging the insights of the first two guidelines can better formulate and prioritize the lines of defense with the following two principles:**

1. **Verifying all communications entering the production floor from non-production networks**
2. **Continuously monitoring inter-production floor traffic for anomalies**

The first principle is straight forward, since the attack is more likely to start from the non-production networks, the initial planning and configuration should be put into enforcement rules between these two zones including communication from the DMZ

The second principle realizes that the potential damage to the plant of blocking a legitimate traffic could be as high as allowing malicious traffic, therefore a more safety-oriented approach is advisable. Such an approach dictates putting safety consideration first.

The monitoring is not excluded to the IT-OT traffic, complete visibility should merge network traffic flowing from, to and between production level assets. Pick an event and alert tool that is customized to production floor particularities. It will lower false positive and would reduce local and global security team investigating alerts.

1. **How to Design effective and efficient implantation**

Having too many information security controls can become unmanageable. When the organization overextend the security team’s abilities by deploying too many security tools, an opposite effect is achieved by overwhelming the team with too much information to handle decreasing the likelihood of detecting of an incident.

Each plant has an optimal equilibrium between security and manageability and our recommendation is aiming for that point of balance.

Designing for a minimum amount of security gateways deployment will paradoxically elevate security. Focusing the security team’s efforts and resources into a small number of gateways enables maximizations of tuning and problems resolving. Consolidation is a key guideline when designing optimal deployment.

The Design of an efficient network security strategy must take into account the challenges of a potential attacker and use it to its advantage.

Executing an attack on the production floor’s network is not a straight forward operation, knowledge of the specific assets and processes must be gained before delivering the malware. Stopping the attack in its reconnaissance or lateral movements phase has a very high probability of succeeding by detecting unusual network traffic or asset manipulation and responding swiftly according to IR methodologies.

Prediction of the enemy operations and its limitation leads to a maximum efficiency of the plant’s cyber security resources by mitigating the highest prioritized risks.

When addressing the most crucial risk observed in the previous section, the first mandatory requirement advocates strong segmentation between hall networks and the rest of the plant’s networks. Thorough knowledge of communication (protocol and port) must be acquired and properly configured. Traffic should be encrypted (at least in the non-hall networks) as a protection against fraud and impersonation and validated by the firewall. Strong authentication is also advisable as a countermeasure against the two types of attacks mentioned.

The second principal suggests an initial implementation of traffic monitoring mode starting inside the production level networks. As mentioned earlier, blocking anomalous yet legitimate traffic within the shop floor could have dire consequences as much as allowing non-legitimate traffic. The right process is building confidence and trust with the gateway’s rules in detection mode and later switching to prevention policy only after a achieving an acceptable maturity for the gateway operation and traffic policy.

The advantages of detection architecture are:

1. No interference with legitimate traffic of any kind

2. Alerts have a high tolerance of response time for resolution when legitimate traffic does not correspond with traffic rules since no blocking is enforced

3. Flexible and transparent modification rule set as new rules and configuration changes can be set without any impact on traffic which allow trial and error without disrupting traffic

4. Deployment of out-of-band architecture require minor network architecture and routing changes since the network topology is going through minor changes

The segmentation design should include the time frame of shifting from detective to preventative mode.

Progressing to prevention architecture, as soon as possible, is highly recommended but requires thorough design of network segmentation, analyzing inter processes dependencies and setting the correct traffic rules that will not block legitimate traffic. Prevention mode has the following advantages:

1. Immediate enforcement of non-legitimate protocols, ports and signature

2. High resistance and visibility of the attacker’s lateral movements due to real-time traffic analysis and pre-approved routing policies

3. Quick response and containment to incidents with immediate isolation of infected assets by the prevention gateway’s capabilities

**PUT TABLE DETECTION VS PREVENTION**

7. **Recommendation and summary**

We present an effective segmentation planning guideline which concludes and summarizes the segmentation strategy described in this document.

The analysis process took into account the deployment options in MB SITS 2.0 segmentation planning document:

1. Placement of the firewall on hall level with the possible settings:

a. VLAN

b. VRF

c. No enforcement point (critical production equipment only)

2. Placement of the firewall on production equipment level with the possible setting:

a. Access switch

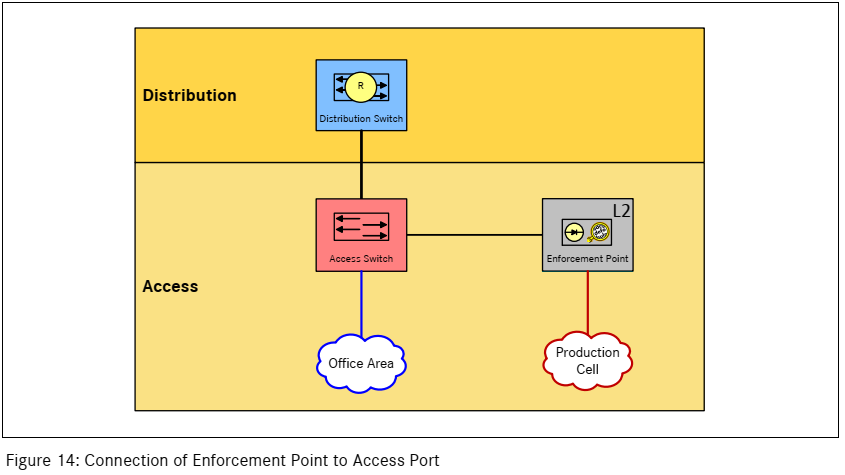
b. Access port

c. Distribution port

d. Automation access area

Unification of the suggested options with our threat modeling and the attack vectors leads to prioritization and guidelines of the following segmentation implantation:

1. Stringent prevention measure between production equipment level and any non-production equipment level (office LANs, DCN, DMZ …) as shown in SITS 2.0 document – figure 14



The main advantages of this implementation are:

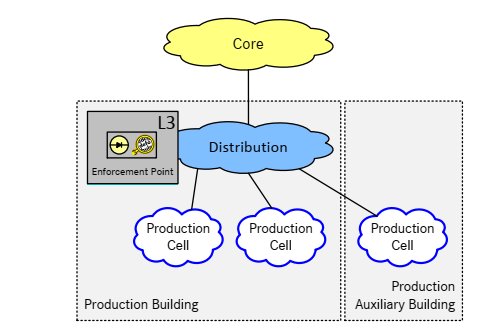
* Small access rules set to maintain by production level network/security team
* Tighter traffic shaping and better anomaly detection
* Uncoupling from the non-production networks for maintenance and topology changes
* Provides flexible segmentation changes and rapid incident response operations

The following points offer guidelines to a safe gateway deployment:

* The gateway should be configured as a L3 (layer 3) device to allow for DCN/hall independent IP ranges in the production level
* All external communication from/to production equipment level must comply with a preapproved whitelist of protocols and ports.
* Encryption of production equipment related traffic between the gateway and the external source/destination – since most production equipment do not support inherent encryption capabilities. It is sufficient to provide encryption between the gateway and non-production devices.
* Management of the gateway should be allowed only from isolated hardened workstations (i.e. computer without internet browsing or email features)
* Any policy violation or anomaly behavior attempt should raise an appropriate alert, recorded and sent to the production floor’s SOC/SIEM.
* Frequent regular updates of attack signatures and IOCs

1. Segmentation for inner-production level assets/processes plays a major role in preventing malwares from spreading inside the production network, since safety issues should take precedence over security requirements allow a short learn and adjust period for inner hall segmentation and only later to switch it gradually to preventive mode.

Our recommendation is to use the same gateway to analyze and prevent malicious traffic from/to and between production level assets. Initially allow for a short learn and adjust period for entire production level traffic as an IDS but setting a time frame for shifting to prevention policy as shown in SITS 2.0 – figure 5



**TIP LIKE**

The following points offer guidelines to a safe gateway deployment in production floor:

* Choose a gateway that support OT’s protocols deep packet inspection as an additional important layer of anomaly detection
* Merge assets’ action logs into gateway for improved detection rate of true incidents
* Configure functional (based on business knowledge) zones for processes communication to detect policy violations

A major addressable topic when deploying preventative controls in a production environment is an emergency function when a rule misconfiguration is blocking a legitimate traffic.

**TIP DON’T LIKE**

**We strongly advise against a creation of physical bypass of the gateway unless logical reconfiguration to detective mode is not feasible swiftly enough to prevent any kind of damage or loss to safety or productivity.**

The risks in making a physical bypass are creating an attack vector without visibility or control and generating a hard to revert process due to fear of causing the same fault without performing a laborious root cause analysis.

The segmentation plan should address such a process by assigning a security role for managing the return to the original prevention mode.

If production risk analysis presents a major concern of gateway failure blocking legitimate traffic, we suggest a high availability cluster design of the gateway. An example of such an optional design is depicted in the following logical drawing figure:

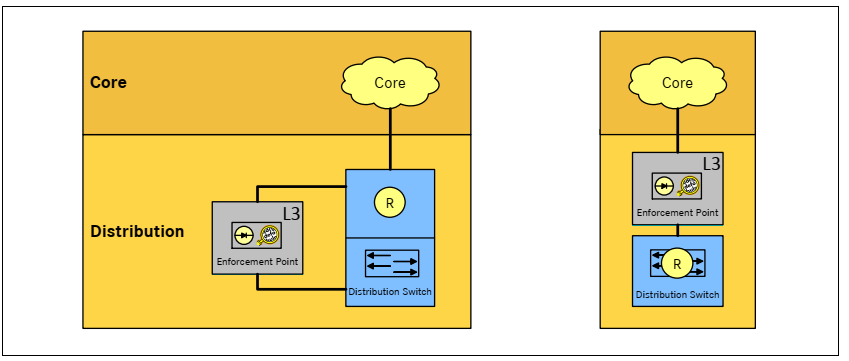
A screenshot of a cell phone

Description generated with very high confidence

1. segmentation for non-production level network traffic

Security in “pure” IT network has some key differences than OT networks: easier deployment of additional security layers, more flexibility to enforce prevention policy and usually a larger team of security personnel.

Our recommendation is to deploy a separate gateway for the IT networks in Untertürkheim supporting the full range of the gateway capabilities (i.e. firewall, IPS, application visibility, SSL VPN …). The gateway should provide security for the non-production networks. The following diagram SITS 2.0 – figure 12 presents a possible deployment



The following points offer guidelines to a safe gateway deployment:

* Deployment of the gateway should adhere to MB IT network security policies in all regards
* Since most OT cyber attacks start at the IT network, merging the traffic alerts and anomalies of the IT security gateway into the OT security gateway would provide a significantly higher success of attack detection rate
* As mentioned above, creating physical bypass of the security gateway in cases of fault is highly discouraged (refer to previous comment for explanation)

**In conclusion of the assessment, follow the three segmentation guidelines:**

**1. Stringent prevention between production and non-production networks**

**2. Allow for a learn and adjust period for inner production traffic segmentation and gradually transform into prevention rules. Defining rules and monitoring them is a crucial factor in responding quickly for an attack**

**3. Design for a minimum number of security gateway deployment due to maintenance issues but allow for a separate gateway deployment for external production network segmentation (i.e. IT networks) enabling most security features for detecting early stages of a potential attack.**

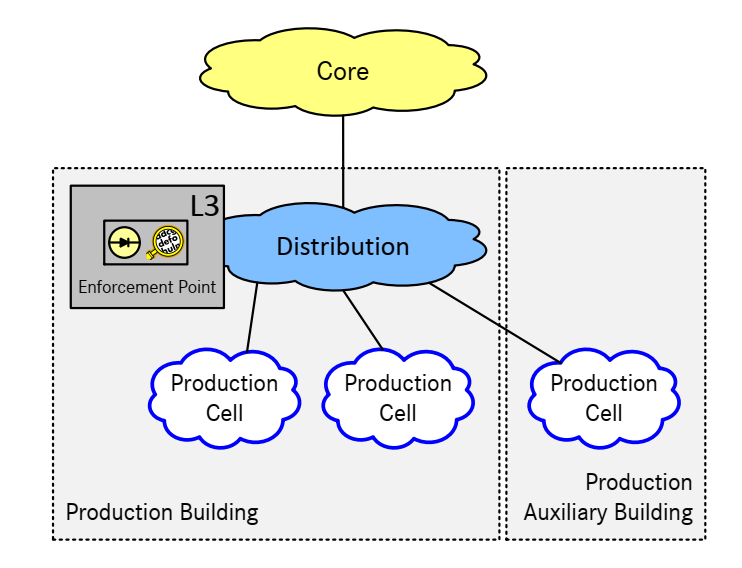
**Stay safe**

**Appendix A – Enforcement points locations comparisons**

A short advantages and disadvantages description of each enforcement point architecture suggested in the “Planning Manual – for protecting manufacturing equipment against IT threats”

**DO NOT REDESIGN DIAGRAMS**

**2.5 Enforcement point on Hall level (figure 5)**

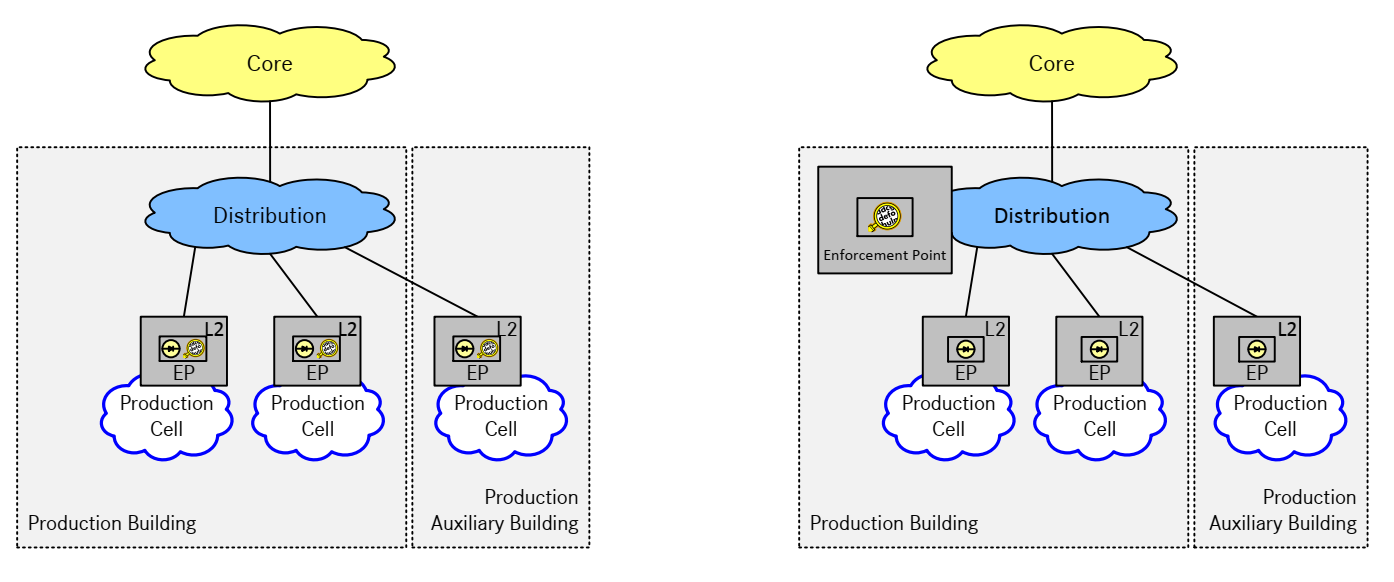


This architecture provides good separation between IT and OT networks. The gateway, whether it is deployed as a physical barrier between the distribution and access switches or as a logical routing machine, allows easy configurable preventative rule-set tool for IT-OT traffic. Changes made to the rule-set have minimal impact on inner-production floor traffic.

Using this deployment as the only gateway of the plant might result in traffic performance issues when configuring VLANs for traffic anomaly behavior between and inside production cells.

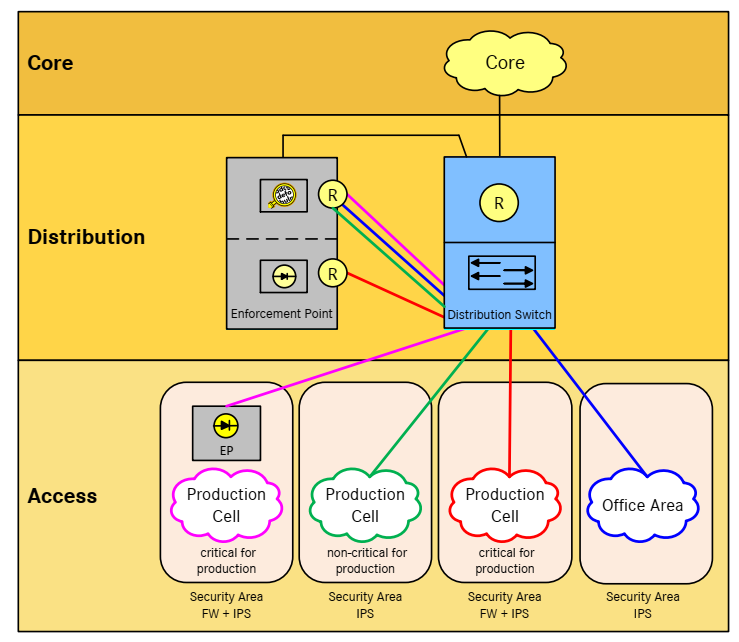
Managing and monitoring a single gateway does not require additional management tools.

**2.6 Enforcement point on equipment level (figure 6)**



This architecture simplifies rules-set for inner-production floor traffic. Each production cell has it own gateway with its specific rules. A malfunction or substitution of a single gateway does not require shutdown on the entire production floors. The disadvantages of such a deployment is high overhead of management and synchronization (with other gateways). Most likely, a gateway management software will have to be deployed in order to successfully orchestrate this deployment.

**3.1 Enforcement point (Logical design) on hall level with VLANs (figure 8)**

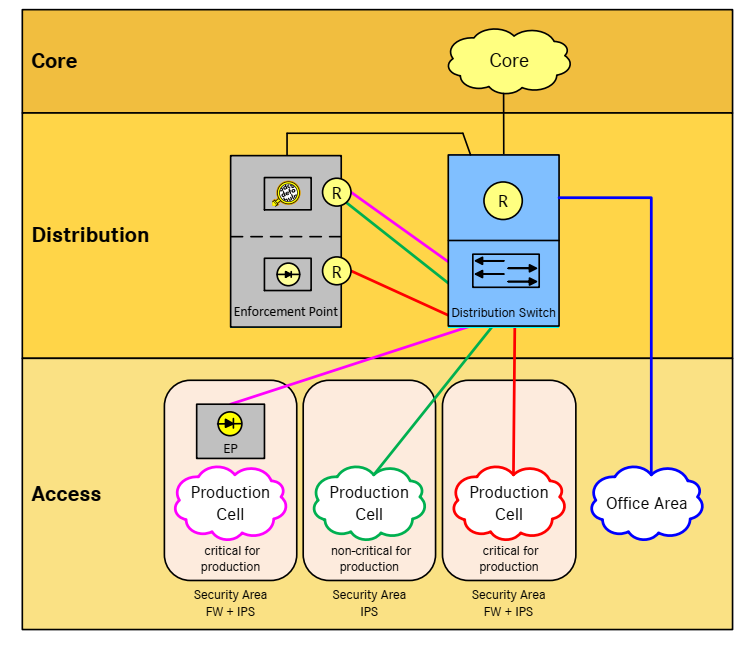


This architecture represents a hybrid solution for multiple gateway deployment (maintenance issues) and performance concerns (e.g. VLANs traffic to enforcement point).

Each security area (VLAN) has an IPS function checking ingoing/outgoing traffic for anomalies or attacks.

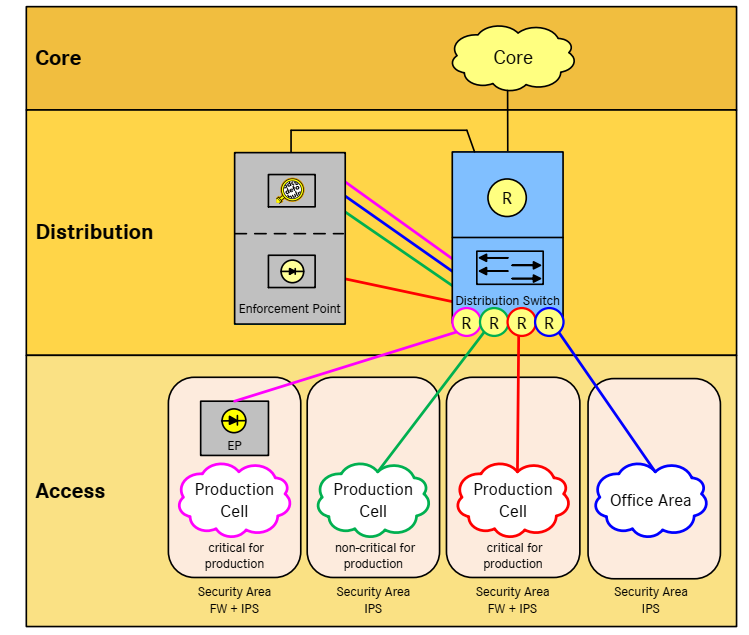
However, deploying a dedicated gateway to each critical production cell might lead to the same issues mentioned in the previous solution.

**3.1 Alternative connection with enforcement point on hall level via VLANs (figure 9)**



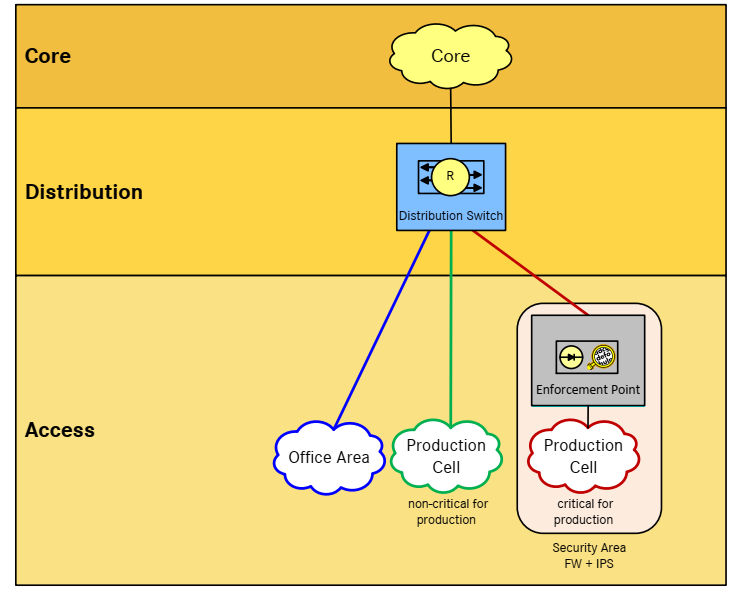
Very similar to the preceding solution with one difference which is neglecting security for inner office traffic. This architecture is not recommended due to the security issue, since a major portion of OT attacks are launched from IT environments and its common internet services (i.e. email, browsing etc..) early detection on unusual behavior in the IT networks might prevent the attack from reaching the production floor.

**3.2 Enforcement point (Logical design) on hall level with VRF (figure 10)**



This architecture sacrifices security visibility for inner production cell in favor of performance and maintenance (i.e. once an attacker penetrated a production cell, he can move freely within this cell without being detected – until the damage is done).

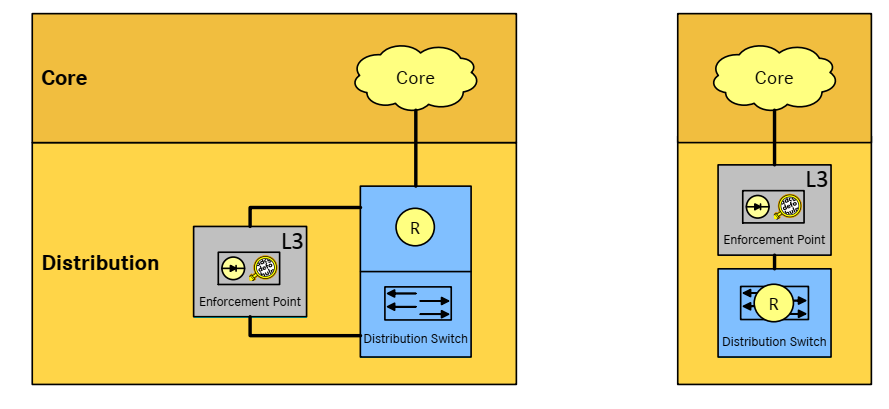
**3.3 No enforcement point on hall level (figure 11)**



This architecture assumes that only attacks on critical production cell have significant impact on the plant. Unfortunately, that is not so. An accumulation of minor disturbance in non-critical production cell as well as office areas would probably have a big impact on production as well, albeit not on the critical equipment itself but on supporting services, such as logistics, inventory management etc…

An effective segmentation solution must encompass every production floor asset.

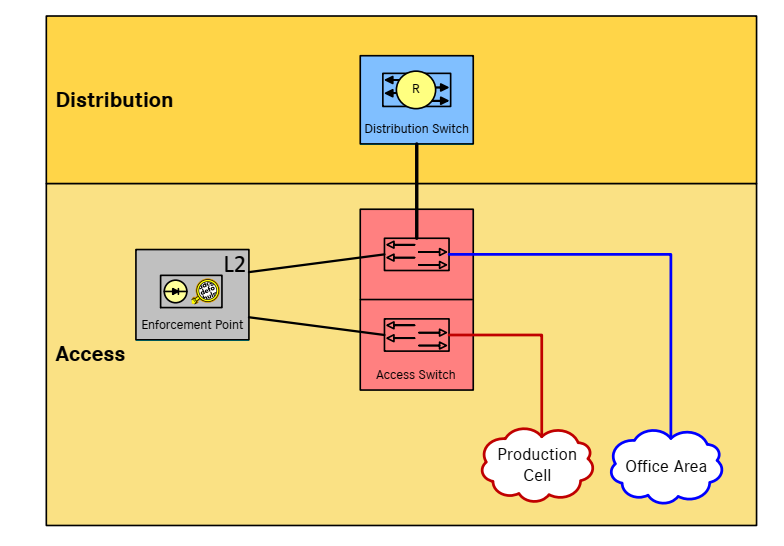
**3.4 Enforcement point (Physical design) on Hall level (figure 12)**



These architectures are less a security visibility issue and more a network maintenance question. Should the enforcement point be a physical barrier on a logical one? There are good arguments to either case, and no definitive preference to one or the other. As a physical barrier it is less prone to accidentally bypass configuration, a malfunction will completely block traffic.

The major consideration should be network administrators’ existing policies and procedures.

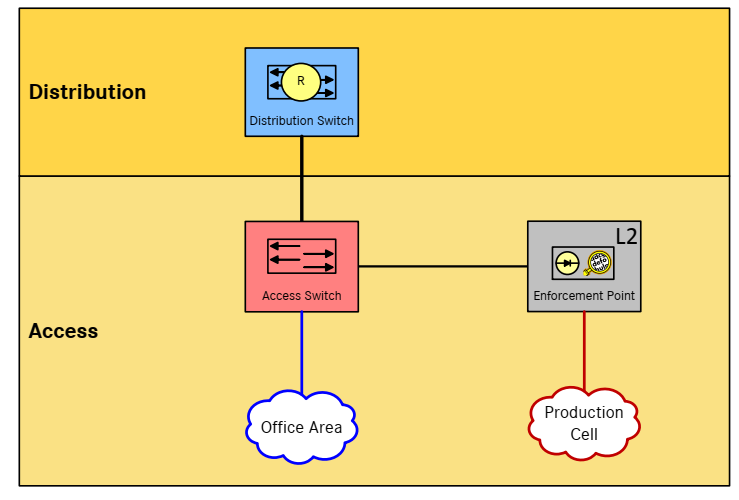
**4.1 Enforcement point at access switch (figure 13)**



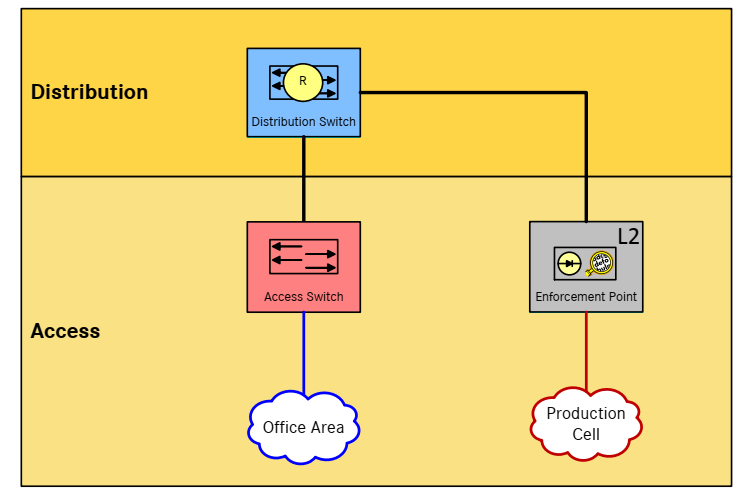
This is A good example of secure and robust architecture. Security visibility can be maximized for both office area and production cell, while the deployment is limited to minimum gateways.

Performance issues should not pose any trouble with proper configuration. The only downside is that both IT and OT rule-set is configured on the same gateway which might lead to mutual administration of separate teams (plant specific) with a potential of conflicting interests.

**4.2 Enforcement point at access port (figure 14)**

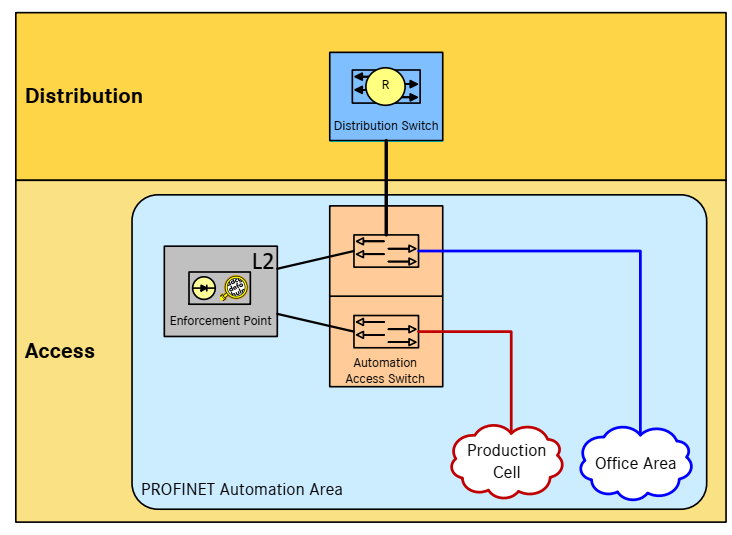


Much the same as the previous architecture. A good balance between security and manageability. As before, a mutual IT, OT, IT-OT gateway could lead to conflicting interests and maintenance issues as each party (IT, security teams) might have a different default configuration.

**4.3 Enforcement point at distribution port (figure 15)**

This architecture has the same security and network advantages and disadvantages as the last two architectures (4.2 and 4.1).

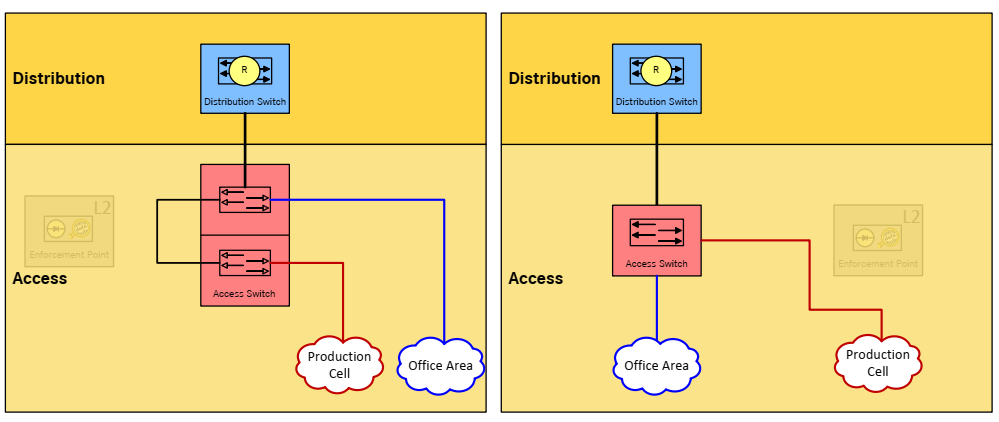
**4.4 Enforcement point within automation area (figure 16)**



Relatively similar to the former architecture, the big difference is the office area network which is connected to the automation access switch. As a best practice, it is recommended to deploy separate networking devices for production cells assets and office areas for multitude of reasons such as: different maintenance policies and configuration, high availability considerations, security factors (e.g. accessibility and monitoring) and performance issues.

Compared to the previous architectures this deployment solution is less favorable.

**6.1 Emergency function on manufacturing equipment level (figure 19)**



There are several security issues with these suggestions:

1. Committing a physical bypass of security gateway is hard to recover from as returning to the past configuration must be approved by all stakeholders (i.e. production floor operators and engineers, network and security teams and plant manager due to downtime required). Most organizations find it hard to re-deploy security gateway after removing them from the network due to mistrust in the solution.

2. Deactivating IPS and FW rules is a perfect opportunity for an attacker to strike, there is no limitation on network movement and no traffic monitoring, this is the ideal situation to strike or expand holdings on production floor assets. A good attacker will try to create a situation where the gateway seems at fault and consequently make the network team deactivate the gateway and allow the attacker to continue his plan unhindered.

A more suitable emergency plan should design a quick and easy to commit degradation from prevention to detection mode, thereby keeping network visibility continuously, even during gateway failure. An example to such a contingency plan is preparing a standby port mirroring configuration or tap devices ready for quick deployment and gateway replacement.

The new mode should be treated as high risk mode and the BISO team should strive to return to the original gateway deployment as soon as possible.

The next table summarizes the different architectures according to several parameters,

As seen, there is no single leading architecture, therefore our recommendation (as detailed in the conclusion part of this document) is a combination of architectures creating an optimal mixture of security and manageability.

**REPLACE WITH BETTER GRAPHICS**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 5 – very high 4 high | | 3 - moderate | | 2 – low 1 – very low | |
| Figure # | Security visibility\* | | Maintenance overhead | | Configuration complexity | | Performance impact |
| 5 | 3 | | 1 | | 1 | | 4 |
| 6 | 5 | | 5 | | 5 | | 1 |
| 8 | 5 | | 3 | | 3 | | 2 |
| 9 | 1 | | 3 | | 3 | | 2 |
| 10 | 1 | | 3 | | 3 | | 2 |
| 11 | 2 | | 2 | | 2 | | 2 |
| 12 | 3 | | 2 | | 2 | | 4 |
| 13 **Enforcement point at access switch** | 4 | | 2 | | 4 | | 2 |
| 14 **Enforcement point at access port** | 4 | | 2 | | 4 | | 2 |
| 15 **Enforcement point at distribution port** | 4 | | 2 | | 4 | | 2 |
| 16 **Enforcement point within automation area** | 3 | | 3 | | 4 | | 3 |
| 19 **Emergency function on manufacturing equipment level** | 1 | | 5 | | 5 | | 1 |

\*Opposite to the other columns, in which score 1 is the most desirable, in this column, score 5 represents the most beneficial outcome.

1. The same mechanism also interferes with the exfiltration of data [↑](#footnote-ref-1)
2. [↑](#footnote-ref-2)