

Zero trust architectures for interconnected industry

Max Ortmann, Robert H. Schmitt
DOI: 10.24406/publica-3778

Extract from:
ICNAP Report 2024
International Center for Networked,
Adaptive Production, Aachen
DOI: 10.24406/publica-3748

Zero trust architectures for interconnected industry

Max Ortmann

Research Fellow

Digital Infrastructures

Fraunhofer Institute for Production Technology IPT

Prof. Dr.-Ing. Robert H. Schmitt

Member of the board of directors of Fraunhofer IPT and holder of the chair for Production Metrology and Quality Management at the WZL | RWTH Aachen University

Introduction

The manufacturing sector has witnessed a transformative shift in recent years, driven by the rapid adoption of digital technologies. This paradigm shift, often referred to as Industry 4.0, has resulted in the seamless integration of physical and digital systems, leading to enhanced operational efficiency and growth. While these technological advancements offer numerous benefits, they also introduce significant cybersecurity risks, which are constantly increasing due to a multitude of vulnerabilities in digital elements and growing global tensions. Data theft, industrial espionage, and sabotage caused a total loss of 205.9 billion euro in Germany alone in 2023, and this trend is on the rise [5]. In 2024, both analog and digital attacks are projected to increase by approximately 29 %, reaching a total of 266.6 billion euro [6]. The alarming trend observed in Germany is mirrored on a global scale, with the cost of cybercrime anticipated to escalate to 13.82 trillion Dollar (approximately 11.73 trillion euro) by 2028, up from 9.22 trillion Dollar (approximately 7.83 trillion euro) in 2024 [7].

Emerging threats and challenges in Germany's security landscape

The recent study by Bitkom e.V., the industry association for the German information and telecommunications sector, surveyed 1,003 participants from various industry interest groups [6]. The findings reveal that 8 out of 10 companies have experienced cyber attacks, and two-thirds of these companies feel that their very existence is at risk. Cyberattacks have risen by 7 % compared to the previous year, particularly targeting operational processes, information, and production systems. According to the surveyed companies, 70 organizations from German economy were affected or suspected of being affected between June 2023 and June 2024. Simultaneously, physical attacks have also surged, with a 15 % increase in the theft of physical documents, personnel files, patents, machines, and components compared to the previous year. Additionally, there has been a 13 % rise in the interception of meetings and phone calls on-site over the same period.

Enhanced security and regulatory requirements for smart factories

The global increase in cyberattacks, which are mainly attributed to state actors and organized crime, is causing the production sector to be increasingly targeted. As digitalization advances and the interconnection of operational technologies (OT) expands, not only IT systems but also various aspects of manufacturing companies could become the prime targets for cyberattacks. The integration of modern technologies such as 5G, AI, cloud systems, and smart sensors into traditionally isolated fieldbus systems is driving a convergence of information technology (IT) and operational technology (OT). This convergence significantly broadens the attack surface in production environments and creating new security vulnerabilities, especially when legacy systems are integrated into digitalized production environments. To summarize, according to a study by Allianz SE, companies see the greatest risks in data breaches, cyberattacks on critical infrastructure and physical assets, the increase in malware/ransomware attacks and disruptions due to the failure of digital supply chains, cloud and service platforms [8].

In response to these escalating threats, the European Union has implemented a series of regulations aimed at enhancing cybersecurity across various sectors, including manufacturing. Regulations such as the Network and Information Security (NIS2) Directive, the EU regulation on machinery and the Cyber Resilience Act (CRA) seek to establish a unified approach to cybersecurity, mandating that organizations adopt specific measures to protect sensitive data and ensure the resilience of critical infrastructures throughout the whole supply chain. Compliance with these regulations is not only a legal obligation but also a crucial step in building trust with customers and partners, reinforcing the need for robust security practices in production environments.

Embracing secure digitalization: Zero Trust as a key strategy for future-proof manufacturing?

One promising approach to addressing these challenges is the adoption of a Zero Trust security model, particularly in digitalized Operational Technology (OT) settings. The Zero Trust framework operates on the principle of “never trust, always verify”, meaning that no device or user is trusted by default, regardless of their location within the network. By implementing strict identity verification protocols and continuously monitoring network traffic, manufacturing companies can significantly reduce the risk of unauthorized access and lateral movement within their systems. This approach is particularly effective in OT environments, where traditional perimeter defenses may no longer suffice due to the convergence of IT and OT systems. By fostering a culture of continuous security vigilance, the Zero Trust model can help mitigate the risks posed by cyber threats, ensuring the integrity and availability of critical production processes. However, implementing a Zero Trust architecture involves significant effort and high complexity. Additionally, the lack of harmonized standards for interoperability of product functionality presents a major challenge for companies. For this reason, the study “Zero Trust Architectures for Interconnected Industry” addresses the question:

“How can Zero Trust be established in OT environments considering industry specific requirements and is it reasonable?”

The first section outlines the obligations imposed on manufacturing companies by the European Union within the framework of cyber regulation. Based on these requirements, a comprehensive study on Zero Trust is conducted, with a particular focus on the adaptation of its concepts in digitalized operating environments. Finally, the study offers a best practice guide, providing companies with a step-by-step overview of the implementation of Zero Trust in production settings, while identifying associated opportunities and risks.

Cyber regulation in the European Union

Due to the rising number of cyberattacks on companies within the European economy and critical sectors, the European Union is enacting an increasing number of cyber regulations, now also impacting the manufacturing industry for the first time. Notably, the Network and Information Security (NIS2) Directive, the EU Machinery Regulation, and the Cyber Resilience Act (CRA) establish a regulatory framework that targets the processes of manufacturing companies in the EU, as well as hardware and software products distributed within the European Single Market. This legal framework not only binds individual companies within the EU but also extends to suppliers, thereby encompassing the entire supply chain. Consequently, companies that manufacture products outside the EU and sell them within the EU are also subject to these regulations. A brief overview of the relevant regulation is given in Figure 7.

The following sections provide a detailed examination of the NIS2 Directive and the CRA and summarize the obligations for companies.

Network and Information Security (NIS2) Directive

With the implementation of the Network and Information Security (NIS2) Directive, which must be transposed into national law by October 18, 2024, the European Union sends a clear message. This directive broadens the definition of critical security sectors to include manufacturing companies as important entities, such as those in the machinery sector, with a workforce of 50 or more employees or an annual revenue exceeding 10 million euro. It is estimated that around 30,000 businesses within Germany will be affected directly by these measures, with approximately 80 % of these companies being unaware of their obligations.




NIS2 Directive	Regulation on Machinery	Cyber Resilience Act
<div></div> <div>Focus on compliance & governance</div> <div>Obligations in governance, awareness, risk management, reporting obligations and risk management in the supply chain.</div>	<div></div> <div>Focus on safety & security of machinery</div> <div>Regulations for safety and security of machinery and industrial control systems (ICS), including risk management and implementation of security measures.</div>	<div></div> <div>Focus on product security for hardware & software</div> <div>Key objectives: “security by design”, risk management, reporting of vulnerabilities and incidents and transparency.</div>
Comes into force on October 17, 2024	Comes into force on January 20, 2027	Expected to come into force in November 2027

Figure 7: Overview of upcoming cybersecurity regulations that affect the manufacturing sector.

Production companies that fall under the NIS2 Directive must comply with certain obligations. These obligations, outlined in the NIS2 Directive, include:

- **Governance:**

Management bodies are responsible for approving risk management strategies, monitoring their implementation, and being held accountable for any violations that occur.

- **Awareness:**

Regular security training should be conducted to enhance knowledge and skills at all levels, including management, to effectively identify risks and apply cybersecurity procedures.

- **Risk management:**

A comprehensive approach to risk management should include risk analysis, incident handling, business continuity planning, security measures for network and information systems, the use of cryptography, multi-factor authentication (MFA), and effective asset management.

- **Reporting obligations:**

Organizations must report any significant security incident within 24 hours of becoming aware of it. An assessment of the incident's severity and impact should be provided within 72 hours, with a final report due within one month.

- **Supply chain:**

It is essential to ensure the security of supply chains by addressing both technical and non-technical risk factors.

As a result, the company's management is directly accountable for the implementation and oversight of cybersecurity measures. Additionally, technical, operational, and organizational measures must be established to manage risks, aiming to prevent, detect, and respond to potential cyberattacks. The scope and scale of these measures should align with various evaluation factors, such as company size, incident likelihood, and the societal and economic impact of security breaches.

In the event of significant security incidents causing serious operational disruptions, affected companies must fulfil reporting obligations. An initial warning must be reported within 24 hours of becoming aware of a significant security incident, followed by a comprehensive assessment within 72 hours, including severity and impact ratings. Interim reports on relevant status updates may be requested, with a final report due no later than one month after the incident. These reporting obligations also apply if third parties or institutions may suffer significant material or immaterial damages. Notably, NIS2 addresses supply chain risk management, acknowledging that attackers may exploit trust within the supply chain to introduce malicious components or compromise its integrity.

For manufacturers affected by NIS2, non-compliance with these obligations can result in fines of up to 7 million euro or 1.4 % of the total global revenue from the previous financial year. Authorities are authorized to conduct on-site inspections and oversight measures, which can also be delegated to third parties, including trained external professionals. In cases of violations, company executives may be held personally accountable.

Cyber Resilience Act (CRA)

The Cyber Resilience Act (CRA) addresses a critical gap in cybersecurity by focusing on the security of products entering the European market, an area that often receives less attention despite investments by companies in their own network security measures. To enhance both corporate governance and product security, the NIS2 Directive and the CRA complement each other effectively. However, while the NIS2 Directive is set to come into force end of 2024, companies will have additional time to fully implement the requirements that are mandatory under the CRA. The CRA was adopted by the EU Parliament in March 2024 and is awaiting ratification by the EU Council at the time of writing. It is anticipated that this ratification will occur before the end of 2024, initiating a 36-month transition period. As a result, effective implementation of the CRA is expected by November 2027.

Its primary objective is to ensure that digital products and services are designed with robust security measures from the outset, thereby reducing vulnerabilities that could be exploited by cybercriminals. One of the key components of the Act is the establishment of specific security requirements that manufacturers must adhere to when developing digital products. This includes ensuring that products are resilient to cyber threats and that they incorporate security features that can withstand potential attacks. Transparency is another critical aspect of the Cyber Resilience Act. Manufacturers are required to provide clear and accessible information regarding the security characteristics of their products. This includes details about potential risks, security updates, and how users can protect themselves. By fostering transparency, the Act aims to empower consumers and businesses to make informed decisions about the digital products they use. In addition to these requirements, the CRA mandates that companies report significant cybersecurity incidents to relevant authorities. This incident reporting obligation is designed to facilitate a swift response to cyber threats and to improve the overall understanding of the cybersecurity landscape within the EU. By collecting data on incidents, authorities can identify trends and develop more effective strategies to combat cybercrime.

The key provisions of the Cyber Resilience Act (CRA) can be summarized as follows:

- **Risk assessment and support throughout the entire product life cycle:**

Manufacturers must conduct risk assessments to identify potential vulnerabilities in their products and services. They are then required to implement appropriate security measures to mitigate these risks. In addition, manufacturers must provide free security updates for at least 5 years.

- **Security by design and by default:**

Products and services must be designed with security as a core consideration from the outset. This means that security features should be built into the products rather than added as an afterthought. Additionally, products must be configured to have secure default settings.

- **Reporting of security vulnerabilities:**

Manufacturers and importers are obligated to report cybersecurity incidents to the relevant national authorities.

- **Product labeling and transparency:**

Products must be labeled with information about their security features and any known vulnerabilities. Consumers will have the right to be informed about the security implications of the products they purchase.

Noncompliance with the CRA can impose substantial sanctions. Violations of fundamental requirements can result in fines of up to 15 million euro or 2.5 % of a company's total global annual revenue, whichever is higher. For breaches of other obligations, fines can reach 10 million euro or 2 % of global revenue. Additionally, providing false or misleading information to notified bodies can lead to fines of up to 5 million euro or 1 % of total global revenue.

Zero Trust as a security strategy in manufacturing

The implementation of security measures involves significant complexity and effort. The production sector presents a unique challenge, as it must consider both IT and OT systems. As these areas converge through digitalization and networking, the potential attack surface for companies expands, making them more vulnerable to threats, even at the field level [9]. A minor oversight can create a critical vulnerability, allowing unauthorized access to internal systems. Therefore, adapting cybersecurity strategies is essential for organizations to effectively plan, assess risks, and monitor their network and information systems. With forthcoming cybersecurity regulations, compliance with established standards may soon become mandatory.

Numerous recognized national and international norms and standards are documented in the literature. In a globalized economy, harmonized standards are especially beneficial, as they are acknowledged across various countries and increasingly serve as prerequisites for trade between institutions. For the manufacturing industry, ISO/IEC 27001, which focuses on information security management systems, could help with compliance with the NIS2 Directive, as ISO 27001 defines measures for implementing the minimum requirements of the NIS2 Directive. For example, through the introduction of an information security management system (ISMS), processes can be introduced for risk management or for handling security incidents. The prior introduction of a quality management system in accordance with ISO 9001 is recommended. IEC 62443 can be used in a similar form for the implementation of the requirements by the CRA in the production sector. In particular, IEC 62443-4-1 and IEC 62443-4-2 define technical and organizational requirements for "Security by Design".

While many standards share common elements, they often have distinct certification requirements, especially in the manufacturing sector. This can pose challenges for organizations seeking compliance, as they must navigate the unique criteria and processes of each standard. Furthermore, differing interpretations of similar concepts can result in inconsistencies in implementation across manufacturing environments. However, obtaining security certification does not guarantee that a company is fully protected against cyber attacks. Often, only minimum requirements are mandated, leading to the implementation of isolated solutions that may not address broader security needs once certification is achieved. To address these challenges, the concept of Zero Trust is gaining prominence. Zero Trust is a strict security strategy that companies can adapt to improve technical and organizational protection and ensure compliance with cyber regulations. The importance and future viability of Zero Trust as a security concept is underlined by the requirement for all US

government agencies to convert their infrastructures to a Zero Trust architecture. The following section outlines the fundamental principles of Zero Trust and presents best practices for its application in manufacturing environments.

Core principles of Zero Trust

Zero Trust is a strict security paradigm that assumes a breach has already occurred. It operates on the principle of least privilege, requiring all entities, for example devices, user or systems, to prove their identity and authorization before accessing resources [10], [11]. This eliminates implicit trust among entities and transforms traditional perimeter-based security into a multi-layered, integrated security approach. Communication between entities necessitates explicit verification and earned trust through reliable evidence. This continuous trust check minimizes the risks to confidentiality and integrity but can impair availability. It should be noted that the availability of resources in particular is essential for production. In summary, Zero Trust is defined by three core principles:

1. Assume breach:

There is no longer a distinction between internal and external networks; the internal network is always considered insecure, and trust is never granted permanently. Trust is continuously assessed based on dynamic access policies, ongoing monitoring, and risk analyses, with access decisions made anew each time.

2. First verify, then trust:

The absence of implicit trust necessitates that every entity must authenticate and be authorized to access resources, with strong authentication playing a crucial role.

3. Least privilege:

The principle of least privilege means that only entities requiring access are granted it. This requires resources to be divided into smaller units and permissions to be assigned as granularly as possible. A smaller access radius limits uncontrolled data exfiltration, data manipulation, and lateral movement in the event of malicious access.

Zero Trust reference architecture

The principles of Zero Trust do not dictate a specific architecture and remain unstandardized [10], [11]. Instead, guiding frameworks are provided for processes, identities, system design, and their interactions. For example, the NIST Special Publication 800-207 "Zero Trust Architecture" provides a reference architecture that is also supported by the German Federal Office for Information Security (BSI) in a "Zero Trust" position paper from 2023 [10]. The reference model and the logical components of a Zero Trust architecture are outlined in the following and shown in Figure 8.

The access decision functionality in a Zero Trust architecture is referred to as "Policy Decision Points" (PDP). The PDP component ensures that access requests are valid. It can be a local entity within the organization or an externally hosted service. For evaluation, it could utilize the organization's access policy and could gather information from various sources to assess trustworthiness. If the trust assessment is validated, the PDP could issue a restricted access permission from a device, user or system to the "Policy Enforcement Point" (PEP). The PEP then enforces the decision made by the PDP. To ensure the integrity of the communication paths, there should also be a separation between the communication required to control and configure the internal network and the communication used for application access. According to the Federal Office for Information Security (German: Bundesamt für Sicherheit in der Informationstechnik, abbreviated as BSI), a physical separation

should take place for requirements with increased protection needs, whereby a logical separation is also sufficient for standard requirements [12]. In the Zero Trust reference model, this is termed the "Control Plane" and the "Data Plane". The process is illustrated in Figure 8.

The specific measures are largely influenced by the company's structure and may include factors such as IP address ranges, geographical access distribution, time-based access controls, the use of certificates, or hybrid dynamic models.

Best practices for adopting Zero Trust in digital production environments

Implementing Zero Trust in digitalized and networked production environments necessitates a well-planned change management process with tailored measures. Understanding the current status of security implementations is crucial. The Zero Trust Maturity Mode (ZTMM) serves as a valuable framework to guide the effective integration of Zero Trust principles [11]. The following section therefore outlines a best practice guideline based on the reference architecture and the ZTMM that focuses on the production sector.

The ZTMM defines seven principles for the successful implementation of Zero Trust, which manufacturers should consider when implementing a Zero Trust architecture [9]. The tenets in the context of manufacturing are outlined in the following.

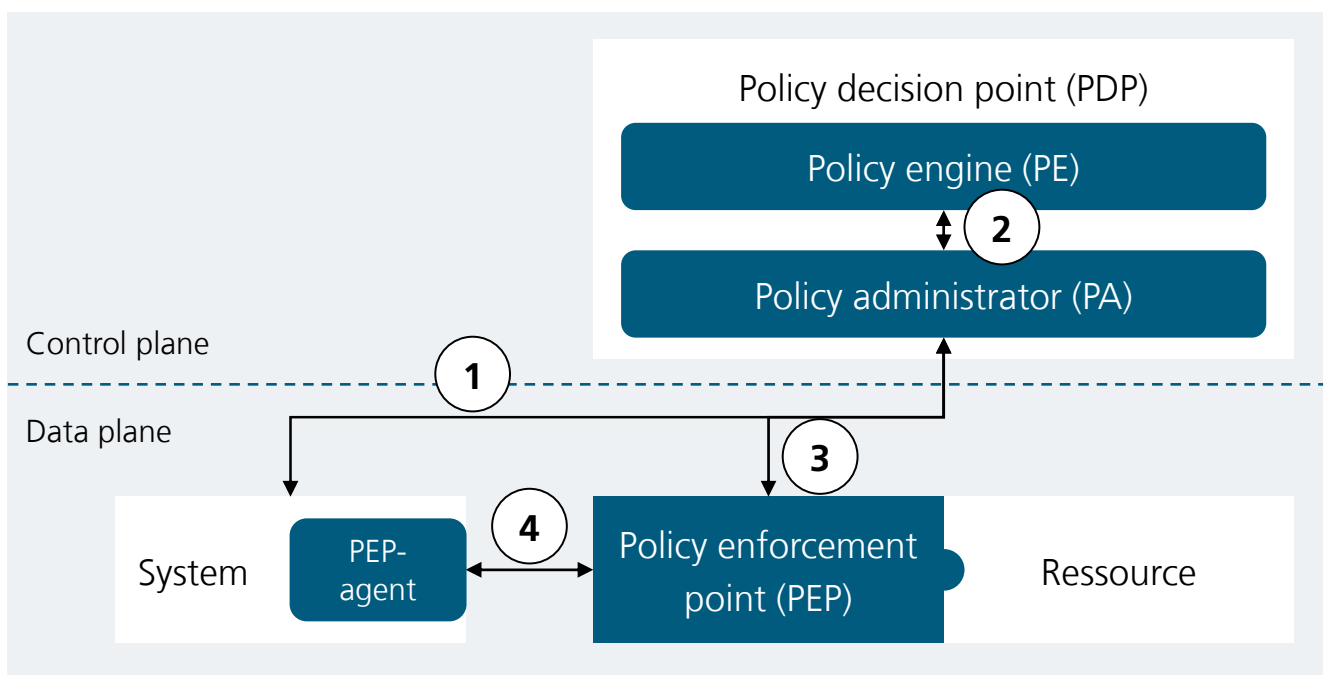


Figure 8: Zero Trust reference architecture and logical components.

1. All data sources and computing services are regarded as resources.

In digitalized manufacturing, production IT components such as programmable logic controllers (PLCs), sensors, edge PCs, etc. are also resources and must be considered as part of a comprehensive Zero Trust architecture. Particular attention must be paid to legacy devices that are frequently used in the production environment.

2. All communication is secured regardless of the location of the network.

In addition to user access, the encryption of Machine-to-Machine (M2M) communication could be required, particularly when interactions between IT- and OT systems occurs. An example could be the usage of edge cloud systems for process monitoring and predictive maintenance. For real-time cloud access to control or sensor data, both hardware and software measures are needed to minimize latency from encryption. Depending on real-time needs, encryption can be implemented using Transport Layer Security (TLS) at layer 5, Internet Protocol Security (IPSec) at layer 3, or MAC Security (MACSec) at layer 2, with lower layers typically supporting stricter real-time requirements [12].

3. Access to individual resources is granted per session.

In the context of digitized production environments, access to resources such as sensors, PLCs, or applications is facilitated through temporary sessions that feature customized permissions based on established policies. As a result, each new session must be verified and evaluated by a Policy Decision Point (PDP).

4. Access to resources is determined by dynamic policies.

Dynamic policies enable real-time adjustments to access authorizations for resources based on predefined factors. In contrast to traditional whitelisting methods, these policies can incorporate various criteria, such as geographical restrictions, time-based controls, User Behavior Analytics or hybrid approaches.

5. Monitoring the integrity and security of all resources.

Monitoring network and resource behavior necessitates the integration of a sensor-probe system for each resource, including an Intrusion Detection and Prevention System (IDS/IPS). In digitized OT environments, the diverse

range of vendors, along with their proprietary operating systems, applications, and network protocols, can complicate the integration of solutions like Security Information and Event Management (SIEM) or Extended Detection and Response (XDR). This complexity demands a strategic approach to achieve effective security monitoring across diverse systems, ultimately contributing to the establishment of a secure ecosystem.

6. Authentication and authorization are dynamic and strictly enforced before access.

In digitalized OT environments, dynamic authentication and authorization are critical to maintaining security and operational integrity. Access controls are not static; instead, they adapt based on real-time factors such as user roles, operational conditions, and context. Depending on the access requirements for a user or application, certificate-based authentication and authorization can facilitate time-based access, complete with detailed logging. A Public Key Infrastructure (PKI) based on the X.509 standard can be utilized to efficiently manage cryptographic keys and issue the required certificates for authentication and authorization.

7. Collection of data on all resources and networks to improve security.

Data collection aligns seamlessly with the principles of Industry 4.0 and can be leveraged within a Zero Trust framework to strengthen security measures. This includes establishing baseline processes, training AI-based anomaly detection systems, managing vulnerabilities, and analyzing access logs. These strategies collectively enhance the security posture of digitalized OT environments, enabling more effective threat detection and response.

As derived from the principles of the Zero Trust Maturity Model (ZTMM), the implementation gradient can be illustrated across five distinct pillars, allowing for incremental advancements toward optimization over time. These pillars, depicted in Figure 9, encompass identity, devices, networks, applications and data. Each pillar outlines some key aspects for the integration of Zero Trust in production environments related to three overarching functions: Visibility and Analytics, Automation and Orchestration, and Governance. These functions align with the demands of digitalized production in Industry 4.0, collectively creating a strong foundation for resilient manufacturing.

Deployment cycle for the implementation of Zero Trust in production environments

As a best practice for the integration of Zero Trust in production environments, the first step will be given by the establishment of OT Cybersecurity Governance, followed by the definition of OT specific policies and procedures. This initial step can be aligned with recognized standards such as ISO/IEC 27001 or IEC 62443-2-1. Simultaneously, the company must enhance its capabilities in automation, orchestration, visibility and analytics to facilitate the integration of selected processes into a Zero Trust architecture in accordance with Figure 8.

Once processes are established, such as through the implementation of an Information Security Management System (ISMS), the deployment cycle can be leveraged to integrate Zero Trust within a change management process as shown in Figure 10. During the preparation and categorization process, a comprehensive assessment of all resources and users, including business processes, must be carried out and inventoried. Depending on the size and complexity of the system under consideration and the company's level of maturity, this step can take a considerable amount of time. After the inventory is complete, the critical processes with the highest associated risks must be identified. A suitable process is then chosen based on the risk analysis and subsequent risk quantification. For the pilot phase, it is advisable to select non-critical processes to mitigate the impact of potential failures during the initial rollout.

If the risk assessment is completed, the implementation phase for the selected candidate process begins. Based on the Zero Trust reference architecture shown in Figure 8, the logical components, such as PDP and PEP, must be developed first. For example, the PDP in the control plane could be deployed either on-premises or in public cloud environments. The PDP and the agent in the data layer must be implemented directly on the relevant systems and resources. If legacy systems are in use or if implementing a PDP on proprietary hardware or software is too complex or costly, integrating a Zero Trust security gateway as a PEP could be considered.

Once the Zero Trust reference architecture for the selected candidate process, along with the policy configurations, is established and tested, the pilot system can be deployed in a real operational environment, a realistic test lab or a sandbox. By establishing a baseline activity pattern, policies can be refined based on practical experience. If the baseline activity is established and evaluated, companies can either expand their strategy to include new candidate processes or enhance their existing Zero Trust architecture by leveraging the five pillars of the ZTMM, as outlined in Figure 9. For instance, an IDS could be integrated for the selected candidate process. If the evaluation is found lacking, the deployment cycle can be adjusted and restarted from the beginning.

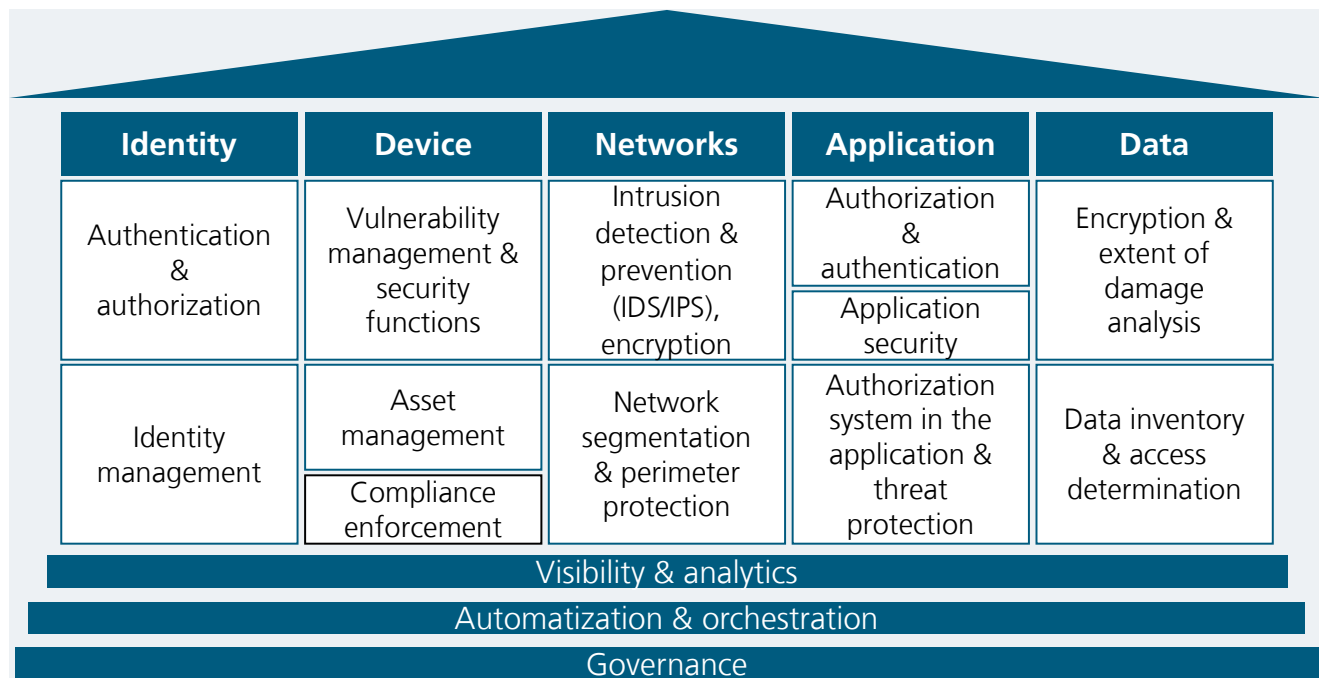


Figure 9: Pillars of the Zero Trust integration model.

In general, organizations can implement a Zero Trust architecture in production environments through various strategies. Common methods that align with the seven tenets of Zero Trust include enhanced identity governance, micro-segmentation, and software-defined perimeters [11]. Each method adheres to Zero Trust tenets but may prioritize different

components. The choice of approach typically depends on specific use cases and existing policies, with some being easier to implement than others. While alternative methods remain feasible, they may necessitate more substantial changes to current business processes.

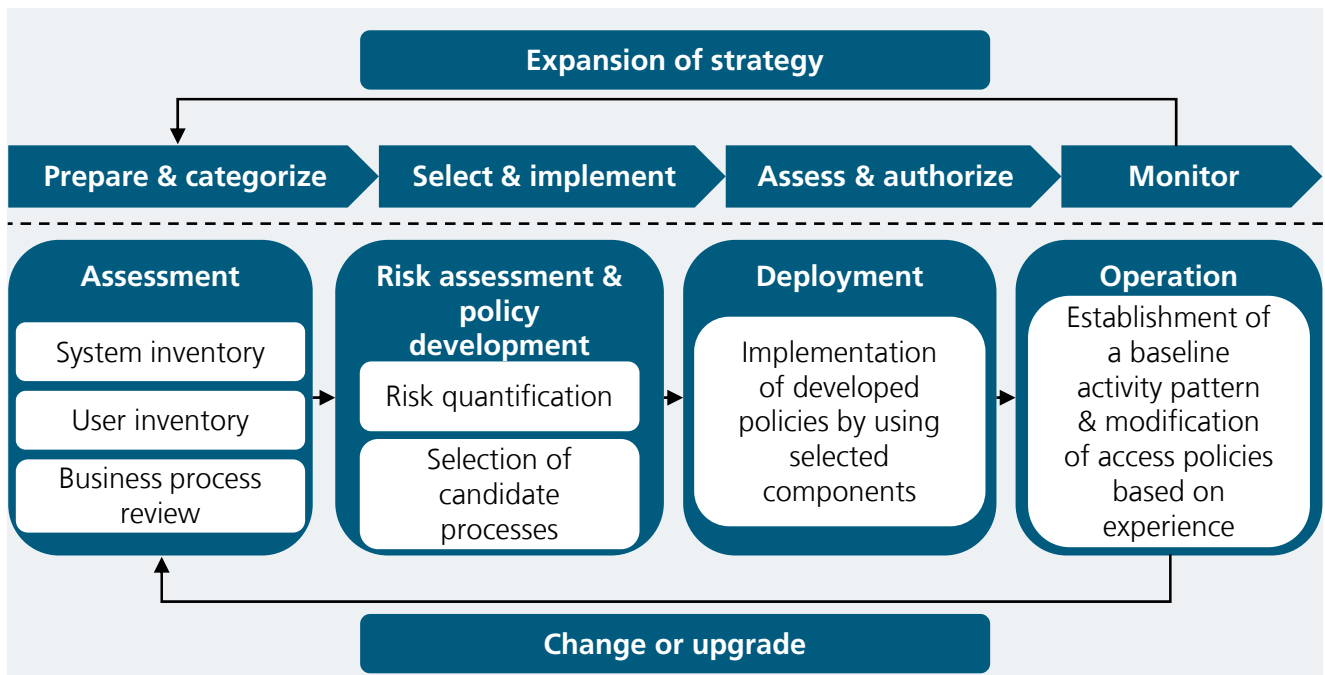


Figure 10: Hybrid Zero Trust architecture deployment cycle.

Conclusion

The recent number of security incidents shows that cybersecurity will remain a pressing issue for organizations, driven by emerging threats and tightening security and regulatory requirements. As these challenges evolve, the importance of robust cybersecurity measures is likely to increase significantly. As a reference, expenditure on IT security in Germany will increase by 13.1 % by 2024 and will exceed the 10 billion euro mark for the first time [13]. However, there is a significant gap compared to the total loss of 266.6 billion euro forecast for Germany in 2024.

In this context, Zero Trust could provide a robust strategy to mitigate the risks associated with digitalized and connected production, enabling companies to improve their cyber resilience and protect themselves from future threats. Adopting a Zero Trust architecture in digitalized production environments presents numerous opportunities to enhance security. By following Zero Trust principles, organizations can strengthen their security posture through targeted measures that establish explicit trust for identities, devices, networks, applications, and data. This strategy considerably lowers the risk of unauthorized access and malicious activities. Furthermore, by minimizing the attack surface through restricted resource access, Zero Trust effectively reduces potential entry points for attackers. This enables companies to meet the obligations to implement security mechanisms as prescribed by NIS2 and prepare their business for the future in the context of upcoming regulations and cyber threats.

However, the integration of a Zero Trust architecture introduces unique challenges, particularly in digitalized production environments. For instance, having a comprehensive data inventory and a clear understanding of necessary data communication is crucial for organizations. Without a well-defined awareness of permissible network interactions, access requirements, and the locations of sensitive data within the

infrastructure, the risk of integration failures rises significantly. Moreover, when planning and designing a Zero Trust architecture, it's essential to consider OT-specific requirements, including the need for high availability, low latency, and the integration of legacy systems. An inadequately designed integration that fails to align with business processes can undermine the effectiveness of a Zero Trust implementation. Furthermore, the lack of standardization, particularly in OT, along with elevated costs, presents considerable obstacles to the successful deployment of Zero Trust within production environments.

Despite the various challenges associated with the implementation of Zero Trust, organizations could position themselves for the future through a strategically planned approach, thereby adapting to the evolving threat landscape. Considering that "the path to Zero Trust is an incremental process that may take years to implement" [14], it would be advisable for companies to proactively address the concept of Zero Trust at this stage and explore the potential for incorporating initial measures, driven by regulatory obligations, into their cybersecurity planning process.

References

- [5] R. Wintergerst. "Wirtschaftsschutz 2024." Accessed: Nov. 6, 2024. [Online]. Available: <https://www.bitkom.org/sites/main/files/2024-08/240828-bitkom-charts-wirtschaftsschutz-cybercrime.pdf>
- [6] Bitkom. "Angriffe auf die deutsche Wirtschaft nehmen zu." Accessed: Sep. 3, 2024. [Online]. Available: <https://www.bitkom.org/Presse/Presseinformation/Wirtschaftsschutz-2024>
- [7] A. Fleck. "Cybercrime Expected To Skyrocket in Coming Years." Accessed: Sep. 10, 2024. [Online]. Available: <https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/>
- [8] Allianz. "Allianz Risk Barometer 2024 - Rank 1: Cyber incidents." Accessed: Sep. 7, 2024. [Online]. Available: <https://commercial.allianz.com/news-and-insights/expert-risk-articles/allianz-risk-barometer-2024-cyber-incidents.html>
- [9] K. Stouffer, M. Pease, C. Tang, T. Zimmerman, V. Pillitteri, and S. Lightman, "Guide to Operational Technology (OT) Security: Initial Public Draft. NIST Special Publication. NIST SP 800-82r3 ipd," 2022, doi: 10.6028/NIST.SP.800-82r3.ipd.
- [10] Bundesamt für Sicherheit in der Informationstechnik. "Positionspapier Zero Trust 2023." Accessed: Oct. 10, 2024. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeLeitlinien/Zero-Trust/Zero-Trust_04072023.pdf?__blob=publicationFile&v=4
- [11] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture: NIST Special Publication 800-207," 2020, doi: 10.6028/NIST.SP.800-207.
- [12] Bundesamt für Sicherheit in der Informationstechnik, *IT-Grundschutz-Kompendium*. Köln: Reguvis, 2023.
- [13] Bitkom. "Cybersicherheit: Deutscher Markt erstmals über 10-Milliarden-Marke." Accessed: Sep. 5, 2024. [Online]. Available: <https://www.bitkom.org/Presse/Presseinformation/Cybersicherheit-Deutscher-Markt-ueber-10-Milliarden-Marke>
- [14] Cybersecurity and Infrastructure Security Agency. Cybersecurity Division. "Zero Trust Maturity Model." Accessed: Nov. 6, 2024. [Online]. Available: https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf