PROFINET Security Guideline

Guideline for PROFINET

Version 2.0 – Date November 2013

Order No.: 7.002

File name : PN-Security_7002_V20_Nov13

Prepared by the PI Project Group 10 “PN Security” in the Committee CB “PROFINET”.

In this specification the following key words (in **bold** text) will be used:

may: indicates flexibility of choice with no implied preference.

should: indicates flexibility of choice with a strongly preferred implementation.

shall: indicates a mandatory requirement. Designers shall implement such mandatory requirements to ensure interoperability and to claim conformance with this specification.

Publisher:
PROFIBUS Nutzerorganisation e.V.
Haid-und-Neu-Str. 7
76131 Karlsruhe
Germany
Phone: +49 721 / 96 58 590
Fax: +49 721 / 96 58 589
E-mail: info@profibus.com
Web site: www.profibus.com

Content

List of figures

List of tables

Revision Log

Version	Originator	Date	Change Note / History / Reason
1.1	S. Hein	05-03-2012	Initial version
1.2	S. Hein	20-05-2012	Review
1.2a	S. Hein	07-07-2012	Added intro from V. Goller
1.2b	S. Hein	31-07-2012	Several content added, review comments added
1.3	S. Hein	01-09-2012	Review comments added
1.3a	S. Hein	10-10-2012	Added some major content
1.3b	S. Hein	03-11-2012	Added measures chapter
1.4	S. Hein	13-12-2012	Changes during WG meeting
1.4a	S. Hein	13-01-2013	Changed structure, measures and methodology splitted
1.4b	S. Hein	18-01-2013	Added some missing content
1.4c	S. Hein	19-01-2013	Added some missing content
1.5	S. Hein	11-02-2013	Started to prepare final version, added input “intro technical measures” from F. Klasen
1.6	S. Hein	26-02-2013	Review meeting, comments added
1.7	S. Hein	5/13/2013	Added Input from F. Köbinger for Defense-In-Depth Added some comments Added some missing text
1.8	S. Hein	5/29/2013	Added some comments Added new chapter “Access controls/access points”
1.9	S. Hein	6/25/2013	Prepared Review-Version
1.91	F. Köbinger	7/3/2013	Small changes page16
1.92	F. Köbinger	10/31/2013	PI Review comments incorporated

1 Management Summary - Scope of this document

Ethernet-based communication is taking on an increasingly central role in the automation field. For example, Industrial Ethernet is increasingly be used at the field level, e.g., PROFINET. In addition to enabling use of open, standardized IT technologies, such as wireless LAN and web servers, the chief advantage of Ethernet-based communication is to allow integrated networking. However, because this comes with an increased risk of access violations and attacks by viruses and other malicious programs, there is a need to assess the potential risks for automation networks and to implement appropriate Security concepts.

For this reason, PROFIBUS/PROFINET International (PI) has developed a security concept for automation systems, which incorporates its member companies' experience and detailed knowledge of the automation environment – to the benefit of users. Simply protecting plant networks and automation components is not enough. It is also essential that the security mechanisms and concepts used do not disturb production operation and are practical and affordable.

With its Security Guideline, PI is presenting a concept for the first time that takes into account the threats and special requirements of the automation world. This concept aims to protect automation components, irrespective of the communication protocols used or the network structure. Through the use of proven and open security mechanisms, the integration into existing security concepts is also possible. This guideline is intended for users and operators of industrial networks, particularly those using Ethernet-based PROFINET. It points out the key aspects for the establishment of a security concept in this environment and provides appropriate recommendations.

1.1 Demarcation

Safety vs. security

We will start with a brief explanation of the terms “security” and “safety”. While safety is understood to mean functional safety, i.e., protection from danger to life and the environment arising from machines and the like, security is understood to mean protection from unauthorized access to information and automation devices. The terms “IT security” and “cyber security” are often used synonymously with “security”. However, these synonyms are used sparingly in this guideline in order to separate the industrial automation area from the IT area. This guideline addresses the assurance of industrial security based on national and international security standards.

1.2 Target audience

- System designers
- Commissioning engineers

2 List of affected patents

No affected patents are known at this time. Up to now, a patent search has not been performed by any of the Working Group members.

PROFIBUS&PROFINET International does not guarantee the completeness of this list.

3 Related documents and references

3.1 References

[1] M. Popp, Industrielle Kommunikation mit PROFINET [Industrial Communication with PROFINET], Karlsruhe: PROFIBUS Nutzerorganisation e.V. PNO

[2] F. Klasen, “Security für Ethernet Systeme” [Security for Ethernet Systems], in Industrielle Kommunikation mit Feldbus und Ethernet [Industrial Communication with Fieldbus and Ethernet], Berlin, VDE Verlag, 2010, pp. 271-279.

[3] Siemens AG, „Operational Guidelines für Industrial Security,“ [Online]. Available: http://www.industry.siemens.com/topics/global/en/industrial-security/Documents/operational_guidelines_industrial_security_en.pdf. [access on June 16, 2012].

[4] 1) VDI/VDE, *Informationssicherheit in der industriellen Automatisierung - Allgemeines Vorgehensmodell* [Information Security in Industrial Automation - General Procedure Model]*,* Berlin: Beuth Verlag, 2011.

[5] PROFIBUS Nutzerorganisation e.V., *PN-Security_7002_V10_05Mar29.pdf,* 2005.

3.2 Related Documents

Bundesamt für Sicherheit in der Informationstechnik (BSI) [German Federal Office for Information Security], *IT-Grundschutz-Profil für das produzierende Gewerbe - Anwendungsbeispiel für IT-Grundschutz im.* [Basic IT Security Profile for Industry - Application Example for Basic IT Security], Bonn, 2008.

Bundesamt für Sicherheit in der Informationstechnik (BSI) [German Federal Office for Information Security], “Notfallmanagement_Standard_1004.pdf” *BSI-Standard 100-4 - Notfallmanagement* [Emergency Management] *V1.0,* Bonn: BSI, 2008.

Bundesamt für Sicherheit in der Informationstechnik (BSI) [German Federal Office for Information Security], *BSI-Standard 100-4 - Notfallmanagement* [Emergency Management] *V1.0,* Bonn, 2008.

Klasen, Frithjof, “Security für Ethernet Systeme” [Security for Ethernet Systems], in *Industrielle Kommunikation mit Feldbus und Ethernet* [Industrial Communication with Fieldbus and Ethernet], by Frithjof Klasen, Volker Oestreich, and Michael Volz, 271-279, Berlin: VDE Verlag, 2010.

NAMUR, “IT-Sicherheit für Systeme der Automatisierungstechnik” [IT Security for Systems of Automation Technology], *NAMUR Arbeitsblatt* [NAMUR Worksheet] *NA115,* June 19, 2006

Popp, Manfred, *Industrielle Kommunikation mit PROFINET* [Industrial Communication with PROFINET], Karlsruhe: PROFIBUS Nutzerorganisation e.V., 2007.

PROFIBUS Nutzerorganisation e.V. “PN-Security_7002_V10_05Mar29.pdf”, *PROFINET Security Guideline V1.0,* March 29, 2005,

Siemens AG, “Operational Guidelines for Industrial Security” *Siemens Industry SectorIndustrial Security,* undated,http://www.industry.siemens.com/topics/global/en/industrial-security/Documents/operational_guidelines_industrial_security_en.pdf (access on June 16, 2012).

VDI/VDE, “Informationssicherheit in der industriellen Automatisierung - Allgemeines Vorgehensmodell” [Information Security in Industrial Automation - General Procedure Model] *Richtlinie* [Guideline]*VDI/VDE 2182 Blatt* [Sheet] *1,* Berlin: Beuth Verlag, 2011.

IEC 62443/ISA-99 Part1-4

VDI/VDE examples for 2182, sheets 2-3

4 Definitions and abbreviations

4.1 Definitions

Table 1 - Definitions

Term	Definition
Authenticity	[4]There are two basic forms of authenticity: user authenticity and data authenticity **User authenticity** means that a user is really who he says he is. Authentication refers to the corresponding verification. **Data authenticity** means that data really came from the indicated sender or generator and was not altered along the transmission path or while saving it. Data integrity is a sub-aspect of data authenticity.
AR - Application Relation	Defines a relation between a PROFINET sender and a PROFINET receiver, also referred to as a provider and consumer.
BIOS - Basic Input Output System	Represents the firmware of an x86 PC It is used to start the actual operating system.
Blacklisting	A list containing elements that are denied access or that are otherwise treated differently than elements not on the list.
Broadcast	A message that is transmitted to all nodes within a network.
CycleCounter	Internal time stamp of a PROFINET device for user data exchange.
Defense-In-Depth	Sequence of multiple network levels and security measures intended used to achieve more in-depth security.

DMZ - Demilitarized zone	A defined separate area that is accessible only via controlled access points.
DoS - Denial-Of-Service	Attack whose objective is to crash a service.
DynDNS - Dynamic Domain Name System	Dynamic IP addresses mapped onto a fixed domain name
Ethernet	Layer 2-based protocol for transmission of data within a LAN.
Firewall	Hardware or software system for limiting network accesses.
Firmware	Software that is embedded in a piece of hardware. The firmware describes the functionality of the hardware.
FrameID	PROFINET mechanism for identifying the communication link.
Device name	The device name identifies a PROFINET device uniquely within a network.
Integrity	[4]Integrity is the property whereby a user (user = persons and/or applications →see VDI 2182, definition of user) is prevented from generating, altering, replacing, or deleting data unnoticed.
IDS - Intrusion Detection System	System that detects intrusions. Unlike an IPS, the IDS does not prevent intrusions.
IO controller	Initiator of the user data exchange
IO device	[1]PROFINET device in the direct vicinity of the process that is used to connect the IO controller to the process.
IP - Internet Protocol	[1]The protocol that enables the transfer of data e.g in an Ethernet network from end point to end point.
Intrusion Prevention System - IPS	System that can detect and prevent attacks and attack sequences
IPsec - Internet Protocol Security	Protocol for secure communication in an insecure network.
LAN - Local Area Network	Local network
Layer 2 communication	
Layer 3 communication	
LLDP - Link Layer Discovery	Protocol for exchange of neighborhood information. The protocol is used, for example to acquire the topology in a PROFINET network.
Logging	Logging of important events.
MAC - Media Access Control	Controls the shared use of a transmission medium.

MAC address	[1]Also referred to as Ethernet address; used to identify an Ethernet node. The Ethernet address has a length of 6 bytes and is assigned by IEEE.
Multicast	A message that is transmitted to a defined set of nodes within a Layer 2-based network.
NAT - Network Address Translation	Process for automatic exchange of IP addresses in an IP packet. This process is used to tie private address areas to public address areas or to conceal internal IP addresses from being seen outside.
Non-repudiation	[4]Non-repudiation is the property whereby the object under consideration is able to verify the originator of an action (with proof) after the fact.
Packet filter	Filters data traffic in a network.
Patch	Software update, including software corrections.
Port	TCP or UDP ports act as an address supplement. Services can use this to establish their connection.
PROFINET domain	Ethernet-based multicast and broadcast area within a network.
Real-time communication	[1]Real-time capability of a system to solve a task in a certain amount of time.
Robustness	Robustness describes the capability of a device to ensure normal operation, even under unfavorable conditions and/or in case of unexpected input.
Router	Network device for forwarding IP network packets between two independent subnets.
Safety	Refers to the operational safety of a device or a group of devices. Here, operational safety means that human beings are not permitted to be endangered during operation.
Security-related requirements	Security-related requirements describe the elements that must be made secure.
Security level	
Security Assessment	
SNMP - Simple Network Protocol	[1]Standard Internet protocol for management and diagnostics of network components.
PLC - Programmable Logic Controller	Device that can be used for open-loop and closed-loop control of an I/O system.
SSL - Secure Socket Layer	Network protocol for secure transmission of data.
Stateful Inspection	State-oriented packet inspection for packets within a network. It represents an expanded form of the packet filter.
Subnet	A subnet in the network.

Supervisor	[1]Initiator of control, commissioning, and configuring tasks. For example,an engineering station or PC/PG that can read or write data of an IO device. A supervisor is connected only temporarily and does not assume an active role in an IO system.
Switch	Controls the Layer 2-based communication in networks.
TCP - Transport and Control Protocol	[1]Higher-level protocol of IP that ensures data exchange and flow control.
TLS - Transport Layer Security	Network protocol for secure transmission of data.
Availability	[4]The probability that the status of an object under consideration enables it to satisfy a required function under specified conditions at a specified time or during a specified time period.
Confidentiality	[4]Confidentiality is the property whereby data or the information contained therein can be accessed only by authorized users.
VLAN - Virtual Local Area Network	Logical subnet that is created by a switch for a specific port.
VPN - Virtual Private Network	Logical, typically secured connection between two separate networks.
Whitelisting	List containing elements that are considered trustworthy.
WLAN - Wireless Local Area Network	Wireless LAN

4.2 Abbreviations

AR	Application Relation
BIOS	Basic Input Output System
DCP	Discovery and basic Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name Service
DoS	Denial of Service
DynDNS	Dynamic Domain Name System
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPS	Intrusion Prevention System

IPsec	Internet Protocol Security
IO	Input / Output
LAN	Local Network Area
LLDP	Link Layer Discovery Protocol
MAC	Media Access Control
NAT	Network Address Translation
PLC	Programmable Logic Controller
SNMP	Simple Network Management Protocol
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
USB	Universal Serial Bus
VDI	Verein Deutscher Ingenieure
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WLAN	Wireless Local Area Network

5 Foreword

Ethernet-based communication is assuming a central role in the automation environment. The advantages of Ethernet-based communication are obvious: besides enabling the use of open, standardized IT technologies, such as wireless LANs and web servers, it also allows the implementation of integrated networks. However, because this comes with an increased risk of access violations, there is a need to assess the potential risks for automation networks and to implement appropriate Security concepts.
The public frequently associates security in information systems with terms such as “hackers”, “attacks”, and “cyberterrorism” But it is not just terrorist activities involving hacker attacks that can disturb process operations. Rather, a disturbance can be caused by a service technician who accidentally establishes a connection to a control network. Then, by simply starting a few applications, this service technician may load the network to such an extent that some automation devices fail, thereby triggering a complete interruption of operation.

In the context of automation systems, therefore, a security problem can be regarded as any operational disturbance caused by intended use and subsequent failure of the automation system.

Security is not a matter that can be pinned down to just one place. Everyone involved in an automation installation must be incorporated in the security concept. This may include the IT department, PLC experts, company/site security team, management, and even security guards, as well as the manufacturers of automation components.

There are many aspects to be considered when it comes to security. One of these is *robustness*, or the ability of a device to withstand an expected volume of data traffic. Another aspect is *access control,* which can be used to specify who is permitted to access a system. Also relevant is the question of whether certain individual such as service technicians are to be allowed to connect to the network.
These are just a few of the aspects that must be considered. The approach taken by a user in considering these aspects is the basis for a *security architecture*. A generally-applicable solution to the problem of defining a security architecture does not exist. Rather, the solution is dependent on many factors, including the requirements for the application, the company philosophy, and other user requirements, as well as the results of a risk analysis.
Nevertheless, there are a few rules that facilitate the definition of a *security architecture*. These rules specify a basic framework that serves as a guide.

A good *security architecture* should be…

- …as simple as possible but not simpler (Albert Einstein). A good security system must be understood by all parties involved so that it can be put into practice by the team. It should not just be in the hands of a few security experts.
- …as uniform as possible. If a rule is applicable in one case, it must also be followed in comparable cases. Broad exceptions from the general rules make it difficult to recognize violations and deficiencies.
- …understood and supported by all parties involved. If a team knows the whys and hows of security and understands its relevance, the team is very likely to work effectively.
- …called into question by all team members. Security should offer protection from the unknown. When your team discovers a weak point or deficiency, correct the problem before damage occurs and, if necessary, expand your Security architecture.
- …a daily activity and not a one-time-only task.

6 Introduction

In recent years, automation systems used in process and production plants have evolved from individual isolated computers with proprietary operating systems and networks into high-grade networked systems and applications that rely on popular, well-known technology of “open systems”, such as Microsoft® Windows™, and network protocols such as TCP/IP.
The automation systems of today are also now integrated into enterprise systems and other site-wide business applications as well as into company-wide communication networks. This type of integrated architecture offers significant economic advantages. The visibility of activities at the

plant level (ongoing work, status of systems and devices, production schedules) is increased, thereby enabling the design of better end-to-end information systems and facilitating decision making. The information exchange between production systems and other enterprise systems is more direct, which allows the company to react more quickly. Uniform interfaces reduce the total costs for diagnostics and support, in particular, since remote support of production processes is now possible. Easier access to data allows analyses to be performed that can lead to lower production costs and higher productivity. In addition, the function for remote monitoring of control systems provides for faster troubleshooting and reduced support costs.
Ever since specialized malicious software first appeared, the question has been how to integrate security elements into new network environments and in automation systems. Which measures must be taken?
Security concepts developed for office environments cannot simply be transferred to automation networks. Security measures implemented for automation systems and networks must not conflict with PROFINET-related requirements. The goal of security measures in the automation area is a reliable automation network that meets requirements. Another point to be aware of is that automation systems are designed for maximum performance and not for maximum security. For example, many systems do not employ proper authentication measures to protect access.
The objective now is to fulfill the central security objectives of the automation world.
A secure system shall ensure the confidentiality, integrity, and availability of systems and data, even in the face of malicious attacks.

To achieve the maximum reasonable level of security for automation systems and networks, a suitable security management process is essential. As part of a consistent security management process, consideration must be given to the following:

» Risk analysis, including identification of counter measures for reducing the risk to a reasonable level.

» Coordinated organizational/technical measures (systems engineering)

» Periodic/event-triggered repetition

7 Challenges posed by the networked automation world

The increasing use of information technology and network technology in automation might suggest that existing IT solutions would also suitable for networked production plants and automation systems and could simply be transferred to the production environment. In fact, however, the requirements and applicable solutions differ significantly between the business IT and automation worlds. The main differences are described in more detail in the following.

7.1 Different performance and functional requirements

In typical IT systems, the emphasis is on data throughput and reliable data transmission. Delays and jitter in the data transmission are tolerable.
By contrast, the delay time and jitter are among the characteristics that define an automation system's real-time performance capability Reactions are time-critical and delays represent a serious problem.
Consideration must also be given to the fact that automation systems rely on a wide variety of automation components and solutions, some of which entail devices with limited resources. These frequently do not have the same security features found in typical business IT computer systems.

7.2 Human-machine interaction

Reliable control and operation of technical processes must be possible in all situations. Automation systems and functions must remain available even in critical situations. For this reason, security measures must not interfere with the operability of the automation solution.

7.3 Security objectives

A central objective in the business IT area is the protection of data from loss or modification. The suitable security measures in this case often involve the server systems (access control, backup,

etc.). By contrast, production lines are dominated by granular structures and applications that are subdivided into many sub-components.
A comparison of the priority setting of objectives in business IT and automation systems reveals a different ranking.
In business IT systems, security objectives are typically ranked in terms of priority as follows :

(1) Confidentiality
(2) Integrity
(3) Availability

In many automation systems, the ranking of security objectives in terms of priority is completely opposite:

(1) Availability
(2) Integrity
(3) Confidentiality

The availability of an automation system has top priority here. This objective is an important aspect, above all, for the protection of humans and the environment

7.4 Availability and reliability

Many production processes run continuously. Sudden failures of systems that control the production processes are not acceptable. Extensive testing is required prior to commissioning to ensure the high availability of production and control systems. In addition to the problems posed by sudden failures, it is not possible to simply switch off and restart many control systems without adversely affecting production. The need for high availability, reliability, and maintainability makes IT measures such as system restarts less applicable. Beta tests during operation are possible for many IT systems, whereas automation systems must pass a quality assurance test. Consequently, security updates cannot always be implemented promptly because software changes require detailed testing beforehand. The necessary test environments for this are often lacking because complete systems and production systems for test purposes are generally not economically feasible.

7.5 Different focus of security architecture

Availability and reliability are critical factors for automation systems. To accomplish the automation task, several automation devices generally act as a group. This means that uninterrupted, error-free, and simultaneous operation of all devices is also an important criterion. If one of these devices fails, the result can be an immediate production or system failure.
Like in the IT field, automation systems also use redundancy mechanisms. However, for cost reasons, these are mainly used where a device failure would cause serious damage to the plant or the product.
The security concept must therefore always regard the automation system as a whole, since it must function reliably and continuous as a unit.

7.6 Risks and safety requirements

The requirements for functional safety of production plants and the associated risks differ significantly from the risks that are normally considered by the business IT world. Risk assessments are not transferable and generally yield different results that, in turn, lead to more stringent security measures.

7.7 Firmware update/patch management

The availability of components and automation systems is of prime importance. This is because faulty components generally trigger an interruption of operation and thus a production shutdown. In particular, the installation of firmware updates and patches requires at least a restart of the affected components. When a component with an updated/modified system restarts, it cannot be ensured that the component will exhibit the same behavior as before the the update or modification. In addition, changes may have to be made to individual modules in process automation systems before updates or patches can be installed. And, individual

modules/components may be changed independently of each other. Depending on the system architecture, interdependent hardware elements must be replaced at the same time.
Thus, the conditions under which firmware updates can be performed in the automation world are complicated at best and require special planning.

8 PROFINET-specific requirements

8.1 PROFINET architecture

The PROFINET protocol suite includes different methods of addressing: MAC-based addressing for Layer 2 communication and IP-based communication for Layer 3. Automation systems with this type of architecture tend to be less proprietary. When TCP/IP is used, PROFINET can be integrated completely without additional measures required for IP-based applications and networks. It is even possible to integrate systems, for example, that transfer quality data to a top-level server system. It is precisely this function for integrating real-time and non-real-time applications that is one of the central advantages of PROFINET technology. These different communication relations must be taken into consideration in the security concepts.
In PROFINET, the protocol is distributed as follows:

(1) PROFINET IO real-time communication (process data, Layer 2-based), e.g., RT/IRT

(2) PROFINET services (Layer 2-based), e.g., DCP for requesting or specifying device names

(3) PROFINET services (Layer 3-based), e.g., read/write services used, for example, for reading and writing of data objects during device parameter assignment

(4) Network management and application-related services (Layer 7-based), e.g., SNMP

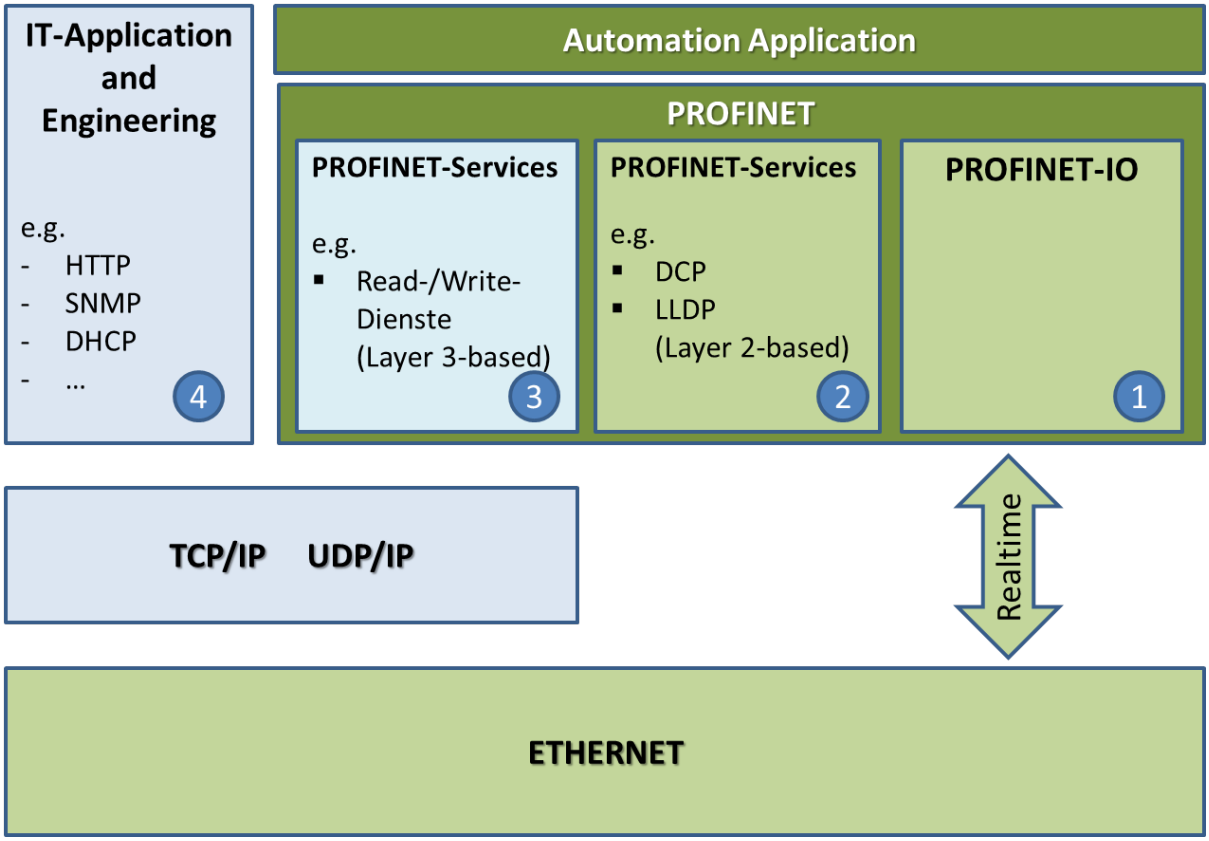

Figure 1 - PROFINET protocols

8.1.1 Switch-based networks

By using dedicated switches that are integrated into IO devices, PROFINET enables an integrated switch-based network infrastructure with star, ring, tree, and line topologies. PROFINET IO devices thus have both the properties and functions of a network infrastructure component and the automation-related functions of a field device or sensor/actuator. Conversely, dedicated switches have properties of IO devices and thus support automation-related diagnostic functions of the IO controller.
A PROFINET network is therefore not a pure 'network service' but an integrated communication system within an automation cell or system.

Consequences:

- *IO controllers assume the functions of network management systems*
- *External network management systems can access PROFINET devices (e.g., SNMP)*

This yields a combination of real-time communication and other services

- Services can be used within a PROFINET domain, i.e., by PROFINET nodes (integrated) and by engineering systems, and also by higher-level systems (e.g., network management systems).

8.1.2 PROFINET domain

Due to the integration capability of PROFINET, the network structure and the size of the subnets used can differ significantly. Based on the PROFINET IO real-time communication and the Layer 2-based PROFINET services (DCP, LLDP), the following domains must be differentiated:

- Controller domain: Logical grouping of an IO controller with its associated IO devices
- Broadcast domain: Network area in which the IO controller and IO devices can be accessed via Layer 2-based IO communication and services
- PROFINET domain: Arrangement of multiple controllers that are operated independently of one other or as a logically-linked group in a subnet of a broadcast domain.

The dimensioning and segmentation of PROFINET domains is a central planning task, whose result will be critical in determining the magnitude of the multicast and broadcast loads occurring during operation. At the same time, PROFINET nodes must also be able to operate reliably with these corresponding communication loads. This is one of the main reasons why network load tests are performed and the robustness of devices is validated during certification testing of PROFINET devices Details about the requirements for robustness, about the concept, and about the function of the network load test are presented in Section 7.3.4.

8.1.3 Functions for ensuring ease of use

The engineering concept behind PROFINET is based on a function-oriented and open architecture approach and includes the following architecture features:

- Addressing using device names to ensure assignment of unique addresses for PROFINET devices that are independent from MAC addresses and IP addresses (important for problem-free device replacement and other reasons)
- Use of files (GSDML files) to describe the device-specific functions and parameters
- Diagnostics concept (device diagnostics, network diagnostics, etc.)
- Cyclic Layer 2 communication for real-time user data
- Acyclic Layer 2 and Layer 3 communication for configuring PROFINET nodes

The engineering concept uses open communication standards, such as LLDP and SNMP, in addition to the PROFINET-specific protocols.

To simplify the configuring of PROFINET nodes during commissioning and service (e.g., device replacement) as much as possible, the architecture concept of PROFINET provides for the assigning and modifying of configuration parameters of IO devices (e.g., Device Name) by the IO controller and supervisor stations.

8.2 PROFINET protocol properties

PROFINET devices are orientated to reliability and real-time communication. In addition, usability aspects play an important role in the technology design. An example of this is the use of the DCP protocol to assign device names. The implementation of security functions must therefore be reconciled with the usability aspects for day-to-day work with the technology.
PROFINET already includes security increasing measures.. These include the FrameID, which is used for detecting and identifying communication relations. The CycleCounter also represents a security function to a certain extent because it is used to monitor the IO data exchange.

The purpose of the PROFINET-specific security properties is to improve the availability and operational reliability of production plants. An important feature is the robustness of PROFINET devices against high network loads. Network load tests, i.e., Security Level 1 tests, are therefore an important component of certification testing (see Section 7.3.4).
In addition, PROFINET devices have no inherent (intrinsic) security functions in the sense of endpoint security. Targeted attacks on PROFINET devices must therefore by prevented by the operating concept and additional protective measures.

8.3 Requirements for secure operation of PROFINET

Below is a list of points and basic conditions that must be observed particularly when establishing a security concept in the PROFINET environment. It is not enough simply to implement suitable measures for countering threats. The implemented measures are also not permitted to weaken or otherwise impair the vital functions of PROFINET, which would be counterproductive and make little sense. A knowledge of the essential requirements for PROFINET operation is therefore useful for selecting the appropriate security mechanisms and creating an optimal security concept.

8.3.1 Security for systems without their own security functions

There are several reasons why some automation systems currently do not have their own autonomous security functions. As previously explained, some automation systems do not have the technical resources necessary for security functions. Security functions have also not been integrated in some existing systems for economic reasons. In many cases, these requirements preclude the installation or timely update of security measures. Nevertheless, the PROFINET security concept should provide adequate security in all of these cases.

8.3.2 Real-time operation

The PROFINET security concept must not interfere with the ability to meet real-time requirements. In addition, the security functions must not slow down the often critical reaction time associated with the interaction between human and machine. An example of this would be the activation of an Emergency Stop switch using a key or even a password. Such series-connected security mechanisms would conflict glaringly with functionality.

8.3.3 Transparent and cost-efficient integration

The PROFINET security concept should support the transparent and cost-efficient integration of security into an industrial environment. The integration of security functions without significant configuration effort will increase the acceptance of the solution. It must be also be remembered here that automation experts are generally not security experts. Cost effectiveness can be achieved, above all, by integrating security measures that also offer security for larger groups of automation solutions. Only this approach will enable the realization of an accepted security concept for PROFINET.

8.3.4 Robustness

Robustness refers to the capability of devices to withstand temporary exceptionally-high communication loads Robustness thus describes the ability of a device to ensure normal operation, even under unfavorable conditions and/or in case of unexpected input.
To test this type of robustness, the certification testing for PROFINET devices has been expanded to include the so-called Security Level 1 test. This test simulates real-world communication loads and exposes the PROFINET devices to such a load. From the device perspective, the goal during this testing is to maintain the PROFINET services. Or, in exceptionally-high load situations, the communication must be stopped and afterwards resumed automatically.

9 Establishment of a security management process

The approach for securing automation networks will be described in detail in the following sections. This description is geared to Guideline 2182 published by VDI. This guideline describes a process-oriented procedure model whose purpose is to support the determining and validating of possible security solutions through a cyclic application Figure 2 shows an example of a procedure module based on the VDI 2182 Guideline.

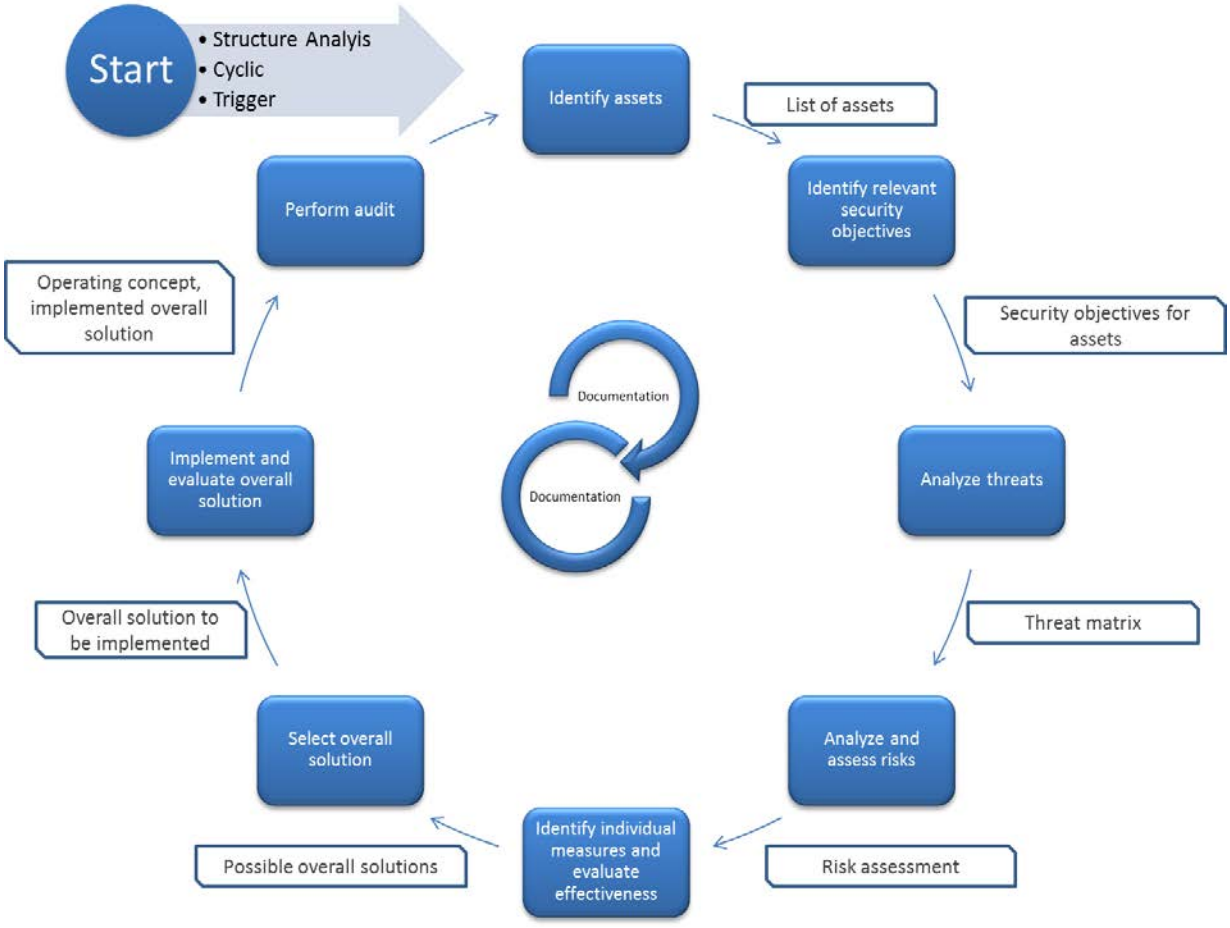

Figure 2 - Procedure model according to VDI2182

In principle, the procedure model describes individual steps that are to be performed cyclically or when triggered. Each individual step requires input information and generates a result, which in turn represents the input information for the next step.
The basic steps of this procedure model are the identification of assets and related security goals and an assessment of the risks associated with the identified threats. The magnitude of a risk must ultimately be defined and evaluated individually for each use case.

These steps are subdivided into the following sections:

» Initiation of the process

» Gathering of the requirements:

» Definition of measures

» Implementation of the defined measures

» Preservation and, if necessary, improvement of existing mechanisms

9.1 Initiation of the process

Before the planning and implementation of security mechanisms can commence, the organizational framework must first be defined. The making of financial, personnel, and time resources available is included in this step. Furthermore, the procedure must be stated precisely, resulting in written guidance materials for the actual process.
The need for a security concept is based not only on the needs of the company but also on legal requirements. Examples of legal requirements include statutory requirements, contractual obligations, and even insurance-related requirements. These not only call for the development of a security concept but they also directly affect the definition of the security measures. A basic step in the defining of security measures is thus the screening of existing guidelines, regulations, and standards in order to identify requirements requiring further clarification.
Since security must be practiced as a process and integrated into the company structure, the roles and responsibilities for this must also be defined and awarded. For example, VDI Guideline 2182 describes the following roles and related responsibilities and activities:

- Security experts
  Security expects are knowledgeable about the capabilities and applications of a wide range of security solutions

- System experts
  System experts are knowledgeable about the communication technology used, e.g., PROFINET.

- Application experts
  Application experts are knowledgeable about the system from the user's perspective. For example, they know which accesses are required and which communication links must be established for operation.

- Coordinators
  Coordinators are responsible for coordinating activities and for information flow

Depending on the company structure and size, these roles may have different names or may already be defined and awarded.

Viewed as a whole, the initiation steps will result in the following:

» Awareness raising of management

  - Presentation of general security risks and associated costs and damages
  - Identification of legal, insurance, and certification requirements
  - Benefits
  - Procedure/problem-solving approach

» Establishment of general organizational framework

- Clarification of available finances
- Clarification of available resources (personnel and time)
- Identification of roles
- Awarding of roles
- Definition of responsibilities
- Definition of guidance materials
- Exact definition and demarcation of the object under consideration

Result

- Approval and understanding of management is obtained
- Roles and responsibilities are clarified
- General financial framework is established
- The guidance materials for the remaining work are created

9.2 Structure analysis

To enable gathering of requirements that are as specific as possible, a structure analysis should be performed first. This analysis should determine at least the following:

» Required applications and services

» Utilized IT systems

» Necessary communication links

» Infrastructure conditions

» Existing data flow

» Available interfaces

» Necessary accesses

This actual analysis forms the basis for an exact definition of requirements that the subsequent security concept must meet.

Result

- Overview of all applications in the automation network
- Overview of all IT systems used, e.g., operating systems on panel PCs
- All communication links within the network and all communication links to other networks, e.g., for sending data to a quality data server
- Necessary interfaces, e.g., for service technicians
- Overview of all services including ports used for this purpose
- Overview of all interfaces, for example, to higher-level systems

9.3 Gathering of requirements

Once an "inventory" has been taken, the actual gathering of specific functional requirements can commence. An example of a functional requirement would be the requirement for remote access by service technicians. The aim here is to answer the question, “What must be protected?"
The gathering of requirements also includes the relevant security objectives. Security objectives define what the security concept must achieve and can be understood as higher-level requirements.

Result
The result of this step is an overview of all elements requiring security, including the security objectives. In addition, the general legal conditions are also listed here.

9.4 Evaluation of requirements

Once all of the requirements have been gathered and all elements requiring security have been identified, an evaluation must be performed in order to ensure that the subsequent security concept is cost-effective. In order to successfully perform this evaluation, the possible threats to fulfillment of the requirements must be identified. Therefore, the aim of this step is to identify the relevant threats related to the previously defined requirements.
One possible method for evaluating requirements is described in the VDI 2182 Guideline and can be used as a procedure model. The "IT-Grundschutz-Profil für das produzierende Gewerbe" [Basic IT Security Profile for Industry] published by BSI also describes an evaluation method. A corresponding description is available internationally in IEC 62443-2-1 and ISA99 2-1.

Result
Comparison of requirements and threats

9.5 Risk analysis and evaluation

A risk analysis is used to evaluate the previously documented requirements and potential threats. The risks are qualitatively classified in this analysis. The acceptance of the risks must also be evaluated. Not every risk represents a real risk for the respective use case.
A risk can be assessed by multiplying the probability of its occurrence by the magnitude of the resulting damage.

Result

The result of the risk assessment is the identification of intolerable risks for which security measures must be taken.

9.6 Definition of measures

Once all the necessary factors have been examined and evaluated, the definition of measures can begin.
A basic distinction can be made between the following:

» Organizational measures

» Technical measures

The two types of measures must be tuned to one another since a combination is necessary to produce meaningful and effective security. In most cases, technical measures must also be accompanied by organizational measures, since the implementation of measures, such as complex passwords, is of no benefit if it is not accompanied by measures to control and monitor access to these passwords. On the other hand, some security objectives can be achieved in different ways; in some cases it is possible to choose between an organizational measure and a technical measure. For example, if switches are located in locked control cabinets, the switch ports do not necessarily have to be secured using port security mechanisms to prevent unauthorized access. Obviously, a combination of measures would be the most effective.
For many measures that involve prohibitions, the implementation of alternative measures is also generally recommended. This is because measures involving prohibitions can incite employees to bypass the security mechanisms. The goal should be to create a concept that ideally does not constrain employees and can be implemented without noticeable effects.

9.6.1 Organizational measures

Once a successful risk analysis has been completed, the defined security measures must now be implemented The first step should aim to establish the practice of security in the company. This will form the basis for successful security measures. Only when security is practiced as a

continuous process will it be possible to achieve and maintain long-term security. However, this also brings up questions, such as:

- Where is training needed?
- How can employee awareness be raised?
- Who are the contact persons for particular topic areas?
- Does the security concept to be created have a clear scope? (clarify the handover point/interface to the higher-level IT infrastructure)

Furthermore, a clear set of guidelines forms the basis for a sound security management process. Examples for this include:

- Definition of the roles that will subsequently bear the responsible for security matters
- Definition of guidelines for ensuring a uniform procedure
- Definition of sanctions in the event of non-compliance with guidelines
- Communication and documentation of security-relevant incidents (logging and change management)
- Creation of policies
- Guidelines for handling passwords
- Guidelines for handling mobile devices within and, in particular, outside of the production level.
- Guidelines for handling third-party personnel, such as service technicians and their access to the production network
- Guideline for disposal, replacement, or archiving of existing components

The goal is therefore to create guidance material for the security process as such.
The result represents a definition for a measure. On the basis of this definition, the means for subsequent implementation can be selected.
Adherence to these basic provisions is essential for subsequent effective implementation of technical measures.

9.6.2 Technical measures

Organizational measures form the basis for an appropriate security concept, while technical measures represent the core of its implementation. Depending on the type of threat, a wide range of technical measures can be taken.
A complete security solution emerges when a variety of measures are implemented and a variety of technical components are used. A combination of technical manners is essential for providing a high level of security, since it is the combination of different kinds of solutions, and not individual components, which typically pose a challenge for potential attackers.

9.6.2.1 Physical security measures

Physical measures describe the partitioning of systems and/or automation systems and areas from unauthorized access/entry. The simplest form of a physical security measure is the use of lockable control cabinets.
Still, the access to production areas should also be controlled with access authorizations. This can be realized in different ways: gatekeepers at the plant entrance, entry controls for particular production areas, special keys and card reader devices, and even camera surveillance. These measures can help to keep better control over access to production or plant premises by unauthorized persons. As a result, loss of confidential information can be limited. In addition,

damage or modifications to production equipment can be prevented by installing critical components in locked areas.
The implementation of physical measures can be a relatively easy means of significantly raising plant security.

9.6.2.2 Network infrastructure measures

The consistent use of Ethernet at all company levels (from office to production) simplifies integration and enables direct data exchange between all components of the company network. Flat network structures facilitate and simplify the communication between systems and components. However, these present a tremendous challenge to maintaining the availability, stability, and security of the network operation because a single access to the network is sufficient to reach all nodes. For this reason, uniform flat network structures offer little protection from attacks and represent a serious security risk.

Infrastructure measures can therefore contribute significantly to secure automation networks. An example of an infrastructure measure is the functional division of networks into smaller, physically-independent cells.

9.6.2.3 Endpoint security

To minimize weak points and security gaps in a network, it is recommended to also make each installed component as secure as possible. For a device, this not only includes the hardware but also the applications that run on the device.
This can be achieved by selectively disabling unneeded services and applications. In addition, inactive user accounts can also be disabled.
A basic requirement for performing this action is the availability of manufacturer documentation that identifies the security-relevant properties of the device, e.g., which services are supported and whether user administration is provided.
This information makes it easier for the user to disable unneeded services and to change or deactivate existing default passwords and users.

Result

Individual measures that contribute to risk reduction.

9.7 Identifying and evaluating individual measures

An overall concept consists of a combination of several individual measures. Once these individual measures have been sifted through and identified, they can be evaluated and combined to form a uniform concept. Only a systematic combining of the individual measures will produce an effective and efficient security concept that will successfully achieve the defined objectives.

Result
Overview of all security measures that contribute to risk reduction An important aspect of this is an overview of the costs that will arise from implementation.

9.8 Implementation of the defined measures

Once creation of the security concept is complete, work can begin on implementing the defined measures.

Result
All defined measures – both organizational and technical – have been implemented.

9.9 Checking the effectiveness of the measures

Once all security mechanisms have been implemented, a check must be made to determine whether the desired security level has been achieved. An audit, performed ideally by an independent entity, is recommended for this check. Consideration should also be given at this point to performing a security assessment. In order to carry out a complete check, the overall concept must have been documented previously and made available. This document is the

necessary basis for checking whether the planned measures have been implemented and the desired risk reduction has been achieved.

Result
The result of this audit will indicate whether a need for further action exists due to unimplemented or inadequately implemented measures and, if so, where further action is needed.

9.10 Training and awareness raising of employees

The implementation and practice of a security concept requires a common basic understanding by all employees. To achieve this, employees must be trained and briefed on a regular basis. The successful establishment and practice of a suitable security culture depends on these regularly-scheduled activities.
Because the existence of an active security culture is the basis and prerequisite for a functioning security solution, training and awareness raising activities must be focused on sustainability.

Result
Qualified, informed, and trained employees who are aware of security risks and likewise understand what security means.

9.11 Maintenance of the security level

The changing conditions in networks and their surroundings necessitate regular checking of existing security measures. The establishment of a sound change management process is particularly important in this regard. It enables quick identification and evaluation of changing conditions and implementation of any necessary optimizations. In addition to change management, another cyclic process is the security management process. These steps must be carried out on a regular basis over the long term in order to ensure a high level of security.

Result

High and consistent level of security

9.12 Incident management

In spite of all the measures taken, no one can rule out the possibility of a security incident. There is no such thing as 100% security. For this reason, it is necessary to make arrangements for such incidents and to set up an incident management process. This process includes detecting an incident, eliminating the danger, and restoring security, so that normal operation can be resumed. The responsibilities must be assigned and the resources must be available for this. From the technical perspective, options for backing up and restoring data must exist in case of data loss or corruption. The objective is to resume normal operation as quickly as possible, thereby minimizing losses.

10 Problem-solving approaches

When security solutions are being developed and implemented, the focus is typically on finding suitable measures (physical measures or network infrastructure measures) for controlling and securing access to areas, systems, and components that require security.
The following sections describe a selection of possible organizational and technical measures.

10.1 Problem-solving approaches for organizational measures

The central task of organizational measures is not only to establish security in the company but also to define guidelines and policies. These guidelines describe all necessary rules governing the handling of security mechanisms.

10.1.1 Guidelines and policies

Examples of these include:

- **Handling of third-party personnel**

  - » Supervision/escorting of third-party personnel
  - » Confidentiality agreements
  - » Visible wearing of visitor identification

- **Access regulation**
  e.g., awarding of rights for remote access

- **Handling of data carriers**
  e.g., clarification and regulation of the taking and use of data carriers and IT components
  - » Who is permitted to take IT components and data carriers out of the office
  - » Which IT components and data carriers are permitted to be taken out of the office
  - » Which basic IT security measures must be observed when taking components and data carriers out of the office
  - » Virus protection, encryption of sensitive data, custody, etc.
  - » Who is permitted to take data carriers into the company and what type of data carriers are permitted?

- **Logging**
  e.g., of system events, such as logging of login actions or activities on the network

- **System hardening**
  e.g., disabling of unneeded performance features/system features or disabling of automatic starts, e.g., for USB data carriers

- **Password and key management**
  - » Suitable key management for use of WLAN
  - » Password protection, e.g., in BIOS
  - » Changes to preset passwords
  - » Use of password memory tools

- **Guideline** for **disposal, replacement, or storing** of existing components, data carriers, and documents

- **Sanctions in case of non-compliance**
  e.g., access prohibition

10.1.2 Patch management

From the previous discussion in Section 6.7, it is apparent that patch management in automation technology is a difficult undertaking. Nevertheless, a method must be found for providing existing systems with patches and security updates for the purpose of closing security gaps. Security-relevant weak points may arise not only in standard PC operating systems but also in automation systems.
The recommended procedure on becoming aware of a weak point is as follows:

As soon as information is available about a weak point, it should be evaluated initially for its relevance to the particular application.
Depending on the result of the evaluation, a decision can then be made as to whether additional measures must be taken:

- No action, because existing measures provide adequate security
- Additional external measures in order to maintain the security level
- Installation of the latest FW update to eliminate the weak point

10.1.3 Emergency management

A security concept is not only created to prevent attacks and eliminate security gaps. Clearly defined arrangements for emergencies must also be provided. The creation of an appropriate action plan for emergencies is indispensable. This plan should clarify the following questions and information:

- Definition of roles and responsibilities for emergency operation as well as processes designated for that purpose
- List of persons to be notified
- Concept for data backups and measures for restoring data

To create a list of measures like this, it is necessary to perform a separate process. One possible procedure model is described in the BSI Basic Security Catalog BSI Standard 100-4.

10.1.4 Security as a company process

Security management is an essential component of any industrial security concept. Once the concept has been implemented, it must be checked at regular intervals to verify the effectiveness of the implemented measures. If the check of the measures yields different results than expected, the measures must be revised and implemented again. The procedure model must be run through again. Security objectives may also change; provision should be made for a periodic risk analysis to address such changes. A consistent security management process is essential for achieving and maintaining the defined security level.

10.2 Problem-solving approaches for technical measures

Besides organizational measures, the options for implementing technical measures play a critical role in achieving network security.
Basic security concepts are currently based on two basic principles: segmentation and defense-in-depth
The basic segmentation concept takes the approach of structuring both the vertical and horizontal communication in order to:

1) Limit the effect of intentional or unintentional attacks and mishandling to small, well-defined areas
2) Hinder and limit the access to reachable attack targets Attacks are only possible if an opportunity to invade the particular area is found.

These types of solutions are often referred to as a cell security concept.

10.2.1 Cell security concept

The first step for implementing a cell security concept is to define the security cells. Each cell can consist of one or more lower-level cells and must function independently from other cells as a stand-alone cell. In addition, the number of components may differ in each cell. All components located within a cell are classified as trustworthy, so that additional security measures for communication within the cells are not required. This principle is beneficial when upgrading existing systems. For previously defined cells, only the access control at the incoming point of

the cell has to be defined. Conventional security components can be used for this. The primary advantage is that the cell is protected from network overload by a limiting of the bandwidth, and the data traffic within the cell can continue undisturbed. This means that the real-time communication within the cell is not impaired. In addition, safety applications within the cell are equally protected from unauthorized access from the outside.

10.2.1.1 Criteria for the network segmentation

As part of the cell-based security concept, a network segment is secured against unauthorized access from the outside. The security application does not check the data traffic within the cell. The data traffic must therefore be deemed as secure or be provided with security measures inside the cell, e.g., port security for switches. The size of a security cell depends primarily on what the components contained in the cell are to be protected against, because a cell may contain only those components that are subject to the same security requirements.
Depending on the performance requirements, the following recommendations also apply to the network size and network segmentation:

- All devices of a controller domain belong to one cell
- Devices that transmit large amounts of data to one another should be assigned to the same cell
- Devices that communicate only with devices of a single cell should be assigned to this cell if the security requirements are the same

The network can be segmented in two different ways:

» Logical segmentation

» Physical segmentation

10.2.1.2 Logical segmentation with virtual local area network – VLAN

VLANs (Virtual Local Area Networks) offer the ability to create logically separate networks. They enable the physical structure to be divided into logical subnets. Within a switched networked, this is implemented technically by assigning the switch ports to a VLAN. Ports that are assigned to the same VLAN also process the same broadcasts; ports that are assigned to different VLANs do not.

VLANs can be established between network switches but not between devices. Therefore it is not possible to establish different VLANs between PROFINET devices. However segmentation by VLANs can be established between infrastructure network components e.g. switches.

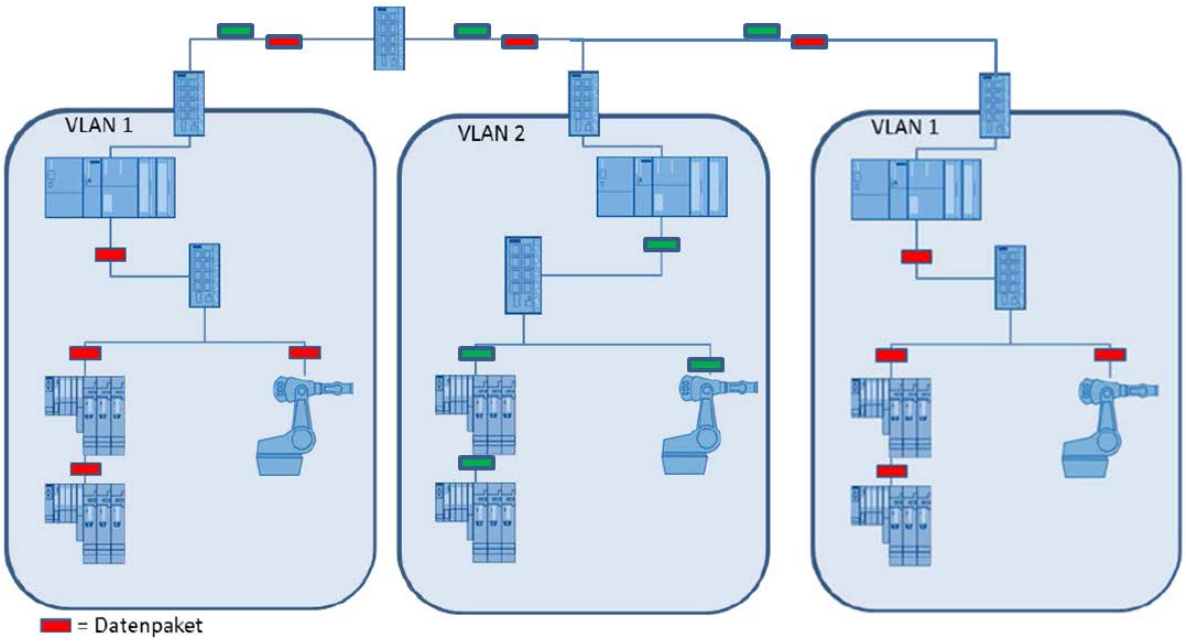

Figure 3 - Possible VLAN

<<key to Figure 3: **Datenpaket** = Data packet>>

10.2.1.3 Physical segmentation

As a result of the physical segmentation, automation networks are subdivided into smaller segments. Each cell protects the components located within it, since there is no possibility to access the cell from the outside for the time being. The result is a number of individual automation islands that can operate independently of one another. For more information, see Chapter Step-by-step example of segmentation.

10.2.1.4 DMZ

Another form of segmentation is the creation of a so-called demilitarized zone, or DMZ. All components that require or provide access to the outside are grouped within this segment.
Another alternative for applications with stringent security requirements is the connection via a perimeter network, which is often also called a demilitarized zone. In this case, direct communication between production and the rest of the company networks is completely blocked by firewalls. Data can only be exchanged indirectly via a server in the DMZ. In this way, internal guidelines for communication exchange can be reliably implemented while preventing unauthorized access from the outside.

A critical advantage of segmentation is the ability to clearly define access points between segments. The boundaries are clearly structured, which enables interfaces to be easily defined.
Chapter 9.2.2 presents various options for implementing access points and access controls.

10.2.1.5 Subnet formation and IP addresses

Access possibilities to automation cells can also be structured by defining subnets.

In this case, a subnet refers to a network area in which all nodes can access one another via Layer 2 communication (broadcast domain) and have the same subnet address. Subnets are physically separate from one another. The gateway between subnets is by means of a router.

Since PROFINET communication is usually Layer 2-based and can therefore not cross over router boundaries, all PROFINET nodes that are to communicate with one another must be located in the same subnet. However, large subnets must be avoided, as this approach increases the risk of mutual interaction between controller domains due to broadcasts and multicasts.

In general, it is recommended to keep subnets in which nodes are to communicate with one another as small as possible. For example, the structure of a subnet could always be cell-related.
The main advantage of this subnet formation is that, for example, multicast or broadcast queries can be sent exclusively within a subnet. This eliminates additional data traffic on other networks not affected by these queries.

From the security perspective, the formation of cell-based subnets is also appropriate for IP-based communication. For example, the cells can be isolated from the higher-level network area simply through the use of private IP addresses (address concept). It is then no longer possible to establish a direct connection from the higher-level network to the cell. Communication is only possible through the use of corresponding address configurations (e.g., NAT) at the gateways.

Advantages of the cell security concept
By implementing a cell security concept using segmentation, you ensure that any unauthorized access to a cell applies only to the nodes located in that cell.

10.2.2 Access points/access controls

Once all network segments have been created, the implementation of access points and access control can begin. Access points should be chosen in such a way that they are not placed directly inside cells. A direct access into a cell would create an access point at the heart of the machine. To avoid this, the access points should always be implemented outside the cell. The access points can be further secured by other measures.

Multifaceted solutions are used for this. The three basic variants (basic technology) for the use of active network infrastructure components are:

» Switches: full integration, no segmentation

» Routers: private vs. company IPs (basic security depending on the selected IP address concept)

» Gateways/proxies: no direct communication; rather, application-based connection between nodes of different segments

Practically all available security solutions are based on one of these basic technologies. For example, the basic technology on which the popular firewall solution is based is the router. Here the router uses additional, configurable rules to control communication on the basis of the IP destination/source address, the utilized services, or even the contents.

Notice:
If access points are consistently implemented using the same products, the danger exists that a known weak point will represent a uniform security gap throughout the network.

10.2.2.1 Routers/switches

The simplest case of access points is the use of routers and/or switches. In principle, routers and switches connect networks to one another. Routers connect networks to one another across network boundaries, while switches are intended only for use within a subnet.

Switch
If a Layer 2-based communication is to take place between the segments, the use of a switch is recommended. However, it must be taken into consideration that the greater the number of switch connections implemented, the greater the size of the Layer 2 domain will be, which can

result in a very large amount of data traffic from the propagation of multicast messages. This can be prevented by using switch components that configure a so-called multicast block for individual ports. A careful check should be made at this point to determine whether this block will affect not just PROFINET-specific multicast queries, such as DCP, but also other queries such as ARP multicast queries

Router
If the cells are in two different IP subnets and IP-based communication is also to be ensured, a router must be used since it is the only means of connecting two different networks together.
The advantage of using a router is the limiting of the multicast domain. Routers do not forward Layer 2-based multicast queries to the other network segment. The data traffic is thus limited to the "sending cell".
Multicast queries can also occur in IP-based services. For this reason, the requirements for a router are also dependent on the applications used and the services they require. Some engineering tools use multicast queries to find their devices in the network. For this reason, the boundaries should also be determined here.

10.2.2.2 Gateway

The use of gateways can constitute a very efficient security gateway, provided no direct communication between nodes of different segments is required. Examples of technical solutions implementing this concept include controllers that have multiple network adapters. Each segment is thereby connected to the gateway using one of these network adapters.
By uncoupling selected functions using gateways, increased security can be achieved.

10.2.2.3 Firewall

A firewall is the best-known mechanism for access control. In its simplest form, a firewall controls accesses between networks. At the same time, protocol types and addresses are defined in the form of so-called firewall rules. The rules also define what is to happen with the packets.
To define these firewall rules, at least the following information must be available:

- Which services are required between the networks to be connected? (ports)
- Who may communicate between the networks? (IP addresses)
- In which direction may this communication take place? (ingoing/outgoing)

A packet filter firewall represents the simplest form of a firewall.

Stateful Inspection
The so-called stateful inspection provides an expanded form of filtering. This method allows context-independent evaluation of the packet content. The context relates to an underlying session management.

When this technology is used, consideration must be given to the fact that connectionless protocols are supported. An example would be UDP. UDP functions as a connectionless protocol. However, the firewall must provide a temporary, virtual connection in order to ensure communication in both directions.

Application layer / Layer 7 firewall
Since attacks can also occur within applications, Layer 7 firewalls are available. This type of firewall can examine the pure user data of a packet and react appropriately, depending on the content. It is possible, for example, to prevent accesses or data exchange with streaming servers.

User-specific firewall
A user-specific firewall represents a special form of a firewall because it can not only filter the data traffic according to device-specific IP addresses but it can also also permit or deny possible

accesses depending on certain users. This requires that a user be authenticated on the firewall, e.g., via password login. A set of firewall rules specially defined for this user in advance is then activated.
In so doing, the IP address of the user's computer is irrelevant since the user-specific firewall rules contain placeholders in which the existing IP address of the users' computer is inserted in each case.

10.2.2.4 IPS / IDS

Intrusion prevention and intrusion detection systems (IPS/IDS) can be used to supplement firewalls. Both systems are able to recognize attacks and attack sequences. The basic difference between an IPS and IDS is that an IPS is able to prevent attacks and an IDS can merely detect them.

10.2.2.5 Virtual Private Network – VPN

A virtual private network (VPN) is used to connect two independent networks together securely. In the classic IT world, VPN is often used for accesses from the Internet to an existing company network. VPN connects both networks by means of a gateway to form a compatible network so that the user, who is located on the outside becomes a logical part of the internal network. The implementation of a VPN is used primarily to realize an access from an external network into the internal network. Two basic elements are required for this: a VPN gateway and a VPN client. The VPN gateway represents the dial-in node and the client provides the actual service. The VPN client packs the communication that is to take place between the two networks into its own protocol. These data packets are then unpacked again on the receiver side and transmitted normally within the network. In other words, the actual data packets are sent to an external network in their original form.

Main tasks:
- Confidentiality
- Integrity
- Authenticity

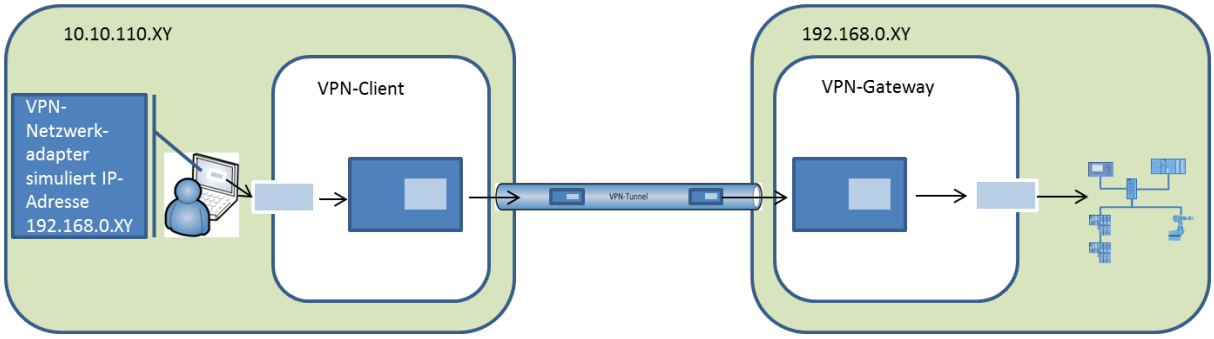

Figure 4 - Principle of a VPN

<<key to Figure 4: **VPN-Netzwerk adapter…** = VPN network adapter simulates IP address 192.168.0.XY>>

The manner in which the packets to be transmitted are now packed can differ: Protocols that allow encryption are typically used here in order to ensure that the security objectives of confidentiality, integrity, and authenticity are met. IPsec, SSL, and even TLS are probably the best-known of these mechanisms. It should be noted here that each of the protocols operate only under defined general conditions. Therefore, before VPN is used, the clarification of all requirements and general conditions must be undertaken as a top priority. The field of application for VPN must also be completely defined. For example, if VPN is to be used for service accesses, it must be made clear that this will open up access to the internal network for a third-party individual. A precise definition of the access management is required. The assignment of access data and a corresponding authentication mechanism is not enough. Consideration must be given here to questions such as “What happens if a service notebook, including saved access data, is stolen?” The potential weak points of the external company or service technician must be considered, since a weak point of the external company may also become your company's weak point.

The principle of encapsulation is an additional point for consideration when using VPN. The data are packed in their original state in encrypted form into a regular data packet. If access is through a firewall or IPS, the original content of the message cannot be viewed by a firewall or another system, because a decryption is only possible between the two connection nodes. The user is thus able to feed any manner of data traffic into the internal network.

10.2.2.6 Lockable cabinets

Access points do not always have be a part of the network. Lockable cabinets are also suitable for the implementation of access points to critical infrastructure. This is a simple way of preventing unauthorized access by unauthorized persons.

10.2.3 Defense-in-depth approach

Defense-in-depth takes the approach of combining technical solutions and concepts in such a way that when an individual security measure fails, other security measures will intervene.
From the perspective of an automation system, the resulting security is all-around and in-depth. This means, on the one hand, that a variety of complementary security measures exist to confront different threats and to meet security objectives such as virus protection or access protection (all-around security). On the other hand, it means that there are multiple barriers that a potential attacker must overcome. The essential components of the concept are plant security, network security, and system integrity. The measures for plant security include all types of physical access protection measures as well as organizational measures and the establishment of a security management process. Network security means protection of automation networks from unauthorized access. This includes the control of all interfaces, such as interfaces between the office and plant networks, and the control of remote maintenance accesses to the Internet and can be accomplished using firewalls and, if necessary, the setup of a demilitarized zone (DMZ). The DMZ is used to make data available for other networks without allowing direct access to the automation network. The security-related segmentation of the plant network into individual protected automation cells serves to minimize risk and increase security. The protection of system integrity concerns devices such as PCs with virus protection or automation systems with access protection mechanisms for devices or applications. Also included here are hardening measures that reduce the weak points of devices and systems. A defense-in-depth approach in which the necessary security measures indicated here seamlessly mesh together is essential for achieving comprehensive and reliable security for an automation plant. These measures include processes for establishing and maintaining security, secure products, and last but not least the necessary security awareness of all parties involved.

This manner of safeguarding will prevent a variety of attacks at various levels and thus poses a greater challenge for a potential attacker. Each individual level in and of itself poses a relatively easy-to-overcome security hurdle. However, when combined with the other levels, the result is very difficult to overcome.

The following points are important when taking the defense-in-depth approach:

» Several defense levels must be present.

» Each level implements a different security mechanism

» Each level is implemented in a context-dependent manner.

11 Examples

11.1 Step-by-step example of segmentation

Figure 6 shows an example of a company network without segmentation. This configuration will serve as the basis for illustrating the principle of the cell protection concept, in which an example segmentation of an automation network will be shown.
The following symbols are used in the example:

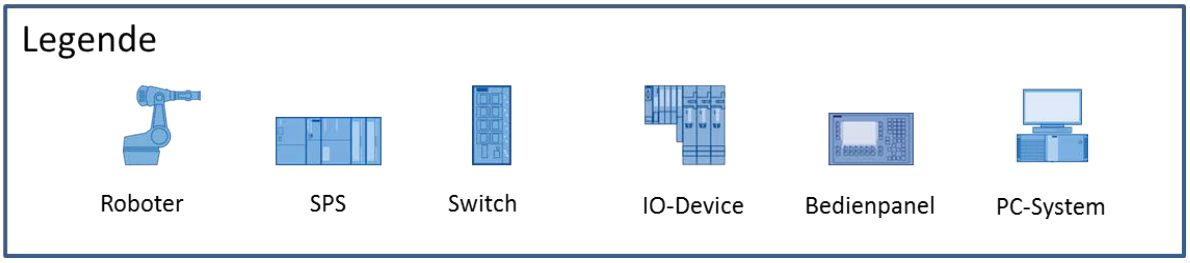

Figure 5 – Key for the following examples

<<key to Figure 5: **Roboter** = Robot; **SPS** = PLC; **Bedienpanel** = operator panel>>

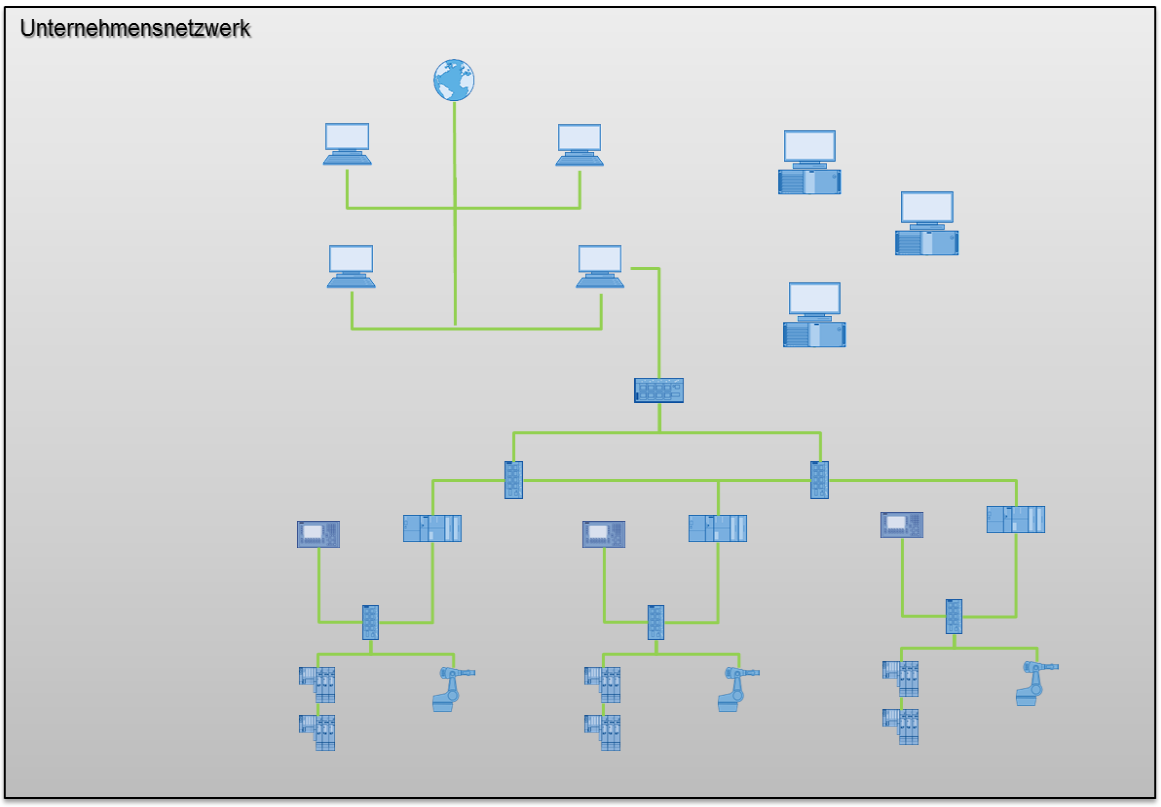

Figure 6 - Company network without segmentation

<<key to Figure 6: **Unternehmensnetzwerk** = company network>>

The simplest form of segmentation for this example network would be to separate the office and production networks in an initial step. This segmentation separates the automation network from the remaining network, thereby preventing access from the outside for the time being.Figure 7 illustrates this first step.

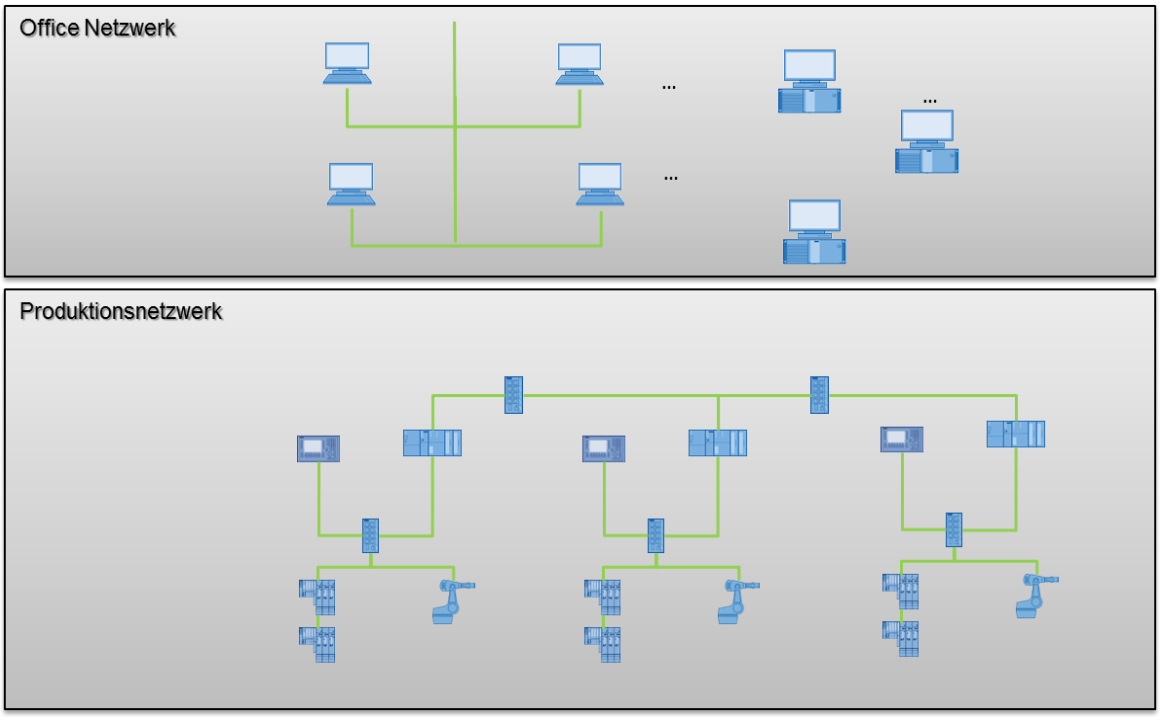

Figure 7 - Simplest form of segmentation

<<key to Figure 7: **Office Netzwerk** = Office network; **Produktionsnetzwerk** = Production network>>

Focusing on the production network, it is possible to create a further subdivision in a second step. Individual automation cells can be defined within the production network. These can be based on a controller domain, for example. Automation cells defined in this way can then be grouped in a subsequent step to form a production line. A PROFINET domain can be used here as a benchmark.
Figure 8 illustrates this additional network segmentation step.

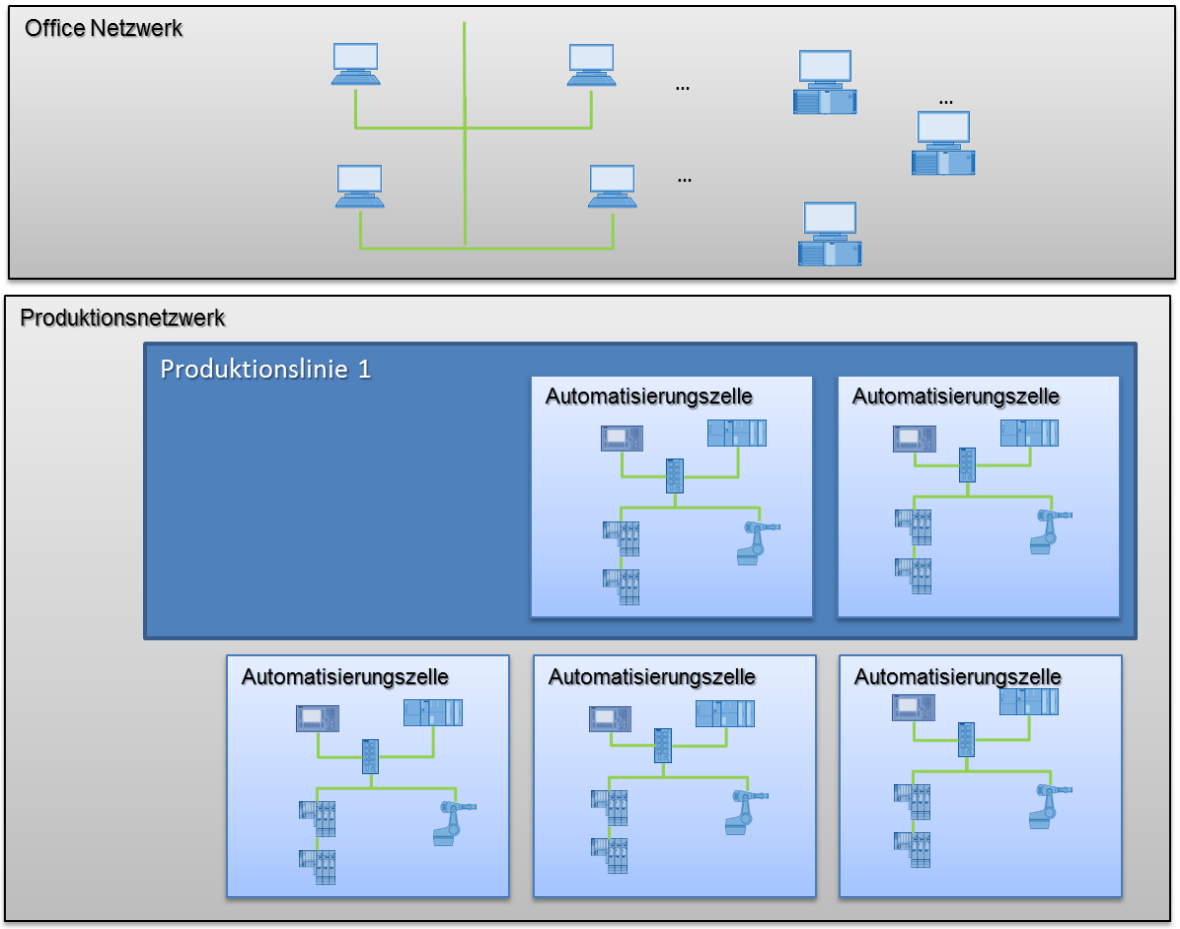

Figure 8 - Segmentation of the production network

<<key to Figure 8: **Office Netzwerk** = Office network; **Produktionsnetzwerk** = Production network; **Produktionslinie** = Production line; **Automatisierungszelle** = Automation cell>>

Production lines and even automation cells can now be defined and combined as often as required.

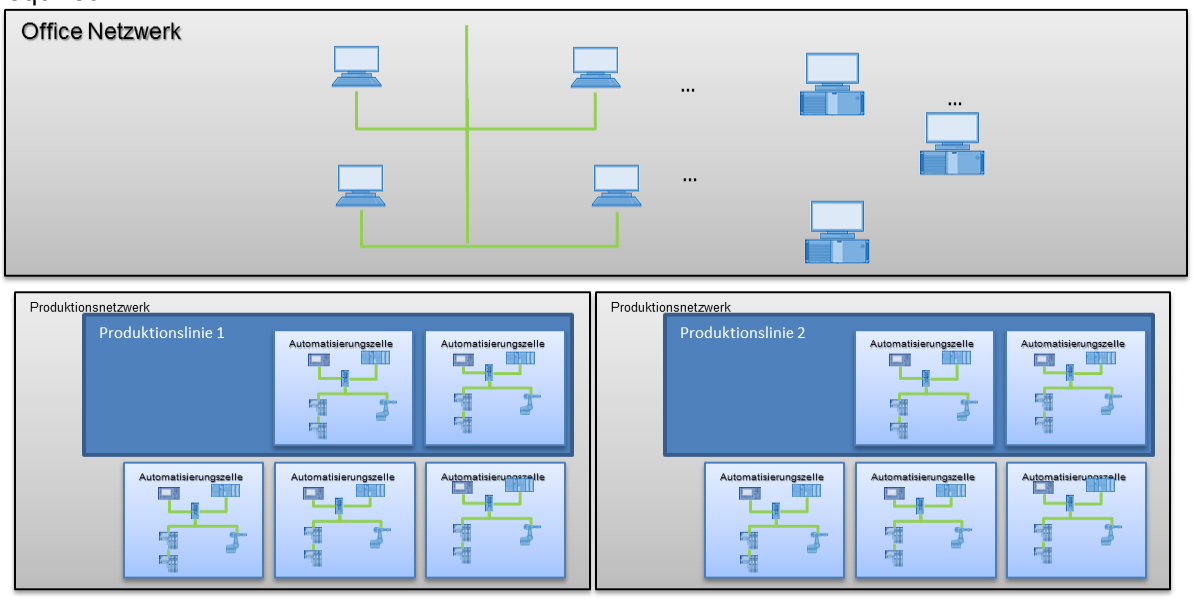

Figure 9 - Multiple segmentation of the production network

Finally, a DMZ can also be introduced in order to remove components that require access to the outside from the cells. A further segmentation level can be achieved by using a DMZ. This enables services and components that are to be made available to the higher-level system to be removed from the cells.

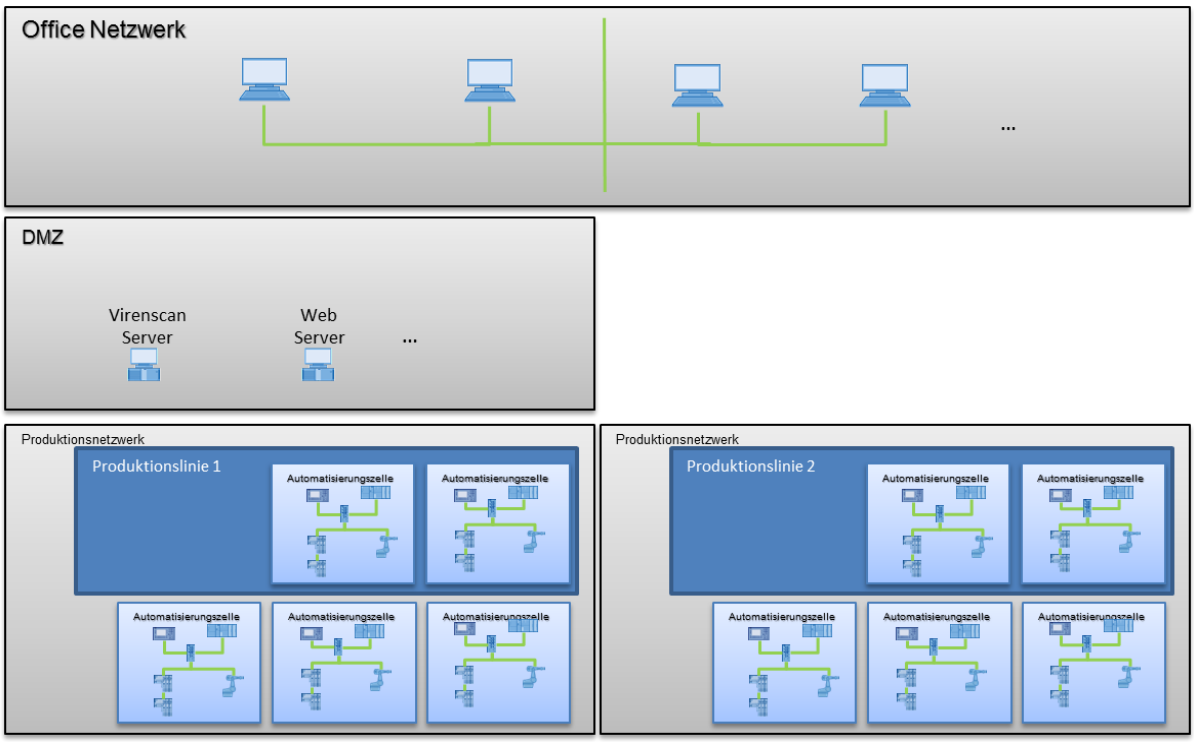

Figure 10 - Segmented production network including DMZ

<<key to Figure 10: <<**Virenscan Server** = Virus scan server>>

11.2 Access points/access controls

Once a segmented network has been created following the step-by-step instructions, the next step is to define the access points and their access options in such a way that all necessary communication paths can be realized in a secure manner.

Requirement

In order to create access points, the following information must be available:

- Which communication links must be set up?
- Which service is required for a communication link to be set up?
- Which port must be activated for this?
- What is the purpose of the communication link?
- Which users (persons or devices) are authorized to use the communication link?

This information is essential for creation of controlled access points.

In the following examples, the use of the access controls and access points described in Chapter 9.2.2 will be described.
The aim of the description of the individual options is to implement accesses, provide a network with example access points, and to examine different use cases. The result will be a structure based on the respective use cases, and the options associated with this structure can be presented.

The segmented network created in Chapter 10.1 represents our starting situation.

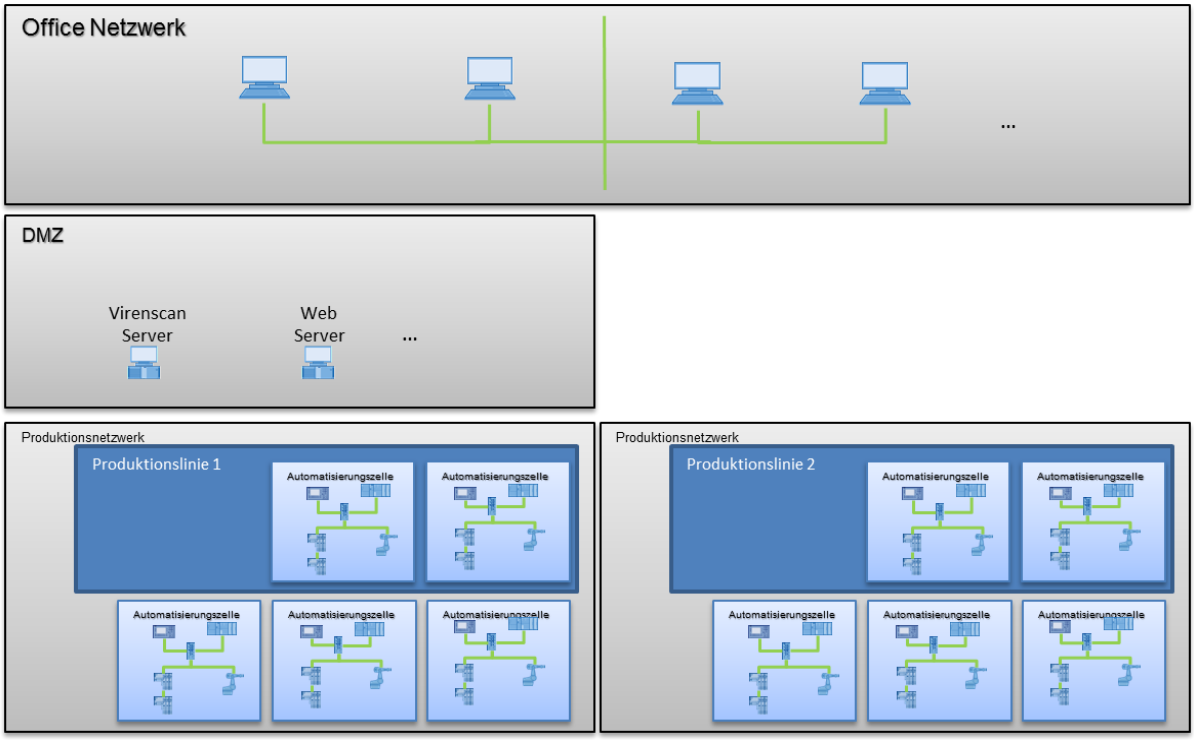

Figure 11 - Starting basis for implementing access points/access controls

The following symbols are used:

Figure 12 - Key of access control points

<<key to Figure 12: **Servicetechniker** = Service technician>>

The basic concept for the examples below takes the approach of separating controller domains from one another to the extent possible and to connect these only when necessary.
For simplification purposes, only a section of the example network will be examined.

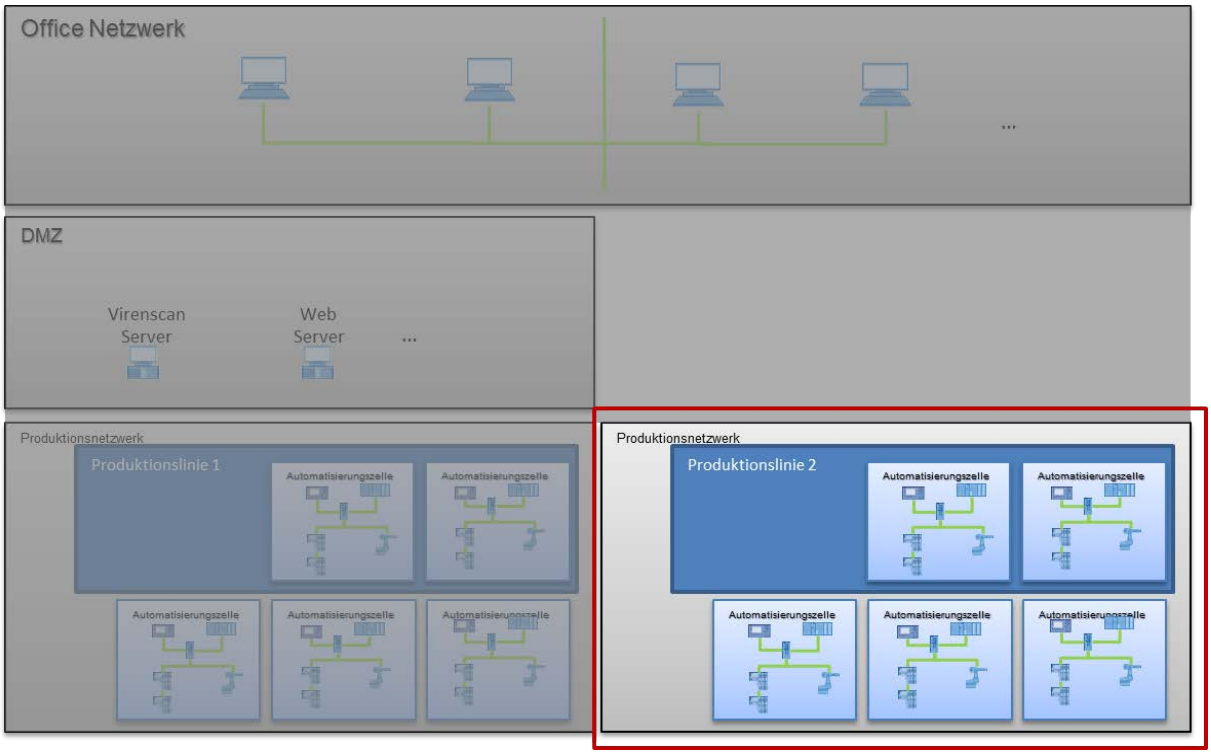

Figure 13 - Starting basis for the use of switches

Individual automation cells have been defined within the production network. These are based on a controller domain; in this case, the production line corresponds to a PROFINET domain.

11.2.1 Z1 – Use of gateways

Use case
Communication between the controllers based on IO signals is required

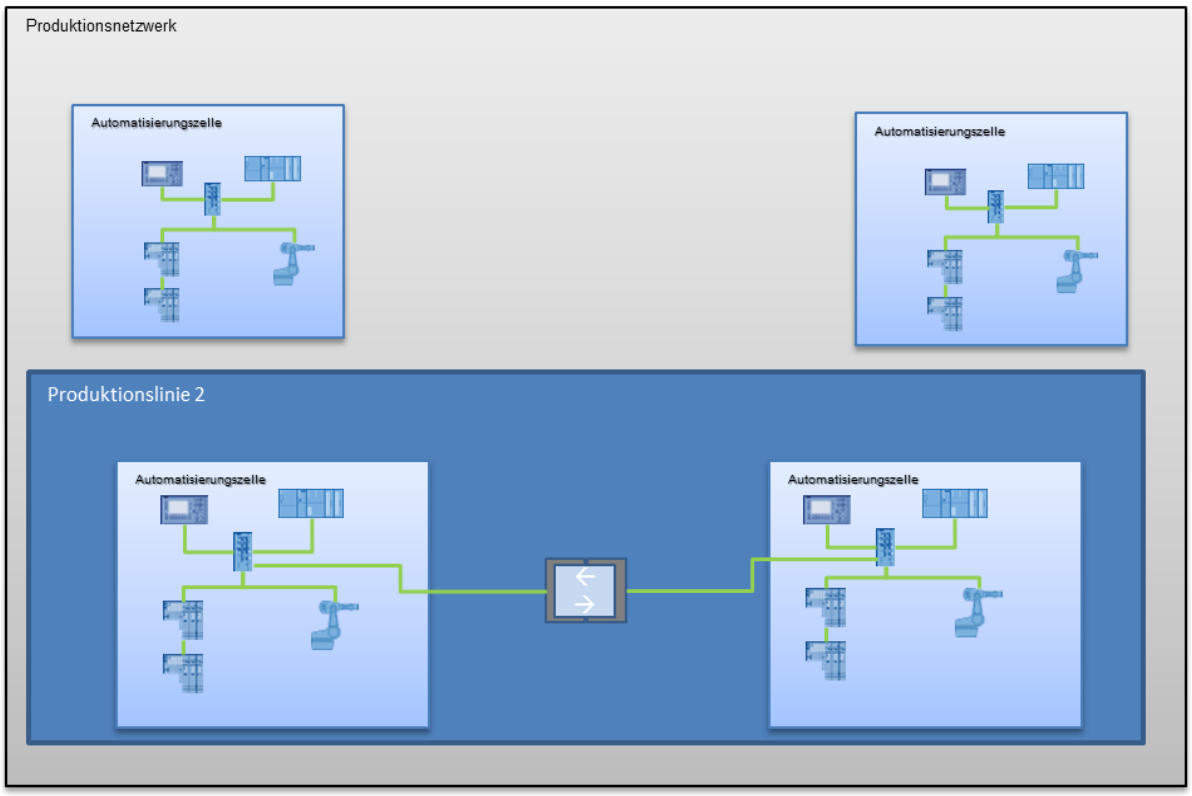

Figure 14 - Use of a PN/PN gateway

Characteristic
The advantage of this communication link is that no communication based on Layer 2 and higher can take place. The necessary communication link is thus limited to the minimum required and fulfills its intended use and no more.

Consequence
No PROFINET services based on Layer 2 and higher can be used.

11.2.2 Z2 – Use of switches

Use case:
A Layer 2-based communication is required. An example of this would be the use of engineering systems for assigning names of PROFINET devices.

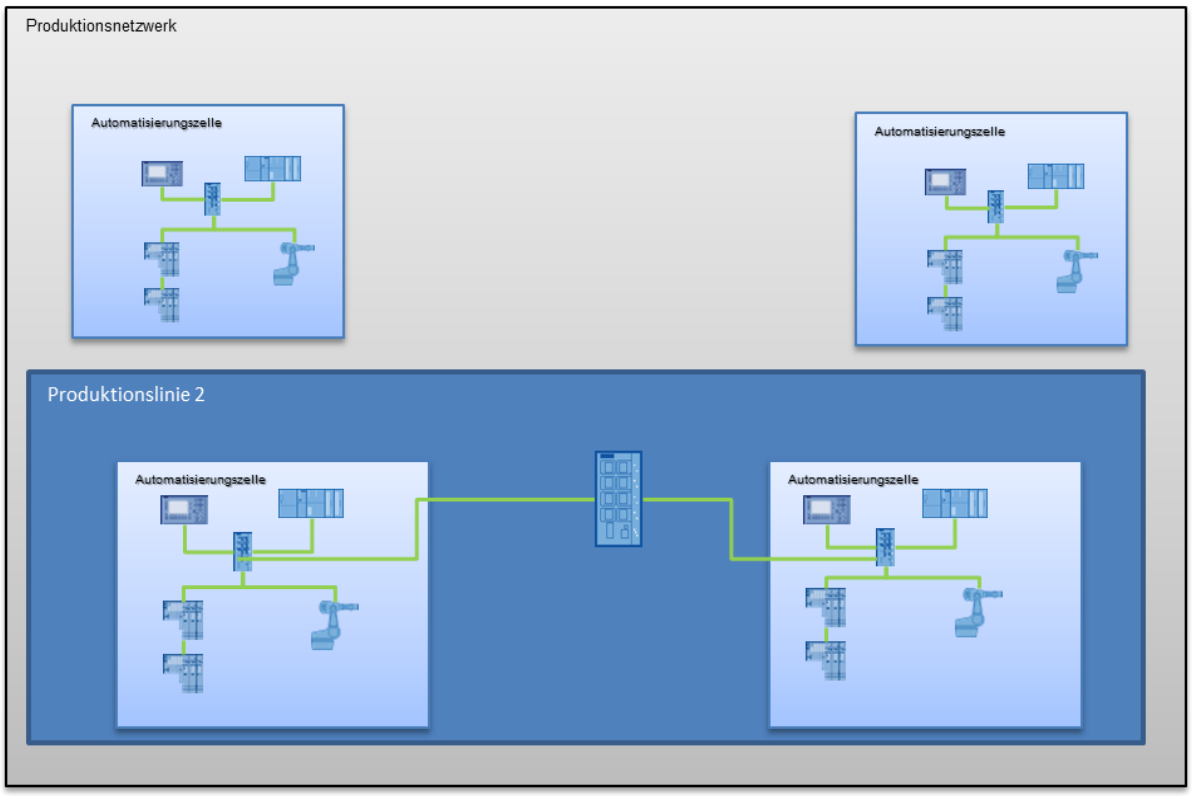

Figure 15 - Use of switches for access control

Characteristic
The use of a switch to establish a connection between two automation cells enables the use of Layer 2-based PROFINET services.

Consequence:
If multicast queries are sent, they can be viewed in both automation cells. A managed switch that permits the suppression of multicast queries can remedy this situation.

11.2.3 Z2 – Use of routers

Use case
An IP-based data exchange between computer systems is to take place, e.g., for backing up quality data.

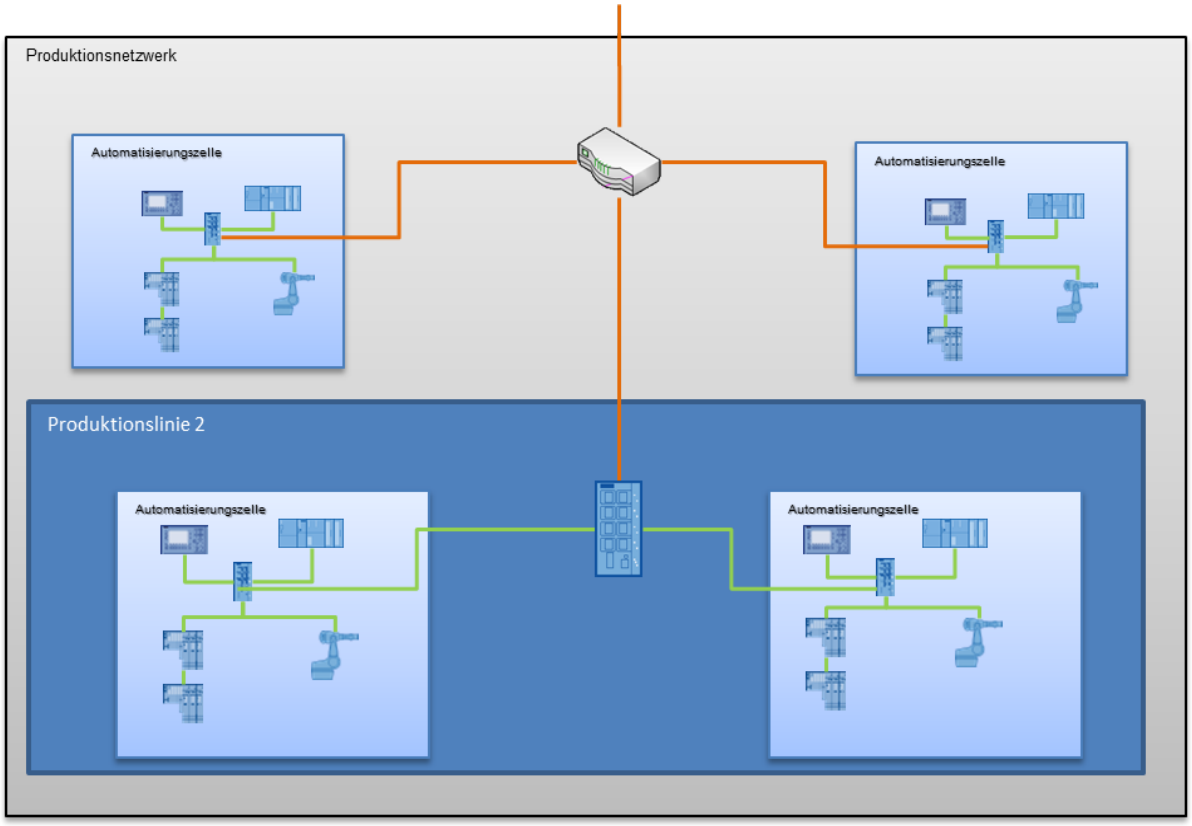

Figure 16 - Use of routers for access control

Characteristic
Communication based on Layer 3 and higher, but not on Layer 2, can take place. The complete use of PROFINET services is not possible.

Consequence
No Layer 2-based services between the individual segments (automation cell, production line) can be used. Only IP-based messages can be exchanged.

11.2.4 Z4 – Use of firewalls

Use case
Access limitations to the individual networks are to be implemented. These limitations can be defined on the basis of various criteria:

- IP-address-specific
- Service/port-specific
- Content-specific
- User-specific

The use case for all types of filter criteria is basically the same. Therefore, the following examples will consider only a conventional firewall using IP addresses/ports as the filter criterion.

In the simplest case, the firewall separates the production network (hall) from the higher-level network Figure 17

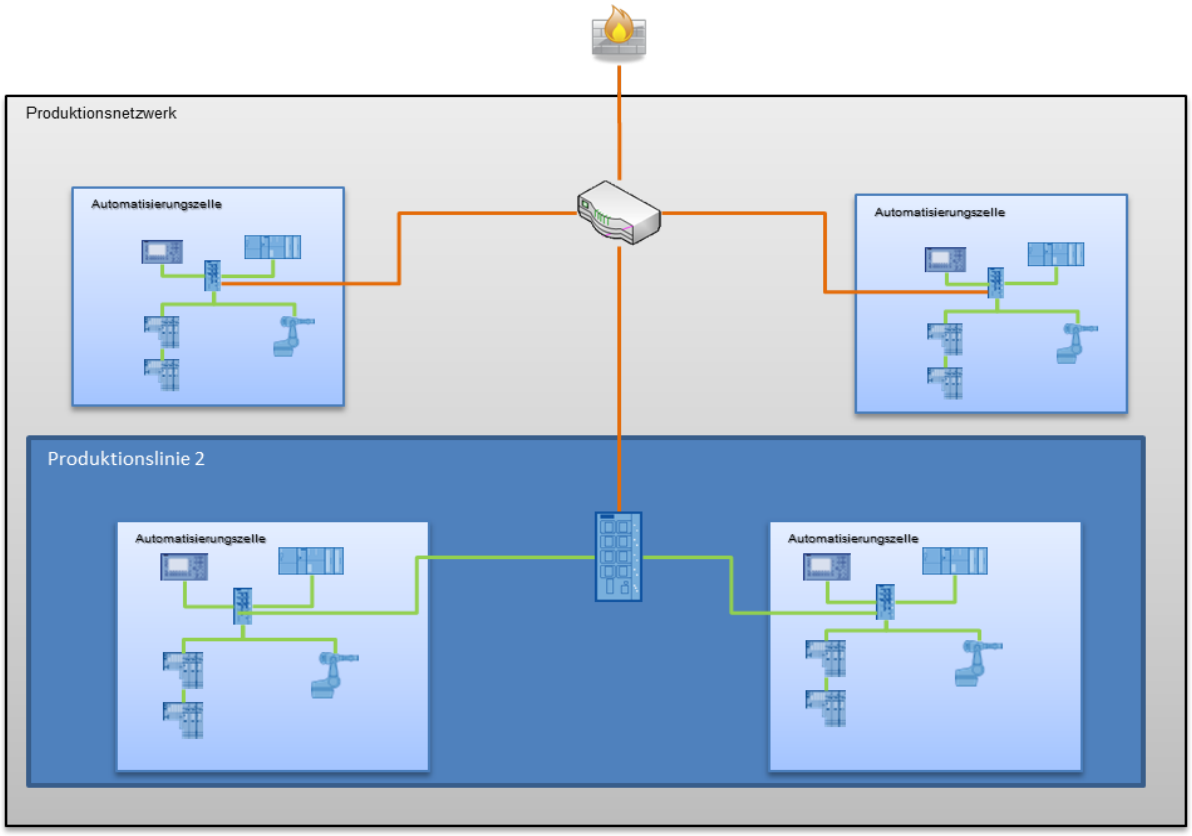

Figure 17 - Simplest use case for a firewall

Consequence

A control of the gateway is achieved, but not a control within the production network.

The use of another firewall placed inside the production network could represent a refinement here Figure 18

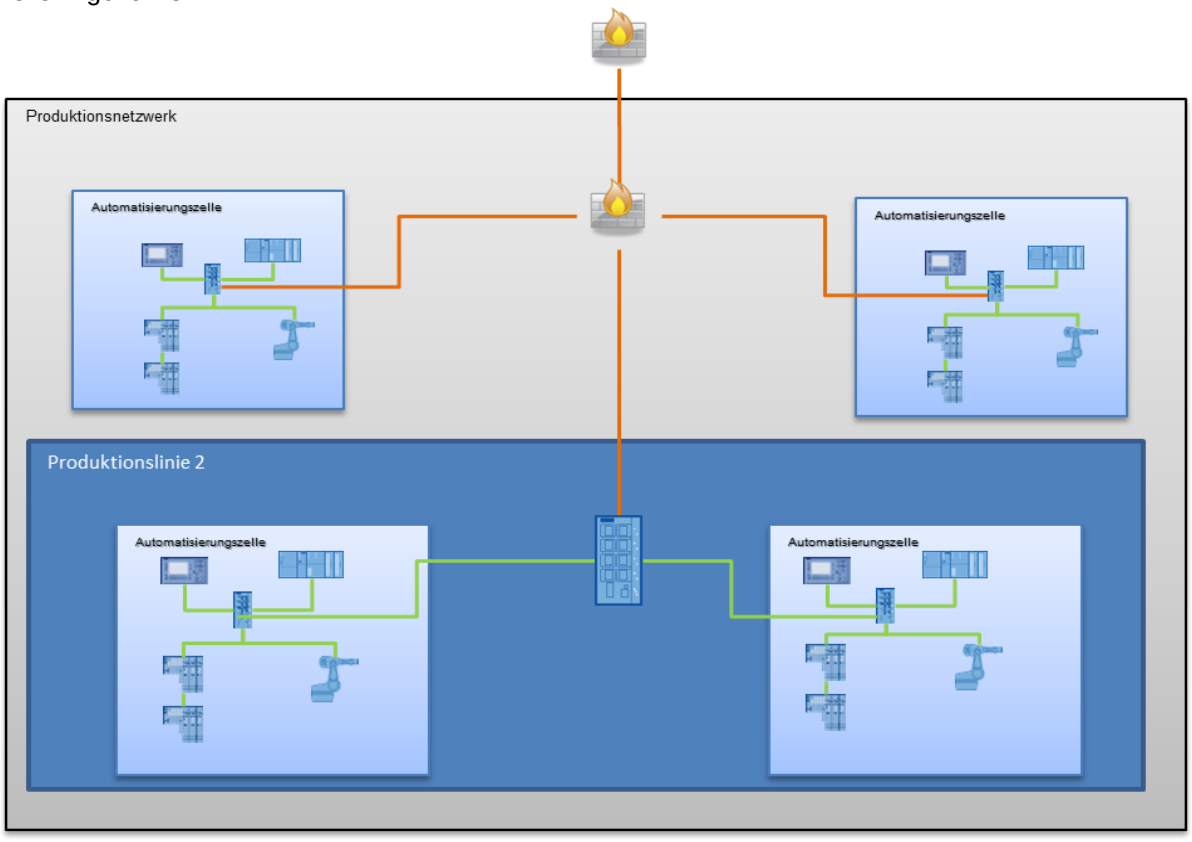

Figure 18 - Firewall within the production network

Consequence
The firewall separates the cells within the production network. Both a control of the gateway and control within the production network are achieved. In this case, the higher-level firewall can serve as the gateway for multiple production networks. This arrangement also enables a division of the area of responsibility for the firewall management, thereby facilitating an organizational separation.

A further refinement of the access control is possible by positioning a firewall before each cell in a granular firewall configuration Figure 19

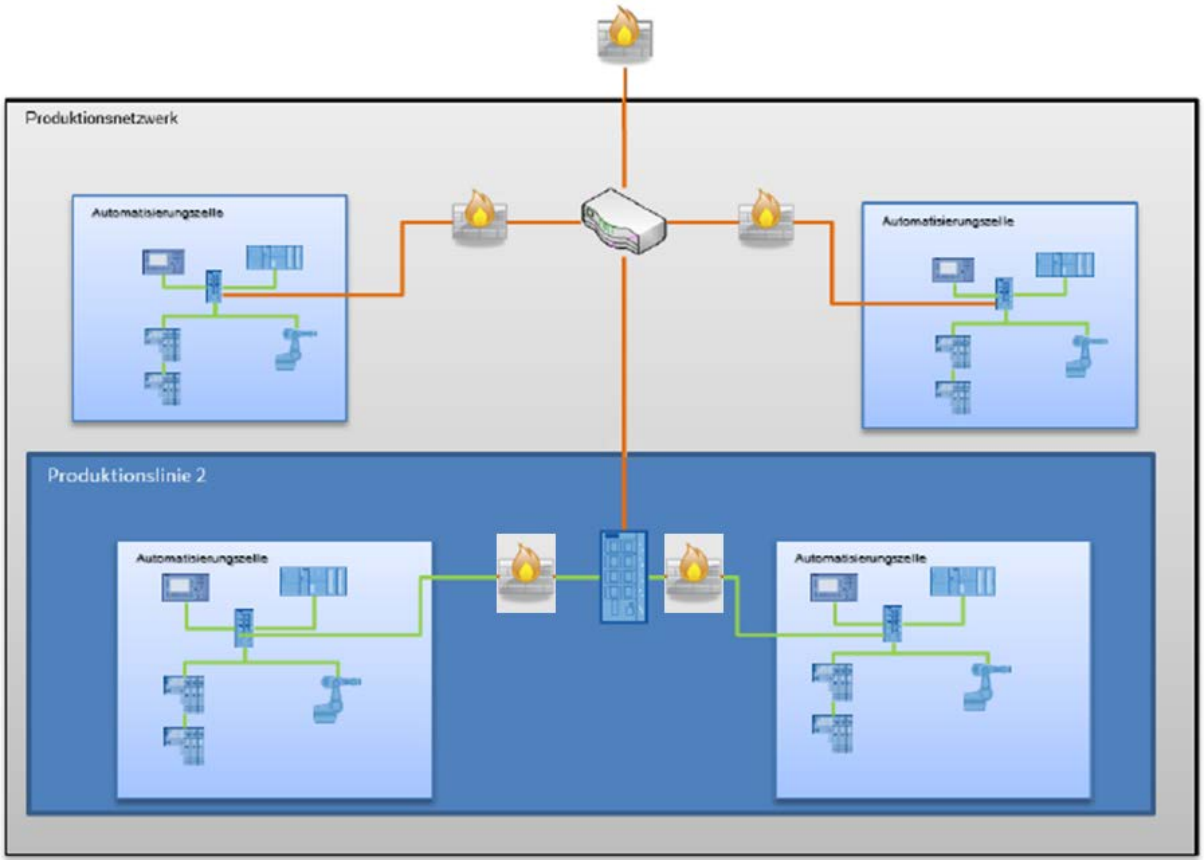

Figure 19 - Use of cell-granular firewalls

The advantage is that the access can be managed separately for each cell.

Consequence
Compared with Figure 17 or 18 this solution means higher management effort but also provides a very clear structure, higher security and availability due to multiple firewall-devices.

11.2.5 Z4 – Use of VPN

Use case
External access for service purposes must be implemented.
The use of VPNs enables the establishment of authenticated and encrypted communication links across network boundaries.
In this case, access is possible via the office network infrastructure, the DMZ, or directly in the production network. An essential criterion for this is the positioning of the VPN gateway and the resulting termination of the VPN connection. This positioning is a critical factor for determining

the downstream systems (e.g., including firewalls) through which additional security functions can be implemented. VPN gateways are therefore also integrated directly into firewalls in some cases.

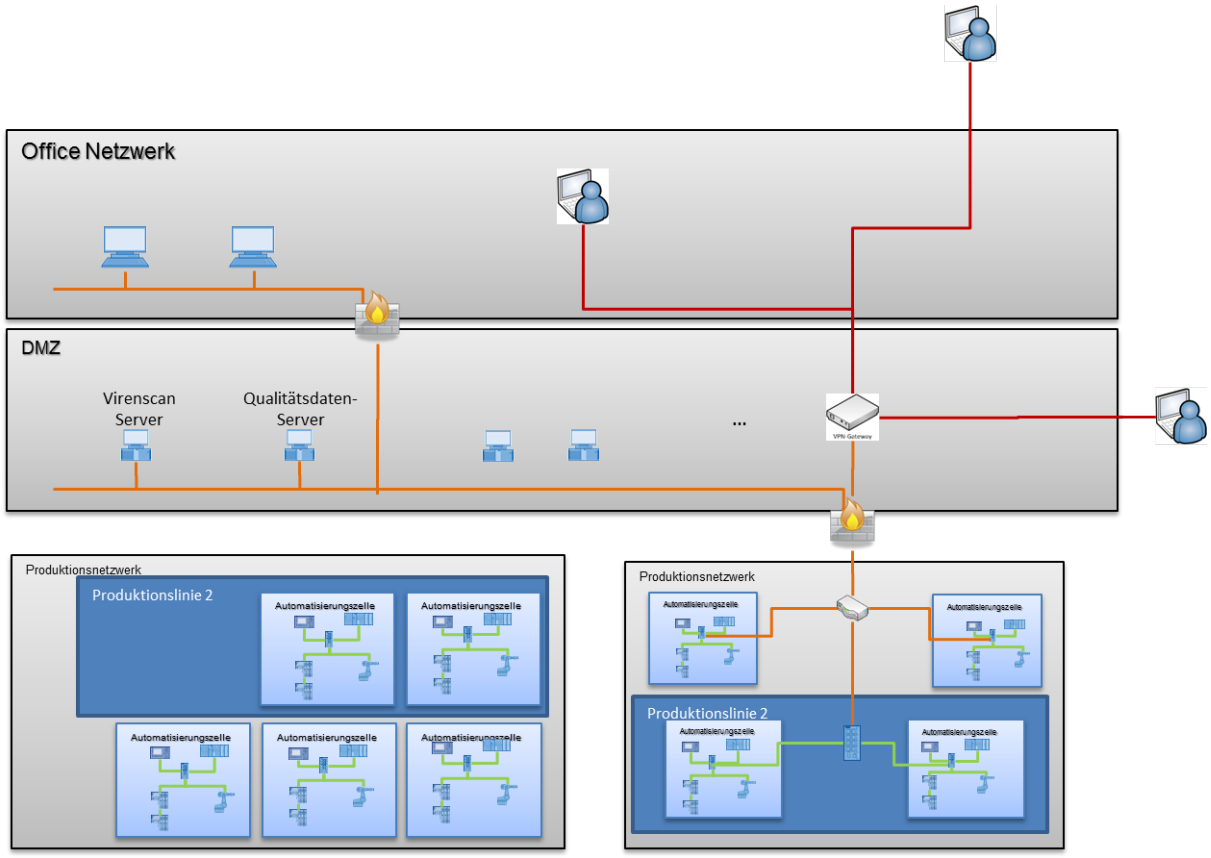

Figure 20 - VPN variant

<<key to Figure 20: **Qualitätsdaten-Server** = Quality data server>>

The required granularity and differentiation for access control determine the distribution and arrangement of VPN gateways.. A solution is therefore conceivable in which a termination of the VPN connection occurs before the automation cells. This also enables VPN connections to be established between the individual automation cells.

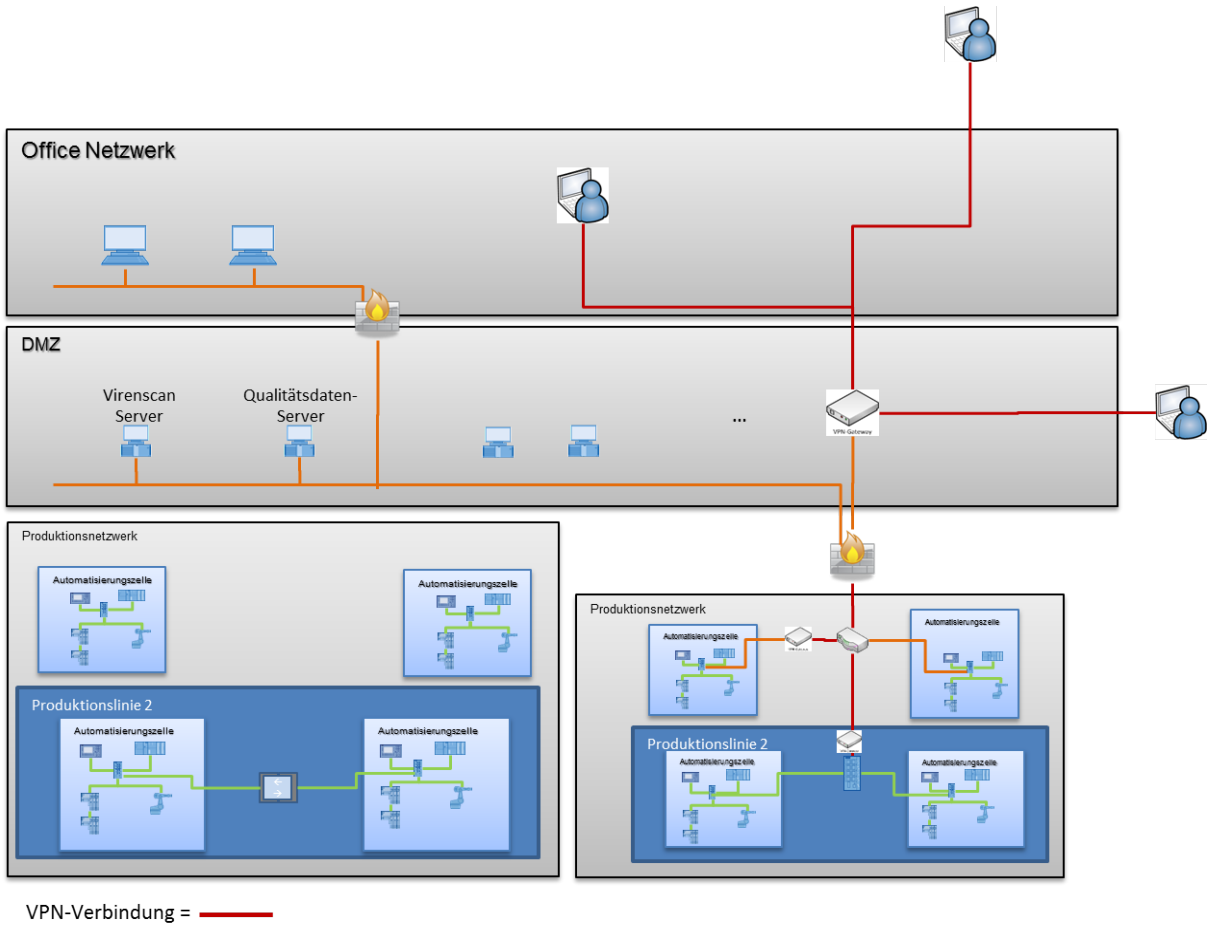

Figure 21 - VPN variant 2

<<key to Figure 21: **VPN-Verbindung** = VPN connection>>

12 Summary

The basic concept for achieving appropriate security for PROFINET-based automation solutions relies on controlling the necessary accesses to the individual PROFINET domains. This is accomplished by segmentation of the network and establishment of defined zones and by control of communication links between the segments and zones (cell security concept). Together with the use of different technologies and methods, this results in the implementation of a defense-in-depth approach.

Because different solutions and technologies may be used depending on the specific requirements and these may be applied in any combination and in connection with segments, the result will be an integrated security concept.

In conjunction with the Security Level 1 Test used during the certification process to verify the robustness of PROFINET devices under real-world network load conditions, a solution concept is now available that can be customized to meet the requirements of the production conditions in each case.

13 Requirements for certification Tests

Requirements for certification tests are specified in document “Test Specification PROFINET IO Security Level 1 / Netload” Order-No. 2.302 version 1.1.2.

PROFIBUS Nutzerorganisation e. V. (PNO)
PROFIBUS & PROFINET International (PI)
Haid-und-Neu-Str. 7 ● 76131 Karlsruhe ● Germany
Phone +49 721 96 58 590 • Fax +49 721 96 58 589
E-mail info@profibus.com
www.profibus.com ● www.profinet.com