PROFINET Security Richtlinie

Richtlinie für PROFINET

Version 2.0 – Datum November 2013

Bestellnr.: 7.001

Dateiname : PN-Security_7001_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

Inhalt

Liste der Abbildungen

Liste der Tabellen

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 - Umfang dieses Dokuments

Die Ethernet-basierte Kommunikation im Automatisierungsumfeld nimmt eine zunehmend zentrale Rolle ein. So wird Industrial Ethernet jetzt auch immer mehr im Feldbereich eingesetzt, wie z.B. PROFINET. Neben der damit möglichen Nutzung von offenen und standardisierten IT-Technologien wie z.B. Wireless LAN oder Webserver liegt der Hauptvorteil vor allem in der damit möglichen durchgängigen Vernetzung. Allerdings steigt so auch die Gefahr von Zugriffsverletzungen, sowie durch Schadprogramme wie Viren, so dass damit einhergehend auch das Gefährdungspotenzial für die Automationsnetze neu bewertet und Sicherheitskonzepte entsprechend umgesetzt werden müssen.

PROFIBUS/PROFINET International (PI) hat konsequenterweise ein Security-Konzept für die Automatisierungstechnik entwickelt, in dem sich die Erfahrung und genaue Kenntnis des Automatisierungsumfeldes der beteiligten Mitgliedsfirmen wiederspiegelt –zum Vorteil der Anwender. Es reicht nicht aus, Anlagennetze und Automatisierungskomponenten einfach nur zu schützen. Die eingesetzten Schutzmechanismen und Konzepte dürfen darüber hinaus auch den Produktionsbetrieb nicht stören und müssen auch praktikabel und bezahlbar sein.

Mit der Security-Guideline stellt PI erstmals ein Konzept vor, das den Bedrohungen und den besonderen Anforderungen der Automatisierungswelt Rechnung trägt. Ziel ist hierbei der Schutz aller Automatisierungskomponenten, unabhängig von den verwendeten Kommunikationsprotokollen oder der Netzstruktur. Durch die Verwendung bewährter und offener Security-Mechanismen ist auch die Integration in bestehende Security-Konzepte möglich. Diese Guideline versteht sich als Leitfaden für Anwender und Betreiber industrieller Netzwerke, speziell mit dem Ethernet-basierten PROFINET, um auf die wesentlichen Aspekte zur Etablierung eines Security Konzeptes in diesem Umfeld hinzuweisen und entsprechende Empfehlungen auszusprechen.

1.1 Abgrenzung

Safety vs. security

Zu Beginn eine kurze Erläuterung der Begriffe „Security“ und "Safety": Während unter Safety funktionale Sicherheit verstanden wird, d.h. der Schutz vor Gefahren für Leben und Umwelt, die von Maschinen (o.ä.) ausgehen, wird unter Security der Schutz vor unberechtigtem Zugriff auf Informationen und Automatisierungsgeräte verstanden. Synonym zum Begriff Security wird häufig der Begriff IT- oder Cyber-Sicherheit verwendet, der in dieser Guideline jedoch kaum benutzt wird, um den Bereich der industriellen Automatisierung von dem IT-Bereich abzugrenzen. In dieser Guideline geht es um die Gewährleistung von Industrial Security basierend auf nationalen und internationalen Security-Standards.

1.2 Zielgruppe

- Anlagenplaner
- Inbetriebnehmer

2 Liste der betroffenen Patente

Zu diesem Zeitpunkt sind keine betroffenen Patente bekannt. Es wurde bis dato keine Patentrecherche durch eines der Working Group Mitglieder durchgeführt.

PROFIBUS&PROFINET International garantiert nicht die Vollständigkeit dieser Liste.

3 Verwandte Dokumente und Referenzen

3.1 Referenzen

[1] M. Popp, Industrielle Kommunikation mit PROFINET, Karlsruhe: PROFIBUS Nutzerorganisation e.V., 2007.

[2] F. Klasen, „Security für Ethernet Systeme," in Industrielle Kommunikation mit Feldbus und 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. [Zugriff am 16 Juni 2012].

[4] VDI/VDE, Informationssicherheit in der industriellen Automatisierung - Allgemeines Vorgehensmodell, Berlin: Beuth Verlag, 2011.

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

3.2 Verwandte Dokumente

Bundesamt für Sicherheit in der Informationstechnik (BSI). IT-Grundschutz-Profil für das produzierende Gewerbe - Anwendungsbeispiel für IT-Grundschutz im. Bonn, 2008.

Bundesamt für Sicherheit in der Informationstechnik (BSI). „Notfallmanagement_Standard_1004.pdf." BSI-Standard 100-4 - Notfallmanagement V1.0. Bonn: BSI, 2008.

Bundesamt für Sicherheit ind der Informationstechnik. BSI-Standard 100-4 - Notfallmanagement V1.0. Bonn, 2008.

Klasen, Frithjof. „Security für Ethernet Systeme." In Industrielle Kommunikation mit Feldbus und Ethernet, von Frithjof Klasen, Volker Oestreich und Michael Volz, 271-279. Berlin: VDE Verlag, 2010.

NAMUR. „IT-Sicherheit für Systeme der Automatisierungstechnik." NAMUR Arbeitsblatt NA115. 19. Juni 2006.

Popp, Manfred. Industrielle Kommunikation mit PROFINET. Karlsruhe: PROFIBUS Nutzerorganisation e.V., 2007.

PROFIBUS Nutzerorganisation e.V. „PN-Security_7002_V10_05Mar29.pdf." PROFINET Security Guideline V1.0. 29. März 2005.

Siemens AG. „Operational Guidelines für Industrial Security." Siemens Industry Sector Industrial Security. kein Datum. http://www.industry.siemens.com/topics/global/en/industrial-security/Documents/operational_guidelines_industrial_security_en.pdf (Zugriff am 16. Juni 2012).

VDI/VDE. „Informationssicherheit in der industriellen Automatisierung - Allgemeines Vorgehensmodell." Richtlinie VDI/VDE 2182 Blatt 1. Berlin: Beuth Verlag, Januar 2011.

IEC 62443/ISA-99 Part1-4

VDI/VDE Beispiele zu 2182, Blatt 2-3

4 Definitionen und Abkürzungen

4.1 Definitionen

Tabelle 1 - Definitionen

Term	Definition
Authentizität	[4]Es gibt zwei grundlegende Formen von Authentizität: Benutzerauthentizität und Datenauthentizität. **Benutzerauthentizität** bezeichnet, dass ein Benutzer wirklich derjenige ist, für den er sich ausgibt. Authentifizierung bezeichnet die entsprechende Prüfung. **Datenauthentizität** bezeichnet, dass Daten wirklich vom angegebenen Sender oder Erzeuger stammen und auf dem Übertragungsweg oder während der Speicherung nicht verändert wurden. Datenintegrität ist ein Teilaspekt der Datenauthentizität..
AR - Application Relation	Applikationsbeziehung zwischen einem PROFINET–Sender und einem PROFINET-Empfänger, auch Provider / Consumer genannt.
BIOS - Basic Input Output System	Stellt die Firmware eines x86 PC's dar. Hierüber wird das eigentliche Betriebssystem gestartet.
Blacklisting	Eine Liste die Elemente enthält, welche nicht zugelassen bzw. anders behandelt werden als diejenigen Elemente welche nicht auf der Liste stehen.
Broadcast	Eine Nachricht die innerhalb eines Netzwerkes an alle Teilnehmer übertragen wird.
CycleCounter	Interner Zeitstempel eines PROFINET-Gerätes beim Austausch von Nutzdaten.
Defense-In-Depth	Aneinanderreihung mehrerer Netzwerkebenen und Security-Maßnahmen um einen tiefenwirksamen Schutz zu erzielen.
DMZ - Demilitarized zone	In sich abgegrenzter Bereich, welcher nur über kontrollierte Zugangspunkte erreichbar ist..
DoS - Denial-Of-Service	Angriff der den Absturz eines Dienstes zum Ziel hat.
DynDNS - Dynamic Domain Name System	Mapped dynamische IP-Adressen auf einen festen Domainnamen
Ethernet	Layer-2 basiertes Protokoll zur Übertragung von Daten in einem LAN.
Firewall	Hardware- oder auch Softwaresystem zur Beschränkung der Netzwerkzugriffe.
Firmware	Software welche fest mit Hardware verbunden ist. Die Firmware beschreibt die Funktionalität der Hardware.

FrameID	PROFINET-Mechanismus zur Identifikation der Kommunikationsverbindung.
Gerätename	Der Gerätename identifiziert ein PROFINET-Gerät eindeutig innerhalb eines Netzwerkes.
Integrität	[4]Integrität ist die Eigenschaft, dass es einem Benutzer (Benutzer = Personen und / oder Anwendungen →siehe VDI 2182, Definition Benutzer) nicht möglich ist, Daten unbemerkt zu erzeugen, zu verändern, zu ersetzen oder zu löschen.
IDS - Intrusion Detection System	System, welche Angriffe erkennt. Im Gegensatz zu einer IPS ergreift eine IDS keine Abwehrmaßnahmen.
IO controller	Initiator des Nutzdatenaustauschs
IO device	[1]Prozessnahes PROFINET-Gerät das zur Ankopplung des IO-Controllers an den Prozess dient
IP - Internet Protocol	[1]Das Protokoll das den Transfer der Daten in einem Ethernet-Netzwerk von Endpunkt zu Endpunkt ermöglicht
Intrusion Prevention System - IPS	Systeme, welche Angriffe und Angriffssequenzen erkennen und abwehren können
IPsec - Internet Protocol Security	Protokoll zur sicheren Kommunikation in einem unsicheren Netzwerk.
LAN - Local Area Network	Lokales Netzwerk
Layer 2 communication	
Layer 3 communication	
LLDP - Link Layer Discovery	Protokoll zum Austausch von Nachbarschaftsinformationen. Das Protokoll wird z.B. zur Erfassung der Topologie in einem PROFINET Netzwerk verwendet..
Logging	Protokollierung von wichtigen Ereignissen.
MAC - Media Access Control	Medienzugriffssteuerung zur Regelung der gemeinsamen Nutzung eines Übertragunsgmediums.
MAC address	[1]Wird auch als Ethernetadresse bezeichnet und dient der Identifikation eines Ethernetknotens. Die Ethernetadresse ist 6 Byte lang und wird vom IEEE vergeben.
Multicast	Eine Nachricht die innerhalb eines Layer-2-basierten Netzwerkes an eine definierte Menge an Teilnehmern übertragen wird.
NAT-Network Address Translation	Verfahren zum automatischen Austausch von IP-Adressen in einem IP-Paket. Dieses Verfahren wird u.a. benutzt um private Adressbereiche an öffentliche anzubinden oder interne IP-Adressen nach außen zu verschleiern.

Nicht-Abstreitbarkeit	[4]Nichtabstreitbarkeit ist die Eigenschaft, dass der Betrachtungsgegenstand in der Lage ist, im Nachhinein den Urheber einer Handlung (beweisbar) nachweisen zu können.
Paketfilter	Filtert Datenverkehr in einem Netzwerk.
Patch	Softwareupdate oder auch eine Softwarekorrektur
Port	TCP- oder UDP-Ports fungieren als Adresszusatz. Hierüber können Dienste ihre Verbindung aufbauen.
PROFINET domain	Ethernet- basierter Multicast- und Broadcastbereich in einem Netzwerk
Realtime-Kommunikation	[1]Echtzeitfähigkeit eines Systems, eine Aufgabe in einer bestimmte Zeit zu lösen.
Robustheit	Robustheit beschreibt die Fähigkeit eines Devices, den normalen Betrieb auch unter ungünstigen Bedingungen und/oder bei unerwartetem Input zu gewährleisten.
Router	Netzwerkgerät zur Weiterleitung von IP-Netzwerkpaketen zwischen zwei unabhängigen Subnetzen.
Safety	Bezeichnet die Betriebssicherheit eines Gerätes oder einem Geräteverbund. Dabei meint Betriebssicherheit dass während des Betriebs keine Gefahr für den Menschen entstehen darf.
Schutzziel	Schutzziele beschreiben die Elemente welche gesichert (im Sinne der Security) werden müssen
Schutzniveau	
Security Assessment	
SNMP - Simple Network Protocol	[1]Internet Standardprotokoll zum Management und zur Diagnose von Netzwerkkomponenten.
SPS - Speicher programmierbare Steuerung	Gerät zur Steuerung und Regelung eines IO-Systems eingesetzt werden kann
SSL - Secure Socket Layer	Netzwerkprotokoll zur sicheren Übertragung von Daten.
Stateful Inspection	Zustandsorientierte Paketprüfung für Pakete in einem Netzwerk. Es stellt eine erweiterte Form des Paketfilters dar.
Subnetz	Subnetz stellt ein Teilnetz im Netzwerk dar.
Supervisor	[1]Initiator von Steuerungs- , Inbetriebnahme- und Projektierungsaufgaben. Beispielsweise Engineering Station oder PC/PG, welches Daten von einem IO-Device lesen oder schreiben kann. Ein Supervisor ist nur temporär zugeschaltet und übernimmt keine aktive Rolle in einem IO-System.

Switch	Steuert die Layer-2 basierte Kommunikation in Netzwerken.
TCP - Transport and Control Protocol	[1]Überlagertes Protokoll von IP, um den Datenaustausch und die Fluss-Steuerung zu ermöglichen.
TLS - Transport Layer Security	Netzwerkprotokoll zur sicheren Übertragen von Daten.
Verfügbarkeit	[4]Die Wahrscheinlichkeit, dass ein Betrachtungsgegenstand in einem Zustand ist, in dem er unter vorgegebenen Bedingungen zu einem vorgegebenen Zeitpunkt oder während einer vorgegebenen Zeitdauer eine geforderte Funktion erfüllen kann.
Vertraulichkeit	[4]Vertraulichkeit ist die Eigenschaft, dass Daten oder die darin enthaltenen Informationen nur für autorisierte Benutzer zugänglich sind.
VLAN - Virtual Local Area Network	Logisches Teilnetz das port-spezifisch über einen Switch aufgebaut wird.
VPN - Virtual Private Network	Logische typischerweise gesicherte Schnittstelle zwischen zwei Netzwerken.
Whitelisting	Liste mit Elementen welche als vertrauenswürdig erachtet werden.
WLAN - Wireless Local Area Network	Kabelloses LAN

4.2 Abkürzungen

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 Vorwort

Die ethernetbasierte Kommunikation nimmt im Automatisierungsumfeld eine zunehmend zentrale Rolle ein. Die Vorteile liegen auf der Hand: neben der Nutzung von offenen und standardisierten IT-Technologien wie z.B. Wireless LAN oder Webserver liegt der Hauptvorteil vor allem in der damit möglichen durchgängigen Vernetzung. Allerdings steigt so auch die Gefahr von Zugriffsverletzungen und durch Schadsoftware, so dass damit einhergehend auch das Gefährdungspotenzial für die Automationsnetze neu bewertet und Sicherheitskonzepte entsprechend umgesetzt werden müssen.

Im Kontext der Automatisierungssysteme sollte ein Security Problem mindestens genauso betrachtet werden, wie irgendeine andere Störung des Normalbetriebes, das eine Fehlfunktion des Automatisierungssystems zur Folge hat und somit vermieden oder beseitigt werden muss.

Security ist kein punktuelles Thema. Die effektive Umsetzung eines Industrial Security Konzeptes erfordert die Mitwirkung sowohl von den Herstellern als auch den Anwendern und Betreibern von Automatisierungstechnik. Um ein gutes Maß an Sicherheit erreichen zu können, denn letztendlich müssen alle Einflussfaktoren zusammenwirken. Dazu gehören Prozesse, sichere Produkte und nicht zuletzt das nötige Security-Bewusstsein aller Beteiligten, beginnend beim Management, der IT- und Automatisierungsverantwortlichen bis hin zu jedem einzelnen Mitarbeiter.

Zu den Produktaspekten gehören die Robustheit, also die (passive) Fähigkeit eines Gerätes Angriffen oder deren Auswirkungen wie erhöhte Netzlast standzuhalten, z.B. durch Vermeidung von Schwachstellen. Weitere Punkte sind Security Funktionen wie einen Zugangsschutz, der unbefugte Zugriffe auf ein System, Netze oder Geräte verhindert aber autorisierte Zugriffe ermöglicht.

Ein Patentrezept, zum Schutz industrieller Anlagen gibt es allerdings nicht, da jede Anlage unterschiedliche Randbedingungen, individuelle Gefährdungen und andere Schutzziele besitzt. Aber es gibt bewährte Vorgehensweisen zum Aufbau eines effizienten Security Konzeptes.

Eine gute Security Architektur sollte auch die richtige Balance haben zwischen Nutzen und Aufwand. Absolute Sicherheit ist nicht erreichbar aber sie muss den Ansprüchen genügen und nicht tolerierbare Risiken auf ein akzeptables Maß absenken und dabei auch noch bezahlbar und handhabbar sein. Dies ist insbesondere in der industriellen Produktion wesentlich.

Die PROFINET Security Richtlinie ist ein Leitfaden, der aufzeigt, welche Punkte berücksichtigt werden sollten, um ein umfassendes Security Konzept in industriellen Umfeld auch speziell im Hinblick auf PROFINET aufzubauen.

6 Einleitung

In den vergangenen Jahren haben sich Automatisierungssysteme zur Unterstützung von Prozess- und Fertigungsabläufen von einzelnen, isolierten Computern mit proprietären Betriebssystemen und Netzwerken zu hochgradig vernetzten Systemen und Anwendungen entwickelt, in denen die weit verbreitete und allgemein bekannte Technologie der „offenen Systeme“ zu Anwendung kommt, zum Beispiel Microsoft® Windows™ und Netzwerkprotokolle wie TCP/IP.
Außerdem ist zu beachten, dass die heutigen Automatisierungssysteme mittlerweile in Unternehmenssysteme und andere Geschäftsanwendungen des Standorts sowie in konzernweite Kommunikationsnetzwerke integriert sind. Eine solche integrierte Architektur bietet erhebliche wirtschaftliche Vorteile. Die Sichtbarkeit der Aktivitäten auf der Werksebene (laufende Arbeiten, Status von Anlagen und Geräten, Produktionspläne) ist erhöht, wodurch bessere, durchgehende Informationssysteme aufgebaut werden können und die Entscheidungsfindung erleichtert wird. Der Informationsaustausch zwischen Fertigungssystemen und anderen Unternehmenssystemen ist direkter und erhöht die Reaktionsgeschwindigkeit der Unternehmen. Durch einheitliche Schnittstellen verringern sich die Gesamtkosten für Diagnose und Support, insbesondere durch

die nun mögliche Fernunterstützung der Produktionsprozesse. Durch den leichteren Zugriff auf Daten können Analysen durchgeführt werden, die Produktionskostensenkungen und Produktivitätserhöhungen ermöglichen. Darüber hinaus können durch die Fernüberwachung der Steuerungssysteme Probleme schneller behoben werden, wodurch die Support-Kosten sinken.
Spätestens seit dem Auftreten von spezialisierter Schadsoftware sind Fragen deutlich geworden, wie Security-Elemente in die neue Netzwerkumgebung und in Automatisierungssysteme integriert werden können. Welche Maßnahmen müssen ergriffen werden?
Security-Konzepte, die für Büro-IT entwickelt wurden, lassen sich nicht einfach auf Automatisierungsnetzwerke übertragen. Der Schutz von Automatisierungssystemen und -netzwerken darf nicht mit den PROFINET-bezogenen Anforderungen in Konflikt treten. Das Ziel der Security-Maßnahmen im Automationsbereich ist ein zuverlässiges und bedarfsorientiertes Automationsnetzwerk. Zudem muss sich bewusst gemacht werden, dass Automatisierungssysteme für möglichst hohe Leistung konzipiert werden, nicht für möglichst hohe Security. Zum Beispiel ist der Zugriff bei vielen Systemen nicht durch geeignete Authentisierungsmaßnahmen geschützt.
Ziel ist es nun die zentralen Schutzziele der Automatisierungswelt abdecken zu können.
Ein sicheres System soll die Vertraulichkeit, Integrität und Verfügbarkeit von Systemen und Daten gewährleisten, auch wenn es zu böswilligen Angriffen kommt.

Um die höchste angemessene Schutzebene für Automatisierungssysteme und Netzwerke zu erreichen, ist es unerlässlich, ein geeignetes Security-Management aufzubauen. Dieses Security-Management muss durch einen konsistenten Prozess folgendes berücksichtigen:
:

- Risikoanalyse einschließlich Festlegung von Gegenmaßnahmen zur Absenkung des Risikos auf ein angemessenes Niveau.
- Koordinierte organisatorische / technische Maßnahmen (Methodiken)
- Regelmäßige / ereignisbezogene Wiederholung

7 Herausforderungen der vernetzten Automatisierungswelt

Der zunehmende Einsatz von Informations- und Netzwerktechnik in der Automation kann schnell zu der Einschätzung führen, dass die für die IT Welt entwickelten Lösungen auch für vernetzte Produktionsanlagen und Automatisierungssysteme ausreichend sind und einfach auf die Produktionsumgebung übertragen werden können. Tatsächlich aber bestehen eine Reihe deutlicher Unterschiede zwischen der Business-IT und der Automatisierungswelt hinsichtlich der Anforderungen und der einsetzbaren Lösungen. Auf die wesentlichen Unterschiede wir im Folgenden näher eingegangen.

7.1 Unterschiedliche Leistungs- und Funktionsanforderungen

Bei typischen IT-Systemen steht der Datendurchsatz und die Zuverlässigkeit der Datenübertragung im Vordergrund; Verzögerungen und Jitter in der Datenübertragung sind tolerabel.
Dagegen gehören Verzögerungszeit und Jitter bei Automatisierungssystemen zu den leistungsbestimmenden Merkmalen der Echtzeitfähigkeit. Reaktionen sind zeitkritisch und Verzögerungen stellen ein ernsthaftes Problem dar.
Aufgrund der notwendigen Vielfalt von Automatisierungskomponenten oder Lösungen, müssen auch Geräte mit begrenzten Ressourcen berücksichtigt werden. Diese beinhalten daher häufig nicht die Security-Funktionen, wie man sie in typischen Rechnersystemen der Business-IT antrifft.

7.2 Mensch-Maschine-Interaktion

Technische Prozesse müssen in allen Situationen sicher geführt und bedient werden können. Auch in kritischen Situationen müssen die Automatisierungssysteme und Funktionen verfügbar bleiben. Daher dürfen Security-Maßnahmen, die Bedienbarkeit der Automatisierungslösung nicht behindern.

7.3 Security-Zielsetzungen

Eine zentrale Zielsetzung im Bereich der Business-IT ist der Schutz von Daten vor Verlust oder Modifizierung. Die geeigneten Security-Maßnahmen sind oft an den Server-Systemen (Zugriffskontrolle, Backup usw.) ausgerichtet. Bei Produktionslinien hingegen dominieren granulare Strukturen und Anwendungen, die in viele Unterkomponenten unterteilt sind.
Wenn man sich die Priorisierung der Zielsetzungen bei Business-IT und Automatisierungssystemen ansieht, erkennt man eine unterschiedliche Gewichtung.
Im Bereich der Business-IT-Systeme gibt es in der Regel die folgende Priorisierung der Security-Zielsetzungen:

(1) Vertraulichkeit
(2) Integrität
(3) Verfügbarkeit

Bei vielen Automatisierungssystemen ist die Priorisierung der Zielsetzungen gegenüber den Business-IT-Systemen hingegen meist anders:

(1) Verfügbarkeit
(2) Integrität
(3) Vertraulichkeit

Die Verfügbarkeit einer Automatisierungsanlage hat hier höchste Priorität. Dies ist vor allen Dingen für den Schutz von Mensch und Umwelt ein wichtiger Aspekt.

7.4 Verfügbarkeit und Zuverlässigkeit

Viele Fertigungsprozesse laufen kontinuierlich ab. Plötzliche Ausfälle von Systemen, die Fertigungsprozesse steuern, sind nicht akzeptabel. Vor der Inbetriebnahme sind umfangreiche Tests erforderlich, um hohe Verfügbarkeit für Fertigungs- und Steuerungssysteme sicherzustellen. Neben der Problematik von plötzlichen Ausfällen ist es bei vielen Steuerungssystemen so, dass sie nicht einfach ausgeschaltet und wieder gestartet werden können, ohne die Produktion zu beeinträchtigen. Die notwendige hohe Verfügbarkeit, Zuverlässigkeit und Wartbarkeit verringert die Einsetzbarkeit von IT-Maßnahmen wie dem Neustart eines Systems. Beta-Tests während des laufenden Betriebs sind bei vielen IT-Systemen möglich, doch Automatisierungssysteme müssen eine Qualitätssicherung durchlaufen. Infolgedessen können Security-Updates nicht immer zeitnah implementiert werden, da Software-Änderungen vor der Implementierung ausführlich getestet werden müssen. Häufig fehlen hierfür die erforderlichen Testumgebungen, da die vollständigen Systeme und Produktionssysteme für Testzwecke in der Regel wirtschaftlich nicht vertretbar sind.

7.5 Unterschiedlicher Fokus der Security-Architektur

Verfügbarkeit und Zuverlässigkeit sind bei Automatisierungsanlagen entscheidende Faktoren. Um die Automatisierungsaufgabe zu bewältigen, agieren typischerweise mehrere Automatisierungsgeräte im Verbund. Damit ist auch der ununterbrochene, fehlerfreie und gleichzeitige Betrieb aller Geräte ein wichtiges Kriterium. Fällt eines dieser Geräte aus, kann dies einen unmittelbaren Produktions- bzw. Systemausfall zur Folge haben.
Ähnlich wie im IT-Umfeld gibt es zwar auch in der Automatisierung Redundanzmechanismen. Diese kommen allerdings aus Kostengründen vor allem dort zum Einsatz, wo ein Ausfall eines Gerätes gravierenden Schaden an der Anlage oder dem Produkt zur Folge hätte.
Im Security-Konzept muss die Automatisierungsanlage daher immer als Gesamtanlage betrachtet werden, denn diese muss insgesamt zuverlässig und dauerhaft funktionieren.

7.6 Risiken und Safety-Anforderungen

Die Anforderungen an die funktionale Sicherheit (Safety) von Produktionsanlagen und die damit verbundenen Risiken unterscheiden sich gravierend von den Risiken, die üblicherweise von der Business-IT betrachtet werden. Risikoanalysen sind daher nicht übertragbar und führen in der Regel auch zu anderen Bewertungen und damit zu verschärften Security- Maßnahmen.

7.7 Firmware-Update / Patch-Management

Die Verfügbarkeit von Komponenten und Automatisierungssystemen ist von besonderer Wichtigkeit. Denn fehlerhafte Komponenten führen in der Regel zur Betriebsunterbrechung und damit zu einem Produktionsstillstand. Insbesondere bei der Installation von Firmware-Updates oder Patches müssen die betroffenen Komponenten zumindest neu gestartet werden. Nach dem Neustart einer Komponente mit einem geänderten System kann nicht sichergestellt werden, dass die Komponente das gleiche Verhalten an den Tag legt wie vor dem Update bzw. vor der Modifikation. Zudem kann es in der Prozessautomation vorkommen, dass an einzelnen Modulen zuerst Änderungen vorgenommen werden müssen, um Updates oder Patches installieren zu können. Auch können einzelne Module/Komponenten unabhängig voneinander geändert werden. Je nach Systemarchitektur müssen zusammenhängende Hardwareelemente gemeinsam getauscht werden.
Firmware-Updates können in der Automatisierungswelt somit nur unter erschwerten Bedingungen durchgeführt werden und bedürfen besonderer Planung.

8 PROFINET spezifische Anforderungen

8.1 PROFINET-Architektur

Die PROFINET-Protokollsuite beinhaltet unterschiedliche Arten der Adressierung: MAC-basierte Adressierung für Layer 2-Kommunikation und IP-basierte Kommunikation für Layer 3. Bei dieser Art der Architektur sind Automatisierungssysteme eher weniger proprietär. Bei Verwendung von TCP/IP lässt sich PROFINET ohne zusätzliche Vorkehrungen im Rahmen von IP-basierten Anwendungen und Netzwerken vollständig integrieren. Es können auch Systeme integriert werden, die beispielsweise Qualitätsdaten an ein Server-System oberster Ebene übertragen. Genau diese Integrationsfunktion für Echtzeit- und Nicht-Echtzeit-Anwendungen gehört zu den zentralen Vorteilen der PROFINET-Technologie. Diese verschiedenen Kommunikationsrelationen müssen im Rahmen der Security-Konzepte berücksichtigt werden.
Bei PROFINET liegt folgende Protokollverteilung vor:

(1) PROFINET-IO Echtzeit Kommunikation (Prozessdaten, Layer 2-based), z.B. RT/IRT

(2) PROFINET-Dienste (Layer 2-based), z.B. DCP zur Anforderung oder Festlegung von Gerätenamen

(3) PROFINET-Dienste (Layer 3-based), z.B. Read-/Write Dienste, z.B. zum Lesen und Schreiben von Data Objects u.a. während der Parametrierung von Geräten

(4) Netzwerk-Management und anwendungsbezogene Dienste (Layer 3-based), z.B. SNMP

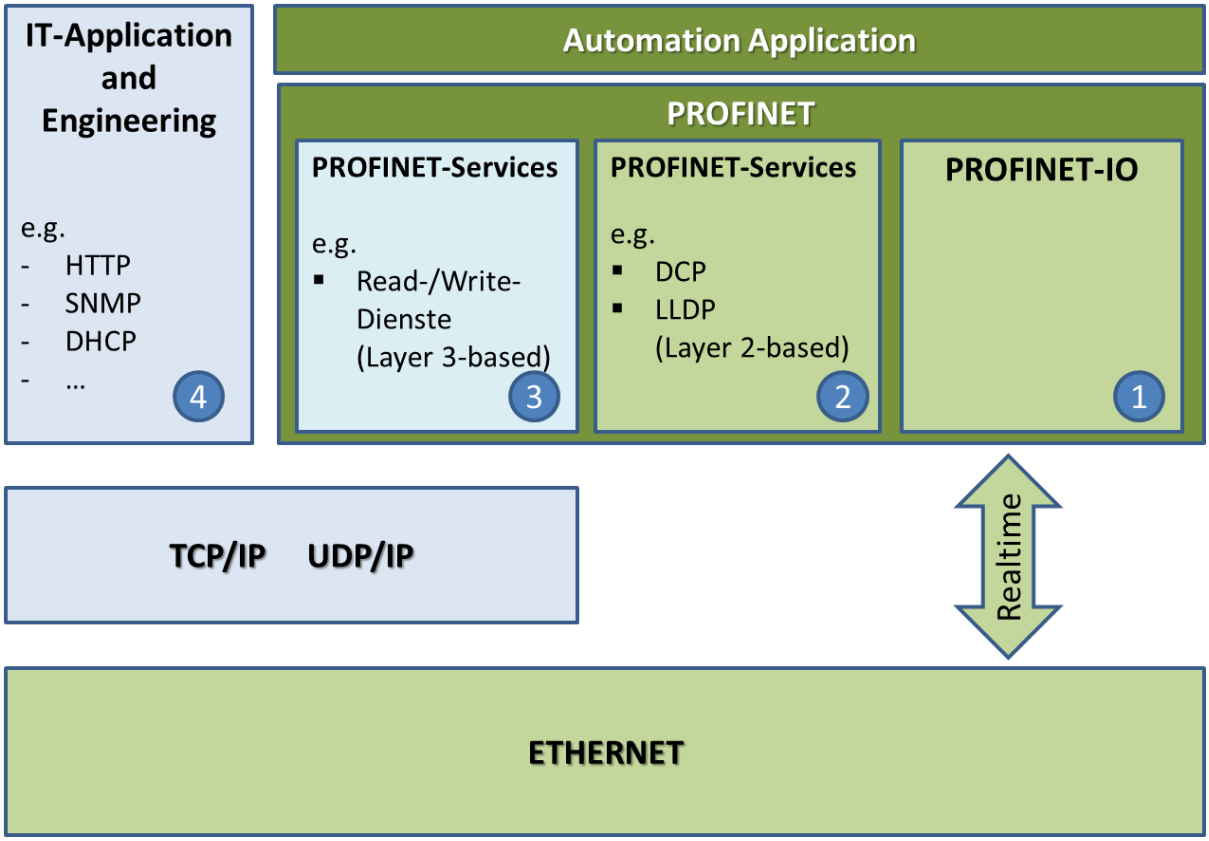

Bild 1 - PROFINET Protokolle

8.1.1 Switch-basierte Netzwerke

Durch den Einsatz von dedizierten und in IO-Devices integrierten Switchen ermöglicht PROFINET eine durchgängig Switch-basierte Netzwerkinfrastruktur mit Stern-, Ring-, Baum- und Linien-Topologien. PROFINET IO-Devices verfügen damit sowohl über Eigenschaften und Funktionen einer Netzwerkinfrastrukturkomponente als auch über automatisierungstechnische Funktionen eines Feldgerätes bzw. Sensors/Aktors. Umgekehrt verfügen dedizierte Switche über Eigenschaften von IO-Devices und unterstützen damit automatisierungstechnische Diagnosefunktionen des IO-Controllers.
Ein PROFINET-Netzwerk ist somit kein reiner 'Netzwerk-Dienst' sondern ein integriertes Kommunikationssystem innerhalb einer Automatisierungszelle oder – Anlage.

Konsequenzen:

- *IO-Controller übernehmen Funktionen von Netzwerkmanagementsystemen*
- *externe Netzwerkmanagement-Systeme können auf PROFINET-Devices zugreifen (z.B. SNMP)*

Es ergibt sich eine Mischung aus Realtime-Kommunikation und weiteren Diensten.

- Dienste können sowohl innerhalb einer PROFINET-Domäne genutzt werden, d.h. von PROFINET-Teilnehmern (integrated) und von Engineering-Systemen als auch von übergeordneten Systemen (z.B. Netzwerkmanagement-Systemen).

8.1.2 PROFINET Domäne

Aufgrund der Integrationsfähigkeit von PROFINET kann die Netzwerkstruktur und die Größe der verwendeten Subnetze sehr unterschiedlich ausfallen. Aufgrund der PROFINET-IO-Echtzeit-Kommunikation und der Layer-2-basierten PROFINET-Dienste (DCP, LLDP) sind folgende Domänen zu unterscheiden:

- Controller-Domäne: Logischer Verbund eines IO-Controllers mit den zugehörigen IO-Devices
- Broadcast-Domäne: Netzwerkbereich, in dem IO-Controller und IO-Devices, über Layer-2-basierte IO-Kommunikation und -Dienste erreichbar sind
- PROFINET-Domäne: Anordnung mehrerer Controller, die voneinander unabhängig oder im logischen Verbund in einem Subnetz einer Broadcast-Domäne betrieben werden.

Die Dimensionierung und Segmentierung von PROFINET-Domänen ist eine zentrale Planungsaufgabe, von deren Lösung die Höhe der im Betrieb auftretenden Multicast- und Broadcast-Lasten entscheidend abhängig ist. Gleichzeitig ergibt sich hieraus die Anforderung an PROFINET-Teilnehmer, mit entsprechenden Kommunikationslasten betriebssicher umgehen zu können. Dies ist einer der wesentlichen Gründe dafür, dass bei der Zertifizierungsprüfung von PROFINET-Geräten entsprechende Netzlasttests durchgeführt werden und die Robustheit der Geräte damit validiert wird. Einzelheiten zu den Anforderungen an Robustheit sowie zum Konzept und zur Funktion des Netzlasttestes werden in 7.3.4 dargestellt.

8.1.3 Funktionen zur Gewährleistung der Bedienerfreundlichkeit

Das Engineering-Konzept von PROFINET setzt auf einen funktionsorientierten und offenen Architekturansatz und verfügt u.a. über folgende Architekturmerkmale:

- Adressierung über Gerätenamen, um unabhängig von MAC-Adressen und IP-Adressen eine eindeutige Adressierung der PROFINET-Geräte zu gewährleisten (wichtig u.a. für den problemlosen Gerätetausch)
- Beschreibung der gerätespezifischen Funktionen und Parameter über Dateien (GSDML-Dateien)
- Diagnosekonzept (Gerätediagnose, Netzwerkdiagnose, ...)
- Zyklische Layer2-Kommunikation für die Realtime-Nutzdaten
- azyklische Layer2- und Layer 3-Kommunikation für die Konfiguration der PROFINET-Teilnehmer

Es nutzt dabei neben den PROFINET-spezifischen Protokollen offene Kommunikationsstandards wie z.B. LLDP und SNMP.

Um eine möglichst einfache Konfiguration der PROFINET-Teilnehmer bei der Inbetriebnahme und der Instandhaltung (z.B. Gerätetausch) zu ermöglichen, sieht das Architektur-Konzept von PROFINET vor, dass IO-Controller und Supervisor-Stationen die Konfigurationsparameter der IO-Devices parametrieren und modifizieren können (z.B. den Gerätenamen / Device Name).

8.2 PROFINET Protokolleigenschaften

PROFINET-Geräte sind ausgerichtet auf Zuverlässigkeit und Echtzeit-Kommunikation. Zusätzlich spielen Usability-Aspekte eine tragende Rolle im Technologie-Design. Die Verwendung des DCP-Protokolls gehört hier beispielsweise dazu, welches zur Vergabe von Gerätenamen verwendet wird. Die Implementierung von Security-Funktionen und Usability-Aspekten für den täglichen Umgang mit der Technologie müssen sich also vereinen lassen.
PROFINET berücksichtigt bereits Security-verbessernde Maßnahmen. Dazu zählt die FrameID, welches dazu dient Kommunikationsbeziehungen zu erkennen und identifizieren zu können. Auch der CycleCounter stellt in gewisser Weise eine Security-Funktion dar, da hierüber der Austausch der IO-Daten überwacht wird.

Ziel der PROFINET-spezifischen Security-Eigenschaften ist es, die Verfügbarkeit und Betriebssicherheit der Produktionsanlagen zu verbessern. Ein wichtiges Merkmal die Robustheit der PROFINET-Geräte gegen hohe Netzlasten. Die Durchführung von Netzlasttests, den sog. Security Level1 Tests ist daher ein wichtiger Bestandteil bei der Zertifizierungsprüfung (siehe 7.3.4).
Darüber hinaus verfügen PROFINET-Geräte jedoch über keine inherenten (intrinsichen) Security-Schutzfunktionen im Sinne einer Endgerätesicherheit. Gezielte Angriffe auf PROFINET-

Geräte müssen daher durch das Betriebskonzept und zusätzliche Schutzmaßnahmen abgewehrt und verhindert werden.

8.3 Anforderungen für den sicheren Betrieb von PROFINET

Im folgenden werden einige Punkte und Randbedingungen aufgeführt, die speziell bei der Etablierung eines Security Konzeptes im PROFINET-Umfeld zu beachten sind. Denn es reicht nicht, nur Maßnahmen einzurichten, die geeignet sind den Bedrohungen begegnen zu können. Diese Maßnahmen dürfen auch elementar wichtige Funktionen von PROFINET nicht beeinträchtigen oder gar aushebeln. Das wäre kontraproduktiv und wenig sinnvoll. Es ist daher nützlich, die wesentlichen Anforderungen des PROFINET Betriebes zu kennen, um diese bei der Auswahl der Security Mechanismen berücksichtigen zu können und ein optimales Security Konzept erstellen zu können.

8.3.1 Security für Systeme ohne eigene Security-Funktionen

Es gibt mehrere Gründe dafür, dass Automatisierungssysteme zur Zeit nicht über eigene, autonome Security-Funktionen verfügen. Wie bereits erläutert wurde, verfügen manche Automatisierungssysteme nicht über die technische Leistungsfähigkeit, die für Security-Funktionen nötig ist. Bei bereits bestehenden Systemen werden oft aus wirtschaftlichen Gründen keine Security-Funktionen integriert. In vielen Fällen verhindern diese Anforderungen die Installation oder rechtzeitige Aktualisierung der Security-Maßnahmen. Das PROFINET-Security-Konzept sollte jedoch in all diesen Fällen einen angemessenen Schutz bieten.

8.3.2 Echtzeit-Betrieb

Das PROFINET-Security-Konzept darf die Echtzeit-Anforderungen nicht beeinträchtigen. Darüber hinaus darf auch die oft zeitkritische Reaktionszeit bei der Interaktion zwischen Mensch und Maschine nicht durch Security-Funktionen beeinträchtigt werden. Ein Beispiel hierfür wäre die Freischaltung eines Not-Halt-Schalters mittels einem Schlüssel oder gar einem Passwort. Solche vorgeschalteten Sicherheitsmechanismen würden in großem Wiederspruch zur Funktionalität stehen.

8.3.3 Transparente und kosteneffiziente Integration

Das PROFINET-Security-Konzept sollte eine transparente und kosteneffiziente Integration der Security in eine industrielle Umgebung unterstützen. Die Integration von Security-Funktionen ohne großen Konfigurationsaufwand wird zu erhöhter Akzeptanz der Lösung führen. Hierbei muss zusätzlich bedacht werden, dass Automatisierungsexperten in der Regel keine Security-Experten sind. Kosteneffizienz kann vor allen Dingen durch die Integration von Security-Maßnahmen erzielt werden, die den Schutz größerer Gruppen von Automatisierungslösungen gleichzeitig bieten. Nur so kann ein akzeptiertes Security-Konzept für PROFINET realisiert werden.

8.3.4 Robustheit

Robustheit bezieht sich auf die Fähigkeit der Geräte auch temporären außerordentlichen Kommunikations-Lasten Stand zu halten. Robustheit beschreibt somit die Fähigkeit eines Devices, den normalen Betrieb auch unter ungünstigen Bedingungen und/oder bei unerwartetem Input zu gewährleisten.
Um diese Art der Robustheit zu prüfen wurde die Zertifizierungsprüfung für PROFINET-IO Geräte um den sogenannten Security-Level-1 Test erweitert. Dieser Test simuliert praxisrelevante Kommunikationslasten und setzt die PROFINET-Geräte dieser Last aus. Aus Sicht der Geräte ist es dabei das Ziel, die PROFINET-Dienste aufrecht zu erhalten. Oder, in außerordentlich hohen Last-Situationen, die Kommunikation einzustellen und danach selbstständig wieder den Kommunikationsbetrieb aufzunehmen.

9 Etablierung eines Security Management Prozesses

Die Herangehensweise um Automatisierungsnetze abzusichern soll in den nachfolgenden Kapiteln näher beschrieben werden. Diese Beschreibung orientiert sich an der von der VDI veröffentlichten Richtlinie 2182. Diese Richtlinie beschreibt ein prozessorientiertes

Vorgehensmodell, welches durch zyklische Anwendung bei der Bestimmung und Validierung von möglichen Sicherheitslösungen unterstützen soll. Bild 2 zeigt beispielhaft ein Vorgehensmodell anhand der VDI 2182 Richtlinie.

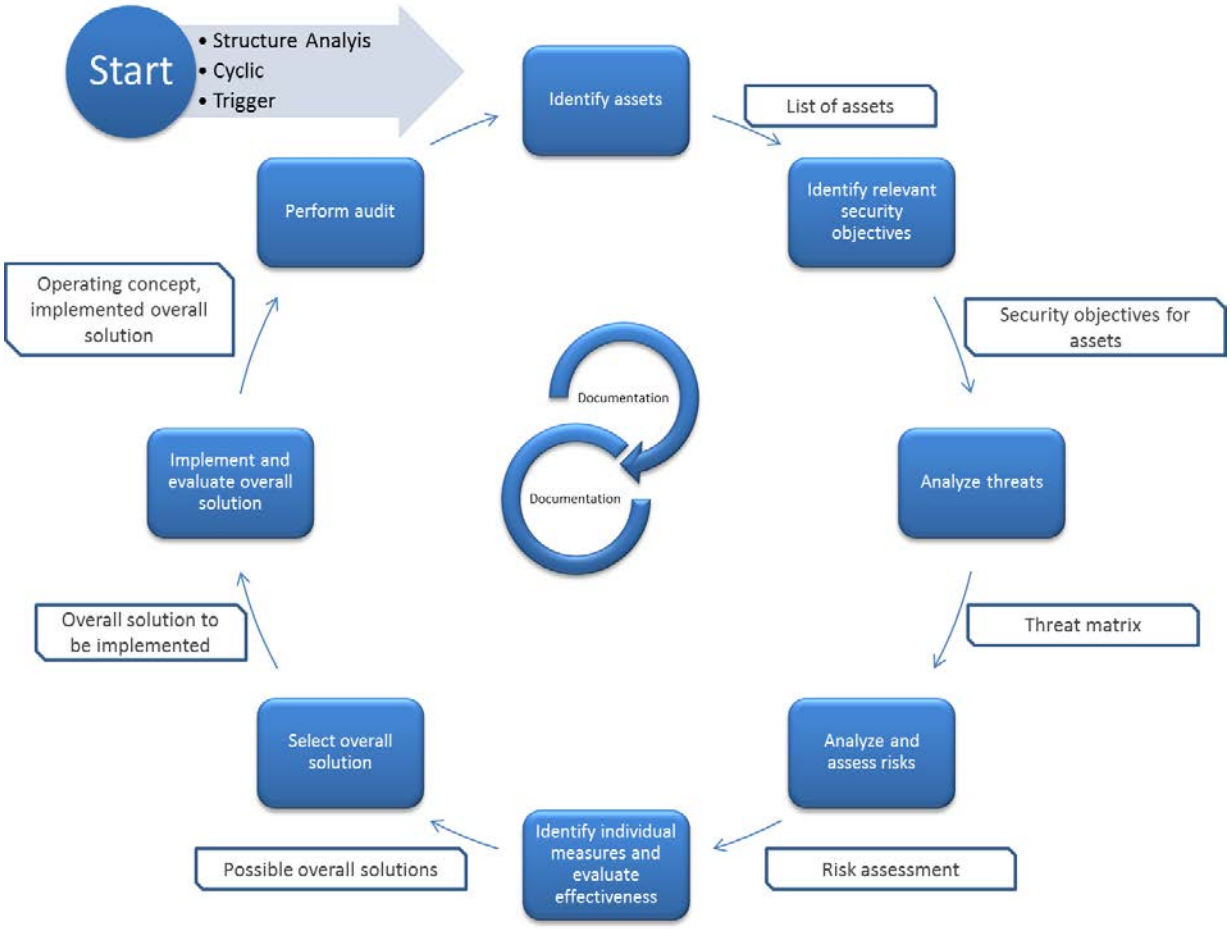

Bild 2 - Vorgehensmodell nach VDI2182

Grundsätzlich beschreibt das Vorgehensmodell einzelne Schritte die zyklisch oder trigger-basiert durchlaufen werden sollen. Jeder einzelne Schritt benötigt dabei Eingangsinformationen und generiert jeweils ein Ergebnis, was wiederum die Eingangsinformation des nächsten Schrittes darstellt.
Die grundlegenden Schritte dieses Vorgehensmodells sind dabei die Identifikation der Assets und den damit verbundenen Schutzzielen, sowie die Bewertung des Risikos das von den identifizierten Bedrohungen ausgeht. Wie hoch ein Risiko letztendlich ist, ist individuell für jeden Anwendungsfall zu definieren und neu zu bewerten.
Diese Schritte werden in den nachfolgenden Kapiteln in folgende unterteilt:

» Initiierung des Prozesses

» Sammeln der Anforderungen

» Definition von Maßnahmen

» Umsetzung der definierten Maßnahmen

» Aufrechterhaltung und ggf. Verbesserung bestehender Mechanismen

9.1 Initiierung des Prozesses

Bevor damit begonnen werden kann Sicherheitsmechanismen zu planen und zu realisieren muss zuvor der organisatorische Rahmen definiert werden. Dazu zählt beispielsweise auch die Bereitstellung von finanziellen sowie personellen und zeitlichen Ressourcen. Weiterhin muss das Vorgehen genau geklärt und somit ein Leitfaden für den eigentlichen Prozess geschaffen werden.
Die Notwendigkeit eines Sicherheitskonzeptes ergibt sich nicht nur aus den Bedürfnissen eines Unternehmens, sondern auch durch rechtliche Randbedingungen. Dazu zählen beispielsweise gesetzliche Gegebenheiten, vertragliche Verpflichtungen wie auch versicherungstechnische Anforderungen. Durch diese Rahmenbedingungen wird nicht nur ein Sicherheitskonzept gefordert, sie wirken sich vielmehr auch auf die Ausgestaltung von Sicherheitsmaßnahmen aus. Eine grundlegende Voraussetzung für die Definition von Sicherheitsmechanismen ist also die Sichtung bestehender Richtlinien, Vorschriften und Normen um die Anforderungen später genau klären zu können.
Da Security als Prozess gelebt werden muss und in die Unternehmenskultur integriert werden soll, müssen dafür auch Rollen und somit Verantwortlichkeiten geklärt und benannt werden. Die VDI Richtlinie 2182 beschreibt beispielsweise folgende Rollen mit den zugehörigen Verantwortlichkeiten und Aufgabengebieten:

- Securityexperte
  Der Securitsexperte kennt die Möglichkeiten und die Einsatzfelder von diversen Security-Lösungen

- Systemexperte
  Der Systemexperte kennt die eingesetzte Kommunikationstechnologie, z.B. PROFINET.

- Anwendungsexperte
  Der Anwendungsexperte kennt die Anlage aus Anwendersicht. Er weiß z.B. welche Zugänge benötigt werden oder welche Kommunikationsverbindungen für den Betrieb bestehen müssen.

- Koordinator
  Koordiniert das Vorhaben und den Informationsfluss

Je nach Unternehmensstruktur und –größe können diese Rollen auch unterschiedlich benannt oder bereits definiert und besetzt sein.

Werden die einzelnen Schritte der Initiierung betrachtet, so ergeben sich folgende Elemente:

» Sensibilisierung des Managements

  - Darstellung der Sicherheitsrisiken und damit verbundene Kosten
  - Rechtliche Ansprüche / Ansprüche der Versicherung / Notwendige Zertifizierungen aufzeigen
  - Vorteile
  - Vorgehen / Lösungsansatz

» Organisatorische Rahmenbedingungen schaffen

  - Klärung der finanziellen Möglichkeiten
  - Klärung der zur Verfügung stehenden Ressourcen (personell und zeitlich)
  - Benennung der Rollen
  - Besetzung der Rollen
  - Definition der Zuständigkeiten

- Definition des Leitfadens
- Genaue Definition und Abgrenzung des Betrachtungsgegenstandes

Ergebnis

- Zustimmung und Verständnis des Managements eingeholt
- Rollen und Verantwortungen geklärt
- Finanzielle Rahmenbedingungen geschaffen
- Leitfaden für das weitere Vorgehen erstellt

9.2 Strukturanalyse

Um eine Anforderungssammlung so konkret wie möglich durchführen zu können, sollte zuerst eine Strukturanalyse durchgeführt werden. Dabei sollten mindesten folgende Punkte ermittelt werden:

» Benötigte Anwendungen und Dienste

» Verwendete IT-Systeme

» Notwendige Kommunikationsverbindungen

» infrastrukturelle Gegebenheiten

» bestehender Datenfluss

» gegebene Schnittstellen

» Notwendige Zugriffe

Diese Ist-Analyse bildet die Grundlage für eine genaue Definition der Anforderungen die an das spätere Sicherheitskonzept gestellt werden.

Ergebnis

- Übersicht über alle Anwendungen in dem Automatisierungsnetzwerk
- Übersicht aller eingesetzten IT-System, z.B. Betriebssysteme auf Panel-PC's
- Alle Kommunikationsverbindungen innerhalb des Netzwerkes und alle Kommunikationsverbindungen zu anderen Netzwerken, z.B. Daten an Qualitätsdatenserver schicken
- Notwendige Schnittstellen, z.B. für Servicetechniker
- Übersicht über alle Dienste inkl. dafür verwendeter Ports
- Übersicht aller Schnittstellen zu beispielsweise übergeordneten Systeme

9.3 Anforderungssammlung

Nachdem eine "Bestandsaufnahme" durchgeführt wurde, kann mit der konkreten Sammlung der funktionalen Anforderungen begonnen werden. Eine funktionale Anforderung kann beispielsweise der Remote-Zugriff von Servicetechnikern sein. Das Ziel ist demnach die Beantwortung der Frage „Was soll geschützt werden?"
Zu den Anforderungen gehört auch die Sammlung von relevanten Schutzzielen. Schutzziele definieren hierbei die Ziele, welche durch das Sicherheitskonzept erreicht werden sollen und können als übergeordnete Anforderungen verstanden werden.

Ergebnis
Das Ergebnis dieses Schrittes ist eine Übersicht aller schützenswerten Elemente inklusive der Schutzziele. Zusätzlich werden hier auch die rechtlichen Rahmenbedingungen aufgeführt.

9.4 Anforderungsbewertung

Nachdem alle Anforderungen gesammelt und alle schützenswerten Elemente erfasst wurden, müssen diese noch bewertet werden um eine Wirtschaftlichkeit des späteren Sicherheitskonzeptes zu gewährleisten. Um diese Bewertung durchführen zu können, müssen die dafür möglichen Bedrohungen erfasst werden. Ziel ist es daher die relevanten Bedrohungen für die bereits definierten Anforderungen zu erfassen.
Eine mögliche Bewertungsmethode der Anforderungen ist in der Richtlinie VDI 2182 beschrieben und kann als Vorgehensmodell verwendet werden. Auch das “IT-Grundschutz-Profil für das produzierende Gewerbe“ das vom BSI veröffentlich wurde beschreibt eine Bewertungsmethode. International ist eine entsprechende Beschreibung in der IEC 62443-2-1 und ISA99 2-1 verfügbar.

Ergebnis
Gegenüberstellung von Anforderungen und Bedrohungen

9.5 Risikoanalyse und Bewertung

Die Risikoanalyse dient der Bewertung der zuvor dokumentierten Anforderungen bzw. den möglichen Bedrohungen. Dabei werden die Risiken qualitativ klassifiziert. Ebenso muss die Akzeptanz der Risiken bewertet werden. Nicht jedes Risiko stellt ein reales Risiko für den jeweiligen Anwendungsfall dar.
Ein Risiko kann dadurch bewertet werden, indem das Produkt aus Eintrittswahrscheinlichkeit und der daraus resultierenden Schadenshöhe ermittelt wird.

Ergebnis
Ergebnis der Risikobewertung ist die Identifizierung der nicht tolerierbaren Risiken für die Schutzmaßnahmen ergriffen werden müssen.

9.6 Definition von Maßnahmen

Nachdem nun alle notwendigen Faktoren betrachtet und bewertet wurden, kann mit der Definition der Maßnahmen begonnen werden.
Grundsätzlich kann zwischen

» organisatorischen und

» technischen Maßnahmen

unterschieden werden. Dabei müssen die definierten Maßnahmen aus den zwei Kategorien aufeinander abgestimmt werden, da diese nur im Verbund zu einem sinnvollen und wirksamen Schutz verhelfen. Technische Maßnahmen benötigen meist auch begleitende organisatorische Maßnahmen, denn was nützen z.B. komplizierte Passwörter, wenn nicht geregelt und überwacht wird, dass diese nicht offen zugänglich sind. Andererseits können bestimmte Sicherheitsziele auf unterschiedliche Weise erreicht werden; manchmal auch wahlweise mit einer organisatorischen oder technischen Maßnahme. Wenn beispielsweise Switche sich in abgesperrten Schaltschränken befinden müssen die Switchports nicht notwendigerweise über Portsecurity Mechanismen abgesichert sein, damit unbefugte Zugriffe verhindert werden können. Eine Kombination beider Maßnahmen wäre natürlich am effektivsten.
Grundsätzlich empfiehlt es sich, bei vielen Verboten auch Alternativen zu schaffen. Denn viele Verbote verleiten auch zum Umgehen von Sicherheitsmechanismen. Ziel sollte es sein ein Konzept zu schaffen, welches im Idealfall keine Einschränkungen für die Mitarbeiter bedeutet und nach Möglichkeit ohne spürbare Auswirkungen realisiert werden kann.

9.6.1 Organisatorische Maßnahmen

Nachdem eine erfolgreiche Risikoanalyse durchgeführt wurde gilt es nun die definierten Schutzmaßnahmen zu realisieren. Im ersten Schritt sollte der Umgang und die Etablierung von Security im Unternehmen angestrebt werden. Diese Maßnahme bildet die Basis für erfolgreiche Schutzmaßnahmen. Nur wenn diese in einem kontinuierlichen Prozess gelebt werden, kann ein langfristiger Schutz erzielt und gehalten werden. Das bedeutet jedoch auch die Klärung u.a. folgender Fragestellungen:

- In welchen Bereichen müssen Schulungen durchgeführt werden?
- Wie können Mitarbeiter sensibilisiert werden?
- Wer sind die Ansprechpartner und für welche Themen?
- Gibt es einen klaren Geltungsbereich des zu erstellenden Securitykonzeptes? (Übergabepunkt/Schnittstelle zur übergeordneten IT-Infrastruktur klären)

Die Basis für ein solides Security Management bilden außerdem klare Richtlinien. Dazu zählen beispielweise

- Definition der Rollen die später die Verantwortlichkeit für Security-Angelegenheiten tragen
- Definition von Richtlinien für ein einheitliches Vorgehen
- Definition von Sanktionen bei Nichteinhaltung von Richtlinien
- Kommunikation und Dokumentation von Security-relevanten Vorkommnissen (Stichpunkt Logging und Änderungsmanagement)
- Erstellung von Policies
- Richtlinien für den Umgang mit Passwörtern
- Richtlinien für den Umgang mit mobilen Geräten innerhalb und vor allen Dingen außerhalb der Produktionsebene
- Richtlinien für den Umgang mit Fremdpersonal wie beispielsweise Servicetechnikern und deren Zugriffe auf das Produktionsnetzwerk
- Richtlinie für die Entsorgung, den Tausch oder der Archivierung von bestehenden Komponenten

Ziel ist somit die Erzeugung eines Leitfadens für den Security-Prozess als solchen.
Das Ergebnis stellt eine Definition der Maßnahme dar, auf Basis dieser die Mittel für die spätere Implementierung gewählt werden können.
Nur durch diese grundsätzlichen Regelungen können spätere technische Maßnahmen wirksam realisiert werden.

9.6.2 Technische Maßnahmen

Die organisatorischen Maßnahmen bilden die Grundlage für ein angemessenes Security-Konzept, die technischen Maßnahmen stellen hierbei den Kern der Realisierung bzw. des Konzeptes dar. Je nach Bedrohungsart können verschiedenste technische Maßnahmen ergriffen werden.
Durch die Realisierung verschiedenster Maßnahmen und den Einsatz unterschiedlichster technischer Komponenten, entwickelt sich eine vollständige Security-Lösung. Nur im Verbund können technische Maßnahmen einen hohen Sicherheitsschutz bieten, denn einzelne Komponenten stellen in der Regel für potentielle Angreifer keine Herausforderung dar, sondern es sind die verschiedensten Lösungen im Verbund.

9.6.2.1 Physikalische Schutzmaßnahmen

Physikalische Maßnahmen beschreiben die Abschottung von Systemen und/oder Automatisierungsanlagen und -bereichen vor unbefugtem Zugriff/Zutritt. Die einfachste Form einer physikalischen Schutzmaßnahme stellt das Verwenden von abschließbaren Schaltschränken dar.
Doch auch der Zutritt zu Produktionsbereichen sollte mit Zugangsberechtigungen geregelt werden. Dies kann auf verschiedene Art und Weise realisiert werden. Angefangen von Pförtnern am Werkseingang oder einer Eintrittskontrolle zu bestimmten Produktionsbereichen über

spezielle Schlösser und Kartenlesegeräte und sogar Kameraüberwachung. Diese Maßnahmen können dazu beitragen, das Betreten des Produktions- oder Werksgeländes von Unbefugten besser unter Kontrolle zu halten. Dadurch lässt sich der Verlust von vertraulichen Informationen einschränken. Zusätzlich können durch das Einbauen kritischer Komponenten in abgeschlossene Bereiche Beschädigungen oder Veränderungen an Produktionseinrichtungen verhindert werden.
Durch die Umsetzung physikalischer Maßnahmen kann mit relativ einfachen Mitteln dazu beigetragen werden die Anlagensicherheit entscheidend zu erhöhen.

9.6.2.2 Netzwerk-infrastrukturelle Maßnahmen

Der durchgängige Einsatz von Ethernet auf allen Unternehmensebenen vom Office bis zum Produktionsbereich vereinfacht die Integration und ermöglicht einen direkten Datenaustausch zwischen allen Komponenten den Unternehmensnetzes. Flache Netzwerkstrukturen erleichtern/vereinfachen dabei die Kommunikation von Systemen und Komponenten. Sie stellen aber für die Verfügbarkeit, die Stabilität und die Sicherheit des Netzwerkbetriebes eine große Herausforderung dar, da bereits ein einzelner Zugang zum Netz ausreicht, um alle Teilnehmer zu erreichen und daher für Angriffe wenig Schutz bieten. Durchgängige, flache Netzwerkstrukturen stellen daher ein nicht unerhebliches Sicherheitsrisiko dar.

Einen entscheidenden Beitrag zu sicheren Automatisierungsnetzwerken tragen daher infrastrukturelle Maßnahmen bei. Hierzu zählt beispielsweise die funktionale Aufteilung der Netzwerke in kleinere und physikalisch unabhängige Zellen.

9.6.2.3 Endgerätesicherheit

Um Schwachstellen bzw. Sicherheitslücken in einem Netzwerk zu minimieren, empfiehlt es sich auch die jeweiligen verbauten Komponenten weitestgehend sicherer zu machen. Zu einem Gerät zählt dabei nicht nur die Hardware, sondern auch die Applikationen, welche sich auf dem Gerät befinden.
Dies kann durch die gezielte Deaktivierung nicht benötigter Dienste und Anwendungen realisiert werden. Dazu zählt auch die Deaktivierung von nicht verwendeten Benutzeraccounts.
Grundlegende Voraussetzung für dieses Vorhaben ist eine aussagekräftige Dokumentation des Herstellers zu security-relevanten Eigenschaften des Gerätes, z.B. welche Dienste unterstützt werden oder ob eine Benutzerverwaltung angeboten wird.
Mit dem Vorliegen dieser Informationen wird es für den Benutzer einfacher nicht benötigte Dienste abzustellen oder bestehende Default-Passwörter und Benutzer zu ändern oder gar zu deaktivieren.

Ergebnis

Einzelmaßnahmen, welche zur Risikoreduzierung beitragen.

9.7 Einzelmaßnahmen erfassen und bewerten

Ein Gesamtkonzept setzt sich aus der Kombination mehrerer Einzelmaßnahmen zusammen. Nachdem diese Einzelmaßnahmen gesichtet und erfasst wurden, können diese nun bewertet und zu einem einheitlichen Konzept verbunden werden. Nur die Einzelmaßnahmen in systematischer Verbindung zueinander ergeben ein wirkungsvolles und effektives Sicherheitskonzept, das zum Erreichen der definierten Ziele führt.

Ergebnis
Übersicht über alle Schutzmaßnahmen die zur Risikoreduzierung beitragen. Ein wichtiger Aspekt ist hier auch die Übersicht der Kosten, die durch eine Implementierung / Realisierung entstehen.

9.8 Umsetzung definierter Maßnahmen

Nach einer erfolgreichen Erstellung des Sicherheitskonzeptes kann nun mit der Realisierung der definierten Maßnahmen begonnen werden.

Ergebnis
Alle definierten Maßnahmen, sowohl organisatorischer als auch technischer Natur wurden umgesetzt.

9.9 Wirksamkeit der Maßnahmen prüfen

Nachdem alle Schutzmechanismen implementiert wurden, muss geprüft werden ob das gewünscht Schutzniveau erreicht werden konnte. Dazu empfiehlt sich ein Audit, welches im Idealfall von einer unabhängigen Instanz durchgeführt wird. Auch die Durchführung eines Security Assesment sollte an dieser Stelle in Betracht gezogen werden. Damit eine vollständige Prüfung durchgeführt werden kann muss das zuvor erstellte Gesamtkonzept als Dokument vorliegen. Nur so kann geprüft werden ob alles Geplante auch realisiert wurde und die gewünschte Risikoreduzierung eingetreten ist.

Ergebnis
Das Ergebnis dieses Audits gibt Auskunft ob und wo aufgrund nicht oder nur unzureichend umgesetzter Maßnahmen noch ein Handlungsbedarf besteht.

9.10 Schulung und Sensibilisierung der Mitarbeiter

Die Umsetzung eines Securitykonzeptes und das Betreiben eines solchen setzen voraus, dass alle Mitarbeiter das gleiche Grundverständnis haben. Damit das erreicht werden kann, müssen die Mitarbeiter in regelmäßigen Abständen geschult und informiert werden. Nur durch diese regelmäßigen Maßnahmen kann eine entsprechende Sicherheitskultur aufgebaut und gelebt werden.
Da diese gelebte Sicherheitskultur die Grundlage und somit die Voraussetzung für eine funktionierende Securitylösung ist, muss bei Schulungs- und Sensibilisierungsmaßnahmen auf Nachhaltigkeit gesetzt werden.

Ergebnis
Kompetente sowie informierte und geschulte Mitarbeiter mit Bewusstsein für Sicherheitsrisiken sowie einem gleichen Verständnis was Security bedeutet.

9.11 Aufrechterhaltung des Sicherheitsniveaus

Aufgrund sich ändernder Gegebenheiten in Netzwerken und deren Umgebung, muss eine regelmäßige Prüfung der bestehenden Security-Maßnahmen durchgeführt werden. Dazu ist es vor allen Dingen wichtig ein solides Änderungsmanagement etabliert zu haben. Denn darüber können geänderte Umstände schnell erfasst und bewertet, sowie gegebenenfalls Optimierungen durchgeführt werden. Neben dem Änderungsmanagement stellt auch der Security-Management-Prozess ein zyklisches Vorgehen dar. Nur wenn diese Schritte regelmäßig und langfristig durchgeführt werden, kann ein hohes Maß an Sicherheit gewährleistet werden.

Ergebnis
Hohes und gleichbleibendes Maß an Sicherheit.

9.12 Incident Management

Trotz aller Maßnahmen kann niemand ausschließen, dass es nicht doch zu Sicherheitsvorfällen, sogenannten Incidents kommen kann. 100% Sicherheit gibt es nicht. Daher müssen auch für diesen Fall Vorkehrungen getroffen werden und ein Incident Management Prozess aufgesetzt werden. Das beinhaltet die Erkennung eines Incidents, die Beseitigung der Gefahr und die Wiederherstellung der Sicherheit, damit der Normalbetrieb wieder aufgenommen werden kann. Hierfür müssen die Verantwortlichkeiten festgelegt und die Ressourcen verfügbar sein. Technisch gesehen müssen Back-Ups und Wiederherstellungsmöglichkeiten bei Datenverlust oder -Verfälschung vorhanden sein. Das Ziel ist es, möglichst schnell wieder den Normalbetrieb aufnehmen zu können, um die Verluste möglichst gering zu halten.

10 Lösungsansätze

Die Entwicklung und Implementierung von Sicherheitslösungen konzentriert sich in der Regel auf geeignete Maßnahmen, um den Zugang (physisch oder über die Netzwerkinfrastruktur) zu den schützenswerten Bereichen, Systemen oder Komponenten zu kontrollieren und zu schützen.
In den folgenden Kapiteln wird eine Auswahl von möglichen organisatorischen Maßnahmen sowie technischen Maßnahmen beschrieben.

10.1 Lösungsansätze für organisatorische Maßnahmen

Die zentrale Aufgabe für organisatorische Maßnahmen stellt neben der Etablierung von Security im Unternehmen, die Definition von Richtlinien und Policies dar. In diesen Richtlinien werden alle notwendigen Regelungen beschrieben, welche den Umgang mit Security-Mechanismen betreffen.

10.1.1 Richtlinien und Policies

Beispiele hierfür können folgende Regulierungen sein:

- **Umgang mit Fremdpersonen**
  - » Beaufsichtigung/Begleitung von Fremdpersonen
  - » Vertraulichkeitsvereinbarungen
  - » Besucherausweis sichtbar tragen
- **Zugriffsregulierung**
  z.B. die Rechtevergabe für den Fernzugriff
- **Umgang mit Datenträgern**
  z.B. Klärung und Regelung der Mitnahme und Verwendung von Datenträgern und IT-Komponenten
  - » wer IT-Komponenten bzw. Datenträger außer Haus mitnehmen darf,
  - » welche IT-Komponenten bzw. Datenträger außer Haus mitgenommen werden dürfen
  - » welche grundlegenden IT-Sicherheitsmaßnahmen dabei beachtet werden müssen
  - » Virenschutz, Verschlüsselung sensitiver Daten, Aufbewahrung, etc.
  - » Wer darf welche Datenträger mit in das Unternehmen nehmen?
- **Logging**
  z.B. von Systemevents, z.B. Protokollierung bei Anmeldevorgängen oder Aktivitäten im Netz
- **Systemhärtung**
  z.B. abschalten nicht benötigter Leistungsmerkmale / Systemmerkmale oder Deaktivierung automatischer Starts z.B. bei USB-Datenträgern
- **Passwort- und Schlüsselmanagement**
  - » Geeignetes Schlüsselmanagement für den Einsatz von WLAN
  - » Passwortschutz, z.B. bei BIOS
  - » Änderungen voreingestellter Passwörter
  - » Verwendung von Passwortspeichertools
- **Richtlinie** für die **Entsorgung, den Tausch oder der Einlagerung** von bestehenden Komponenten, Datenträgern oder Dokumenten

- **Sanktionen bei Nichteinhaltung**
  z.B. Zutrittsverbot

10.1.2 Patchmanagement

Aus Kapitel 6.7 geht bereits hervor, dass Patchmanagement in der Automatisierungstechnik ein schwieriges Unterfangen ist. Dennoch muss ein Weg gefunden werden, bestehende Systeme mit Patches und Updates versehen zu können um bestehende Sicherheitslücken zu schließen. Nicht nur Standard-PC-Betriebssystem sondern auch Automatisierungssysteme sind nicht vor Security-relevanten Schwachstellen gefeit.
Das empfohlene Vorgehen beim Bekanntwerden einer Schwachstelle sollte folgendes sein:
Sobald Informationen über eine Schwachstelle verfügbar sind, sollte diese zunächst auf Relevanz für die eigene Anwendung bewertet werden.
Davon abhängig kann dann entschieden werden, ob weitere Maßnahmen zu treffen sind:

- Keine Aktion, da vorhandene Maßnahmen ausreichenden Schutz bieten
- Zusätzliche externe Maßnahmen um Security-Niveau weiterhin zu gewährleisten
- Installation des aktualisierten FW-Updates um Schwachstelle zu beheben

10.1.3 Notfallmanagement

Nicht nur die Abwehr von Angriffen und das Beseitigen von Sicherheitslücken gehört zur Erstellung eines Sicherheitskonzeptes, auch eine klare Regelung für den Notfall muss vorgesehen werden. Es ist unabdingbar für Notfälle einen entsprechenden Maßnahmenplan zu erstellen. Dieser Plan sollte folgende Fragen und Informationen klären:

- Definition von Rollen und Verantwortlichkeiten für den Notfallbetrieb, sowie dafür vorgesehene Prozesse
- Liste aller zu informierender Personen
- Datensicherungskonzept bzw. Wiederherstellungsmaßnahmen

Zur Erstellung eines solchen Maßnahmenkataloges ist die Durchführung eines eigenen Prozesses notwendig. Die Beschreibung eines möglichen Vorgehensmodelles wird beispielsweise im BSI-Grundschutzkatalog BSI-Standard 100-4 beschrieben.

10.1.4 Security als Unternehmensprozess

Security Management bildet einen wesentlichen Bestandteil jedes Industrial Security Konzeptes. Nachdem das Konzept realisiert wurde, muss es in regelmäßigen Abständen kontrolliert werden, um die Wirksamkeit der getroffenen Maßnahmen zu verifizieren. Treten bei der Prüfung der Maßnahmen Abweichungen zum gewünschten Ergebnis auf, so müssen die Maßnahmen neu überarbeitet und realisiert werden. Das Vorgehensmodell muss somit erneut durchlaufen werden. Auch können sich Schutzziele ändern, hierfür sollte eine regelmäßige Durchführung der Risikoanalyse vorgesehen werden. Nur durch einen konsequenten Security Management Prozess kann das definierte Security Level erreicht und beibehalten werden.

10.2 Lösungsansätze für technische Maßnahmen

Neben den organisatorischen Maßnahmen spielen vor allen Dingen die technischen Realisierungsmöglichkeiten eine entscheidende Rolle in der Umsetzung der Netzwerksicherheit.
Security-Grundkonzepte setzen heute auf zwei Grundprinzipien – Segmentierung und Defense-in-Depth.
Das Grundkonzept der Segmentierung verfolgt den Ansatz, sowohl die vertikale wie auch die horizontale Kommunikation zu strukturieren, um

1) die Auswirkung von beabsichtigten oder auch unbeabsichtigten Angriffen und Fehlhandlungen auf kleine, abgegrenzte Bereiche zu limitieren und

2) den Zugriff auf erreichbare Angriffsziele zu erschweren und zu begrenzen. Angriffe sind nur möglich, wenn eine Möglichkeit gefunden wird, in den jeweiligen Bereich einzudringen.

Üblicherweise spricht man bei derartigen Lösungen vom sogenannten Zellenschutzkonzept.

10.2.1 Zellenschutzkonzept

Der erste Schritt zur Implementierung eines Zellenschutzkonzepts besteht in der Definition der sogenannten Security-Zellen. Jede Zelle kann wiederum aus einer oder mehreren untergeordneten Zellen bestehen und muss unabhängig von anderen Zellen als eigenständige Zelle funktionieren. Jede Zelle kann zudem eine unterschiedliche Anzahl von Komponenten haben. Alle in einer Zelle befindlichen Komponenten werden als vertrauenswürdig eingestuft, so dass innerhalb der Zellen keine weiteren Sicherheitsmaßnahmen für die Kommunikation erforderlich sind. Dieses Prinzip ist bei der Nachrüstung bereits bestehender Anlagen nützlich. Bei bereits definierten Zellen muss nur die Zugangskontrolle am Eingangspunkt der Zelle definiert werden. Dazu können klassische Security-Komponenten verwendet werden. Der große Vorteil besteht darin, dass die Zelle durch Begrenzung der Bandbreite vor Überlastung des Netzwerks geschützt und der Datenverkehr innerhalb der Zelle ungestört aufrechterhalten werden kann. Dies bedeutet, dass die Echtzeit-Kommunikation innerhalb der Zelle nicht beeinträchtigt wird. Auch Safety-Anwendungen innerhalb der Zelle werden gleichermaßen vor unbefugten Zugriffen von außen geschützt.

10.2.1.1 Kriterien für die Netzwerksegmentierung

Im Rahmen des auf Zellen basierenden Schutzkonzeptes wird ein Netzwerksegment von außen gegen unbefugten Zugriff geschützt. Der Datenverkehr innerhalb der Zelle wird von der Security-Anwendung nicht kontrolliert. Er muss also als sicher erachtet oder aber mit Schutzmaßnahmen innerhalb der Zelle versehen werden, beispielsweise durch Port-Security bei Switchen. Die Größe einer Security-Zelle richtet sich in erster Linie danach, wogegen die enthaltenen Komponenten geschützt werden sollen, da eine Zelle nur solche Komponenten umfassen darf, die den gleichen Schutzanforderungen unterliegen.
Außerdem wird in Abhängigkeit von den Leistungsanforderungen für die Netzwerkgröße und Netzwerksegmentierung Folgendes empfohlen:

- Alle Devices einer Controller-Domäne gehören einer Zelle an
- Devices, zwischen denen viele Daten übertragen werden, sollten der gleichen Zelle zugeordnet werden
- Devices, die nur mit Devices einer einzigen Zelle kommunizieren, sollten dieser Zelle zugeordnet werden, sofern die Schutzanforderungen identisch sind

Die Netzwerksegmentierung kann dabei auf zwei unterschiedliche Arten erfolgen:

» Logische oder

» Physikalische Segmentierung

10.2.1.2 Logische Segmentierung mit Virtual Local Area Network – VLAN

Eine Möglichkeit Netzwerke logisch zu trennen bieten VLANs (Virtual Local Area Networks). Durch VLANs wird es möglich die physische Struktur in logische Teilnetze zu gliedern. Die technische Realisierung innerhalb eines Switched-Netzwerkes erfolgt durch die Zuordnung der Switch-Ports zu einem VLAN. Ports, die dem gleichen VLAN zugeordnet sind, verarbeiten auch die gleichen Broadcasts; Ports, die unterschiedlichen VLANs zugewiesen sind, tun dies nicht.

Eine Segmentierung mit VLANs kann durch Netzwerkinfrastruktur-Komponenten, z.B. Switchen) aber nicht durch End-Geräte erfolgen. PROFINET Devices, die miteinander kommunizieren sollen, müssen also dem gleichen VLAN zugeordnet werden (Bild 3).

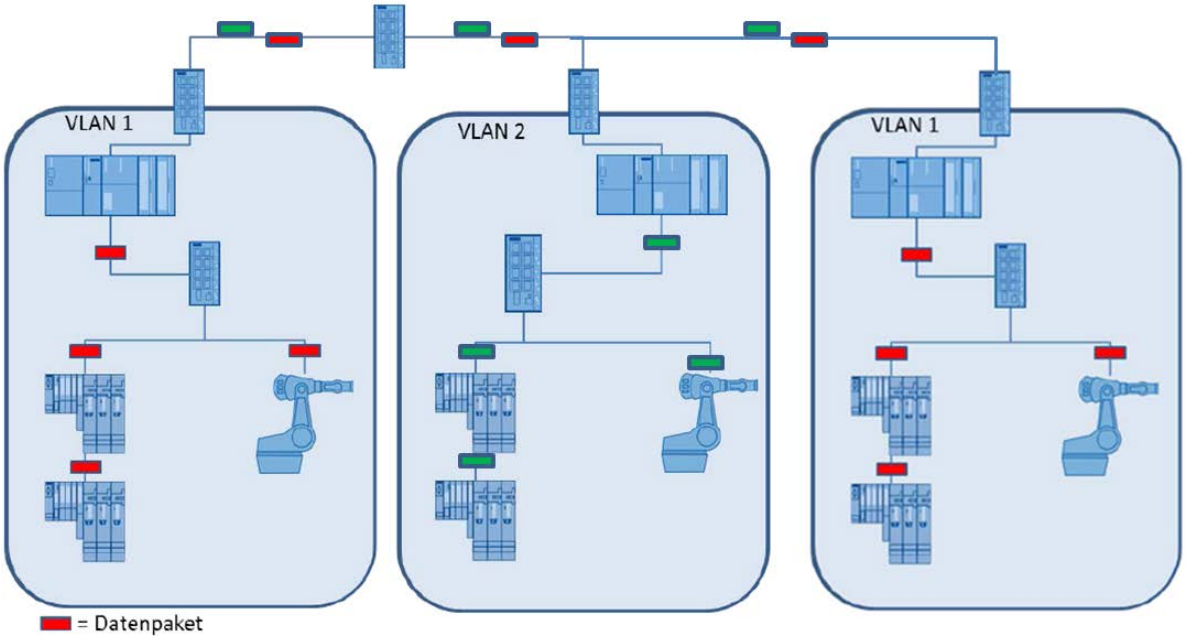

Bild 3 - Mögliches VLAN

10.2.1.3 Physikalische Segmentierung

Durch physikalische Segmentierung werden Automatisierungsnetzwerke in kleinere Segmente unterteilt. Jede Zelle schützt ihre Komponenten die sich in ihr befinden, da von außen vorerst keine Zugriffsmöglichkeit besteht. Das Ergebnis sind einzelne Automatisierungsinseln welche unabhängig voneinander funktionieren können Siehe hierzu auch Kapitel Step-by-Step Beispiel für Segmentierung

10.2.1.4 DMZ

Eine weitere Form der Segmentierung stellt die Erstellung einer sogenannten demilitarized Zone, der DMZ dar. In dieses Segment werden alle Komponenten zusammengefasst, welche einen Zugang nach Außen benötigen bzw. bereitstellen.
Eine weitere Alternative für Anwendungen mit erhöhten Sicherheitsanforderungen bietet die Anbindung über ein Perimeternetzwerk – oft auch als DMZ (Demilitarized Zone) bezeichnet. Dabei wird die direkte Kommunikation zwischen der Produktion und den restlichen Unternehmensnetzen vollständig durch Firewalls blockiert. Ein Austausch ist nur indirekt über Server in der DMZ möglich. Auf diese Weise können interne Richtlinien für den Kommunikationsaustausch zuverlässig umgesetzt werden, während der nichtautorisierte Zugriff von außen unterbunden wird.

Ein entscheidender Vorteil der Segmentierung ist die Möglichkeit die Zugriffspunkte zwischen den Segmenten klar definieren zu können. Die Grenzen sind klar strukturiert, wodurch die Definition von Schnittstellen einfach realisiert werden kann.
Kapitel 9.2.2 stellt verschiedene Möglichkeiten der Umsetzung von Zugriffspunkte bzw. der Zugriffskontrollen dar.

10.2.1.5 Subnetzbildung und IP-Adressen

Auch durch die Definition von Subnetzen können Zugriffsmöglichkeiten auf Automatisierungszellen strukturiert werden.

Unter einem Subnetz versteht man hierbei einen Netzbereich, in dem alle Teilnehmer untereinander per Layer2-Kommunikation erreichbar sind (Broadcast Domäne) und dieselbe Subnetzadresse besitzen. Subnetze werden physikalisch voneinander getrennt. Der Netzübergang zwischen Subnetzen erfolgt über Router.

Da die PROFINET-Kommunikation Layer2-basiert ist und daher nicht über Router-Grenzen erfolgen kann, müssen sich daher alle PROFINET-Teilnehmer, die miteinander kommunizieren sollen, im selben Subnetz befinden. Große Subnetze sind jedoch zu vermeiden, da hierdurch das Risiko der gegenseitigen Beeinflussung zwischen Controller-Domänen durch Broadcasts und Multicasts zunimmt.

Generell empfiehlt es sich daher die Subnetze, in denen Teilnehmer miteinander kommunizieren sollen, möglichst klein zu halten. Beispielsweise könnte ein Subnetz immer zellenbezogen aufgebaut sein.
Der Vorteil dieser Subnetzbildung liegt vor allem darin, dass beispielsweise Multicast- oder Broadcastanfragen lediglich innerhalb eines Subnetzes versendet werden. Dadurch werden andere Netze, welche nicht von diesen Anfragen betroffen sind, von dem zusätzlichen Datenverkehr entlastet.

Auch für die IP-basierte Kommunikation ist aus Security-Sicht die Bildung zellenbasierter Subnetze sinnvoll. So lassen sich beispielsweise die Zellen allein schon durch den Einsatz privater IP-Adressen vom übergeordneten Netzwerkbereich abgrenzen (Adresskonzept). Ein Verbindungsaufbau vom übergeordneten Netz in die Zelle ist dann nicht mehr direkt möglich. Erst durch den Einsatz entsprechender Adress-Konfigurationen (z.B. NAT) an den Netzübergängen wird eine Kommunikation ermöglicht.

Vorteile des Zellenschutzkonzeptes
Durch die Realisierung des Zellenschutzkonzeptes mittels Segmentierung, wird sichergestellt, dass ein ggf. unberechtigter Zugriff auf eine Zelle sich nur auf die sich in der Zelle befindlichen Teilnehmer bezieht.

10.2.2 Zugriffspunkte/Zugangskontrollen

Nachdem alle Netzwerksegmente erstellt wurden, kann damit begonnen werden die Zugriffspunkte bzw. die Zugangskontrolle zu realisieren. Zugangspunkte sollten grundlegend so gewählt werden, dass diese nicht direkt in Zellen hinein gelegt werden. Durch einen direkten Zugang in eine Zelle würde ein Angriffspunkt genau im Herz der Maschine geschaffen werden. Um dies zu verhindern sollten die Zugangspunkte immer außerhalb realisiert werden. Zusätzlich können die Zugangspunkte noch weitere Maßnahmen geschützt werden.

Die anzutreffenden Lösungen sind vielschichtig. Die wesentlichen drei Varianten (Basistechnologien) für den Einsatz von aktiven Netzwerkinfrastrukturkomponenten sind:

- Switche: volle Integration , keine Segmentierung
- Router: private vs. firmen IPs: (Basisschutz abhängig vom gewählten IP-Adresskonzept)
- Gateways/Proxy: keine direkte Kommunikation, sondern applikative Kopplung zwischen Teilnehmern unterschiedlicher Segmente

Praktisch alle verfügbaren Security-Lösungen setzen auf einer dieser Basistechnologien auf. So handelt es sich bei der häufig eingesetzten Firewall aus Sicht der dargestellten Basistechnologien um Router, die mit zusätzlichen, konfigurierbaren Regelwerken die Kommunikation auf Basis der IP-Ziel-/Quelladresse, der verwendeten Dienste oder auch der Inhalte kontrollieren.

Hinweis:

Wenn Zugangspunkte bzw. Zugriffspunkte durchgängig mit dem gleichen bzw. identischen Produkten realisiert werden, so besteht die Gefahr bei Bekanntwerden einer Schwachstelle, dass diese Schwachstelle eine durchgängige Sicherheitslücke im Netzwerk darstellt.

10.2.2.1 Router / Switche

Der einfachste Fall der Zugangspunkte besteht im Einsatz von Router und/oder Switche. Grundsätzlich verbinden Router und Switche Netzwerke miteinander. Wobei Router Netzwerke über Netzwerkgrenzen hinaus miteinander verbinden und Switche lediglich für den Einsatz innerhalb eines Subnetzes bestimmt sind.

Switch
Soll zwischen den Segmenten eine Layer-2-basierte Kommunikation stattfinden, so empfiehlt sich der Einsatz eines Switches. Es muss jedoch an dieser Stelle bedacht werden, je mehr Switch-Verbindungen realisiert werden, desto größer wird die Layer-2-Domäne, womit das Ausbreiten von Multicast-Nachrichten zu einem sehr hohen Datenaufkommen führen kann. Eine Möglichkeit dieses zu unterbinden ist der Einsatz von Switch-Komponenten, welche eine sogenannte Multicast-Sperre für einzelne Ports konfigurieren können. Es sollte jedoch an dieser Stelle genau geprüft werden, ob auch beispielsweise ARP-Multicastanfragen von dieser Sperre betroffen sind, und nicht nur PROFINET-spezifische Multicastanfragen wie beispielsweise DCP.

Router
Sind die Zellen in zwei unterschiedlichen IP-Subnetzen und soll zudem eine IP-basierte Kommunikation gewährleistet werden, so muss ein Router zum Einsatz kommen, da nur darüber zwei unterschiedliche Netzwerke miteinander verbunden werden können.
Der Vorteil beim Einsatz eines Routers liegt in der Begrenzung der Multicast-Domäne. Layer-2-basierte Multicast-Anfragen werden von Routern nicht in das andere Netzwerksegment weitergeleitet. Das Datenaufkommen wird also auf die „sendende Zelle“ beschränkt.
Multicastanfragen können auch bei IP-basierten Diensten auftreten. Daher sind auch hier die Anforderungen an einen Router abhängig von den eingesetzten Anwendungen und deren benötigte Dienste. Engineering Tools verfügen teilweise über Multicast-Anfragen um ihre Geräte im Netzwerk zu finden. Daher sollten auch hier die Grenzen erfasst werden.

10.2.2.2 Gateway

Der Einsatz von Gateways kann einen sehr effizienten Security-Netzübergang darstellen, wenn keine direkte Kommunikation zwischen Teilnehmern unterschiedlicher Segmente erforderlich ist, Technische Realisierungsbeispiele dieses Konzeptes sind z.B. Steuerungen, die über mehrere Netzwerkadapter verfügen, Jedes Segment ist hierbei über einen dieser Netzwerkadapter mit dem Gateway verbunden.
Durch eine Entkopplung von ausgewählten Funktionen durch Gateways kann eine Erhöhung der Sicherheit erreicht werden.

10.2.2.3 Firewall

Eine Firewall stellt wohl den bekanntesten Mechanismus der Zugriffskontrolle dar. Eine Firewall kontrolliert in ihrer einfachsten Form die Zugriffe zwischen Netzwerken. Dabei werden Protokolltypen und Adressen in Form von sogenannten Firewall Regeln definiert. Die Regeln definieren dabei zusätzlich was mit den Paketen passieren soll.
Um diese Firewall Regeln definieren zu können müssen also mindestens folgende Informationen vorliegen:

- Welche Dienste werden zwischen den zu verbindenden Netzwerken benötigt? (Ports)
- Wer darf zwischen den Netzwerken kommunizieren? (IP-Adressen)
- In welche Richtung darf diese Kommunikation stattfinden? (Ein- / ausgehend)

Die einfachste Form der Firewall stellt eine Paketfilter-Firewall dar.

Stateful Inspection

Eine erweiterte Form der Filterung ist die sogenannte Stateful Inspection. Diese Methodik erlaubt die kontextabhängige Auswertung des Paketinhaltes. Der Kontext bezieht sich dabei auf ein zugrunde liegendes Sessionmanagement.

Beim Einsatz dieser Technologie ist darauf zu achten, dass verbindungslose Protokolle unterstützt werden. Ein Beispiel hierfür wäre UDP. UDP arbeitet als Protokoll verbindungslos. Die Firewall muss jedoch, um eine Kommunikation in beide Richtungen zu gewährleisten eine temporäre, virtuelle Verbindung hinterlegen.

Application layer / Layer 7 firewall
Da Angriffe auch innerhalb von Applikationen stattfinden können, existieren Layer 7 Firewalls. Diese Art der Firewall kann die reinen Nutzdaten eines Pakets betrachten und je nach Inhalt entsprechend reagieren. Beispielsweise können Zugriffe bzw. der Datenaustausch mit Streamingservern unterbunden werden.

Nutzerspezifische Firewall
Eine userspezifische Firewall stellt eine Sonderform einer Firewall dar, da sie den Datenverkehr nicht nur nach gerätespezifischen IP-Adressen filtern kann, sondern auch abhängig von bestimmten Usern Zugriffsmöglichkeiten erlauben oder ablehnen kann. Hierbei ist es erforderlich, dass sich ein User an der Firewall authentifiziert, z.B. mittels Passwort-Login. Anschließend werden für diesen User ein spezieller vordefinierter Satz von Firewallregeln aktiviert.
Hierbei spielt es keine Rolle, welche IP-Adresse der Rechner des Users hat, da in den userspezifischen Firewallregeln Platzhalter sind in denen die jeweils vorhandene IP-Adresse des User-Rechners eingefügt wird.

10.2.2.4 IPS / IDS

Ergänzend zu Firewalls können Intrusion Prevention bzw. Intrusion Detection Systeme (IPS/IDS) eingesetzt werden. Beide Systeme sind in der Lage Angriffe bzw. Angriffssequenzen zu erkennen. Der grundlegende Unterschied zwischen IPS und IDS ist dabei der, dass ein IPS in der Lage ist die Angriffe abzuwehren und ein IDS diese lediglich erkennen kann.

10.2.2.5 Virtual Private Network – VPN

Ein Virtual Private Network (VPN) wird dazu eingesetzt zwei unabhängige Netze miteinander sicher zu verbinden. In der klassischen IT-Welt wird VPN häufig für Zugriffe aus dem Internet heraus in ein bestehendes Unternehmensnetzwerk genutzt. VPN verbindet dabei beide Netze mittels einem Gateway zu einem kompatiblen Netz, so dass der Benutzer, der sich außerhalb befindet, logisch gesehen Teil des internen Netzwerkes wird. In erster Linie wird also durch die Realisierung eines VPN ein Zugang aus einem fremden Netz in das interne Netz realisiert. Um dies zu realisieren werden zwei grundlegende Elemente benötigt. Ein VPN-Gateway und ein VPN-Client. Das VPN-Gateway stellt dabei den Einwahlknoten dar und der Client stellt den eigentlich Dienst bereit. Die Kommunikation die zwischen beiden Netzen stattfinden soll, wird dabei vom VPN-Client in ein eigenes Protokoll eingepackt. Diese Datenpakete werden dann auf der Empfängerseite wieder entpackt und ganz normal im Netzwerk versendet. Das bedeutet, dass die eigentlichen Datenpakete in ihrer ursprünglichen Form in ein fremdes Netz gesendet werden.

Hauptaufgaben:
- Vertraulichkeit
- Integrität
- Authentizität

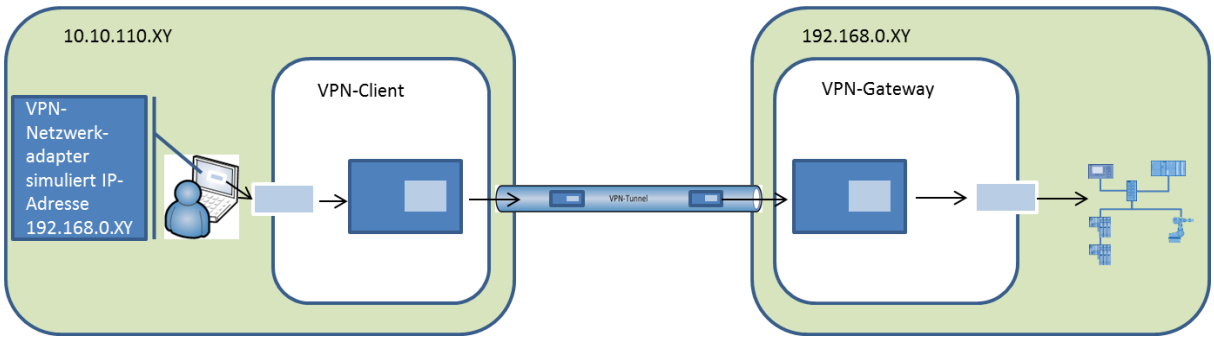

Bild 4 - Prinzip eines VPN

Die Art und Weise wie nun die zu versendenden Pakete verpackt werden, kann auf unterschiedliche Weise erfolgen. In der Regel werden hier Protokolle eingesetzt, welche Verschlüsselung erlauben, um so die Schutzziele Vertraulichkeit, Integrität und Authentizität zu gewährleisten. IPsec, SSL bzw. auch TLS sind wohl die bekanntesten Mechanismen unter Ihnen. An dieser Stelle sei darauf hingewiesen, dass die Protokolle jeweils nur unter bestimmten Rahmenbedingungen funktionieren. Bevor VPN eingesetzt wird müssen also dringend alle Anforderungen und Rahmenbedingungen geklärt werden. Auch das Einsatzfeld für VPN muss ganz klar definiert werden. Soll VPN beispielsweise für die Realisierung für Servicezugänge verwendet werden, muss sich klar gemacht werden, dass damit ein Zugang für eine fremde Person in das interne Netzwerk geöffnet wird. Das Zugriffsmanagement muss hier genau geklärt werden. Die Vergabe von Zugangsdaten und einem entsprechenden Authentifizierungsmechanismus ist nicht ausreichend. Fragen wie “Was passiert beim Diebstahl eines Servicenotebooks inkl. gespeicherter Zugangsdaten?” müssen sich an dieser Stelle vor Augen gehalten werden. Auch die potentiellen Schwachstellen der externen Firma bzw. Des Servicetechnikers müssen berücksichtigt werden. Denn eine Schwachstelle der externen Firma kann auch zu einer Schwachstelle des eigenen Unternehmens werden.
Ein zusätzlicher Punkt beim Einsatz von VPN ist das Prinzip der Einkapselung. Die Daten werden in ihrem originalem Zustand in verschlüsselter Weise in ein reguläres Datenpaket gepackt. Soll der Zugang durch eine Firewall oder einer IPS gehen, kann der originale Inhalt der Nachricht weder von einer Firewall noch einem anderen System eingesehen werden, da eine Entschlüsselung nur zwischen den beiden Verbindungsteilnehmern möglich ist. Somit wird es für den Benutzer möglich jegliche Art des Datenverkehrs in das interne Netz zu schleusen.

10.2.2.6 Abschließbare Schaltschränke

Zugriffspunkte müssen nicht immer Bestandteil des Netzwerkes sein. Zur Realisierung von Zugangspunkten zu kritischer Infrastruktur eigenen sich auch abschließbare Schaltschränke. Dadurch wird der unbefugte Zugriff durch nicht autorisierte Personen auf einfache Weise verhindert.

10.2.3 Defense-In-Depth-Ansatz

Defence-in-Depth verfolgt den Ansatz, unterschiedlichste technische Lösungen und Konzepte so zu kombinieren, dass selbst bei Versagen eines einzelnen Schutzmechanismus, andere Schutzmaßnahmen greifen.
Aus Sicht einer Automatisierungsanlage wird diese dadurch sowohl rundum als auch in die Tiefe geschützt. Das bedeutet einerseits, dass verschiedene sich ergänzende Schutzmechanismen vorhanden sind, um den unterschiedlichen Bedrohungen begegnen und Schutzziele wie Virenschutz oder Zugriffsschutz jeweils erfüllen zu können (Rundumschutz) und andererseits dass es mehrere Barrieren gibt, die von einem potenziellen Angreifer überwunden werden müssen. Das Konzept beinhaltet als wesentliche Komponenten Anlagensicherheit, Netzwerksicherheit und Systemintegrität. Die Maßnahmen zum Anlagenschutz umfassen alle Arten des physischen Zugangsschutzes aber auch organisatorische Maßnahmen und die Etablierung eines Security Managment Prozesses. Netzwerksicherheit bedeutet Schutz von Automatisierungsnetzen vor unbefugten Zugriffen. Dies beinhaltet die Kontrolle aller Schnittstellen wie z. B. zwischen Büro- und Anlagennetzwerk oder der Fernwartungszugänge zum Internet und kann mittels Firewalls und gegebenenfalls Aufbau einer DMZ (demilitarisierte Zone = sicherheitstechnisch abgeschirmte Zone) erfolgen. Die DMZ dient zur Bereitstellung von Daten für andere Netze, ohne direkten Zugang zum Automatisierungsnetz zu gewähren. Die

sicherheitstechnische Segmentierung des Anlagennetzwerks in einzelne geschützte Automatisierungszellen, dient der Risikominimierung und Erhöhung der Sicherheit. Der Schutz der Systemintegrität betrifft Endgeräte, wie PCs mit Virenschutz oder Automatisierungssysteme mit Zugriffschutzmechanismen für Geräte oder Applikationen. Auch Härtungsmassnahmen, die Schwachstellen von Geräten und Systemen verringern gehören dazu. Nur mit einem Defense-in-Depth-Ansatz bei dem die erforderlichen und hier aufgezeigten Sicherheitsmassnahmen lückenlos ineinandergreifen wird ein umfassender und verlässlicher Schutz einer Automatisierungsanlage erreicht. Dazu gehören Prozesse zur Herstellung und Beibehaltung von Sicherheit, sichere Produkte und nicht zuletzt das nötige Security-Bewusstsein aller Beteiligten.

Durch diese Art und Weise der Absicherung werden auf verschiedenen Ebenen verschiedene Angriffe abgewehrt und stellen so eine größere Herausforderung für einen potentiellen Angreifer dar. Jede einzelne Ebene stellt für sich gesehen eine relativ einfache Sicherheitshürde, in Kombination mit den anderen Ebenen jedoch eine nur sehr schwer überwindbare.

Wichtig beim Entwurf des Defense-In-Depth-Ansatzes sind dabei folgende Punkte:

» Mehrere Verteidigungsebenen müssen vorhanden sein

» Jede Ebene realisieren einen anderen Schutzmechanismus

» Jede Ebene ist dabei kontextabhängig realisiert

11 Beispiele

11.1 Step-by-Step Beispiel für Segmentierung

In Bild 6 wird ein beispielhaftes Unternehmensnetzwerk dargestellt, welches über keine Segmentierung verfügt. Anhand dieses Aufbaus soll beispielhaft eine mögliche Form der Segmentierung von Automatisierungsnetzen aufgezeigt werden, um das Prinzip des Zellenschutzkonzeptes zu verdeutlichen.
Für die Darstellung wird folgende Symbolik verwendet:

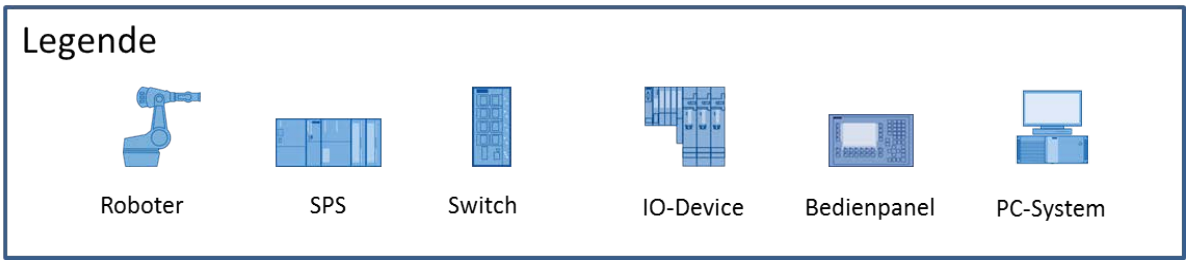

Bild 5 – Legende für nachfolgende Beispiele

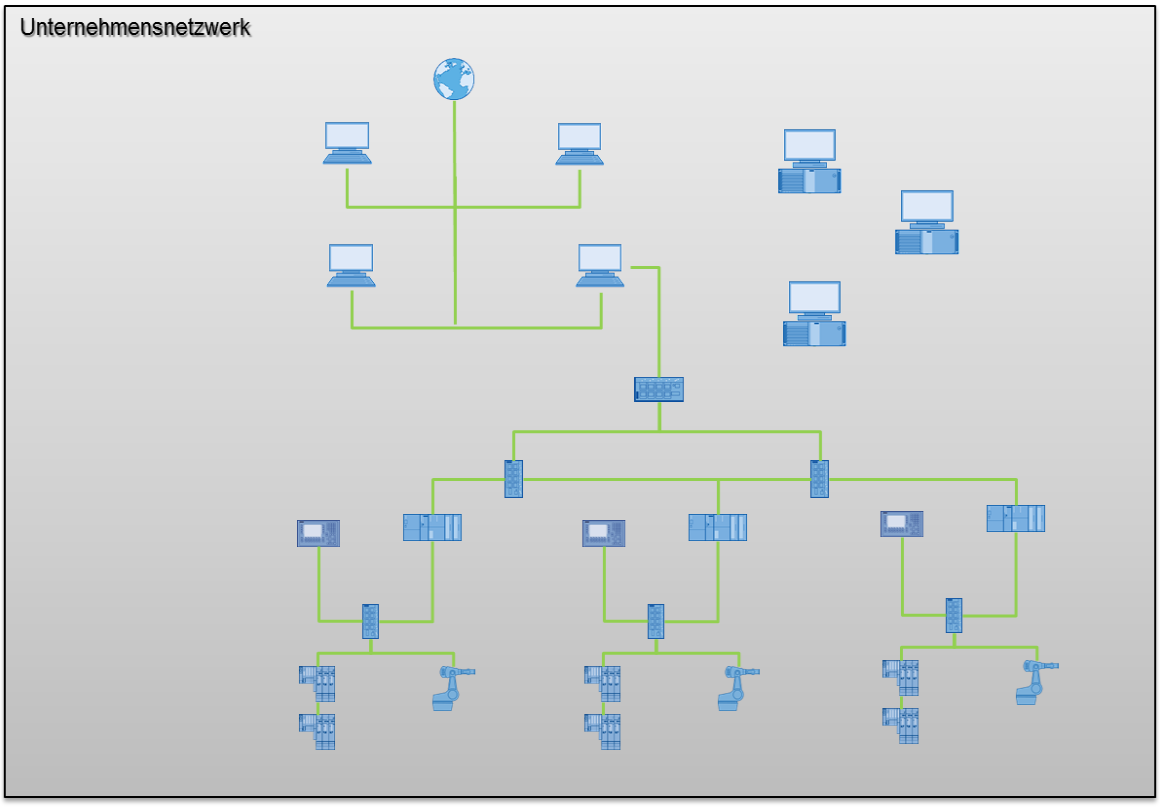

Bild 6 – Unternehmensnetzwerk ohne Segmentierung

Die einfachste Form der Segmentierung für dieses Beispielnetzwerk kann in einem ersten Schritt die Trennung zwischen Office- und Produktionsnetzwerk sein. Durch diese Unterteilung ist das Automatisierungsnetzwerk vom restlichen Netzwerk abgeschnitten und es können vorerst keine Zugriffe von außerhalb erfolgen. Bild 7 verdeutlicht diesen ersten Schritt.

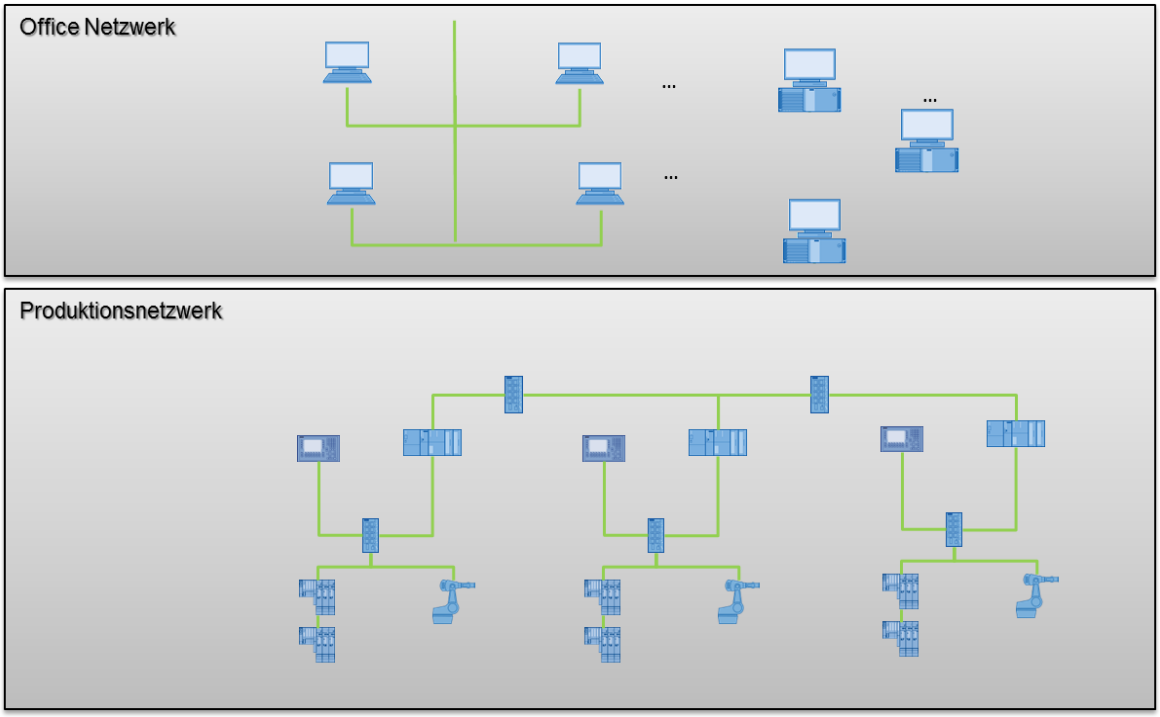

Bild 7 - Einfachste Form der Segmentierung

Wird in einem weiteren Schritt das Produktionsnetzwerk betrachtet, so kann auch hier eine weitere Unterteilung vorgenommen werden. Innerhalb des Produktionsnetzwerkes können

einzelne Automatisierungszellen definiert werden. Diese können sich beispielsweise an einer Controller-Domäne orientieren. So definierte Automatisierungszellen können dann in einem weiteren Schritt zu einer Produktionslinie zusammengefasst werden. Als Richtgröße könnte hier eine PROFINET-Domäne verwendet werden.
Bild 8 verdeutlicht diesen weiteren Schritt der Netzwerksegmentierung.

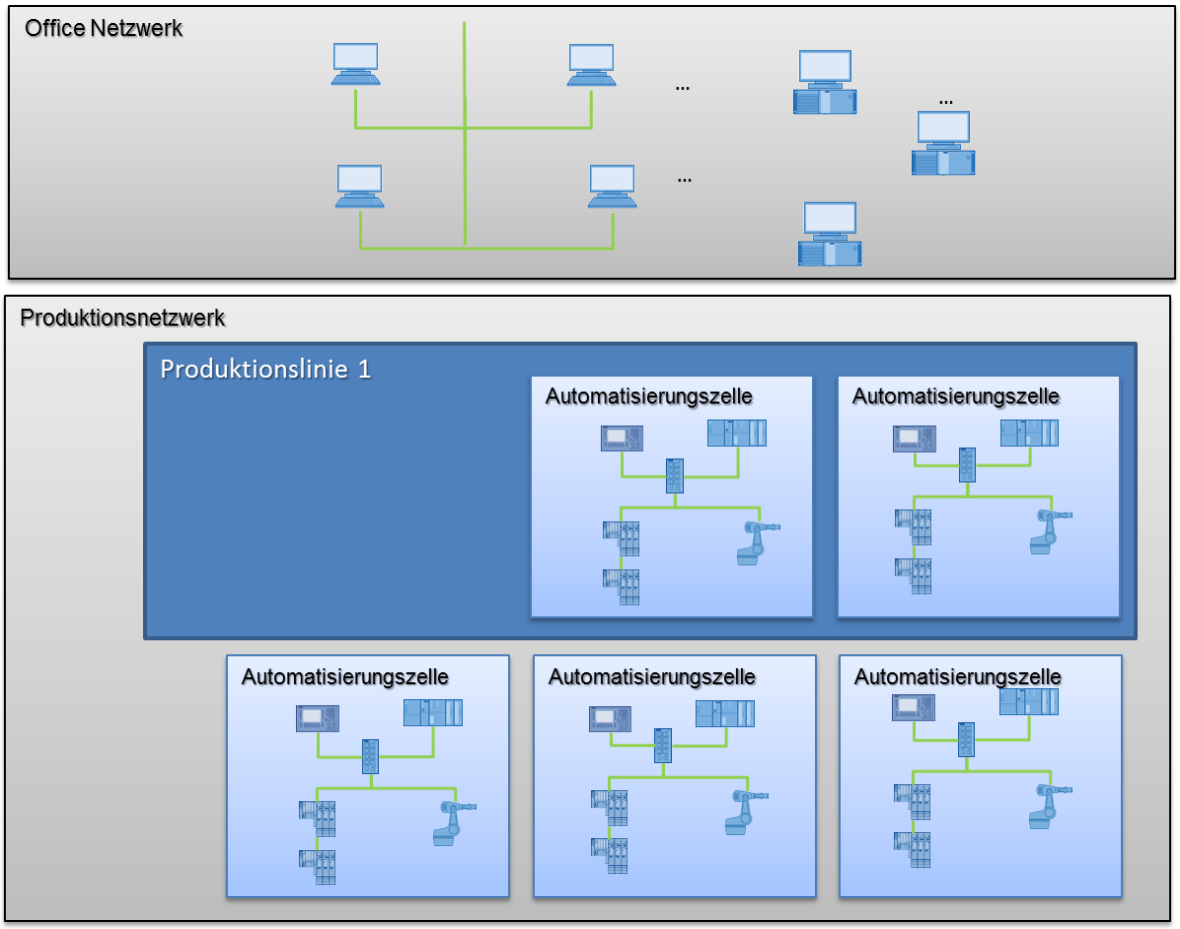

Bild 8 - Segmentierung des Produktionsnetzwerkes

Produktionslinien und auch Automatisierungszellen können nun beliebig oft definiert und miteinander kombiniert werden.

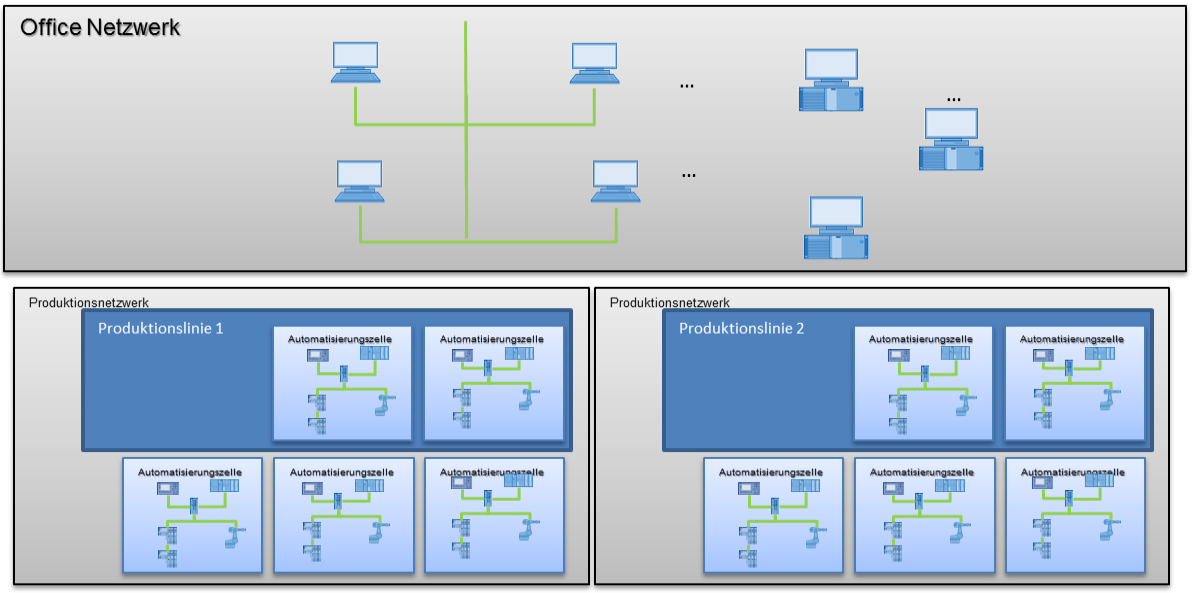

Bild 9 - Mehrfach-Segmentierung des Produktionsnetzwerkes

Letztendlich kann noch eine DMZ eingeführt werden, um Komponenten, die einen Zugriff nach Außen benötigen, aus den Zellen herauszuziehen. Eine weitere Segmentierungsebene kann durch den Einsatz einer DMZ erreicht werden. Damit ist es möglich, Dienste und Komponenten, die dem übergeordneten System bereit gestellt werden sollen, aus den Zellen herauszulösen.

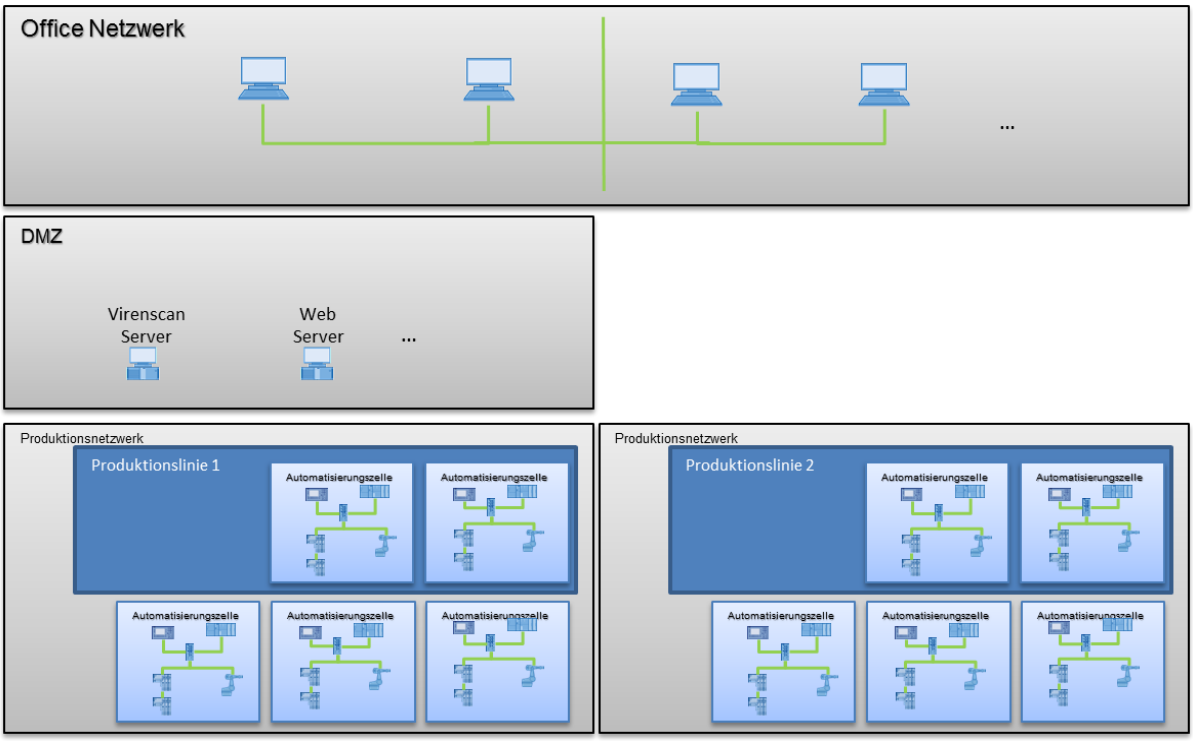

Bild 10 - Segmentiertes Produktionsnetzwerk inkl. DMZ

11.2 Zugriffspunkte / Zugangskontrollen

Nachdem durch die Step-by-Step-Anleitung ein segmentiertes Netzwerk geschaffen wurde, geht es nun darum, die Zugriffspunkte und deren Zugriffsmöglichkeiten so zu definieren, dass alle notwendigen Kommunikationswege auf sichere Weise realisiert werden können.

Voraussetzung

Um nun Zugriffspunkte schaffen zu können, müssen folgende Informationen vorliegen:

- Welche Kommunikationsverbindungen müssen realisiert werden?
- Welcher Dienst wird für eine zu realisierende Kommunikationsverbindung benötigt?
- Welcher Port muss dazu freigeschaltet werden?
- Welchen Verwendungszweck hat die Kommunikationsverbindung?
- Welche Nutzer (Personen oder Geräte) sind berechtigt, die Kommunikationsverbindung zu nutzen?

Nur mithilfe dieser Informationen können nun kontrolliert Zugriffspunkte geschaffen werden.

In den nachfolgenden Beispielen soll die Verwendung der unter Kapitel 9.2.2 beschriebenen Zugangskontrollen bzw. Zugangspunkte beschrieben werden.

Ziel ist es, durch die Beschreibung der einzelnen Möglichkeiten, Zugänge zu realisieren, ein Netzwerk beispielhaft mit Zugangspunkten zu versehen und dabei unterschiedliche Anwendungsfälle zu betrachten. Dadurch entsteht eine Struktur anhand derer die jeweiligen Anwendungsfälle und die damit verbundenen Möglichkeiten dargestellt werden können.

Unsere Ausgangssituation stellt das in Kapitel 10.1 erstellte segmentierte Netzwerk dar.

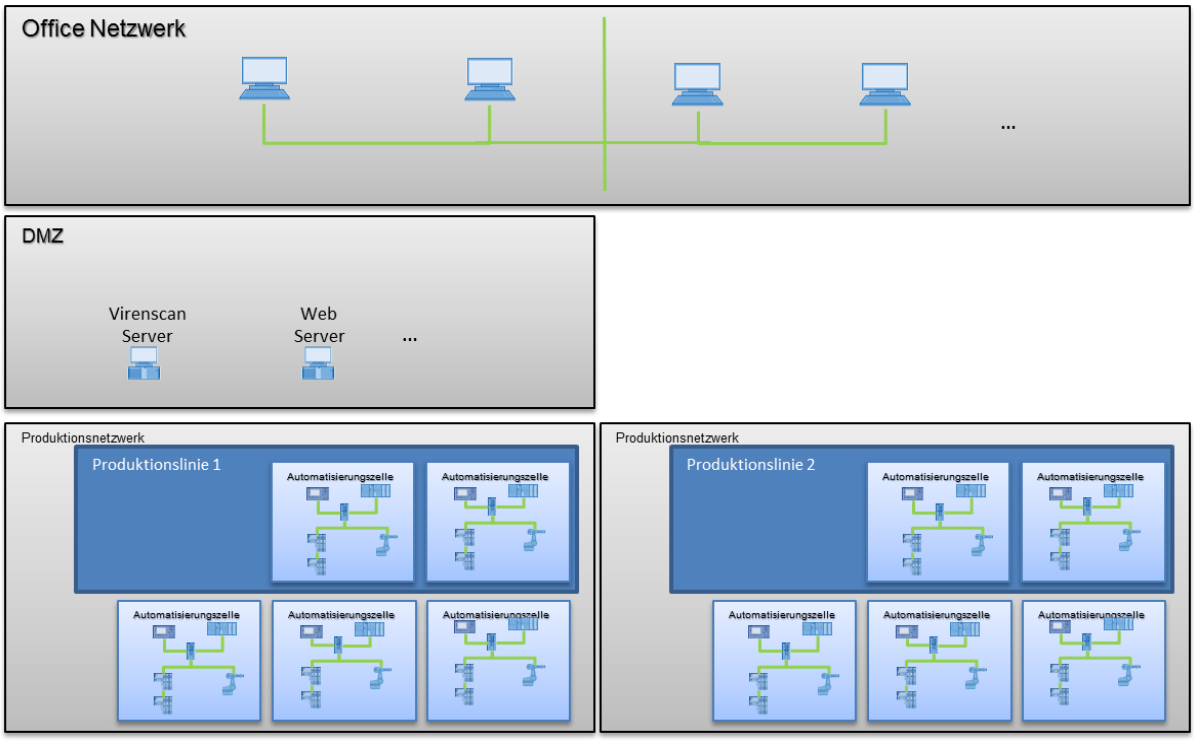

Bild 11 - Ausgangsbasis zur Realisierung von Zugriffspunkten/Zugangskontrollen

Folgende Symbolik wird verwendet:

Bild 12 - Legende Zugangskontrollpunkte

Das Grundkonzept für die nachfolgenden Beispiele folgt dem Ansatz, Controller-Domänen möglichst voneinander zu trennen und nur wenn nötig miteinander zu verbinden.
Es soll der Einfachheit halber lediglich ein Ausschnitt des Beispielnetzwerkes betrachtet werden. Das Produktionsnetz.

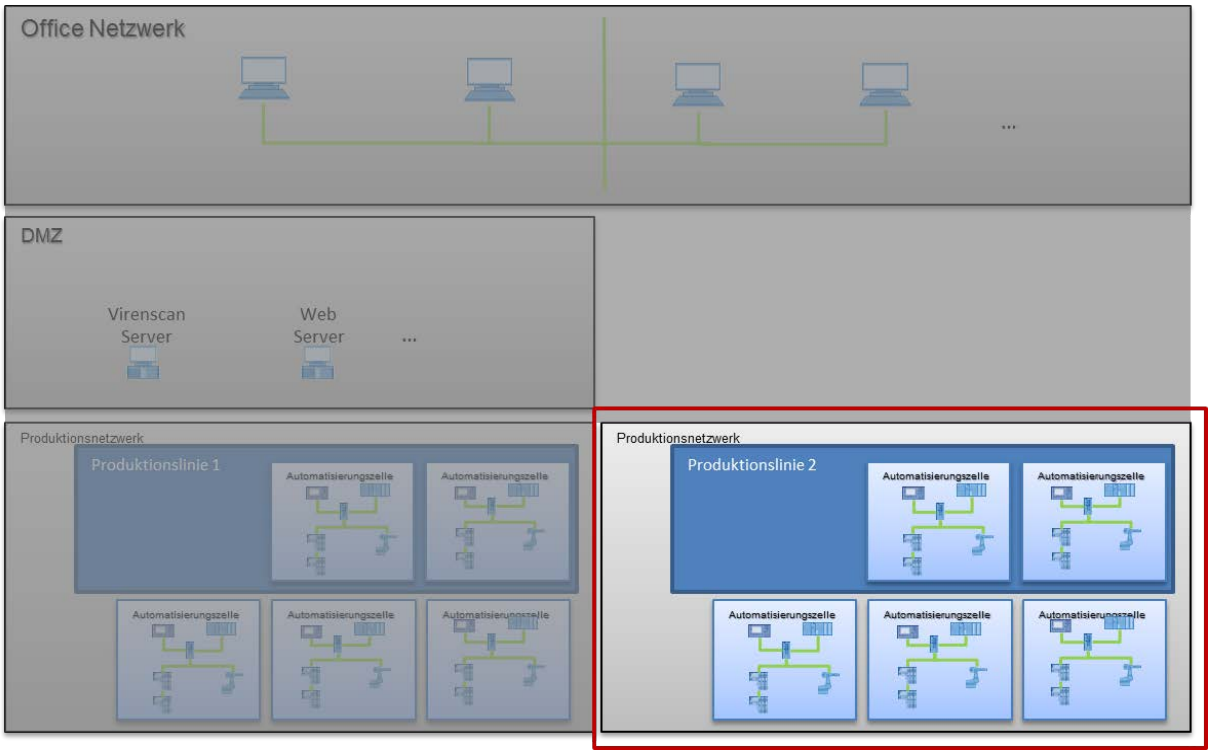

Bild 13 - Ausgangsbasis für die Verwendung von Switchen

Innerhalb des Produktionsnetzwerkes wurden einzelne Automatisierungszellen definiert. Diese orientieren sich an einer Controller-Domäne, die erstellte Produktionslinie entspricht hier einer PROFINET-Domäne.

11.2.1 Z1 – Verwendung von Gateways

Anwendungsfall
Es wird eine Kommunikation zwischen den Controllern auf Basis von IO-Signalen benötigt.

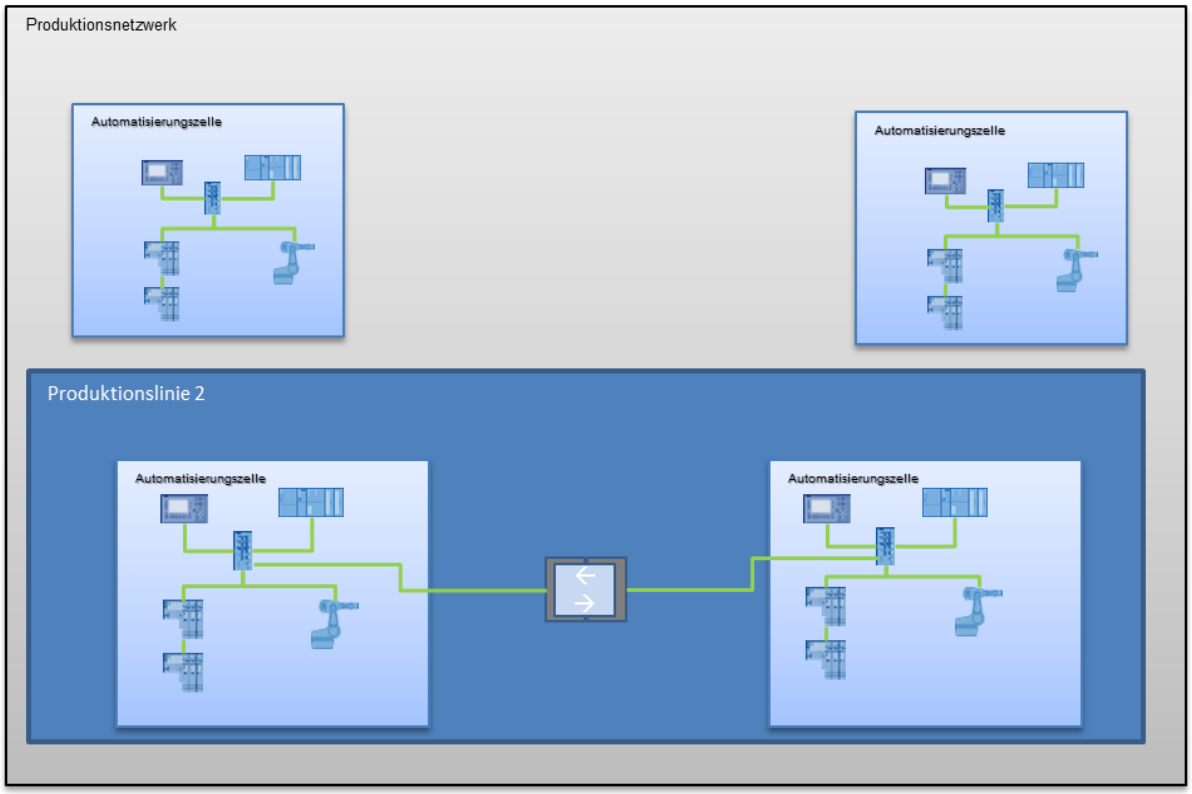

Bild 14 - Verwendung eines PN/PN-Gateways

Charakteristik
Der Vorteil dieser Kommunikationsstrecke besteht darin, dass keinerlei Layer 2 oder höher

basierte Kommunikation stattfinden kann. Die notwendige Kommunikationsverbindung ist somit auf ein Minimum beschränkt, und erfüllt maximal den für die Kommunikationsstrecke vorgesehenen Verwendungszweck.

Konsequenz
Es können keine PROFINET-Dienste auf Basis von Layer 2 und höher benutzt werden.

11.2.2 Z2 – Verwendung von Switchen

Anwendungsfall:
Es wird eine Kommunikation auf Basis von Layer 2 benötigt. Dazu zählt beispielsweise der Einsatz von Engineering Systemen zur Namensvergabe von PROFINET-Gerätenamen.

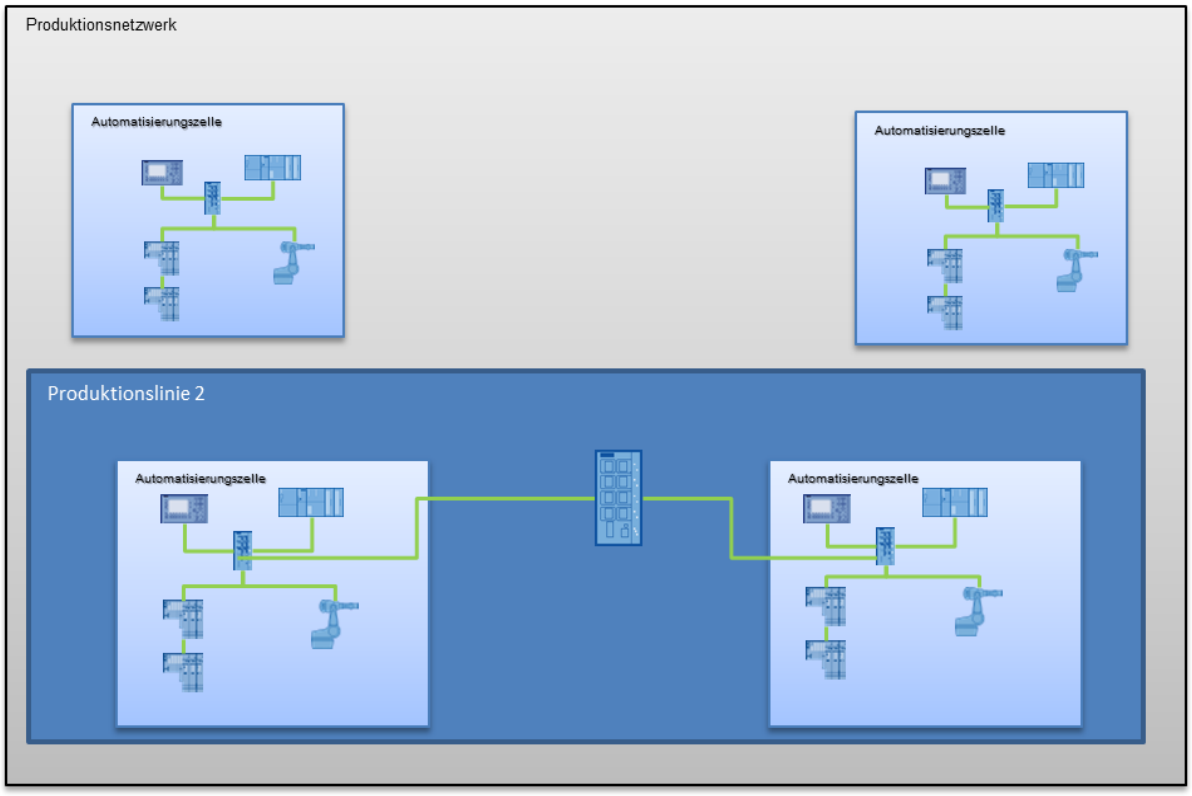

Bild 15 - Verwendung von Switchen zur Zugangskontrolle

Charakteristik
Durch die Realisierung einer Verbindung zwischen zwei Automatisierungszellen durch einen Switch ermöglicht die Nutzung von Layer-2 basierten PROFINET-Diensten.

Konsequenz:
Werden Multicast-Anfragen geschickt, können diese in beiden Automatisierungszellen gesehen werden. Abhilfe kann hier ein managed Switch schaffen, welcher die Unterdrückung von Multicastanfragen erlaubt.

11.2.3 Z3 – Verwendung von Routern

Anwendungsfall
Es soll ein IP-basierter Datenaustausch zwischen Rechnersystemen stattfinden, z.B. zur Sicherung von Qualitätsdaten.

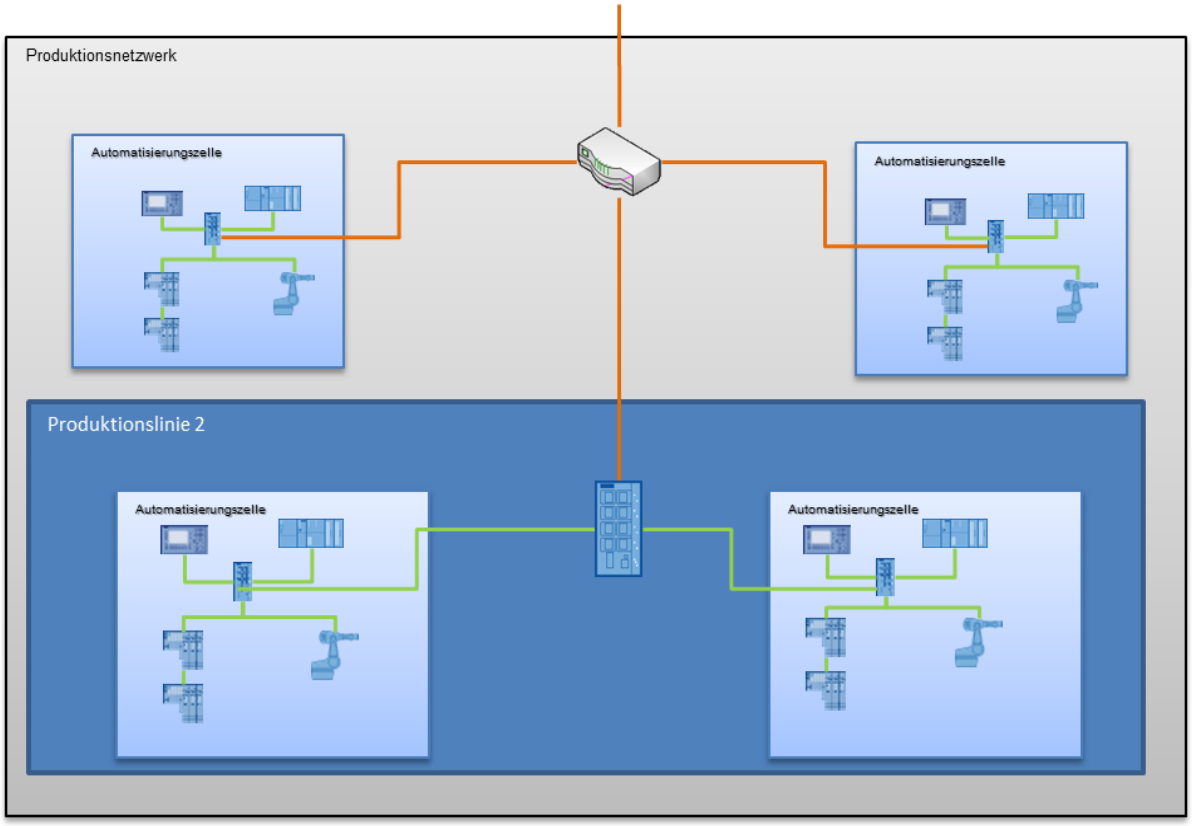

Bild 16 - Verwendung von Routern zur Zugangskontrolle

Charakteristik
Es kann eine Kommunikation auf Basis von Layer-3 und höher und keine Layer-2 Kommunikation stattfinden. PROFINET-Dienste können nicht vollständig genutzt werden.

Konsequenz
Es können keine Layer-2 basierten Dienste zwischen den einzelnen Segmenten (Automatisierungszelle bzw. Produktionslinie) verwendet werden. Lediglich IP-basierte Nachrichten können ausgetauscht werden.

11.2.4 Z4 – Verwendung von Firewalls

Anwendungsfall
Es sollen Zugriffsbeschränkungen zu den einzelnen Netzen realisiert werden. Die Beschränkungen können dabei auf Basis verschiedener Kriterien definiert werden:

- IP-Adressen spezifisch
- Dienst/Port spezifisch
- Content-spezifisch
- Nutzer-spezifisch

Betrachtet wird in den folgenden Beispielen lediglich eine klassische Firewall mit Filterkriterium IP-Adressen/Ports, da der Anwendungsfall für alle Arten der Filterung grundsätzlich identisch ist. Im einfachsten Fall trennt die Firewall das Produktionsnetz (Halle)vom übergeordneten Netz.

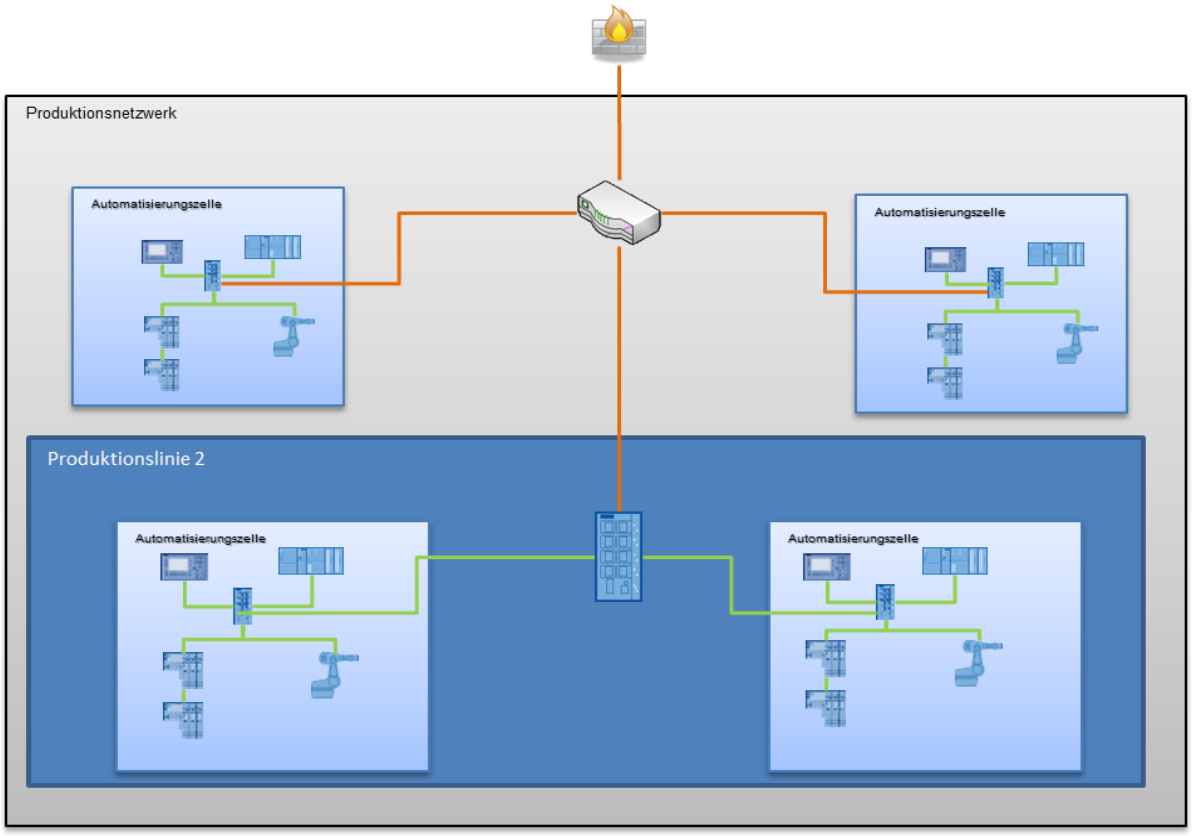

Bild 17 - Einfachster Use-Case für eine Firewall

Konsequenz

Es wird eine Kontrolle des Netzübergangs erreicht, jedoch keine Kontrolle innerhalb des Produktionsnetzes.

Eine Verfeinerung könnte an dieser Stelle die Verwendung einer weiteren Firewall darstellen welche innerhalb des Produktionsnetzwerkes eingesetzt wird.

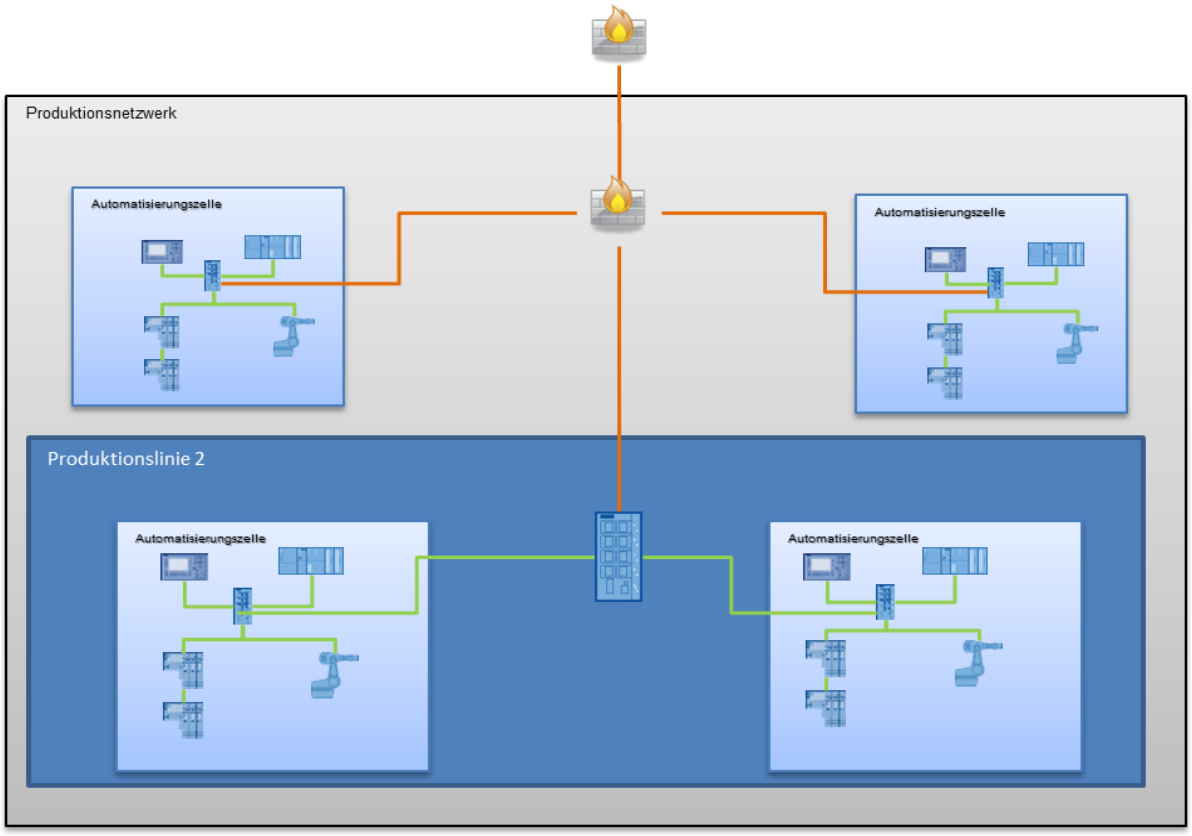

Bild 18 - Firewall innerhalb des Produktionsnetzwerkes

Konsequenz
Die Firewall trennt die Zellen innerhalb des Produktionsnetzes. Somit wird eine Kontrolle des Netzübergangs und innerhalb des Produktionsnetzes erreicht. Die übergeordnete Firewall kann dabei den Netzübergang zu mehreren Produktionsnetzen darstellen. Durch diese Anordnung kann auch der Verantwortungsbereiches für das Management der Firewalls aufgeteilt und damit eine organisatorische Trennung erleichtert werden.

Eine weitere Verfeinerung der Zugriffskontrolle ist möglich,indem je eine Firewall granular vor jeder Zelle positioniert wird.

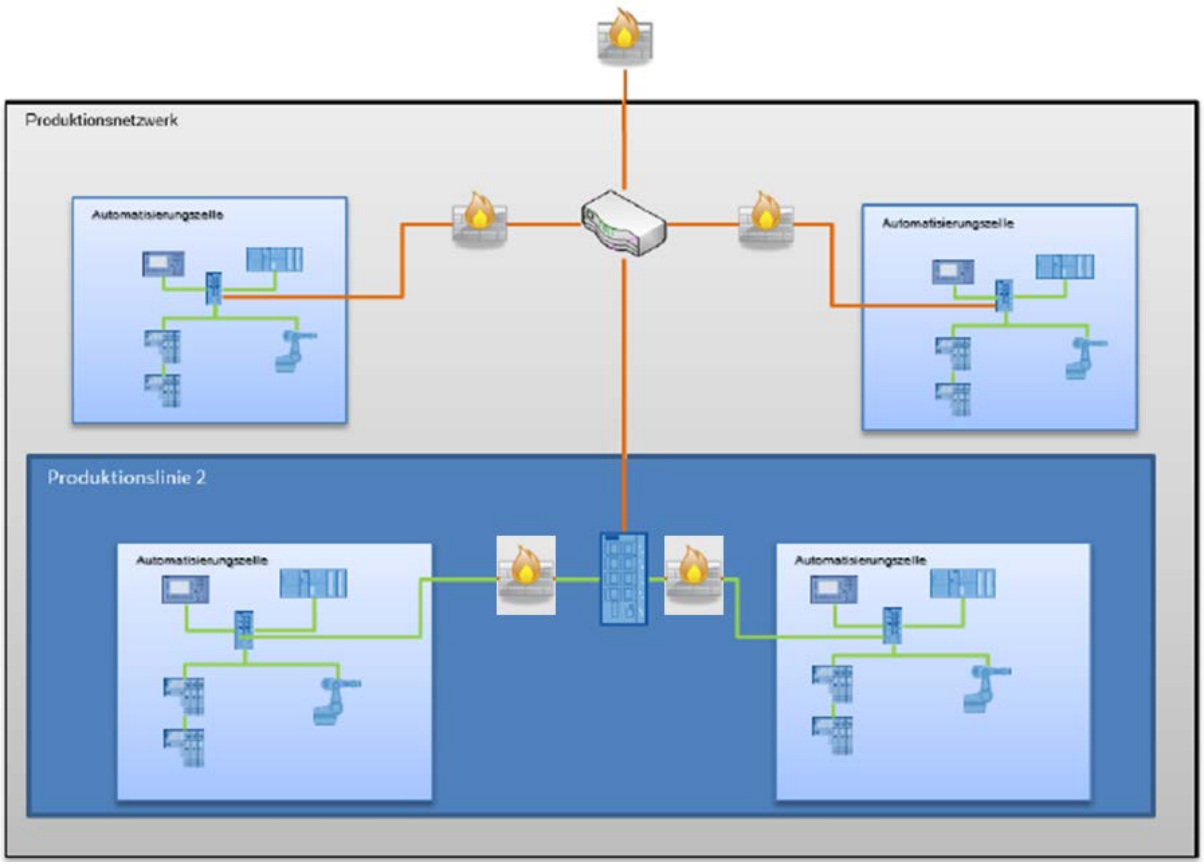

Bild 19 - Firewall Zellengranular verwendet

Der Vorteil liegt darin, dass für jede Zelle der Zugang separat verwaltet werden kann.

Konsequenz
Im Vergleich zu Bild 17 oder 18 bedeutet diese Lösung zwar einen höheren Verwaltungsaufwand, sie ermöglicht aber eine sehr klare Strukturierung, höhere Sicherheit und Verfügbarkeit durch die Verwendung mehrerer Firewalls.

11.2.5 Z5 – Verwendung von VPN

Anwendungsfall
Externer Zugriff für Service-Zwecke muss realisiert werden.
Durch den Einsatz von VPN's können authentifizierte und verschlüsselte Kommunikationsverbindungen über Netzwerkgrenzen hinweg aufgebaut werden.
Dabei sind sowohl Zugänge über die Infrastruktur des Office-Netzes, über die DMZ oder auch über einen direkten Zugang ins das Produktionsnetz realisierbar. Ein wesentliches Kriterium ist hierbei, an welcher Stelle die Positionierung des VPN-Gateways und damit die Terminierung der VPN-Verbindung erfolgt. Denn die Lage beeinflusst entscheidend, durch welche nachgelagerten Systeme (z.B. auch Firewalls) weitere Sicherheitsfunktionen realisiert werden können. VPN-Gateways sind daher auch teilweise direkt in Firewalls integriert.

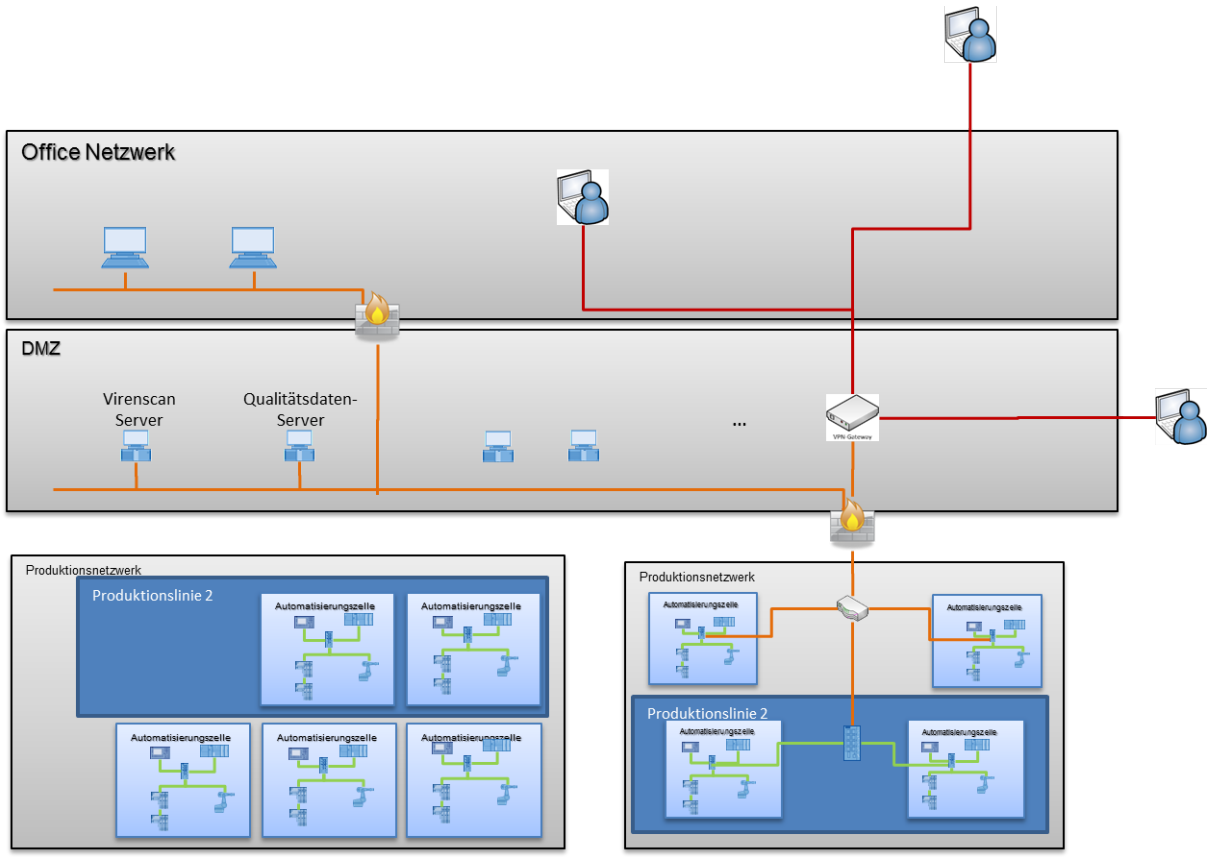

Bild 20 - VPN-Variante

Entscheidend für die Aufteilung und Anordnung der VPN-Gateways ist die erforderliche Granularität und Differenzierung für die Zugriffskontrolle. Es sin daher auch Lösungen denkbar, bei denen eine Terminierung der VPN-Verbindung vor den Automatisierungszellen erfolgt. Hierdurch ist es dann auch möglich, zwischen den einzelnen Automatisierungszellen VPN-Verbindungen zu realisieren.

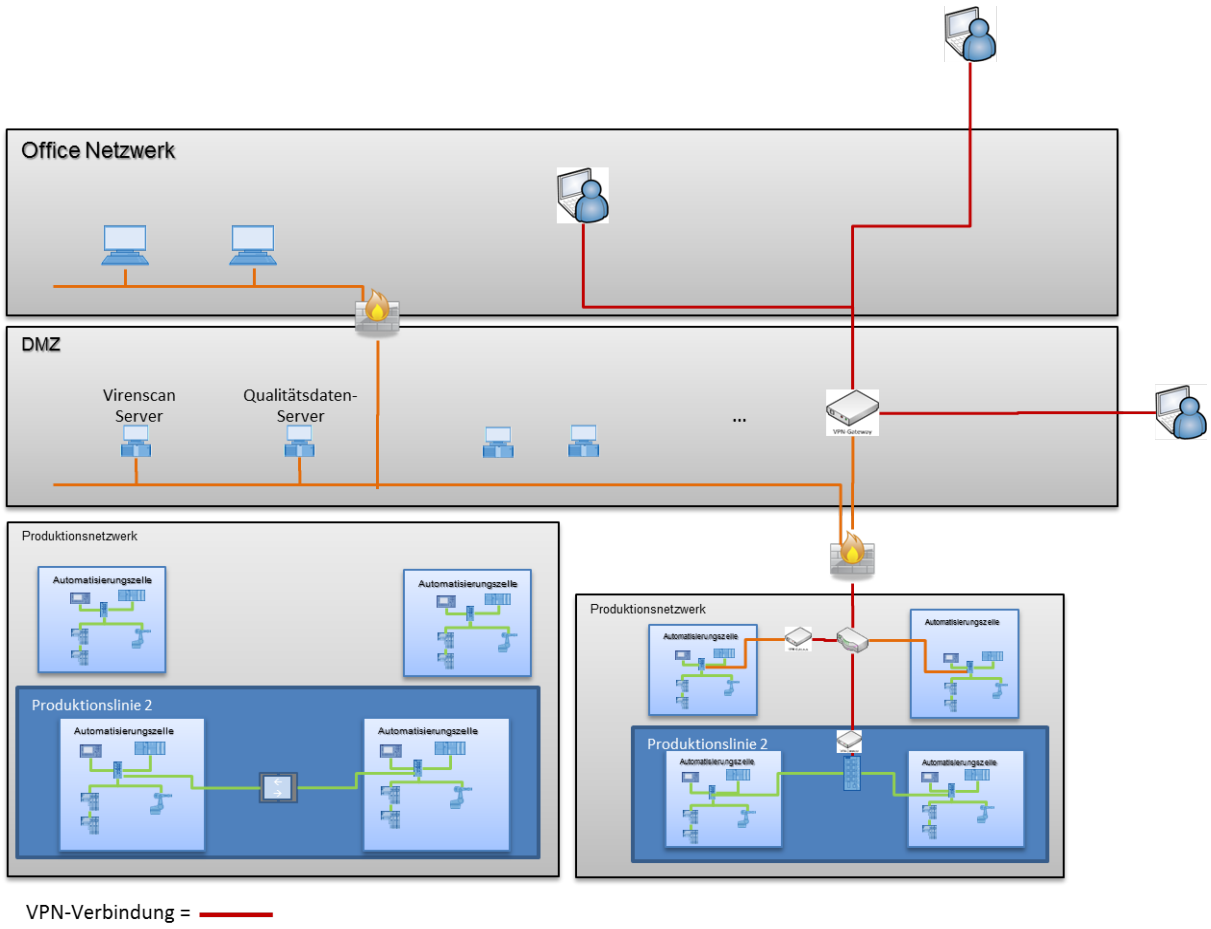

Bild 21 - VPN Variante 2

12 Zusammenfassung

Das Grundkonzept zur Erreichung eines angemessenen Schutzes für PROFINET-basierte Automatisierungslösungen basiert auf der Kontrolle der notwendigen Zugriffe auf die einzelnen PROFINET-Domänen. Dies wird erreicht durch die Segmentierung des Netzwerkes und den Aufbau von abgegrenzten Zonen und die Kontrolle der Kommunikationsverbindungen zwischen den Segmenten und Zonen (Zellenschutzkonzept). In Verbindung mit dem Einsatz unterschiedlicher Technologien und Methoden wird hierdurch ein Defence-In-Depth-Ansatz umgesetzt.

Da je nach Bedarfsfall unterschiedliche Lösungsmöglichkeiten sowie Technologien verwendet werden können und diese wiederum in individueller Kombination zueinander und in Verbindung mit den Segmenten angewendet werden können, wird ein durchgängiges Sicherheitskonzept geschaffen.

In Verbindung mit dem im Rahmen der Zertifizierung eingesetzten Security Level-1 Test, der die Robustheit der PROFINET-Geräte unter praxisbezogenen Netzlastbedingungen prüft, kommt hiermit eine Lösungskonzept zum Einsatz, das sich an die Anforderungen der jeweiligen Produktionsbedingungen anpassen lässt.

13 Anforderungen an Zertifizierungstests

Anforderungen an Zertifizierungstests werden im Dokument “Test Specification PROFINET IO Security Level 1 / Netload” Order-No. 2.302 version 1.1.2 spezifiziert.

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