Echtzeitfähige Protokollerweiterung zum Schutz Ethernet-basierter Automatisierungskomponenten

DISSERTATION

zur Erlangung des akademischen Grades

Doktoringenieur
(Dr.-Ing.)

von Markus Runde M.Eng.
geb. am 10.05.1984 in Papenburg (Ems)

Genehmigt durch die Fakultät Elektrotechnik und Informationstechnik
der Otto-von-Guericke-Universität Magdeburg

Gutachter:

Prof. Dr.-Ing. Christian Diedrich

Prof. Dr.-Ing. habil. Martin Wollschlaeger

Prof. Dr.-Ing. Karl-Heinz Niemann

Promotionskolloquium am 25.06.2014

Vorwort

Die vorliegende Arbeit ist von September 2010 bis Juni 2014 während meiner Tätigkeit als wissenschaftlicher Mitarbeiter an der Hochschule Hannover im Fachgebiet Prozessinformatik und Automatisierungstechnik entstanden. An dieser Stelle möchte ich mich bei allen Menschen im privaten und im Hochschulumfeld bedanken, die zum Gelingen dieser Arbeit beigetragen haben.

Mein besonderer Dank gilt Herrn Prof. Dr.-Ing. Karl-Heinz Niemann, der mich während meines gesamten Studiums und im Rahmen der vorliegenden Arbeit jederzeit unterstützt hat und mit Rat und Tat zur Seite stand. Durch seine Erfahrung, die Unterstützung und die zahlreichen Anregungen sowie die angenehme Arbeitsatmosphäre und die gegebenen Freiheitsgrade in der Bearbeitung der Themenstellung, war er maßgeblich an dem Gelingen der vorliegenden Arbeit beteiligt.

Besonders danke ich Herrn Prof. Dr.-Ing. Christian Diedrich an der Otto-von-Guericke Universität Magdeburg, für das entgegengebrachte Vertrauen zur Betreuung der Arbeit sowie die Übernahme der Aufgabe als Gutachter. Seine umfangreichen Hinweise und Ratschläge, insbesondere hinsichtlich der inhaltlichen Gestaltung der Arbeit, waren ein wichtiger Beitrag zum Erfolg dieser Arbeit.

Herrn Prof. Dr.-Ing. habil. Martin Wollschlaeger von der Technischen Universität Dresden danke ich für die Übernahme der Aufgabe als Gutachter. Weiterhin gilt mein Dank Herrn Prof. Dr.-Ing. Roberto Leidhold als Vorsitzenden, Herrn Dr.-Ing. Peter Eichelbaum als Fachprotokollant sowie Jun.-Prof. Dr.-Ing. Sören Hirsch als Beisitzer der Promotionskommission.

Weitere wichtige Beiträge die zum Gelingen dieser Arbeit beigetragen haben, entstammen dem Hochschulumfeld und den Partnern im Rahmen des Forschungsprojektes „SEC_PRO“. Dabei danke ich Christopher Tebbe und Stefan Hausmann für deren Diskussionsbereitschaft und die gemeinsame Arbeit an dem Projekt sowie den beteiligten Mitarbeitern bei der Firma KW Software GmbH. Mein Dank gilt weiterhin allen Studierenden, die durch ihre Mitarbeit in Form von Praxisphasen sowie Bachelor- und Masterarbeiten einen erheblichen Teil zum Erfolg dieser Arbeit beigetragen haben sowie an Irmgard Perk für das Korrekturlesen der Arbeit.

Mein Dank wäre jedoch nicht vollständig, würde ich mich nicht bei meiner gesamten Familie bedanken. Im Besonderen gilt mein Dank meiner Frau Romana sowie meinem Sohn Jonas für ihren liebevollen Rückhalt.

„ […] Wären wir bei der Pferdekutsche geblieben,
dann wäre der Airbag auch nicht innovativ gewesen.“

Unbekannt

Zusammenfassung

Die Automatisierungstechnik ist in den letzten Jahren verstärkt einem Strukturwandel unterworfen. Der Einsatz von standardisierten Kommunikationstechnologien wie Industrial Ethernet hat diesen Strukturwandel zusätzlich beschleunigt. Durch die Anwendung einheitlicher Netzwerktechnologien in verschiedenen Produktionsstandorten können übergreifend Produktionsanlagen über das Internet miteinander vernetzt werden. Diese Situation lässt Netzwerkstrukturen entstehen, die Optimierungen von Produktionsprozessen ermöglichen. Damit einher geht jedoch auch eine gesteigerte Bedrohungssituation, da vormals gegenüber der Außenwelt abgeschottete Automatisierungssysteme geöffnet werden.

Die Bedrohungssituation erfordert Schutzmaßnahmen für die IT-Sicherheit auch für Automatisierungssysteme. Aktuelle Zielsetzung ist primär die Adaption und Anwendung von Schutzmaßnahmen der Standard-IT für das industrielle Umfeld, wobei der produktive Betrieb des Automatisierungssystems unbeeinflusst bleiben muss. Dieser Ansatz birgt jedoch verschiedene Defizite, bspw. hinsichtlich des Strukturwandels in der Automatisierungstechnik, da bei aktuellen Schutzmaßnahmen von starren Strukturen ausgegangen wird. Wesentlich jedoch betrachten aktuelle Schutzmaßnahmen nicht konkret die Anforderungen der Automatisierungstechnik. Aus den zuvor genannten Gründen ist es sinnvoll und notwendig Schutzmaßnahmen zu konzipieren, die speziell für die Automatisierungstechnik gedacht sind.

Die Verwendung der Kryptografie in der Automatisierungstechnik wird bisher nicht gezielt verfolgt, argumentiert mit einem möglichen unerwünschten Einfluss auf den produktiven Betrieb der Anlage. Der gezielte Einsatz von kryptografischen Maßnahmen kann jedoch einen maßgeblichen Beitrag zur IT-Sicherheit in der Automatisierungstechnik leisten. Eine Kombination dieser kryptografischen Maßnahmen in einer IT-Sicherheitsschicht auf den verteilten Automatisierungskomponenten deckt die oben genannten Defizite ab, wobei eine wirksame und ressourcenschonende Implementierung und Anwendung der kryptografischen Verfahren sicherstellt, dass der Einfluss auf den produktiven Betrieb minimal bleibt. Dies wird durch eine Evaluierung der kryptografischen Funktionen der IT-Sicherheitsschicht auf verschiedenen Rechnerplattformen gezeigt. Der Nachweis der Schutzwirkung der konzipierten IT-Sicherheitsschicht ist durch eine Validierung nachgewiesen worden.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

ABK	**A**nzeige- und **B**edien**k**omponente
AES	**A**dvanced **E**ncryption **S**tandard
AH	**A**uthentication **H**eader
APDU	**A**pplication **P**rotocol **D**ata **U**nit
ASIC	**A**pplication-**s**pecific **I**ntegrated **C**ircuit
BNK	**B**enutzer**n**ahe **K**omponente
BSI	**B**undesamt für **S**icherheit in der **I**nformationstechnik
CA	**C**ertification **A**uthority
CBC	**C**hipher **B**lock **C**haining
CERT	**C**omputer **E**mergency **R**esponse **T**eam
CMAC	**C**ipher-based - **M**essage **A**uthentication **C**ode
CPS	**C**yber **P**hysical **S**ystems
CRC	**C**yclical Redundancy Check
DH	**D**iffie-**H**ellman
DHS	**D**epartment of **H**omeland **S**ecurity
DP	**D**ezentrale **P**eripherie
E/A	**E**in-/ und **A**usgabe
EAP	**E**xtensible **A**uthentication **P**rotocol
ECC	**E**lliptic **C**urve **C**ryptography
ECDH	**E**llipctic **C**urve **D**iffie **H**ellman
ECDSA	**E**lliptic **C**urve **D**igital **S**ignature **A**lgorithm
EK	**E**ngineering **K**omponente
EMV	**E**lektro**m**agnetische **V**erträglichkeit
ENISA	**E**uropäische **N**etz- und **I**nformations**s**icherheits**a**gentur
ESP	**E**ncapsulating **S**ecurity **P**ayload
FPGA	**F**ield **P**rogrammable **G**ate **A**rray
GCM	**G**alois **C**ounter **M**ode
GMA	**G**esellschaft für **M**ess- und **A**utomatisierungstechnik
GMAC	**G**alois – **M**essage **A**uthentication **C**ode
HMAC	**H**ash-Based **M**essage **A**uthentication **C**ode
HMI	**H**uman **M**achine **I**nterface
I^2C	**I**nter- **I**ntegrated **C**ircuit
ICS	**I**ndustrial **C**ontrol **S**ystems
ID	**Id**entifikator
IDS	**I**ntrusion-**D**etection-**S**ystem
IEC	**I**nternational **E**lectrotechnical **C**ommission
IEEE	**I**nstitute of **E**lectrical and **E**lectronics **E**ngineers
IKEv2	**I**nternet **K**ey **E**xchange (Protocol)- **V**ersion **2**
IO	**I**nput/**O**utput

IP	**I**nternet **P**rotokoll
IPS	**I**ntrusion-**P**revention-**S**ystem
ISMS	**I**nformation **S**ecurity **M**anagement **S**ystem
ISO	**I**nternational **O**rganization for **S**tandardization
IT	**I**nformations**t**echnik
MAC (Kryptografie)	**M**essage **A**uthentication **C**ode
MAC (Netzwerk)	**M**edia **A**ccess **C**ontrol
MHz	**M**ega-**H**ertz
NAMUR	Interessengemeinschaft Automatisierungstechnik der Prozessindustrie (vormals: **N**ormen**a**usschuss für **M**eß- **u**nd **R**egelungstechnik)
NAT	**N**etwork **A**ddress **T**ranslation
NIST	**N**ational **I**nstitute of **S**tandards and **T**echnology
NSA	**N**ational **S**ecurity **A**gency
ODVA	**O**pen **D**evice **V**endor **A**ssociation
PC	**P**ersonal **C**omputer
PDCA	**P**lan-**D**o-**C**heck-**A**ct
PIN	**P**ersönliche **I**dentifikations**n**ummer
PNK	**P**rozess**n**ahe **K**omponente
PNO	**P**ROFIBUS/PROFINET **N**utzer**o**rganisation
PSK	**P**re-**S**hared **K**ey
RAM	**R**andom **A**ccess **M**emory
RC4	„**R**on's **C**ode **4**“
RFC	**R**equest **f**or **C**omments
RSA	„**R**ivest **S**hamir **A**dleman“
SA	**S**ecurity **A**ssociation
SHA	**S**ecure **H**ash **A**lgorithm
SPD	**S**ecurity **P**olice **D**atabase
SPI	**S**erial **P**eripheral **I**nterface (Bus)
SPS	**S**peicher**p**rogrammierbare **S**teuerung
SSL	**S**ecure **S**ocket **L**ayer
TCG	**T**rusted **C**omputing **G**roup
TCP	**T**ransmission **C**ontrol **P**rotocol
TLS	**T**ransport **L**ayer **S**ecurity
TS	**T**raffic **S**elektror
UDP	**U**ser **D**atagram **P**rotocol
UML	**U**nified **M**odeling **L**anguage
USB	**U**niversal **S**erial **B**us
VDE	Verband der Elektrotechnik, Elektronik und Informationstechnik e.V. (vormals: **V**erband **D**eutscher **E**lektrotechniker e.V.)
VDI	**V**erein **D**eutscher **I**ngenieure e.V.
VLAN	**V**irtual **L**ocal **A**rea **N**etwork
VPN	**V**irtual **P**rivate **N**etwork

Begriffsverzeichnis

Angriff	Vorgang bei dem eine intentionale Manipulation eines (geschützten) informationstechnischen Systems (wie eines Automatisierungssystems) stattfindet, mit dem Ziel Informationen zu gewinnen oder Schäden zu verursachen.
Authentifizierung	Verifizierung der behaupteten Identität einer Entität gegenüber einer Instanz. Die Instanz authentifiziert in der Folge die Entität, die sich zu authentisieren versucht.
Automatisierungssystem	System zur Steuerung bzw. Regelung eines technischen Prozesses mit daran angeschlossenen Komponenten zur Überwachung des Prozesses.
Autorisierung	Die Autorisierung beschreibt die Einräumung spezieller Rechte gegenüber einer Instanz. Der Autorisierung geht in aller Regel die Authentifizierung voraus.
Autorisierung	Einräumung bzw. Zuweisung von Rechten einer authentifizierten Entität bzw. Identität (siehe Authentifizierung).
Bedrohung	Ein Ereignis, dass in Folge der Ausnutzung einer Schwachstelle eines (informationstechnischen) Systems Risiken für mögliche Schäden am System hervorrufen können.
Betriebsmodus	Vorgabe zur Verarbeitung bzw. Verknüpfung von verschlüsselten Daten(-blöcken) unter Verwendung von blockorientierten Ver- bzw. Entschlüsselungsverfahren.
Datenpaket	Zu übertragene Dateneinheit über ein Übertragungsmedium, die eine Nachricht bzw. Information enthält.
Dolev-Yao-Angreifermodell	Konzept eines omnipotenten und omnipräsenten Angreifers auf ein informationstechnisches System.
Engineering	Der im Umfeld der Automatisierungstechnik beschriebene Vorgang zur Projektierung von Automatisierungsanlagen.
EtherType	Ein durch das IEEE definiertes Datenfeld bei der Standard Ethernet anhand dessen eine Differenzierung von Kommunikationsprotokollen erfolgen kann.
Feldbus	Echtzeitfähiges serielles Kommunikationssystem in der Automatisierungstechnik unter Verwendung eines Busmediums.
FrameID	Datenfeld für PROFINET-Datenpakete anhand derer eine Unterscheidung zwischen den verschiedenen Kommunikationen im PROFINET-Protokoll erfolgt.
Funktionale Sicherheit	(engl. Safety) Sicherheitsbegriff, der die allgemeine Sicherheit (siehe Sicherheit) auf ein System überträgt, wobei das Risiko für einen Schaden an der Umgebung vom System selbst ausgeht.
Gefährdung	Zusammentreffen eines (informationstechnischen) Systems mit einer potentiellen Gefahrenquelle in Folge dessen eine mögliche Bedrohung sowie ein Risiko bzw. Schaden entstehen kann.

Header	Bezeichnung für vorangestellte Daten bzw. Informationen zur Verarbeitung eines nachfolgenden Datenfelds.
Identifikator	Ein einer Entität zugeordnetes Identifikationsmerkmal.
Inbetriebnahme	Die erste Aufnahme eines produktiven Betriebs nach erfolgter Projektierung und Montage des Automatisierungssystems.
Industrial Ethernet	Ein für das industrielle Umfeld konzipierte echtzeitfähige Kommunikationssystem auf Basis des Standard Ethernet.
Interframe Space	Der zwischen zwei Datenpaketen einzuhaltende zeitliche Abstand bei der Übertragung, bspw. zur Kollisionsvermeidung.
(Industrial) Switch	Komponente zum Aufbau der Kommunikationsinfrastruktur eines auf Standard Ethernet basierenden Netzwerkes, welche anhand der MAC-Adresse (ggf. unter Einbeziehung von IP-Adressen) eine Weiterleitentscheidung von Datenpaketen trifft.
Internet Protokoll (Adresse)	Verbindungsloses Protokoll, auf Schicht 3 des ISO/OSI-Referenzmodells, welches anhand der IP-Adresse eine Adressierung der Kommunikationsendpunkte vornimmt.
Intrusion-Detection-System	Schutzmaßnahme für die IT-Sicherheit bei der Angriffe auf das informationstechnische System erkannt werden.
Intrusion-Prevention-System	In Erweiterung zum Intrusion-Detection-System ist das Intrusion-Prevention-System in der Lage entdeckte Angriffe abzuwehren bzw. Gegenmaßnahmen zu ergreifen.
ISO/OSI-Schichtenmodell	Referenzmodell für Kommunikationsprotokolle als Schichtenarchitektur, bei der Kommunikationsendpunkte auf der jeweiligen Schicht eine identische Interpretation der Daten durchführen.
(IT)-Schutzziele	Zu erfüllende Grundbedingungen zur Gewährleistung der IT-Sicherheit eines informationstechnischen Systems.
IT-Sicherheit	(engl. Security) Sicherheitsbegriff, der die allgemeine Sicherheit (siehe Sicherheit) auf informationstechnische Systeme überträgt, wobei das Risiko für einen Schaden am System aus einer Bedrohung von außen auf das System entsteht.
Kommunikation	Austausch von Daten(paketen) über ein Übertragungsmedium.
Kryptoanalyse	Anwendung von Verfahren und Methoden, um Informationen aus einer verschlüsselten Nachricht zu gewinnen. Ziel ist unter anderem der Nachweis der kryptografischen Sicherheit eines Algorithmus oder die Umgehung des Algorithmus.
Network Address Translation	Verfahren, bei dem die Adressierungsinformationen eines internen Netzwerk gegenüber einem externen Netzwerk ersetzt werden, um direkten Zugriff auf Entitäten des internen Netzwerks zu unterbinden.
PROFIBUS	Echtzeitfähiges Kommunikationsprotokoll, welches ein gemeinsames Busmedium verwendet.
PROFINET	Ein auf Standard Ethernet basierendes echtzeitfähiges Kommunikationsprotokoll (auch PROFINET IO)

PROFIsafe	Technologie zur Sicherstellung der funktionalen Sicherheit für die Kommunikationsprotokolle PROFIBUS und PROFINET.
Request for Comments	Reihe von technischen sowie organisatorischen Dokumenten zur öffentlichen Diskussion, teils als Quasi-Standard etabliert.
Risiko	Qualitative bzw. quantitative Aussage über das Auftreten eines möglichen Schaden, welche sich aus verschiedenen Risikofaktoren (Eintrittswahrscheinlichkeit, Bedrohung, Schadenspotential) als Produkt berechnen lässt.
Router	Komponente der Kommunikationsinfrastruktur eines auf Standard Ethernet basierenden Netzwerkes, welche anhand der IP-Adresse eine Weiterleitung der Datenpakete an bestimmte Netzwerke durchführt.
Schadenspotential	Ausmaß einer unerwünschten und nachteiligen Veränderung (Schaden) einer Sache, Person bzw. Systems.
Schadsoftware	(auch Malware) Bezeichnung für Software, die eine schadhafte Wirkung bei Ausführung auf den Entitäten des informationstechnischen Systems haben kann.
Schutzmaßnahmen	Maßnahmen zur Erfüllen der IT-Schutzziele der IT-Sicherheit.
Schwachstelle	Eigenschaft eines (informationstechnischen) Systems, durch die eine Bedrohung auf ein System wirken kann und Schäden bzw. Risiken nach sich ziehen kann.
Sicherheit	Zustand, in dem ein mögliches Risiko für einen Schaden kleiner ist, als ein noch vertretbares Risiko.
(Standard) Ethernet	Kommunikationstechnologie mit gemeinsamem Zugriff auf ein Übertragungsmedium und Kollisionskontrolle und variabler Netzwerktopologie.
Standard IT	Informationstechnisches System im Büroumfeld.
Trailer	Bezeichnung für nachgestellte Daten bzw. Informationen zur Verarbeitung bzw. Überprüfung eines vorangegangenen Datenfeldes.
Transmission Control Protocol	Verbindungsorientiertes Protokoll auf Schicht 4 des ISO/OSI-Referenzmodells.
Trusted Computing	Ein durch die TCG dargestelltes Konzept, welches die Vertrauenswürdigkeit einer Entität in einem informationstechnischen System gegenüber einer weiteren Entität sicherstellen soll.
User Datagram Protocol	Verbindungsloseses Protokoll auf Schicht 4 des ISO/OSI-Schichtenmodells.
Virtual LAN (VLAN)	Technologie zur logischen Trennung von Kommunikation in einem auf Standard Ethernet basierenden Netzwerks, welche die Priorisierung von Datenströmen und die Aufteilung von Netzwerken in logische Teilnetzwerke ermöglicht.

1 Einleitung

In Kapitel 1 wird die Motivation dieser Arbeit hinsichtlich der Verwendung von Schutzmaßnahmen für die IT-Sicherheit in der Automatisierungstechnik dargestellt. Dazu wird zunächst eine allgemeine Übersicht zu dieser Thematik gegeben, gefolgt vom Aufbau dieser Arbeit.

1.1 Sicherheit im Umfeld vernetzter Automatisierungssysteme

Die Sicherheit besitzt im Bereich der Automatisierungstechnik einen großen Stellenwert. Der Begriff Sicherheit lässt sich in zwei Ansätze aufteilen, zum einen in die funktionale Sicherheit und zum anderen in die informationstechnische Sicherheit.

Während eigenständige Lösungen im Bereich der funktionalen Sicherheit (Safety, z.B. PROFIsafe [PNO2007]) für die Automatisierungstechnik existieren, ist der Bereich der informationstechnischen Sicherheit bzw. Datensicherheit (IT-Sicherheit) in der Automatisierungstechnik durch Lösungen der Standard-IT geprägt. So unterstreicht das VDI-Thesenpapier „Automation 2020“ [VDI2009], dass die informationstechnische Sicherheit in der Automatisierungstechnik ein wichtiges Handlungsfeld darstellt:

> *„IT-Sicherheit muss als eigenständiges und wichtiges Thema in den Prozessen des Anlagenengineerings, der Betriebsführung und der Mitarbeiterschulung etabliert werden. Ebenso sind die Hersteller automatisierungstechnischer Produkte und Systeme gefordert, entsprechende Konzepte in ihre Produktentwicklung weiter zu integrieren. Die Standardisierung spielt hier eine große Schlüsselrolle; die aus dem Internet bekannten Technologien sind jedoch hinsichtlich ihrer Übertragbarkeit auf Engineering und Betrieb einer industriellen Anlage zu überprüfen.“*

Hieraus geht hervor, dass zukünftig Anstrengungen unternommen werden müssen, um Maßnahmen der Informations- und Datensicherheit auf die Automatisierungstechnik abzustimmen, wobei die Standardisierung eine Schlüsselrolle übernimmt. Dabei muss die IT-Sicherheit als eigenständiges Thema angesehen werden, wobei bestehende Technologien bspw. aus dem Büro-Umfeld oder dem Internet auf Ihre Anwendbarkeit in der Automatisierungstechnik zu überprüfen sind.

Darüber hinaus definiert [VDI2009] weitere Anforderungen an zukünftige Maßnahmen der Informations- und Datensicherheit von Automatisierungssystemen. Hierbei stehen technische Sachverhalte im Vordergrund.

> *„Das Datensicherheitsmanagement in verteilten, offenen und drahtlosen Automatisierungssystemen zählt zu den strategischen Themen, deren Bedeutung bereits kurzfristig stark zunehmen wird. Die Spezifikation einheitlicher Methoden zur Gefahrenanalyse sowie zur Klassifikation von Risiken, [...] bei Veränderungen in der Entwicklungsumgebung von eingebetteten Systemen, die Integration von Security-Modulen in eingebettete Systeme und die Entwicklung von Konzepten für das Datensicherheitsmanagement sind herausfordernde Aufgaben der nächsten Zukunft.“*

Der Schutz von Automatisierungsanlagen bedarf angepasster IT-Sicherheitslösungen, bspw. zur Gefahrenanalyse von Automatisierungssystemen sowie bei Verfahren zur Erkennung von Veränderungen am Automatisierungssystem. Aufgrund der verteilten und offenen Strukturen von Automatisierungssystemen sind hierfür Methoden anzuwenden, die sowohl das Automatisierungsnetzwerk als auch die daran angeschlossenen Netzwerkteilnehmer mit einbeziehen. Mehr noch sollte in Erwägung gezogen werden, ob diese Verfahren z.B. durch zusätzliche (software-)technische Maßnahmen (sogenannte Security-Module) unterstützt werden können.

Die Notwendigkeit dieser Maßnahmen wird durch die zunehmende vertikale Integration von der Feldebene bis zur Betriebsleitebene und der horizontalen Integration über verschiedene Wertschöpfungsnetzwerke hervorgehoben [FOA2013]. Ein Treiber hierfür ist der zunehmende Einsatz einheitlicher Netzwerktechnologien auf Basis von Standard Ethernet. Auf diese Weise erfolgt auch eine Anbindung und Öffnung von Automatisierungsanlagen bspw. gegenüber dem Internet. Diese zunehmende Vernetzung führt dazu, dass IT-Sicherheitsprobleme aus der Standard-IT auf die Automatisierungstechnik (bspw. Malware) übertragen werden. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) [BSI2010a] beschreibt die Situation wie folgt:

> *„Wurden bislang Angriffe auf kritische Infrastrukturen und ihre Prozesssteuerungssysteme wegen der vermeintlich geringen Wahrscheinlichkeit als ‚Restrisiko' akzeptiert, gilt es nun, diese Risikobewertung neu vorzunehmen."*

Die Umsetzung aktueller Maßnahmen der IT-Sicherheit in der Automatisierungstechnik basiert auf Verfahren der Standard-IT. Wie [VDI2009] aufführt, sind diese Maßnahmen zukünftig auf ihre Anwendbarkeit in der Automatisierungstechnik zu überprüfen.

Zum Beispiel differenziert die NAMUR [NAM2006], als Interessengemeinschaft der Automatisierungstechnik und Prozessindustrie, aktuelle Lösungen der IT-Sicherheit in der Automatisierungstechnik in zwei Kategorien:

a) *Maßnahmen, die auf die Erhöhung der IT-Sicherheit von heute installierten und marktgängigen Systemen abzielen.*
b) *Die Berücksichtigung der Belange der IT-Sicherheit bei der Entwicklung der nächsten Generation von Systemen der Automatisierungstechnik. […]*

[NAM2006] führt zudem an, dass aktuelle Schutzmaßnahmen primär den in Punkt a) adressierten Aspekt berücksichtigen. Hierbei wird der Einsatz dieser Schutzmaßnahmen nicht in Frage gestellt, jedoch wird der erhöhte Bedarf spezieller Lösungen aus Punkt b) unterstrichen.

> *„Thema […] sind beide Aspekte, d. h. neben den für heutige Systeme unausweichlichen Maßnahmen wird auch die Entwicklung zukünftiger Systeme der Automatisierungstechnik unter dem Gesichtspunkt IT-Sicherheit beleuchtet."* [NAM2006]

Schäden an Mensch oder Maschine sind im Umfeld der Automatisierungstechnik in jedem Fall zu verhindern. Neben der funktionalen Sicherheit erlangt die IT-Sicherheit im Umfeld der Automatisierungstechnik eine zunehmende Bedeutung. Daher werden zunehmend angepasste IT-Sicherheitslösungen für das Umfeld der Automatisierungstechnik benötigt.

Die IT-Sicherheit von Automatisierungsanlagen unterliegt ständig wechselnden Einflüssen, wie Beispiele von Angriffen auf vernetzte Automatisierungssysteme zeigen. Die Spanne an Angriffen reicht von einfachen physischen Eingriffen bis hin zu Beeinflussungen der Kommunikation des Automatisierungsnetzwerks.

Ein Vorfall im Jahre 2008 in einem Kohlekraftwerk in England zeigte auf, dass selbst Systeme mit hohen Sicherheitsstandards betroffen sein können. Im besagten Fall verschaffte sich eine unbekannte Person, trotz starker Sicherheitsvorkehrungen, direkten Zugriff auf die Steuerungen von Turbinen im Kraftwerk [VID2008]. In Folge dessen fiel das Kraftwerk für mehrere Stunden, ohne jeglichen Anhaltspunkt über die Angriffsmetode, aus. Bis heute ist unklar, mit welcher Methode die Person die Steuerung der Turbine beeinflusst hat. Damit zeigt sich, dass eine alleinige physische Absicherung von Automatisierungsanlagen nicht ausreichend ist, besonders dann wenn ungehinderter Zugriff auf den Rest der Automatisierungsanlage besteht.

Der „Maroochy Water Breach“ [NIS2008] im Jahr 2000 stellt ein Beispiel für einen Eingriff in die Kommunikation dar. In einer Kläranlage in Australien häuften sich Fehlfunktionen in der Steuerung der Anlage. Anfangs ist man von einfachen Problemen bei der Einführung eines neuen Systems ausgegangen. Wenig später entdeckte ein Ingenieur bei der Beobachtung der Datenkommunikation, dass die Vorfälle keinem Zufall unterlagen und die Ausfälle durch äußere Beeinflussungen verursacht wurden. Es zeigte sich, dass in der weitläufigen Anlage eine Person die Verschlüsselung der drahtlosen Kommunikation der Steuerung umgangen hatte, um die Anlage unter Kontrolle bringen zu können. Die Person leitete anschließend große Mengen an Abwasser unkontrolliert und ungereinigt in die Umwelt.

Wie die beschriebenen Fälle zeigen, führen unzureichend geschützte Automatisierungsanlagen zu Sicherheitsvorfällen. Im Falle des „Maroochy Water Breach“ waren sogar Schutzmaßnahmen vorhanden, konnten jedoch durch einen Angreifer aufgrund von Insider-Wissen umgangen werden. Mit dem gleichzeitigen Einsatz mehrerer Schutzmaßnahmen wird versucht diese Schwachstellen eines Systems bzw. der Schutzmaßnahmen aufzufangen. Dieser gleichzeitige Einsatz erhöht jedoch auch den Aufwand, der zu deren Implementierung und Überwachung aufgewendet werden muss. Nicht zuletzt besteht die Möglichkeit, dass die Verfügbarkeit der Automatisierungsanlage negativ beeinflusst wird.

Ziel eines effektiven Schutzes für die Automatisierungsanlagen ist die Implementierung eines durchgehenden Schutzkonzepts, das von der Feldebene bis zur Betriebsleitebene reichen sollte. Hierbei sind Maßnahmen und Verfahren anzuwenden, die die Rahmenbedingungen in der Automatisierungstechnik erfüllen und zu einem Schutz in der gesamten Automatisierungsanlage führen, ohne dabei die Komplexität der Schutzmaßnahmen als Ganzes zu erhöhen. Hierzu ist es sinnvoll Schutzmaßnahmen transparent zu integrieren und dabei Einflüsse seitens der Schutzmaßnahmen auf die Automatisierungsanlage wie deren Verfügbarkeit zu minimieren.

1.2 Aufbau der Arbeit

Das Ziel dieser Arbeit liegt in der Erarbeitung eines neuartigen Konzepts zum Schutz eines Ethernet-basierenden Automatisierungsnetzwerkes unter Zuhilfenahme von hardwarebasierten IT-Sicherheitstechnologien. Ausgangspunkt hierfür ist die Ermittlung sowie die Erläuterung des derzeitigen Stands der Technik und der Wissenschaft. Abbildung 1-1 erläutert den Aufbau dieser Arbeit.

Abbildung 1-1: Aufbau der Arbeit

2 Grundlagen der IT-Sicherheit im Kontext der Automatisierungstechnik

Kapitel 2 stellt die Grundlagen der IT-Sicherheit vor, wobei diese im Kontext der Automatisierungstechnik beleuchtet werden. Da immer mehr Begriffe der IT-Sicherheit in der Automatisierungstechnik Verwendung finden, ist deren Erläuterung zum Verständnis dieser Arbeit notwendig. Hierfür sollen die Begriffe in Bezug zur Automatisierungstechnik betrachtet und deren Bedeutung für die Automatisierungstechnik hervorgehoben werden.

Ausgangspunkt ist der Begriff Sicherheit sowie die Schutzziele der IT-Sicherheit (►2.1). Daran erfolgt die Beschreibung der Risikofaktoren der IT-Sicherheit (►2.2) sowie durch welche Angreifertypen bzw. Motivation ein Risiko entsteht (►2.3). Die Vorgehensweise der IT-Sicherheit in Abschnitt 2.4 soll anschließend darstellen, wie dieses Risiko minimiert werden kann. Abschließend erfolgt in Abschnitt 2.5 eine Gesamtdarstellung der Situation bezüglich der IT-Sicherheit.

2.1 Begriffsdefinition zur IT-Sicherheit

2.1.1 Der Begriff „Sicherheit“

Im deutschen Sprachgebrauch hat der Begriff Sicherheit verschiedene Bedeutungen. Zum einen wird damit die funktionale Sicherheit (engl. Safety) und zum anderen die Informations- bzw. Datensicherheit (engl. Security) beschrieben. Die funktionale Sicherheit zielt dabei auf Maßnahmen ab, die ein informationstechnisches System (z.B. ein Automatisierungssystem) in einen sicheren bzw. erlaubten Zustand überführen. Im Gegensatz dazu bedeutet Security, dass ein informationstechnisches System nur solche Zustände annimmt, welche keine unerlaubte Informationsveränderung oder -gewinnung ermöglichen. [ECK2009], [DKE2013], [INT2000] In beiden Fällen ist es das Ziel, das Risiko von Schäden am informationstechnischen System zu minimieren. Oft wird der Begriff „Security“ als Synonym zu Informationssicherheit und Datensicherheit bzw. Informations- und Telekommunikations-Sicherheit (kurz: IT-Sicherheit) verwendet [DIE2004]. Im weiteren Verlauf der Arbeit wird der Begriff IT-Sicherheit genutzt, da dieser Begriff sowohl den Schutz der Informationen als auch der Kommunikation adressiert.

2.1.2 Schutzziele der IT-Sicherheit

Ziel der IT-Sicherheit ist es, die Etablierung eines angemessenen Schutzes der in diesem informationstechnischen System zu verarbeitenden Informationen und der informationsverarbeitenden Prozesse zu erreichen. Dabei ist sicherzustellen, dass eine unautorisierte Informationsveränderung und -gewinnung oder Beeinträchtigungen des Systemverhaltens (bspw. Dienste) nicht stattfinden können. Die dabei im System verwendeten Daten sind daher als schützenswerte Güter (engl. assets) anzusehen [ECK2009]. Hieraus ergeben sich entsprechende Rahmenbedingungen die nach den IT-Grundschutz-Katalogen [BSI2010b] als Grundwerte der IT-Sicherheit zu interpretieren sind und maßgebliche Eigenschaften der IT-Sicherheit darstellen. Diese Eigenschaften lassen sich in sogenannten Schutzzielen erfassen, welche in Tabelle 2-1 aufgeführt sind.

Schutzziel	Bedeutung
Integrität (engl. integrity)	Integrität ist die Eigenschaft eines Systems, einen Schutz vor unerlaubten Datenmanipulationen durch geeignete Mechanismen zu gewährleisten (inhaltliche Integrität). Nebenaspekt ist die zeitliche Integrität, die Mechanismen zur Überwachung der Zeitabfolge erfordert (zeitliche Integrität).
Vertraulichkeit (engl. confidentiality)	Vertraulichkeit ist die Eigenschaft, dass Daten oder die darin enthaltenen Informationen nur für bestimmte autorisierte Systemteilnehmer zugänglich und nicht durch Dritte auswertbar sind.
Verfügbarkeit (engl. availability)	Die Verfügbarkeit im Sinne der IT-Sicherheit beschreibt die Eigenschaft, stets die geforderten Funktionen (bspw. die Bereitstellung von Daten) zu erfüllen und den autorisierten Systemteilnehmern, wie vorgesehen, zur Verfügung zu stehen.
Authentizität (engl. authenticity)	Authentizität ist die Eigenschaft, dass die Identität eines Systemteilnehmers (eine Person oder aber auch eine technische Komponente oder Anwendung) und deren Daten zweifelsfrei verifiziert bzw. identifiziert werden können. Dieser Vorgang wird als Authentifizierung bezeichnet.
Verbindlichkeit (engl. non-repudiation)	Verbindlichkeit ist die Eigenschaft, dass die von einem Systemteilnehmer durchgeführten Aktionen (auch gegenüber Dritten) nicht abstreitbar sind.

Tabelle 2-1: Allgemeine Schutzziele der IT-Sicherheit [NIS2009b], [VDI2008]

Die Umsetzung der dargestellten Schutzziele zielt auf wohldefinierte, geschlossene informationstechnische Systeme (bspw. ein Automatisierungsanlage). Dazu wird für alle relevanten schützenswerten Bestandteile des Systems (bzw. Assets) eine Betrachtung anhand der Schutzziele durchgeführt. Durch Anwendung von Schutzmaßnahmen sind diese Assets (bzw. die Schutzziele zu den jeweiligen Assets) zu schützen. Nur durch Erfüllung der Schutzziele ist ein ausreichender Schutz des informationstechnischen Systems zu erreichen. [ISO1998], [VDI2008]

Insbesondere die Verfügbarkeit, Vertraulichkeit und Integrität werden vielfach als grundlegende Schutzziele auch in der Automatisierungstechnik aufgeführt [IEC2012b]. In offenen, verteilten Systemen ist jedoch zusätzlich die Authentizität von Systemteilnehmern sicher zu stellen. Die Feststellung der Authentizität bedarf zusätzlich der Unterscheidung zwischen autorisierten und unautorisierten Vorgängen. So kann ein Systemteilnehmer zwar authentifiziert, jedoch nicht zur Ausführung von bestimmten Funktionen autorisiert sein.

Neben den bisher aufgeführten Schutzzielen können weitere definiert werden, die zur Sicherheit eines informationstechnischen Systems beitragen. Hierunter fällt bspw. der Begriff „Vertrauen“ (engl. Trust) der im Zuge des Trusted Computing eine immer wichtigere Rolle einnimmt [MUE2008], wobei es sich weniger um eine Sicherheitseigenschaft als vielmehr um ein Konzept handelt. Der Begriff „Trust“ bezieht sich dabei auf Funktionen, die verlässliche und korrekte Daten garantieren und nicht durch Dritte korrumpiert werden können. Dieses Ziel wird durch *Autorisierung* von Vorgängen durch Authentifizierung von Nutzern mit Hilfe von Identitätsnachweisen erbracht. [MAM2006], [POR2008]

2.2 Risikofaktoren der IT-Sicherheit

Die IT-Sicherheit hat zur Aufgabe ein auftretendes Risiko auf ein akzeptables Maß zu reduzieren. Die Definition des Begriffs „Risiko“ ist wie folgt:

> *“An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.”* [INT2000]

Demnach ergibt sich das Risiko aus Sicht der IT-Sicherheit aus verschiedenen Größen. Diese Größen sind in Abbildung 2-1 in Beziehung gesetzt.

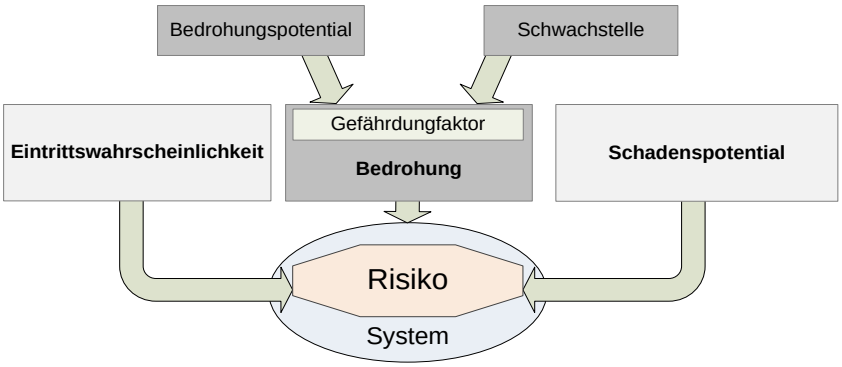


Abbildung 2-1: Begriffsbeziehung der Risikofaktoren (i.A.a. [ECK2009])

Für Maßnahmen zur Gewährleistung der IT-Sicherheit ist zunächst eine Bewertung des Risikos einer Beeinflussung des informationstechnischen Systems notwendig. Die Höhe des Risikos ergibt sich dabei aus dem Schadenspotential, der Eintrittswahrscheinlichkeit eines Ereignisses (bspw. Angriff) sowie der Bedrohung des informationstechnischen Systems. Die einzelnen Risikofaktoren werden durch Zahlenwerte erfasst. Bei diesen Werten handelt es sich um ermitteltes Wissen (z.B. Befragung) bzw. um Erfahrungswerte.

Zur Bewertung der einzelnen Risikofaktoren werden weitere Einflussgrößen berücksichtigt, die in Abschnitt 2.2.1 erläutert werden. Speziell im Falle der Bedrohung sind Gefährdungsfaktoren zu berücksichtigen. Erschwerend kommt bei der Bewertung der Bedrohung die Betrachtung des Bedrohungspotentials und der möglichen Schwachstellen hinzu.

2.2.1 Beschreibung der Risikofaktoren

Wie beschrieben, stehen die Risikofaktoren mit verschiedenen Begriffen in Beziehung. Nachfolgend sollen diese Begriffe grundlegend beschrieben werden.

- **Risikofaktor: „Eintrittswahrscheinlichkeit“**

Bei der Eintrittswahrscheinlichkeit wird die Möglichkeit bzw. Häufigkeit für das Eintreten eines Ereignisses (z.B. eines Angriffs) bewertet. Die Bewertung erfolgt in vielen Fällen auf einer subjektiven Betrachtung [BSI2008b]. Die Begründung hierfür liegt zum einen im dem unterschiedlichen Risikobewusstsein der Personen die eine Bewertung des Risikos durchführen und zum anderen daran, dass sich die Bedrohungen stets in Veränderung befinden [AND2001]. Eine konkrete Quantifizierung wird dadurch erschwert.

- **Risikofaktor: „Bedrohung“**

Allgemein hat der Begriff Bedrohung (engl. threat) die folgende Bedeutung:

> *[…] „A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm.” […]* [INT2000]

Bedrohungen existieren also nur dann, wenn Schwachstellen vorliegen, durch die Einfluss auf die IT-Sicherheit genommen werden kann. Das Ereignis, aus der eine Bedrohung entsteht kann, wird als Gefährdung bezeichnet, welche sich anhand verschiedener Begriffe beurteilen lässt. [BSI2010b]

- *Gefährdungsfaktor*

Abbildung 2-2 zeigt die grundlegenden Gefährdungsfaktoren und entsprechende Beispiele.

Abbildung 2-2: Gefährdungsfaktoren

Gefährdungsfaktoren lassen sich in fahrlässige bzw. zufällige Faktoren (nicht-intentionale Bedrohung) und vorsätzliche Faktoren (intentionale Bedrohung) unterteilen. Nur im Falle von intentionalen Gefährdungsfaktoren (bzw. Bedrohung) wird von einem Angriff gesprochen, da hier gezielt Schwachstellen ausgenutzt werden. Vorsätzliche Gefährdungsfaktoren haben ein gewisses Alleinstellungsmerkmal, da diese aktives Eingreifen voraussetzen. Da darüber hinaus sowohl intentionale wie auch nicht-intentionale Gefährdungsfaktoren die gleichen Auswirkungen haben können, sind stets Schwachstelle und das Bedrohungspotential bei der Betrachtung des Risikofaktors „Bedrohung“ mit zu berücksichtigen.

- *Schwachstelle*

Abbildung 2-1 zeigt, dass ein Risiko für ein informationstechnisches System aus einer Bedrohung nur durch das Vorhandensein einer Schwachstelle entstehen kann.

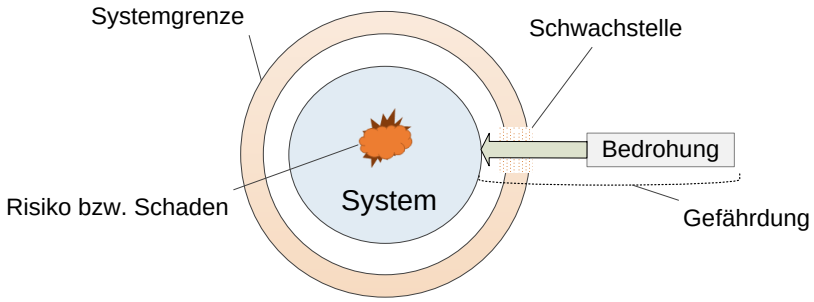


Abbildung 2-3: Wirken einer Bedrohung auf eine Automatisierungsanlage

Eine Schwachstelle ist ein ungeschützter, verwundbarer Punkt an der Systemgrenze. Über diese Schwachstelle wirkt eine Bedrohung ein. Gemeinsam stellen die Bedrohung sowie die Schwachstelle die Gefährdung dar. Über eine Schwachstelle ist eine angreifende Person in der Lage das Systemverhalten unerlaubt zu verändern oder ggf. Kontrolle über das informationstechnische System zu erlangen. Aus diesem Grund ist die Schwachstelle eine Basis zur

Bewertung der Risikofaktor „Bedrohung“. Da die Bedrohung per Definition erst durch eine Schwachstelle wirksam werden kann bzw. entsteht und in der Regel außerhalb des Wirkungsbereichs des Betreibers des informationstechnischen Systems liegt (vgl. Systemgrenze), kann eine Risikoreduzierung durch Schutzmaßnahmen nur durch Etablierung von Schutzmaßnahmen zur Schließung von Schwachstellen erfolgen.

- *Bedrohungspotential*

Bei der Risikobewertung ist zu berücksichtigen welche Stärke diese Bedrohung hat bzw. welche Auswirkung diese Bedrohung auf das Systemverhalten darstellt. Dieser Begriff wird als Bedrohungspotential definiert. Gemeinsam mit der Schwachstelle stellt damit das Bedrohungspotential die zweite Größe dar, um die Auswirkung einer Bedrohung auf das Risiko eines Systems erfassen zu können.

- **Risikofaktor: „Schadenspotential“**

Neben der Bedrohung und der Eintrittswahrscheinlichkeit ergibt sich das Risiko für ein informationstechnisches System, wie einer Automatisierungsanlage, aus dem Schadenspotential. Das Schadenspotential beschreibt allgemein das mögliche Ausmaß eines Schadens (Schadenswert), welcher bspw. in Folge eines Angriffs auf das informationstechnische System auftreten kann. Das Ausmaß des Schadens ergibt sich dabei insbesondere aus der Bedeutung des betrachteten Bestandteils des informationstechnischen Systems woraus ein möglicher Schaden für das System ausgehen kann.

2.2.2 Einstufung der Risikofaktoren

Im Zuge einer Risikoanalyse wird das Gesamtrisiko einer Bedrohung für das Automatisierungssystem ermittelt. Für jede Bedrohung werden die einzelnen Risikofaktoren im Rahmen der Risikobewertung erfasst und mit den Stufen von gering bis hoch bewertet.

Stufe	Beschreibung	Wert
Gering	Ein geringes Risiko betrifft Ereignisse oder Wahrscheinlichkeiten, die nahezu nicht denkbar oder auszuschließen sind. Schäden sind minimal.	**1**
Gering bis Mittel	Ein Ereignis dessen Auftreten möglich und nicht auszuschließen ist. Ein Ereignis dieser Kategorie erzeugt kleine Schäden.	**2**
Mittel	Ein mittleres Risiko betrifft Ereignisse dessen Auftreten wahrscheinlich ist und darüber hinaus zu Schäden führen kann.	**3**
Mittel bis Hoch	Ereignisse dieser Kategorie führen zu nennenswerten Schäden bzw. das Auftreten ist wahrscheinlich.	**4**
Hoch	Ein Ereignis dessen Wahrscheinlichkeit sehr hoch ist oder deren Auswirkungen gravierend sind.	**5**

Tabelle 2-2: Bewertungsstufen der Risikofaktoren

Ist entsprechend Tabelle 2-2 eine Einstufung der Risikofaktoren für die einzelnen Bedrohungen erfolgt, ist das Gesamtrisiko zu ermitteln. Dazu sind die einzelnen Faktoren durch Multiplikation miteinander zu verknüpfen, wodurch das Gesamtrisiko ermittelt wird. Im Gegensatz zur Addition bewirkt die Multiplikation, dass ein einzelner Risikofaktor das Gesamtrisiko einer Bedrohung erheblich steigert und damit die möglichen Folgen dieser Bedrohung hervorhebt. Für das Gesamtrisiko sind analog zu den Risikofaktoren Stufen zu definieren, die das Risiko für eine Bedrohung insgesamt erfassen. Tabelle 2-3 zeigt die Definition der Stufen des Gesamtrisikos.

Gesamtrisiko	Gering	Gering bis Mittel	Mittel	Mittel bis Hoch	Hoch
Wert des Gesamtrisikos	≤ 25	≥ 25 … 49	≥ 50 … 74	≥ 75 … 99	≥ 100

Tabelle 2-3: Bewertungsstufen des Gesamtrisikos

Aufgrund der bereits dargestellten Auswirkungen auf Mensch und Maschine im Umfeld der Automatisierungstechnik, sind Risiken nur in einem geringen bis mittleren Maße akzeptabel. Im Vergleich dazu, stehen einfache sicherheitsunkritische Systeme, wie Standard-IT Netzwerke, bei denen akzeptable Risiken allgemein höher sind. Demnach wird in der folgenden Bewertung für das Risiko einer Automatisierungsanlage das akzeptable Risiko als niedrig angesetzt. Dies hat zur Folge, dass schon kleine Risiken eine Betrachtung finden und bei der Risikoreduzierung berücksichtigt werden.

2.2.3 Problematik der Bewertung der Risikofaktoren

Aufgrund der drei genannten Risikofaktoren ist es schwierig das Risiko in Bezug auf die IT-Sicherheit eines informationstechnischen Systems zu bewerten. Je nach bewertender Person erhalten die Risikofaktoren entweder unterschiedliche Gewichtungen oder die Ursachen dieser Größen werden in ihrer Kritikalität höher oder niedriger angesehen. Um diese Unsicherheit abfangen zu können, werden Risikobewertungsverfahren in interdisziplinären Gruppen durchgeführt. Diesen Gruppen sollten mehrere Personen aus verschiedenen Personenkreisen (bspw. Inbetriebnehmer, Betreiber, Bediener usw.) angehören, um im Ergebnis zu einer realistischen Risikobewertung zu gelangen.

Eine Bedrohung, als Ausgangspunkt eines Risikos, kann intentionaler als auch nicht-intentionaler Art sein. Ob eine Bedrohung jedoch intentionalen oder nicht-intentionalen Ursprungs ist, kann der Betreiber eines informationstechnischen Systems nicht erkennen. Daher schließen Bedrohungsanalysen in der Regel sowohl intentionale als auch nicht-intentionale Bedrohungen mit ein. Gleiches gilt für Schutzmaßnahmen die gegen intentionale Bedrohungen gerichtet sind, da sie gleichermaßen gegen nicht-intentionale Bedrohungen wirken. Der im Rahmen dieser Arbeit angestrebte Schutzansatz zielt primär gegen intentionale Bedrohungen, kann jedoch auch gegen nicht-intentionale Bedrohungen wirken.

Im Falle intentionaler Bedrohungen (Angriffe) sind Motivationen vielfältig und erschweren zusätzlich eine genaue Risikobewertung. Im späteren Verlauf dieser Arbeit wird eine Risikobewertung anhand einer generischen Automatisierungsanlage durchgeführt. Im folgenden Abschnitt erfolgt eine Übersicht von Angriffsarten und deren Motivationen um deren Einfluss auf die Risikobewertung aufzuzeigen.

2.3 Angreifertypen und deren Motivation

IT-Systeme sind unterschiedlichen Angriffen ausgesetzt, die mit Vorsatz durchgeführt werden. Tabelle 2-4 zeigt drei grundlegende Angreifertypen sowie deren Eigenschaften und Motivationen. Beispielhaft führt die Tabelle 2-4 für jeden Angreifertyp eine allgemeine Bewertung der Risikofaktoren auf. Eintrittswahrscheinlichkeit und Bedrohung eines Angriffs ergeben sich aus dem jeweiligen Angreifertyp, bzw. aus dessen Eigenschaften, Motivation und deren Know-How. Das Schadenspotential wird für die folgende Betrachtung zunächst als „Mittel“ definiert. Das Gesamtrisiko wird üblicherweise durch Multiplikation der verschiedenen Risikofaktoren ermittelt.

Know-How		**Niedrig**	**Mittel**	**Hoch**
Angreifertypen		• „Skript-Kiddies“	• Hacker bzw. Cracker • Kriminelle Gruppen	• Nachrichtendienste • Militär / Regierung
Eigenschaft		• Verwendung von standardisierten Angriffswerkzeugen aus dem Internet. • Geringes Wissen über IT-Sicherheit oder das System das sie angreifen.	• Sie sind in der Lage Schwachstellen eines Systems zu finden und für ihre Zwecke einzusetzen. • Weitreichendes Wissen über IT-Sicherheit oder das System das sie angreifen.	• Sehr gute technische und finanzielle Ausstattung. • Weitreichende und tiefgehende Kenntnisse über die IT-Systeme und IT-Sicherheit.
Motivation		• Motivation reicht von Spaß bis hin zu finanziellen Interessen oder Rache.	• *Kriminelle*: Finanzielle Aspekte, Erpressung • *Hacker:* Schwachstellen aufdecken • *Cracker:* Ausnutzung von Schwachstellen (finanzielle Aspekte)	• Beschaffung von Informationen (Spionage) • Sabotage
Risikofaktoren	**Eintrittswahrscheinlichkeit**	Hoch (5)	Mittel (3)	Niedrig (2)
	Bedrohung	Niedrig (2)	Mittel (3)	Hoch (5)
	Schadenspotential	Mittel (3)	Mittel (3)	Mittel (3)
Wert des Gesamtrisikos		Gering bis Mittel (30)	Gering bis Mittel (27)	Gering bis Mittel (30)

Tabelle 2-4: Gegenüberstellung von Angreifertypen und deren Gesamtrisiko

Tabelle 2-4 zeigt, dass je nach Angreifer ein unterschiedlich hoher Wert der Risikofaktoren entsteht. Mit Annahme eines mittleren Schadenpotentials zeigt sich, dass Angriffe, die mit hoher Wahrscheinlichkeit auftreten aber eine geringere Bedrohung aufweisen, ein ebenso großes Gesamtrisiko darstellen können, wie Angriffe die seltener auftreten, aber eine größere Bedrohung aufweisen.

Aufgrund des gleichbleibenden Gesamtrisikos müssen nicht zwingend die größten finanziellen und technischen Anstrengungen unternommen werden um die größtmögliche Bedrohung abzudecken, wenn deren Eintrittswahrscheinlichkeit gering ist [AND2001]. Vielmehr sind effiziente Schutzmaßnahmen der IT-Sicherheit gefragt, die eine realistische Bedrohungssituation betrachten. Dies gilt ebenso für die Entwicklung von neuen Schutzmaßnahmen. Mit Blick auf die Automatisierungstechnik gewinnt dieser Punkt an Wichtigkeit, da effiziente Schutzmaßnahmen gefragt sind.

2.4 Grundmaßnahmen der IT-Sicherheit

In den vorangegangenen Abschnitten sind Begriffe der IT-Sicherheit definiert und ein Bezug zum Risiko für ein informationstechnischen System hergestellt worden. Nachfolgend sollen allgemeine Aufgaben und die Zielsetzung der IT-Sicherheit erläutert werden.

2.4.1 Aufgaben und Zielsetzung der IT-Sicherheit

Die Aufgabe der IT-Sicherheit liegt in der Umsetzung von Maßnahmen zur Risikoreduzierung [GRA2003]. Wie in Abschnitt 2.2.2 dargestellt, besteht dabei die Schwierigkeit in der Risikobewertung [BSI2008a]. So können bei gleicher Faktenlage unterschiedliche Personen zu unterschiedlichen Bewertungen des Risikos kommen und so unterschiedlich starke Schutzmaßnahmen getroffen werden [KKW2012].

Schutzmaßnahmen dienen der Reduzierung von Risiken bzw. der Risikofaktoren. Eintrittswahrscheinlichkeit und Schadenspotential eines Risikos lassen sich jedoch nicht direkt beeinflussen, sind aber direkt mit der jeweiligen Bedrohung verknüpft. Wie Abschnitt 2.2.1 darstellt, existiert eine Bedrohung nur dann, wenn eine entsprechende Schwachstelle existiert. Da die Schwachstelle im Wirkungsbereich des Betreibers des Systems liegt, kann sie durch Einsatz von (verbesserten) Schutzmaßnahmen geschlossen werden, sofern durch entsprechende Analysen die Schwachstelle aufgedeckt wurde. Auf diese Weise wird gleichzeitig die Eintrittswahrscheinlichkeit für einen Angriff über die entsprechende Bedrohung gesenkt. Der potentielle Schaden durch diesen Angriff wird demzufolge auch reduziert.

Eine oder mehrere Schutzmaßnahmen dienen der Erfüllung der definierten Schutzziele. Schutzmaßnahmen wiederum können in verschiedene Schutzfunktionen und -klassen eingeteilt werden [GUT2010]. Nach [JAH2003] ist eine weitere Unterteilung der Schutzfunktionen möglich (Prävention, Detektion und Reaktion). Präventive Systeme (z.B. kryptografische Verfahren) haben zum Ziel Schwachstellen von Vornherein zu schließen. Bei der Detektion werden Schwachstellen erfasst, z.B. durch ein Intrusion-Detection-System [NJW2004]. Intrusion-Detection-Systeme können wiederum um Mechanismen erweitert werden, die Schwachstellen (reaktiv) schließen (Intrusion-Prevention-System).

Die IT-Sicherheit hat die Aufgabe, aus diesen Schutzmaßnahmen geeignete Lösungen auszuwählen, um damit schützenswerte Assets und deren Schutzziele abzudecken. Diese Aufgabe wird durch ein Management-Verfahren übernommen, welches über den gesamten Lebenszyklus des IT-Systems durchgeführt wird. [ECK2009]

2.4.2 Umsetzung von Schutzmaßnahmen für die IT-Sicherheit

Aufgrund der ständig steigenden Bedrohung von informationstechnischen Anlagen [SEC2013], ist es sinnvoll, Schutzmaßnahmen zyklisch zu überprüfen bzw. neue Maßnahmen einzusetzen oder bestehende zu verbessern bzw. zu erneuern. Ein solcher iterativer Ansatz, findet sich in vielen Managementprozessen wieder, oft auch als Plan-Do-Check-Act-Konzept (kurz: PDCA) bezeichnet. [ISO2008] Dieser PDCA-Ansatz lässt sich jedoch nicht nur bei der zyklischen Überprüfung anwenden, sondern auch bei der Entwicklung von neuen Schutzmaßnahmen in der IT-Sicherheit übertragen.

In [AND2001] wird ein solcher iterativer Prozess für die IT-Sicherheit beschrieben. Abbildung 2-4 zeigt diesen iterativen Prozess.

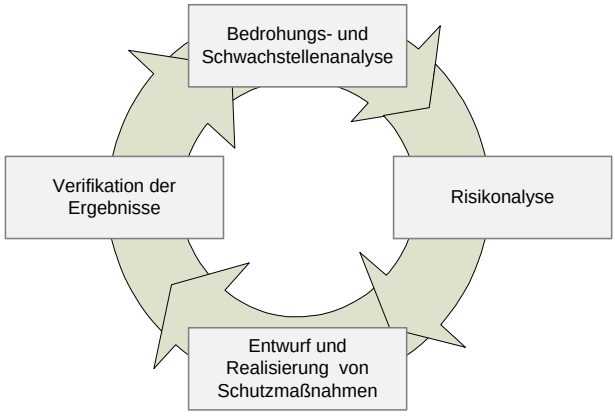


Abbildung 2-4: Vorgehensweise bei der Erstellung von Schutzmaßnahmen

Während der Bedrohungs- und Schwachstellenanalyse werden Gefährdungen eines IT-Systems ermittelt, worauf eine Risikoanalyse folgt. Darauf können geeignete Schutzmaßnahmen entworfen und realisiert werden, die die jeweiligen Schwachstellen schließen, um so eine Risikominderung herbei zu führen. Abschließend sind diese Maßnahmen zu bewerten und ggf. anzupassen. Erst hierdurch wird die Wirksamkeit eines Schutzes nachgewiesen [BSI2013b]. Dieser Analysevorgang wird dann in regelmäßigen Abständen wiederholt durchlaufen.

Dieser generische Ansatz findet in der Automatisierungstechnik bei der Umsetzung von Schutzmaßnahmen in der IT-Sicherheit eine Anwendung. Im folgenden Kapitel 3 wird dabei auf eine spezielle Methode in der Automatisierungstechnik bezogen. Diese systematische Methode dient dann als Grundlage für die Erarbeitung eines Schutzkonzepts, welches im Rahmen dieser Arbeit konzipiert wird.

2.5 Gesamtdarstellung zu den Aufgaben der IT-Sicherheit

Kapitel 2 erläuterte bisher die grundlegenden Begriffe der IT-Sicherheit. Ausgangspunkt war der Begriff „Sicherheit“ der unterschiedliche Bedeutungen aufweisen kann. Schutzziele zeigten dabei auf, wie diese Sicherheit im Sinne von IT-Sicherheit erreicht werden können. Aufgabe der IT-Sicherheit ist die Risikoreduzierung, wobei das Risiko durch drei maßgebliche Größen bestimmt wird: Der Eintrittswahrscheinlichkeit, dem Schadenpotential und der Bedrohung. Die Bedrohung existiert jedoch nur dann, wenn eine Schwachstelle existiert, die durch eine angreifende Person vorsätzlich (intentional) genutzt werden kann.

Die Aufgabe der IT-Sicherheit liegt somit in der Beseitigung von Schwachstellen, da diese im Gegensatz zur Eintrittswahrscheinlichkeit und dem Schadenspotential im direkten Wirkungsbereich des Betreibers einer Anlage liegen. Schutzmaßnahmen werden ergriffen, um Schwachstellen zu schließen. Ziel ist es, die Risiken für Schäden an dem informationstechnischen System auf ein akzeptables Niveau abzusenken. Die dabei angewendeten Schutzmaßnahmen sind dabei iterativ zu bewerten und regelmäßig zu verbessern. Im nachfolgenden Kapitel 3 soll ein Bezug zwischen IT-Sicherheit im Umfeld der Automatisierungstechnik und der Standard-IT hergestellt werden.

3 Grundlagen der Automatisierungstechnik

Kapitel 3 stellt die Grundlagen der Automatisierungstechnik im Kontext dieser Arbeit vor. Zusätzlich wird ein Ausblick auf die IT-Sicherheit in der Automatisierungstechnik gegeben. Die zuvor eingeführten Begriffe aus Kapitel 2 dienen als Ausgangspunkt zur Erläuterung der IT-Sicherheit in der Automatisierungstechnik. Diese Begriffe haben im Umfeld der Automatisierungstechnik inzwischen an Bedeutung zugenommen, da Standard-IT und Automatisierungstechnik immer mehr zusammenwachsen. [BEM2007].

Das Grundlagenkapitel zur Automatisierungstechnik startet zunächst mit dem Aufbau einer Automatisierungsanlage und der darin verwendeten Komponenten sowie Kommunikationslösungen. (► 3.1). Ein dabei abzeichnender Trend ist die Verwendung von Industrial Ethernet, dessen Grundlagen in Abschnitt 3.2 erläutert werden. Diese Verwendung hatte dabei Auswirkungen auf die IT-Sicherheit von Automatisierungsanlagen. Die Aktivitäten bezüglich der IT-Sicherheit in Automatisierungsanlagen und deren Zielsetzung werden daher in Abschnitt 3.3 im Überblick erläutert. Abschließend erfolgt eine Diskussion über die aktuelle Situation hinsichtlich der IT-Sicherheit in der Automatisierungstechnik.

3.1 Aufbau einer Automatisierungsanlage

Abschnitt 3.1 erläutert den Aufbau Automatisierungskomponenten und Automatisierungsanlagen. Kommunikationslösungen beeinflussen maßgeblich den Aufbau einer Automatisierungsanlage. Dieser Einfluss soll speziell betrachtet werden.

3.1.1 Aufbau und Arten von Automatisierungskomponenten

Per Definition handelt es sich bei Automatisierungskomponenten um Geräte, welche die Überwachung bzw. Beeinflussung eines technischen Prozesses übernehmen. Die Definition für ein Gerät ist:

> *„Ein (Gerät ist ein) räumlich materiell abgegrenzter Gegenstand der signalumsetzende (in der Abgrenzung zu energie- und stoffumsetzende Gegenstände) Aufgaben erfüllt.“* [DKE2012], [DKE2013]

Der prinzipielle Aufbau einer Automatisierungskomponente ist in Abbildung 3-1 dargestellt.

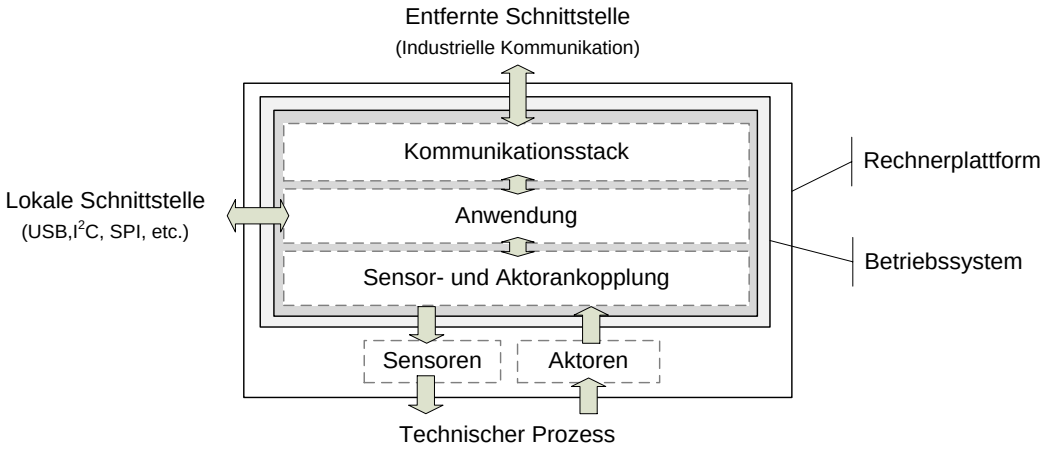


Abbildung 3-1: Aufbau einer Automatisierungskomponente (i.A.a. [DKE2012])

Automatisierungskomponenten basieren auf Rechnerplattformen. Auf diesen Plattformen werden, neben dem Betriebssystem, Softwarebestandteile implementiert, die sowohl die ein- und ausgehenden Signale des technischen Prozesses verarbeiten als auch die Schnittstellen für die lokale sowie entfernte Bedienung und Kommunikation zur Verfügung stellen. Über die lokale und entfernte Schnittstelle wird die Übertragung der Informationen durchgeführt, die über die Anwendung zur weiteren Bearbeitung an andere Bestandteile der Automatisierungsanlage gesendet werden. Die Anwendung führt dazu Mess- Steuer- und Regelfunktionen aus. Je nach Automatisierungskomponente werden unterschiedliche Aufgaben übernommen. Dazu wird zwischen prozessnahen Komponenten (PNK) und benutzernahen Komponenten (BNK) differenziert.

- **Prozessnahe Komponenten (PNK)**

Eigenschaft	Bei PNK handelt es sich um solche Automatisierungskomponenten die direkt in Verbindung mit dem technischen Prozess stehen oder ihn beeinflussen. Unterschieden wird hier zwischen der speicherprogrammierbaren Steuerung und der dezentralen Peripherie.

Speicherprogrammierbare Steuerung (SPS)	**Dezentrale Peripherie**
Die SPS ist eine programmierbare Automatisierungskomponente, welche ein- und ausgehende Signale verarbeitet, die über angeschlossene Sensoren oder Aktoren (z.B. Feldgeräte) anliegen. Die SPS übernimmt dabei die Regelungs- und Steuerungsaufgaben. In weitverteilten Automatisierungsanlagen können ein- und ausgehende Signale auch über entfernte Kommunikationsschnittstellen (z.B. Industrial Ethernet) verarbeitet werden. Komponenten (auch Feldgeräte), die Signale über eine solche Kommunikationsschnittstelle an eine SPS zur Bearbeitung übertragen, werden als dezentrale Peripherie bezeichnet.	Die dezentrale Peripherie übernimmt die Weiterleitung der ein- und ausgehenden Signale an eine SPS, ohne sie selbst zu verarbeiten (z.B. Remote E/A). Aufgrund des geringen Aufwands für die Weiterleitung der Signale, werden dafür kostengünstige und ressourcen-beschränkte Rechnerplattformen eingesetzt. Zur Kommunikation ist die dezentrale Peripherie über eine Kommunikationsschnittstelle an eine Kommunikationsinfrastruktur (z.B. Industrial Ethernet) angeschlossen. Im Kontext dieser Arbeit werden Feldgeräte, die über eine Kommunikationsschnittstelle angebunden sind, ebenso als dezentrale Peripherie bezeichnet. Zur Gruppe der dezentralen Peripherie gehören außerdem Komponenten wie Remote E/A und Antriebe.

Tabelle 3-1: Prozessnahe Komponenten

- **Benutzernahe Komponenten (BNK)**

Eigenschaft	Bei BNK wird zwischen Engineering-Komponente (EK) und Anzeige und Bedienkomponente (ABK) unterschieden. BNK werden durch PCs realisiert und beeinflussen die prozessnahen Komponenten, nehmen jedoch keine Steuerungs- und Regelungsaufgaben war.

Engineering-Komponente (EK)	**Anzeige- und Bedienkomponente (ABK)**
Die Engineering-Komponente dient der Konfiguration und Parametrierung der PNK. Nach vollständiger Erstellung aller Engineering-Daten werden diese auf die PNK übertragen, was bedeutet, dass die EK nicht permanent mit der Anlage verbunden sein muss.	Die ABK dient der Visualisierung von übergeordneten Informationen aus einem Automatisierungssystem. Zusätzlich sind Eingriffe in den technischen Prozess möglich. Aufgrund dieser Eigenschaft, ist die ABK permanent mit der Anlage verbunden.

Tabelle 3-2: Benutzernahe Komponenten

Im folgenden Abschnitt werden die genannten Komponenten zum Aufbau einer Automatisierungsanlage verwendet.

3.1.2 Die Entwicklung der „Automatisierungspyramide“

Digitale Feldbussysteme führten zu einem Durchbruch in der Automatisierungstechnik, da so auf einem Medium mehrere Automatisierungskomponenten gleichzeitig mit hohem Datendurchsatz entfernt voneinander angebunden werden konnten. [REI2002]

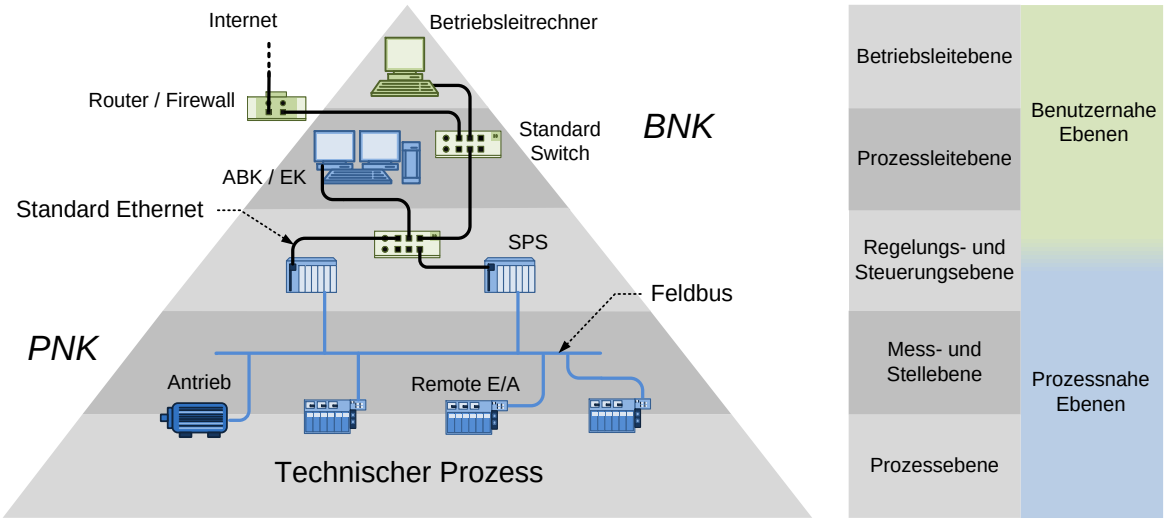


Abbildung 3-2: Automatisierungspyramide auf Basis eines Feldbussystems

Feldbustechnologien wie PROFIBUS [IEC2008b] werden dazu in den prozessnahen Ebenen eingesetzt. Die Vernetzung auf der benutzernahen Ebene erfolgt mit Standard Ethernet, wobei Standard Netzwerkkomponenten (Standard Switches) verwendet werden. Wie in Abbildung 3-2 zu sehen ist, erfolgt die Vernetzung auf den prozessnahen und benutzernahen Ebenen jeweils auf Basis einer eigenen Netzwerktechnologie. Der zunehmende Einsatz von Standard Ethernet und damit verbundene Kostenvorteile führten ab den 90er-Jahren zu einer echtzeitfähigen Adaption dieser Netzwerktechnologie an die Automatisierungstechnik, bekannt als Industrial Ethernet. Die Vorteile liegen in einer homogenen Netzwerkstruktur und einem hohen Datendurchsatz sowie einer durchgehenden Vernetzung auf Basis einer einheitlichen Technologie. [FUR2003]

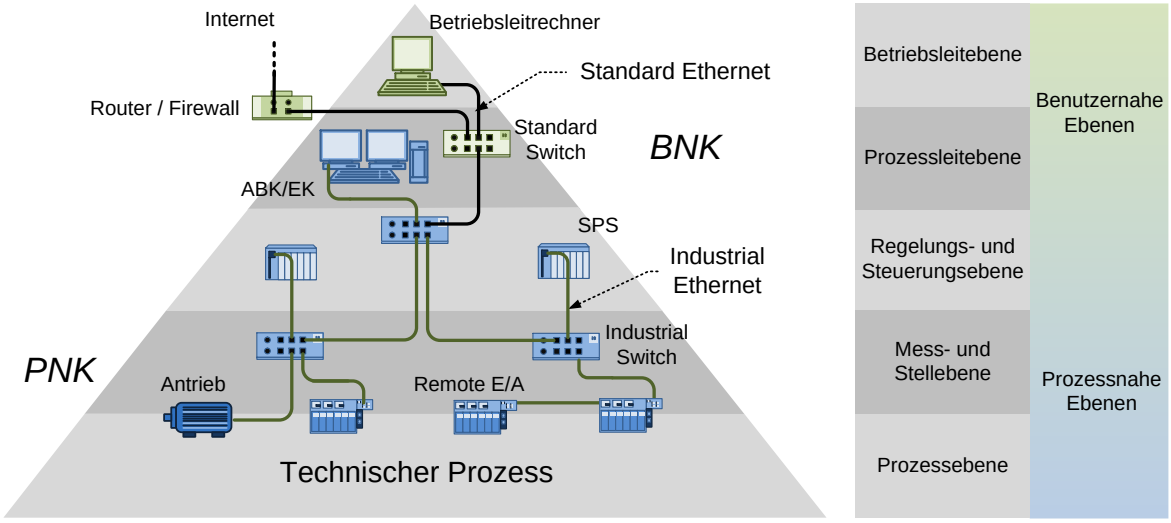


Abbildung 3-3: Automatisierungspyramide auf Basis von Industrial Ethernet

Abbildung 3-3 zeigt die Automatisierungspyramide unter Nutzung von Standard Ethernet (schwarze Verkabelung) und Industrial Ethernet (grüne Verkabelung). Die prozessnahen Komponenten (PNK) sind über speziell für industrielle Umgebungen konzipierte Switches (Industrial Switches) verbunden. Am selben Netzwerk sind Arbeitsstationen zur Konfiguration und Parametrierung der Automatisierungsanlage (EK) sowie Überwachung des technischen Prozesses (ABK) angebunden. Das Industrial Ethernet kann aufgrund der gleichen Basistechnologie direkt mit den Standard Switches der benutzernahen Ebene verbunden werden. Dies ergibt eine durchgehende Vernetzung von der Prozessebene bis hin zur Betriebsleitebene. Zusätzlich kann sowohl bei Verwendung der Feldbustechnologie, als auch beim Industrial Ethernet auf der Betriebsleitebene eine Anbindung an das Internet erfolgen. Dazu ist die Betriebsleitebene via Router (bzw. Firewall) an das Internet angebunden. [HAU2006]

Maßgeblicher Vorteil von Industrial Ethernet ist die flexible Gestaltung der Automatisierungsanlagen. Klassische Feldbussysteme sind auf ein gemeinsames Zugriffsmedium (Bus- bzw. Linientopologie) begrenzt. Industrial Ethernet Lösungen hingegen, ermöglichen gemischte Strukturen aus Stern-, Baum, Linien- sowie Ringtopologien (vgl. Abbildung 3-2 und Abbildung 3-3). Durch die flexible Topologiegestaltung sowie die homogene Netzwerktechnologie ergeben sich Möglichkeiten zur Vereinfachung der Netzwerkstruktur eines Automatisierungssystems und zur Optimierung von Produktionsabläufen.

3.1.3 Umbruch beim Aufbau von Automatisierungsanlagen

Die durchgehende Vernetzung von den prozessnahen bis hin zu den benutzernahen Ebenen wird als vertikale Integration der Automatisierungspyramide bezeichnet. Die Anbindung an externe Netzwerke, wie das Internet, ermöglicht es zusätzlich, Produktionsstandorte miteinander zu vernetzen und so mehrere Standorte bis hinunter zur Prozessebene von zentraler Stelle aus zu überwachen und zu bedienen. Diese Vernetzung mehrerer Produktionsstandorte wird dabei als horizontale Integration bezeichnet. [FOA2013]

Die Verwendung einer standardisierten Kommunikationstechnologie ermöglicht bzw. erleichtert die Integration, wobei Anstrengungen unternommen werden, ein durchgängiges Engineering der Automatisierungsanlage zur den verschiedenen Automatisierungskomponenten zu ermöglichen. Nicht zuletzt bietet die Standardisierung auf Basis von Industrial Ethernet finanzielle Vorteile, da im Gegensatz zu klassischen Feldbusprotokollen auf kostengünstigere Standardkommunikationslösungen zurückgegriffen werden kann. [GDR2007]

Im Umfeld der Automatisierungstechnik wird dazu eine größer werdende Anzahl an eingebetteten Systemen verwendet. Diese Systeme verfügen über zunehmende Rechenleistung. Eingebettete Systeme existieren in unterschiedlichen Ausführungen und Baugrößen [GEG2006]. Diese zum Teil autark arbeitenden Systeme können mit ihrer Umgebung interagieren und direkt sowie indirekt informationsverarbeitende Prozesse beeinflussen [VDI2013]. Sie werden auch „cyber-physische Systeme“ (CPS) genannt und stellen ein großes Potential zur Verbesserung der Automatisierungstechnik dar, da die Interaktionen und dazugehörigen Entscheidungsprozesse der Systeme zu einem großen Teil ohne menschlichen Einfluss erfolgen. Damit werden CPS als wesentlicher Bestandteil der Initiative „Industrie 4.0“ angesehen. [HEN2012]

Abbildung 3-4 zeigt eine Automatisierungsanlage, deren Struktur sich durch die Verwendung einer einheitlichen Kommunikationslösung wie Industrial Ethernet und unter dem Einfluss zuvor genannten Einfluss „Industrie 4.0“ geändert hat. Hierbei ist zu erkennen, dass keine Ebenen, im Sinne der Automatisierungspyramide mehr existieren. Die Anbindung an das Internet ermöglicht die Vernetzung mehrerer Produktionsstandorte.

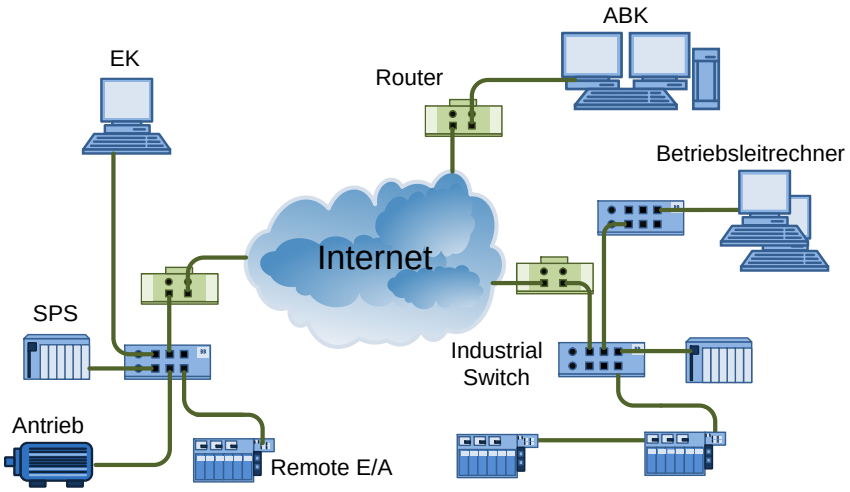


Abbildung 3-4: Strukturwandel in der Automatisierungstechnik

Ziel ist eine Integration der verschiedenen, hierarchisch organisierten Netzwerke zu einem durchgehenden System, über alle Ebenen der Automatisierungspyramide hinweg. Ergebnis ist, dass Produktionsanlagen eine durchgehende, standortübergreifende und räumlich verteilte Erstellung von Produkten ermöglichen. Als weitere Herausforderung gilt es, ein durchgängiges Engineering von Produktionsanlagen zu etablieren, welches die Anforderungen eines solchen verteilten Automatisierungssystems erfüllt [FOA2013].

Die Verwendung offener Standards hat maßgeblich dazu beigetragen, dass sich die geschlossenen Systeme der Automatisierungstechnik zu offenen Systemen entwickelt haben [JAS2012]. Die technologische Entwicklung, wie der Einsatz von Industrial Ethernet und kleinen eingebetteten Systemen, hat diesen Trend zusätzlich beschleunigt.

3.2 Übersicht zu Industrial Ethernet Lösungen

Zahlreiche Industrial Ethernet Technologien prägen derzeit die Automatisierungstechnik. Die Grundlagen der verschiedenen Technologien sind jedoch identisch. In Abschnitt 3.2 werden die grundlegenden Informationen zu den Industrial Ethernet Lösungen dargestellt.

3.2.1 Paketaufbau und Zugriffsverfahren

In Abschnitt 3.1.1 ist der prinzipielle Aufbau einer Automatisierungskomponente beschrieben worden. Im Falle einer dezentralen Peripherie (Sender) erfolgt die Übertragung der Daten (z.B. E/A-Daten) unter Verwendung eines Kommunikationsstacks über das Netzwerk an die zentrale Steuerung (SPS / Empfänger). Die Verarbeitung der Anwendungsdaten bis zur Übertragung auf einem Medium, übernimmt der Kommunikationsstack. Abbildung 3-5 zeigt die Verarbeitung der Daten aus der Anwendung (z.B. Prozessdaten) anhand des ISO/OSI-Referenzmodells [ISO1996].

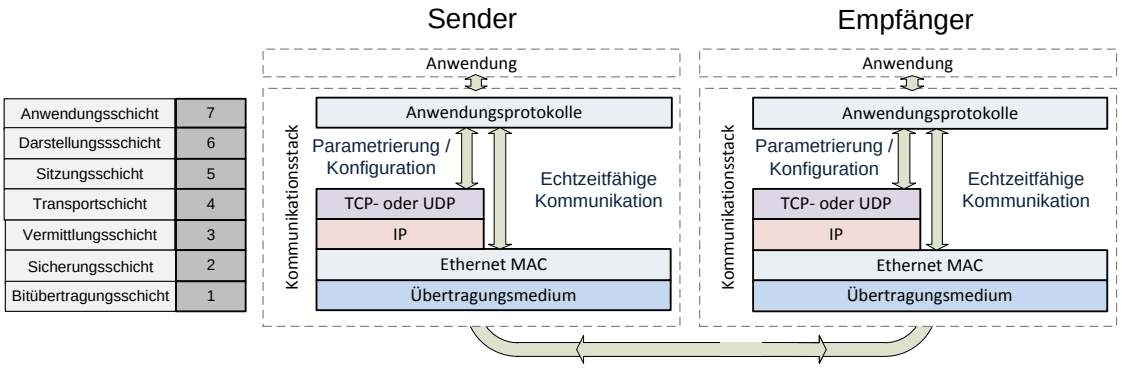


Abbildung 3-5: ISO/OSI-Referenzmodell bei Anwendung im Industrial Ethernet

Die Daten aus der Anwendung durchlaufen die Schichten des Modells, je nach Sende- und Empfangsrichtung. Jede Schicht verarbeitet die Informationen, die entsprechend von Sender und/oder Empfänger auf dieser Ebene benötigt werden. Je nach verwendetem Protokoll (z.B. echtzeitfähige Kommunikation) werden dafür verschiedene Schichten verwendet. Abbildung 3-6 zeigt, wie auf den verschiedenen Ebenen des Kommunikationsstacks aus den Daten der Anwendung das Datenpaket erstellt, welches auf dem Medium übertragen wird.

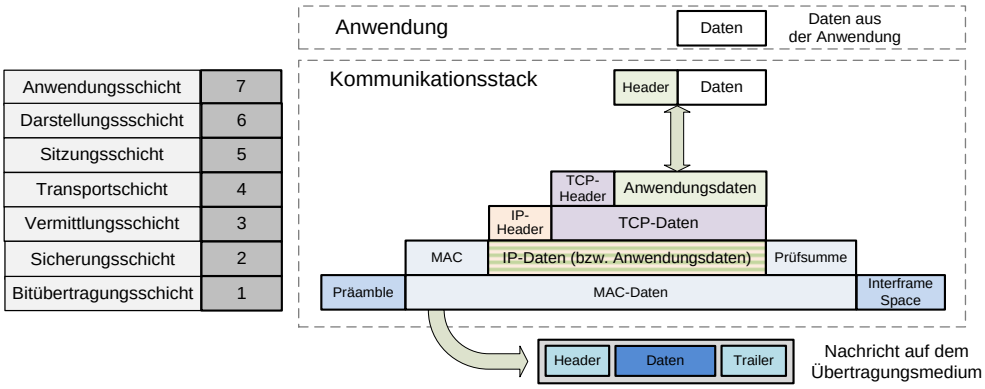


Abbildung 3-6: Aufbau eines Standard Ethernet Datenpakets

Der Kommunikationsstack erhält die Daten zur Übertragung aus der Anwendung. Die einzelnen Schichten erweitern das Datenpaket um Übertragungs- bzw. Verwaltungsinformationen, entweder vor das Datenpaket (Header) und/oder hinter das Datenpaket (Trailer). Diese Informationen beinhalten Adress- und Verwaltungsinformationen wie IP-Adressen, VLAN-ID, TCP-Ports, MAC-Adressen, aber auch den EtherType, zur Differenzierung von Übertragungsprotokollen auf dem Medium. Eine Prüfsumme dient darüber hinaus der Sicherstellung der Integrität des Datenpakets bzw. der darin enthaltenen Informationen.

Beginnend mit dem Anwendungsprotokoll werden die Daten in Schicht 7 verarbeitet bzw. dargestellt, entsprechend des verwendeten Protokolls. Ab dieser Schicht erfolgt die Differenzierung zwischen echtzeitfähiger Kommunikation und der Übertragung auf einem nichtechtzeitfähigen Übertragungsweg. Die Schichten 3 bis 6 werden bei der echtzeitfähigen Kommunikation nicht verwendet (vergl. Abbildung 3-5). Somit erfolgt an dieser Stelle die Weiterleitung der Anwendungsdaten direkt an die Schicht 2. Die Schichten 3 bis 6 werden zusätzlich zur Parametrierung und Konfiguration der Automatisierungskomponenten, z.B. zur Erstellung von Kommunikationssitzungen oder zur Vorbereitung der Nachrichten zur korrekten Darstellung in der Anwendung implementiert. Diese vorbereitenden Maßnahmen finden vor Beginn der echtzeitfähigen Kommunikation statt und werden nicht permanent verwendet.

Schicht 2, steuert den Zugriff auf das Medium (z.B. CSMA/CD-Verfahren [IEE2008] oder proprietäre Zugriffsverfahren, wie im Falle von EtherCAT [IEC2008b]) und führt die Datenflusssteuerung durch. Dieser Datenfluss kann hierbei zyklisch in bestimmten Zeitabständen oder nach Bedarf auf azyklischem Wege in unregelmäßigen Zeitabständen erfolgen. Schicht 2 hat im Falle von Industrial Ethernet eine besondere Bedeutung, da hier deterministischer Zugriff auf das Übertragungsmedium etabliert werden kann. Zu diesem Zweck werden echtzeitfähige Buszugriffsverfahren für Industrial Ethernet sowohl in Hardware (z.B. ASICs) als auch in Software (sogenannte Software-Kommunikationsstacks) realisiert. Letztendlich stellt Schicht 1 das physische Übertragungsmedium (z.B. Kupferkabel, Glasfaser oder drahtlose Übertragung) dar, auf dem die Nachricht übertragen und durch Synchronisationsmechanismen und eine Prüfsummen gesichert wird [SCH2006b].

3.2.2 Übertragungseigenschaften des Industrial Ethernet

Meist finden sich in Kommunikationsprotokollen der Automatisierungstechnik nur Implementationen der Schichten 1 bis 2 und 7 [BOH2006]. Durch effiziente Realisierung dieser Protokolle sowohl in Hardware als auch in Software kann ein hoher Datendurchsatz sowie geringe Zykluszeiten bei der Kommunikation erreicht werden. Bei Industrial Ethernet wird dies durch optimierte Zugriffsmechanismen auf das Übertragungsmedium im Gegensatz zum Standard Ethernet erreicht. Ergänzt wird das Industrial Ethernet dabei durch Paketzähler zur Sicherstellung der Reihenfolgerichtigkeit von eingehenden Datenpaketen. Die Anwendung von CRC-Prüfsummen im Bereich der funktionalen Sicherheit (zusätzlich zum eigentlichen CRC-Prüfsummenverfahren im Industrial Ethernet) dient der Erkennung von weiteren Übertragungsfehlern bzw. der Reduzierung der Restfehlerwahrscheinlichkeit, die durch die besonderen Umgebungsbedingen der Automatisierungstechnik (z.B. EMV) oder Biterkennungsfehlern geschuldet sind [IEE2008].

Insgesamt entstehen durch diese Implementierung gleichzeitig Nachteile bei der Kommunikation in einem Automatisierungsnetzwerk. Durch das Fehlen der Schichten 3 bis 6 bei echtzeitfähigen Industrial Ethernet Protokollen, fehlen Informationen wie IP-Adresse und TCP-Daten, wodurch die Echtzeit-Nachrichten die sogenannte Broadcast-Domäne nicht verlassen können. In diesem Fall wird von einem echtzeitfähigen Teilnetzwerk gesprochen.

Erfolgt eine Parametrierung und Konfiguration der Automatisierungskomponenten, geschieht dies bei der Inbetriebnahme des Automatisierungssystems. Hierfür ist keine permanente Verbindung zu den Automatisierungskomponenten notwendig. Daher erfolgt die Parametrierung und Konfiguration über einen azyklischen Kommunikationsweg, was keine festen Zykluszeiten voraussetzt. Im Gegensatz zu klassischen Feldbusprotokollen, die eine Parametrierung und Konfiguration über einen einzigen Stack ermöglichen, so wird bei Industrial Ethernet durch die Implementierung der Schichten 3 bis 6 ein Einrichtung der Komponenten ermöglicht (vgl. Abbildung 3-5). Dies erlaubt auch eine Parametrierung und Konfiguration von außerhalb des echtzeitfähigen Teilnetzwerks. Mehr noch kann auf diesem Wege eine Prozessdatenkommunikation außerhalb des echtzeitfähigen Teilnetzwerkes etabliert werden [PIM2005], jedoch unter dem Verlust der festen Zykluszeiten. Aus diesem Grund werden in dem in Abbildung 3-5 dargestellten Protokollstack sowohl Echtzeit- und Standardstack parallel verwendet.

3.2.3 Ausprägungsformen

Aktuell existieren zahlreiche Varianten an Industrial Ethernet Protokollen. Dies hängt zum einen eng mit den verschiedenen Eigenschaften der Industrial Ethernet Lösungen und zum anderen mit nationalen und wirtschaftlichen Interessen zusammen. Maßgeblich haben sich dabei Standards wie PROFINET, Ethernet/IP und Modbus/TCP etabliert [IEC2008c], die zusammen mehr als drei Viertel der weltweit verkauften Industrial Ethernet-Lösungen stellen [MOR2012]. Die Verbreitung der Protokolle ist dabei regional unterschiedlich. Während PROFINET in Europa stark vertreten ist, finden Ethernet/IP und Modbus/TCP in den USA und Asien größere Verbreitung. Aufgrund der starken Verbreitung in Deutschland orientiert sich die vorliegende Arbeit am PROFINET (IO)-Standard, wenngleich die vorgestellten Lösungsansätze auf alle Industrial Ethernet Varianten anwendbar sind.

3.3 IT-Sicherheit in der Automatisierungstechnik

Aktuelle Entwicklungen im Bereich der Automatisierungstechnik und der in Abschnitt 3.1.3 dargestellte Strukturwandel haben maßgeblichen Einfluss auf die IT-Sicherheit von Produktionsanlagen. Dieser Einfluss soll nachfolgend erläutert werden, da er weitergehenden Aktivitäten hinsichtlich der IT-Sicherheit in Automatisierungsanlagen führte.

3.3.1 Beurteilung der aktuellen Trends im Bereich der IT-Sicherheit

Standard-IT-Technologien beeinflussen das Umfeld der Automatisierungstechnik. Neben dem Einsatz von Standard-Betriebssystemen und weitverbreiteten Standard-PC-Komponenten hat der Einsatz von Standard Ethernet einen großen Einfluss. Gerade Industrial Ethernet, als Ableger von Standard Ethernet, führte zu einer weitergehenden Vernetzung in der Informationsverarbeitung der Automatisierungstechnik. Die mit der Initiative „Industrie 4.0“ vorangetriebene Nutzung cyber-physischer Systeme, und offene Netzwerkarchitekturen in der Automatisierungstechnik zeigen auf, dass Informationstechnologien immer stärker Einzug in Produktionsanlagen halten [NAM2004]. Damit entsteht jedoch auch eine Abhängigkeit der Automatisierungstechnik von diesen Standard-Technologien [ALL2013]. Diese Abhängigkeit wird in Kauf genommen, um eine Effizienzsteigerung und eine Kostenreduzierung in der Automatisierung erreichen zu können.

Aus Sicht der IT-Sicherheit ist dieser Trend jedoch kritisch zu betrachten. Systeme, die vorher geschlossen waren, öffnen sich nun gegenüber der Standard-IT und den damit einhergehenden Bedrohungen [DHS2012]. Durch diese Öffnung und der weitergehenden Nutzung von Standard-Technologien in der Automatisierungstechnik, sowie der vertikalen und horizontalen Integration der Netzwerke, hat die IT-Sicherheit in der Automatisierungstechnik stark an Bedeutung zugenommen. Dies zeigt sich im Allgemeinen in dem Bestreben der Bundesregierung eine gesetzliche Grundlage für die IT-Sicherheit in der Automatisierungstechnik, insbesondere für kritische Infrastrukturen, zu schaffen [BUN2013]. Darüber hinaus zeugen die zahlreichen Normungsaktivitäten im Bereich der IT-Sicherheit für die Automatisierungstechnik, dass die Notwendigkeit einer Standardisierung gesehen wird [ESC2010]. Allgemein zeigt diese Entwicklung, dass weitergehende Schutzmaßnahmen für Automatisierungsanlagen benötigt werden.

3.3.2 Einstufung der Schutzziele für die Automatisierungstechnik

Die grundlegenden Schutzziele der IT-Sicherheit wurden in Abschnitt 2.1.2 dargestellt. Verfügbarkeit, Vertraulichkeit und Integrität sind dabei die grundlegenden Schutzziele. Diesen Schutzzielen werden in der Automatisierungstechnik andere Prioritäten zugeordnet, als in der Standard-IT.

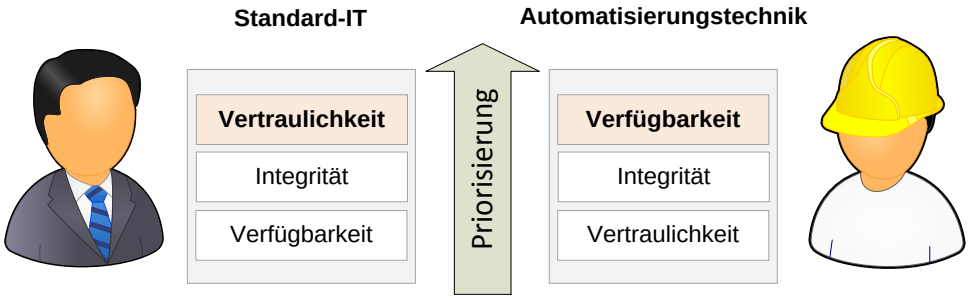


Abbildung 3-7: Vergleich der Schutzziele

Abbildung 3-7 zeigt, dass in der Automatisierungstechnik die Verfügbarkeit das oberste Schutzziel darstellt, da Produktionsprozesse in vielen Fällen ununterbrochen laufen müssen (bspw. Glasherstellung). Der Ausfall einer Automatisierungskomponente führt hierbei zu Produktionsausfällen [CHA2009]. In Büroanwendungen führt der Verlust der Verfügbarkeit zu einer vergleichsweise geringen Beeinträchtigung. Ist hier jedoch die Vertraulichkeit von Informationen betroffen, so könnten durch Ausspähaktionen finanzielle Verluste entstehen [COR2012]. Aus diesem Grund ergibt sich eine unterschiedliche Priorisierung der Schutzziele in Automatisierungstechnik und Standard-IT.

Im Umfeld der Automatisierungstechnik ist die Integrität von Daten mit der Verfügbarkeit eng verbunden. So haben bspw. Prozessdaten, die während der Übertragung verfälscht wurden, Einfluss auf die Verfügbarkeit der Automatisierungsanlage. Aus diesem Grund wird neben der standardmäßig verwendeten CRC-Prüfsumme beim Industrial Ethernet bspw. in funktional sicheren Systemen eine zusätzliche Prüfsumme in der Kommunikation eingesetzt. Auf diese Weise wird die Wahrscheinlichkeit einer verfälschten Übertragung gesenkt. Die Vertraulichkeit der zu übertragenen Daten ist häufig von geringer Relevanz, wobei jedoch im Einzelfall zu beurteilen ist, ob beispielsweise schützenswertes Wissen (Prozesswissen, Rezepturen) aus einer Kenntnis der übertragenen Prozessdaten extrahiert werden kann. Ist dies der Fall so ist der Einsatz geeigneter Schutzmaßnahmen zur Absicherung der Vertraulichkeit in der Automatisierungstechnik (bspw. der Kommunikation) sinnvoll.

Dies macht deutlich, dass die Fokussierung auf ein Schutzziel alleine nicht ausreichend ist. Für eine angemessene Sicherheit sind immer alle Schutzziele gemeinsam zu betrachten. So ist erst mit Sicherstellung der Integrität (in manchen Fällen auch der Vertraulichkeit) auch die Verfügbarkeit ausreichend geschützt. Doch ist ein Schutz der Vertraulichkeit und Integrität von Daten erst möglich, wenn die Authentizität der Kommunikationspartner erfasst wurde. Nur auf diese Weise wird eine sichere Ausgangssituation für weitere Maßnahmen erstellt.

3.3.3 Security vs. Safety – Differenzierung der Begriffe

Zwar ist das Bewusstsein für das Thema „Sicherheit“ in der Automatisierungstechnik stark vertreten, doch liegt der Fokus im Bereich der funktionalen Sicherheit (Safety). Die funktionale Sicherheit betrachtet Schäden jedoch aus einer anderen Wirkungsrichtung als die IT-Sicherheit. Dieser Zusammenhang ist in Abbildung 3-8 dargestellt.

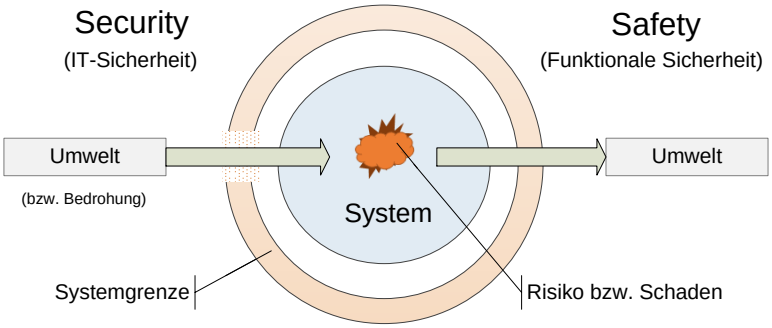


Abbildung 3-8: Einwirkungsrichtung bei Safety- und/oder Security-Aspekten

Safety (funktionale Sicherheit) hat zum Ziel, Risiko bzw. Schaden ausgehend vom System auf die Umwelt auf ein akzeptables Niveau zu minimieren. Dabei stehen zufällige Ereignisse und ungewollte Fehlbedienungen im Fokus. Maßgebliche Faktoren zur Bewertung des Risikos sind hier die Fehlerwahrscheinlichkeit und das Schadenspotential (vergl. Abschnitt 2.2). Diese können mit Hilfe mathematischer Verfahren ermittelt werden [IEC1999].

Security (IT-Sicherheit) befasst sich jedoch im Gegensatz zu Safety mit der Problemstellung des Einwirkens der Umwelt (bzw. der Bedrohung) auf ein System. Die Umwelt stellt in diesem Fall die Bedrohung dar, die über Schwachstellen in das System einwirken. Die Fehlerwahrscheinlichkeit und das Schadenspotential existieren auch in diesem Fall, doch zusätzlich existiert als schwer erfassbare Größe die Bedrohung, der das System ausgesetzt ist. Wie [WFS2013] aufzeigt, liegen die Maßnahmen und Schutzziele von Safety und Security eng beieinander, sind aber klar voneinander getrennt zu betrachten. So sind im Detail Safety-Maßnahmen nicht zwingend security-relevant sein, oder anders herum Security-Maßnahmen nicht safety-relevant.

Dies zeigt sich besonders am Beispiel von safety-bezogener Kommunikation. Die beim Industrial Ethernet (basierend auf Standard Ethernet) angewendete CRC-Prüfsumme zur Fehlererkennung bzw. Fehlerkorrektur bei der Kommunikation, wird um eine zusätzliche (safety-bezogene) CRC-Prüfsumme ergänzt, um die Restfehlerwahrscheinlichkeit weiter senken zu können [BLE2005], [IEE2008]. Jedem Datenpaket werden durch den Sender eine entsprechende Prüfsumme beigefügt, welche der Empfänger überprüft.

Da das Verfahren zur Erstellung der CRC-Prüfsumme bekannt ist, kann eine angreifende Person die Prüfsumme eines manipulierten Datenpakets ersetzen und so die inhaltliche und zeitliche Integrität der Nachricht verändern. Da der Empfänger ein Paket mit passender Prüfsumme erhält, ist er nicht in der Lage die Veränderung zu erkennen. Ein solcher Angriff ist in Abbildung 3-9 als „Man in the Middle“-Angriff zu sehen [AKB2009a].

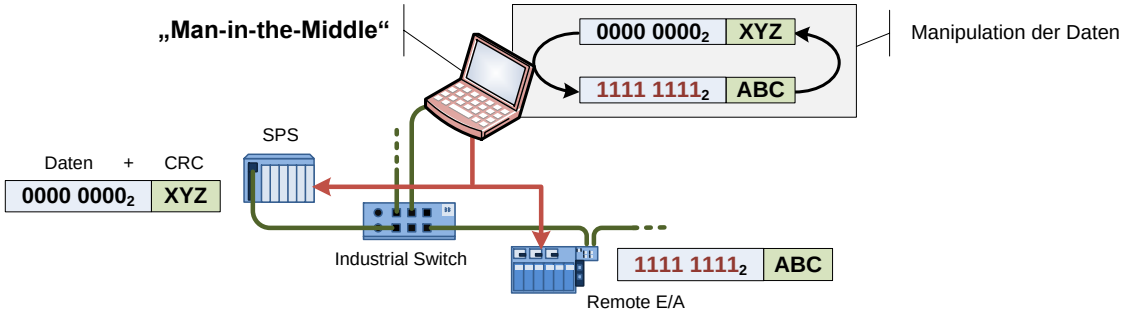


Abbildung 3-9: Angriff auf die Kommunikation („Man in the Middle“)

Beim dargestellten Angriff fängt der „Man in the Middle“-Rechner durch eine Spoofing-Attacke Adressinformationen aus dem Netzwerk ab. Die Anbindung des angreifenden Rechners kann dabei über ungenutzte Switch-Ports der Anlage erfolgen. Mit Hilfe der gewonnenen Adressinformationen wird eine Umleitung der Kommunikation zum angreifenden Rechner provoziert. Dieser empfängt das Paket, ändert die Daten und dazu gehörige Informationen zur Sicherstellung der Reihenfolgerichtigkeit, erzeugt die die dazu passende CRC-Prüfsumme (bzw. Prüfsummen im Fall von safety-relevanter Kommunikation), und leitet die veränderte Nachricht an den ursprünglichen Empfänger weiter. Erfolgt der dargestellte Vorgang in Sende- und Empfangsrichtung, so hat der „Man in the Middle“ die vollständige Kontrolle über die Kommunikation. In diesem Fall ist der angreifende Rechner in der Lage den technischen Prozess zu manipulieren, ohne dass dies auf Bedien- und Anzeigekonsolen erkennbar ist. Dieses Angriffsszenario gilt natürlich nicht ausschließlich für safety-bezogene Kommunikation, sondern ebenso für weitere Kommunikationsformen auf Basis von Standard-Ethernet und konventionellen Feldbussen.

Zufällige Ereignisse (z.B. EMV-Einflüsse auf die Kommunikation) können dazu führen, dass ein System unerlaubte bzw. unsichere Zustände annimmt. Diese Zustände können einen Risiko bzw. Schaden für die Umwelt des Systems darstellen. Safety-bezogene Schutzmaßnahmen (bspw. die Senkung der Restfehlerwahrscheinlichkeit) dienen dazu unerlaubte bzw. unsichere Zustände zu unterbinden und somit Risiken und Schäden von Mensch und Umwelt abzuwenden. Die Senkung der Restfehlerwahrscheinlichkeit (zusätzliche CRC-Prüfsumme) hat hingegen keine Wirkung gegen vorsätzlich herbei geführte Eingriffe in das System. Diese vorsätzlichen Beeinflussungen bedürfen Schutzmaßnahmen, die ein Eingreifen von außen unterbinden. Wie Abbildung 3-8 aufzeigt, weisen demnach safety- und security-relevante Schutzmaßnahmen eine unterschiedliche Wirkrichtung auf.

Dies unterstreicht die Aussage, dass sich safety- und security-relevante Maßnahmen im Kern bestenfalls ergänzen können, sie sich jedoch nicht gegenseitig ersetzen lassen. Im Zuge einer Bedrohungs- bzw. Risikoanalyse des Security- und des Safety-Aspekts ist daher festzustellen, wie und durch welche Maßnahmen Risiken minimiert werden können. Dabei ist zu beachten, dass entsprechende Maßnahmen sich nicht gegenseitig behindern. So kann je nach Bedrohungs- und Risikosituation nur die Anwendung von Safety- und/oder Security-Maßnahmen sinnvoll sein.

3.3.4 Vorgaben an die IT-Sicherheit in der Automatisierungstechnik

Zahlreiche Aktivitäten im Umfeld der Automatisierungstechnik beschäftigen sich mit dem Aspekt der IT-Sicherheit in Produktionsanlagen, sowohl im nationalen als auch im internationalen Umfeld. Dabei werden Vorhaben zu Normen, Standards und Richtlinien von Anwender- und Herstellervereinigungen sowie staatlichen Institutionen umgesetzt. Einerseits ist dies erfreulich, da damit die Wichtigkeit des Themas unterstrichen wird. Andererseits entstehen zahlreiche parallele Dokumente. [ESC2010]

Normungsaktivitäten beziehen sich auf die Einführung von Vorgehens- und Verfahrensweisen, dem Einsatz, der Bewertung und Verbesserung von Schutzmaßnahmen für die IT-Sicherheit. Ausgangspunkt hierfür sind Normensammlungen wie die ISO/IEC 27000 [IEC2012a] oder die „Common Criteria“ [COM2009]. Erweitert werden diese Dokumente durch staatliche Vorgaben wie dem BSI [BSI2008b] und dem NIST [NIS2009b]. Diese Dokumente beziehen sich auf IT-Sicherheit im Allgemeinen und beinhalten keine speziellen Aspekte der Automatisierungstechnik.

Trotz ihrer generischen Ausrichtung finden diese Normen dennoch weite Verbreitung im Umfeld von Produktionsanlagen. In der Normung und Standardisierung der IT-Sicherheit für Produktionsanlagen sind die Aktivitäten seitens der IEC in der IEC 62443 [IEC2012b] ausschlaggebend. Weiter finden Spezialisierungen auf bestimmte Aspekte der Automatisierungstechnik statt, wie im Falle der IEC 62351 [IEC2007], die eine hohe Relevanz in der Energieproduktion und Energieverteilung aufweist.

Diese Dokumente bilden die Grundlage für eine große Anzahl an Richtlinien von Hersteller- und Anwendervereinigungen. Hervorzuheben ist hierbei die Richtlinie VDI 2182 [VDI2008] des VDI, die ihre Arbeiten bezüglich der IT-Sicherheit in Umsetzungsempfehlungen für Anwender und Hersteller gleichermaßen erfasst hat. Zusätzlich werden durch Anwendervereinigungen Aspekte der Prozess- und Fertigungsautomatisierung aufgegriffen, so wie im Falle der NAMUR, als Interessensverband der Prozessautomatisierung [NAM2006], oder der AIDA, als Automatisierungsinitiative der deutschen Automobilhersteller (stellvertretend für die Fertigungsautomatisierung), welche sich auf die PROFINET Security Guideline [PNO2014] der PNO (PROFIBUS Nutzerorganisation e.V.) bezieht.

Normen, Standards und Richtlinien finden weiter direkte Verwendung in anderen IT-Sicherheitsempfehlungen. So erfolgt bspw. auch bei anderen Industrial Ethernet-Lösungen wie Ethernet/IP im Rahmen des Security White Papers [ODV2011], welches durch die Anwendervereinigung ODVA (Open DeviceNet Vendor Association) erstellt wurde, eine konzentrierte Betrachtung der IT-Sicherheit für Automatisierungssysteme. Unabhängig ihrer Herkunft beschreiben die zahlreichen Dokumente einen generischen Ansatz, der die Durchführung eines zyklischen Prozesses zur Erarbeitung, Einsetzung und Bewertung von Schutzmaßnahmen für die IT-Sicherheit beschreibt.

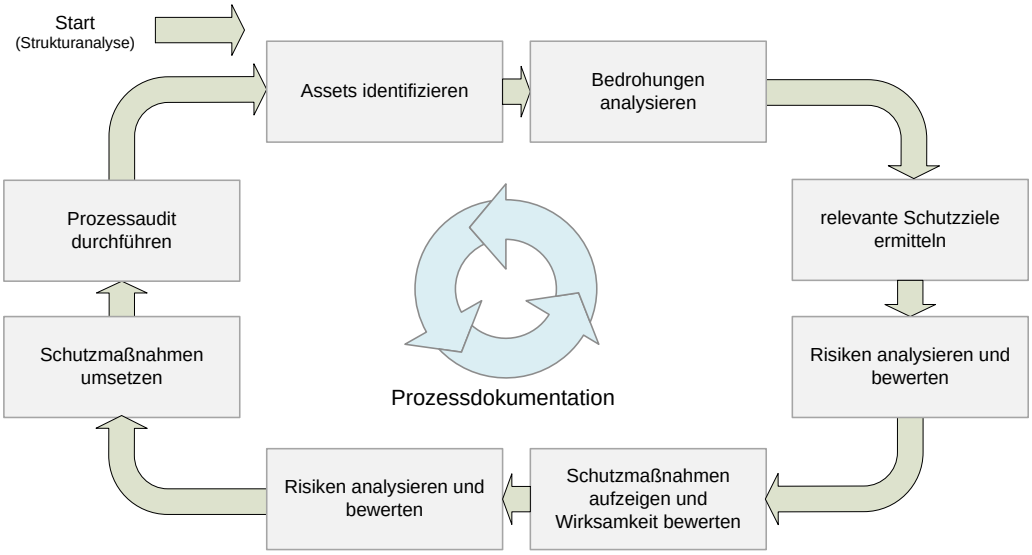


Abbildung 3-10: Zyklisches Vorgehensmodell entsprechend [VDI2008]

Abbildung 3-10 zeigt beispielhaft dieses Vorgehen anhand der VDI-Richtlinie 2182, welches in allgemeiner Form bereits in Abschnitt 2.4.2 beschrieben wurde.

Zunächst erfolgt die nach der Strukturanalyse der Automatisierungsanlage die Identifizierung schützenswerter Bestandteile (Assets) der Produktionsanlage, woraufhin eine Bedrohungsanalyse der Assets folgt. Die Festlegung relevanter Schutzzielen dient dabei als Ausgangspunkt um darauf folgend das Risiko für die Automatisierungsanlage beurteilen zu können. Daraufhin werden Schutzmaßnahmen aufgezeigt und ihre Wirksamkeit zur Reduzierung des Risikos hinsichtlich der Assets bewertet. Daran schließt die Auswahl und Umsetzung von Schutzmaßnahmen an, die zum erwünschten Ziel der Risikoreduzierung führen sollen. Zum Schutz einer Automatisierungsanlage kommen Schutzmaßnahmen für die IT-Sicherheit verschiedenster Art zum Einsatz. Klassifiziert werden diese entweder als technische oder organisatorische Maßnahmen. Empfehlungen hierzu stammen aus verschiedenen Stellen wie dem BSI oder dem DHS (ICS-CERT) [BSI2010b], [DHS2009]. Abschließend erfolgt im Rahmen eines Audits die Überprüfung, ob die ausgewählten Schutzmaßnahmen zur gewünschten Risikoreduzierung geführt haben. Falls erforderlich wird dieser Zyklus nochmals durchlaufen, bspw. nach Strukturänderungen oder falls Schutzmaßnahmen nicht die erwünschte Wirkung zeigen.

Aufgrund der Akzeptanz der VDI Richtlinie 2182 in der Automatisierungstechnik und der konkreten Vorgehensweise für Produktionsanlagen, orientiert sich diese Arbeit an dieser Richtlinie. Dabei werden die Schritte dieses Prozesses durchlaufen, wobei jedoch aufgrund des Umfangs dieser Arbeit auf spezielle Aspekte fokussiert wird.

3.4 Übersicht der derzeitigen Situation

In diesem Abschnitt wurden die Grundlagen zur Automatisierungstechnik erläutert. Automatisierungskomponenten übernehmen in verteilten Systemen über industrielle Kommunikationslösungen die Aufgaben zur Steuerung und Regelung des technischen Prozesses. Die beschriebene Entwicklung der Automatisierungstechnik zeigte auf, dass Einflüsse der Standard-IT, wie Standard Ethernet und Standard-Software, einen großen Einfluss auf die Struktur einer Automatisierungsanlage haben. Im Speziellen führten Industrial Ethernet Technologien dazu, dass die Vernetzung und die Verteiltheit von Automatisierungsanlagen voranschreiten. Trends wie „Industrie 4.0“ auf Basis cyber-physischer Systeme (CPS) verstärken diesen Effekt.

Im Zuge dieser Trends öffnen sich die vormals geschlossenen Systeme gegenüber der Standard-IT sowie dem Internet. Damit erfolgt auch eine Öffnung der (sensiblen) Automatisierungssysteme gegenüber dem Internet. So kann eine Überwachung von mehreren verteilten Automatisierungsanlagen auch über öffentliche Netzwerke wie dem Internet erfolgen. Unweigerlich rückt dabei auch der IT-Sicherheitsaspekt in den Fokus der Automatisierungstechnik, da durch die Öffnung die Möglichkeit von Angriffen auf das Automatisierungssystem steigen kann.

Allgemein zeigt sich im Umfeld der Automatisierungstechnik eine große Sensibilität für das Thema „Sicherheit“, wobei der Schwerpunkt auf der funktionalen Sicherheit liegt. Jedoch ist die IT-Sicherheit als erfolgskritischer Faktor zusätzlich zur funktionalen Sicherheit für das Gelingen der Initiative „Industrie 4.0“ auf Basis cyber-physischer Systeme erforderlich [FOA2013], [FRA2014]. Security- und Safety-Maßnahmen können sich dabei bestenfalls ergänzen.

Im Verlauf der letzten Jahre führten zahlreiche Aktivitäten zu einem großen Umfang an Vorgaben, Richtlinien und Normen für die IT-Sicherheit in der Automatisierungstechnik. Diese Dokumente orientieren sich dabei an bekannten Vorgehensweisen der Standard-IT. Hierbei ist die VDI-Richtlinie 2182 [VDI2008] hervorzuheben, die zahlreiche Aspekte der IT-Sicherheit in der Automatisierungstechnik in sich vereint. Allgemein wird hierbei ein zyklischer Prozess zur Bewertung, Einführung und Neubewertung von gemeinsam eingesetzten technischen und organisatorischen Schutzmaßnahmen für die IT-Sicherheit beschrieben.

In Kapitel 4 folgt, ausgehend von den vorhergehenden Grundlagenkapiteln 2 und 3, eine Analyse der aktuellen Bedrohungssituation der IT-Sicherheit in der Automatisierungstechnik.

4 Bedrohungen von Automatisierungssystemen

In einer nun folgenden Bedrohungsanalyse soll aufgezeigt werden, welchen Bedrohungen die Assets eines Automatisierungssystems ausgesetzt sind. Diese Analyse soll in Kapitel 4 anhand einer Beispielanlage durchgeführt werden. Die Ergebnisse dienen der Bewertung von bereits existierenden Schutzmaßnahmen und stellen die Basis zur Bewertung bzw. Konzeptionierung verbesserter Schutzmaßnahmen im weiteren Verlauf der Arbeit.

Zunächst erfolgt eine Betrachtung der Bedrohungen, die eine Auswirkung auf die IT-Sicherheit der Automatisierungstechnik haben. Entsprechend [VDI2008] sollen zunächst schützenswerte Anlagenbestandteile (Assets) identifiziert und die Bedrohungen (engl. threats) erfasst werden, denen die Automatisierungsanlage ausgesetzt ist. Diese Bedrohungen wirken auf Schwachstellen ein, dessen Auswirkungen dargestellt werden sollen (►4.4). Abschließend erfolgt eine Risikobewertung in deren Ergebnis feststeht, ob eine Reduzierung eines Risikos auf ein akzeptables Niveau notwendig ist.

4.1 Identifizierung von schützenswerten Anlagenbestandteilen

4.1.1 Definition des Betrachtungsgegenstands

Im Vorgang der Bedrohungsanalyse ist zunächst der Betrachtungsgegenstand zu definieren. Hierzu wird zunächst die Struktur der Automatisierungsanlage ermittelt. Für die vorliegende Arbeit wird auf ein generisches Modell zurückgegriffen, um die allgemeine Bedrohungssituation darzustellen. Auf diese Weise sollen Sachverhalte, die für viele Typen an Automatisierungsanlagen gelten, auf ein Modell übertragen werden. Kommunikationsbeziehungen können so auf einfache abstrakte Beziehungen abgebildet werden und eine generische Bedrohungsanalyse ist möglich.

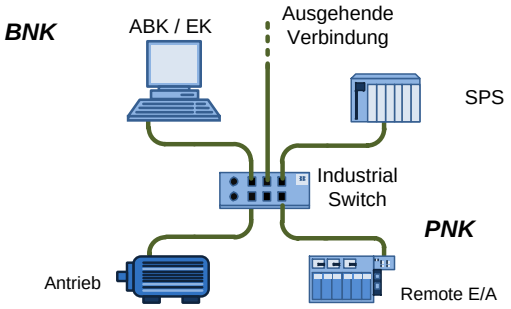


Abbildung 4-1: Struktur eines Minimalaufbaus einer Automatisierungsanlage

Abbildung 4-1 zeigt den Minimalaufbau einer Automatisierungsanlage. Maßgebliche Bestandteile sind die PNK, wie Antriebe, SPS und Remote E/As. Die Steuerung des technischen Prozesses übernimmt hierbei die SPS, während Antrieb und Remote E/A als dezentrale Peripherie in direkter Umgebung zum technischen Prozess zu finden sind. Die Parametrierung und Konfiguration der Automatisierungsanlage erfolgt mittels der BNK. Zur Kommunikation der BNK und PNK wird ein Industrial Ethernet verwendet. Zentraler Bestandteil dieses Netzwerkes ist ein Industrial Switch. Dieser Switch nimmt die Vermittlung der Kommunikation anhand der (MAC-)Adressen der Automatisierungskomponenten vor. Über den Switch ist zudem eine ausgehende Verbindung möglich, wobei es sich um weitere Teile einer Automatisierungsanlage und/oder Verbindungen über das Internet handeln kann.

Neben den Automatisierungskomponenten ist das konkrete Einsatzszenario und die Einsatzumgebung der Automatisierungsanlage Bestandteil des Betrachtungsgegenstandes. Im Falle der gezeigten Anlage kann dies z.B. die Steuerung einer Maschine sein oder die Überwachung eines verfahrenstechnischen Prozesses. Entsprechend Abbildung 4-1 besteht der hier definierte Betrachtungsgegenstand aus folgenden Bestandteilen, die als schützenswerte Anlagenbestandteile zu sehen sind:

- **Automatisierungskomponenten**

Alle Automatisierungsgeräte des Betrachtungsgegenstandes werden erfasst. Hierzu zählen primär alle Komponenten, die über eine eigene Spannungsversorgung verfügen. Es handelt sich zumeist um solche Komponenten, die aktiv an der Steuerung bzw. Regelung des technischen Prozesses beteiligt sind. Im oben angegebenen Anlagenbeispiel sind dies die SPS, die dezentrale Peripherie sowie die ABK- und EK-Station. Alle Kommunikationsschnittstellen dieser Komponenten (vgl. Abbildung 3-1) stellen Assets dar.

- **Kommunikationsinfrastruktur**

Zwischen den Automatisierungskomponenten bestehen logische Kommunikationsbeziehungen. So unterhalten SPS und BNK bzw. SPS und PNK logische Verbindungen untereinander. Hergestellt wird diese Kommunikationsbeziehung über eine entsprechende (physische) Netzwerkinfrastruktur, zu der auch Switches zählen. Sowohl Netzwerkinfrastruktur als auch logische Kommunikationsbeziehungen können als Assets angesehen werden.

Die zuvor genannten Assets adressieren nicht nur materielle Bestandteile wie die Automatisierungskomponenten und Kommunikationsbeziehungen. Vielmehr zählen auch Assets, die als immateriell bezeichnet werden, wie Kenntnisse über Prozessabläufe bzw. Rezepte, dem Anlagenaufbau oder schützenswerter Software auf den Automatisierungskomponenten. Teil des Betrachtungsgegenstandes sind zusätzlich Akteure (z.B. Inbetriebnehmer, Wartungs- sowie Bedienpersonal) in einem Automatisierungssystem, die in direkter Interaktion mit dem System stehen und eine mögliche Quelle für Bedrohungen sein können.

4.1.2 Vereinfachung des Betrachtungsgegenstandes

In der folgenden Bedrohungsanalyse werden Kommunikationsbeziehungen sowie die Automatisierungskomponenten näher betrachtet. Kommunikationsbeziehungen sollen dabei auf ein allgemeines Modell übertragen werden. In diesem allgemeinen Modell sind ein- und ausgehende Verbindungen über den Switch nach außerhalb der Beispielanlage (Betrachtungsgegenstandes, vergl. Abbildung 4-1) mit berücksichtigt.

Der Switch wird im vereinfachten Betrachtungsgegenstand nicht explizit aufgeführt, da dieser in der Regel ein Bestandteil der Kommunikationsinfrastruktur ist. Ein Switch kann ein mögliches Ziel und/oder der Ausgangspunkt eines Angriffes sein, um Zugriff auf die Kommunikationsinfrastruktur zu erhalten. Im Falle des PROFINET-Protokolls ist die Einbindung des Switches als eigenständige Automatisierungskomponente möglich und als solche so berücksichtigen. Im vorliegenden Fall wird auf diesen Aspekt aufgrund einer generellen Betrachtung der Bedrohungssituation im Industrial Ethernet verzichtet und der Switch als Bestandteil der Kommunikationsinfrastruktur betrachtet.

Abbildung 4-2 zeigt das vereinfachte Modell des Betrachtungsgegenstandes. Unterschieden wird dabei zwischen den jeweiligen BNK und PNK, die über ihre Systemgrenze hinweg mit Hilfe von Verbindungen zu anderen Automatisierungskomponenten aufbauen und den Kommunikationsbeziehung der Komponenten zueinander.

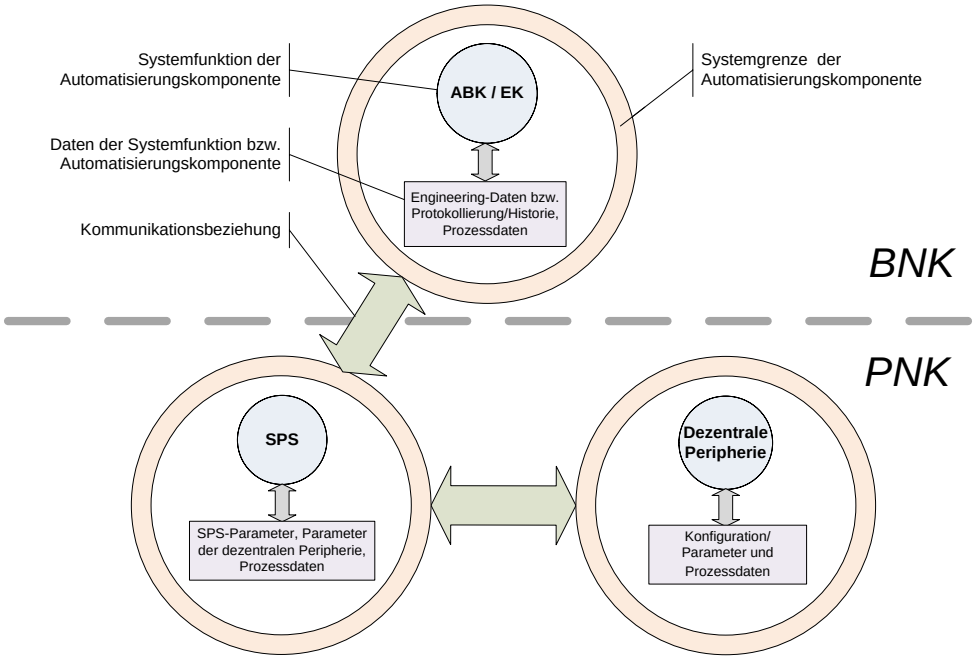


Abbildung 4-2: Vereinfachtes Modell der Beispielanlage (Betrachtungsgegenstand)

Das dargestellte Modell erlaubt eine generelle Betrachtung der möglichen Folgen, die durch Bedrohungen bzw. Angriffe entstehen können. Die Auswirkungen werden aus den genannten Bestandteilen des vereinfachten Modells wie den Kommunikationsbeziehungen sowie den internen Bestandteilen der Automatisierungskomponenten abgeleitet.

4.2 Bedrohungsanalyse eines Automatisierungssystems

Die in Abschnitt 2.2 erläuterten Begriffe zeigen, dass eine Bedrohung aus verschiedenen Gefährdungsfaktoren resultieren kann. Vorsätzliche Gefährdungsfaktoren stehen dabei im Fokus der IT-Sicherheit. Die möglichen Akteure diesbezüglich sind zahlreich, vom ungeschulten Personal ohne Bezug zur Automatisierungstechnik bis hin zu Geheimdiensten mit speziellen Kenntnissen über Automatisierungssysteme. Im vorliegenden Beispiel wird zunächst von einem omnipräsenten und omnipotenten Angreifer ausgegangen [DOY1983]. Dieser verfügt über weitreichendes Wissen um Komponenten und Kommunikation in einem Netzwerk. Er ist damit in der Lage an jedem Punkt im Netzwerk Zugriff zu erlangen und Nachrichten zu lesen, zu manipulieren und zu verschicken. Dafür stehen ihm unbegrenzte Ressourcen zur Verfügung.

Realistisch gesehen sind jedoch Zugriffspunkte auf ein informationstechnisches System für eine angreifende Person beschränkt, so dass bspw. kein gleichzeitiger Zugriff an mehreren Punkten erfolgen kann. Aus diesem Grund minimiert sich der omnipotente Angreifer auf ein realistisches Modell mit eingeschränkten Zugriffsmöglichkeiten auf Nachrichten und Komponenten im Automatisierungsnetzwerk. Weitreichendes Wissen über den Aufbau des Systems und ausreichende Ressourcen können dem Angreifer jedoch nach wie vor zur Verfügung

stehen. Eine Klassifizierung der Angriffe kann dabei in zwei Typen erfolgen, welche in Abbildung 4-3 dargestellt sind [GUG2006].

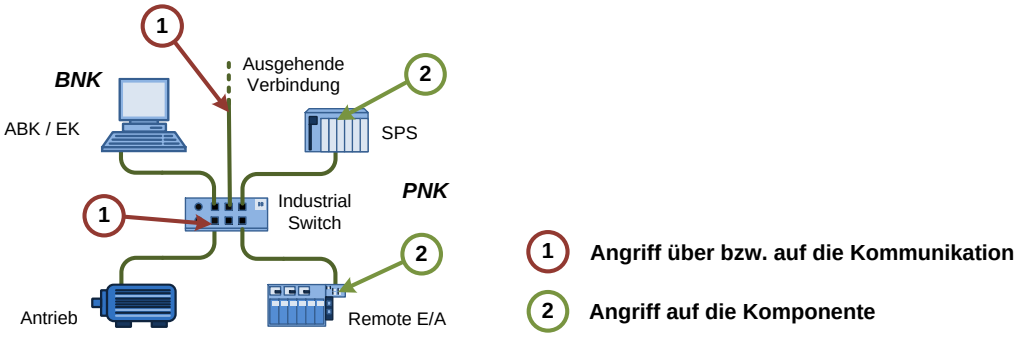


Abbildung 4-3: Angriffsmöglichkeiten in einer Automatisierungsanlage

Hierbei wird zwischen solchen Angriffen unterschieden, die entfernt über die Kommunikationsinfrastruktur oder lokal auf der Automatisierungskomponente erfolgen. Typische Eigenschaften dieser Angriffstypen sind: (vergl. [ZEL2011])

- **Angriff über bzw. auf die Kommunikationsinfrastruktur**

Mit Zugang zum Netzwerk (z.B. durch ungenutzte Ports eines Switch oder eine ungesicherte ausgehende Verbindung) besteht direkter Zugriff auf die Netzwerkkommunikation. Hierdurch ist ein Angreifer in der Lage direkten Einfluss auf die Kommunikation und die an diesem Netzwerk angeschlossenen Automatisierungskomponenten zu nehmen, um so den technischen Prozess oder die Funktionen der Geräte zu manipulieren.

- **Angriff über bzw. auf lokalen Zugang einer Automatisierungskomponente**

Durch direkten physischen Zugang kann eine Manipulation der Automatisierungskomponenten erfolgen. Sowohl die Systemfunktion als auch die gespeicherten Systemdaten können auf diese Weise manipuliert werden. Dabei können lokale Schnittstellen, wie z.B. USB, I^2C, SPI oder Speicherkartenschnittstellen (bspw. SD-Cards) als Zugang verwendet werden. Dies gilt nicht nur im Speziellen für eingebettete Automatisierungskomponenten, sondern auch für klassische BNK auf Basis von Standard-PCs.

Die Angriffsarten zielen somit direkt auf die zuvor genannten Assets ab und decken sich mit dem bereits eingeführten (vereinfachten) Betrachtungsgegenstand. Wie bereits beschrieben, existieren vielfältige Gründe, weshalb ein Angreifer auf die Gewinnung von Informationen bzw. Manipulation der Kommunikation und der daran angeschlossenen Netzwerkteilnehmer bezweckt. Ausgehend vom Angriffstyp und dem Angriffsziel existiert, unabhängig der genutzten Schwachstellen, eine Vielzahl an Bedrohungen für Automatisierungsanlagen [BSI2013a]. So beschreibt bspw. das BSI die Bedrohungssituation speziell für Automatisierungsanlagen. In [BSI2014] werden die Top 10 Bedrohungen für „Industrial Control Systems“ (ICS) aus dem Jahr 2012 aufgeführt, die die höchste Kritikalität aufweisen. Tabelle 4-1 kategorisiert diese Bedrohungen entsprechend dem Angriffstyp.

Nr.	Bedrohung		**Angriff** (mit Vorsatz)		**Ohne Vorsatz**
			Kommunikation	Komponente	
1	Unberechtigte Nutzung von Fernwartungszugängen		●		
2	Online-Angriffe über Büronetzwerk bzw. Leitebene		●		
3	Angriffe auf Standardkomponenten im Netzwerk		●	●	
4	(Distributed) „Denial of Service“-Angriffe / (D)DoS		●		
5	a)	Menschliches Fehlverhalten			●
	b)	Sabotage	●	●	
6	Einschleusen von Schadcode über Wechseldatenträger und externe Hardware		●	●	
7	Lesen und Schreiben von Nachrichten in ICS-Netzen		●		
8	Unberechtigter Zugriff auf Ressourcen		●	●	
9	Angriffe auf Netzwerkkomponenten		●	●	
10	Technisches Fehlverhalten / Höhere Gewalt				●

Tabelle 4-1: Differenzierung relevanter Bedrohungen

Tabelle 4-1 zeigt, dass Bedrohungen mit Vorsatz (intentional) häufiger auftreten als ohne Vorsatz (nicht-intentional). Vorsätzliche Bedrohungen stellen damit eine relevante Gefährdung für Automatisierungsanlagen dar. [BSI2014] beschreibt Bedrohung Nr. 5 als menschliches Fehlverhalten und Sabotage, wobei ersichtlich ist, dass im Falle einer Sabotage ein Vorsatz vorliegt. Lediglich menschliches und technisches Fehlverhalten sowie höhere Gewalt adressieren keinen direkten Vorsatz.

Allgemein wirken die Bedrohungen sowohl auf die Kommunikation als auch auf die Komponente. Dabei stellen Bedrohungen (bzw. Angriffe), die über die Kommunikation ausgeführt werden, den größeren Teil dar. Im Rahmen der Bedrohungsanalyse ist abzuschätzen, welche Auswirkungen durch mögliche Bedrohungen auf die Kommunikation, die Automatisierungskomponente sowie die Funktion einer Automatisierungsanlage entstehen.

4.3 Risikobewertung von Automatisierungssystemen

Im Einsatzfeld der funktionalen Sicherheit, findet im Umfeld der Automatisierungstechnik die Risikoanalyse weite Verbreitung und Verwendung. Diese Analyseverfahren können auf die IT-Sicherheit sinngemäß angewendet werden. Typische Verfahrensweisen sind:

Top-Down-Ansätze	Bottom-Up-Ansätze
Ausgehend von den möglichen Zielen eines Angreifers, wird eine Risikoanalyse der betroffenen Assets erfolgt. Typischer Vertreter dieser Kategorie ist die Fehlerbaumanalyse („Fault Tree Analysis“ (FTA)). [IEC2006b]	Ausgehend von einer Schwachstelle oder einem Fehler eines Assets, wird auf Risiken für das System hingewiesen. Diese Vorgehensweise findet sich in der „Hazard-and-Operability-Analysis“ (HAZOP) oder der FMEA („Failure Mode and Effects Analysis”) wieder. [IEC2001], [IEC2006a].

Tabelle 4-2: Vorgehensweisen zur Risikoermittlung

Sowohl Top-Down- als auch Bottom-Up-Ansätze sind zielführend, um das Risiko für ein Automatisierungssystem ermitteln zu können. Bezogen auf den in dieser Arbeit definierten Betrachtungsgegenstandes lässt sich anhand des Top-Down-Ansatzes keine sinnvolle und begrenzte Risikoanalyse durchführen. Dies resultiert zum einen aus dem breiten Anwendungsfeld des hier dargestellten Betrachtungsgegenstandes, aber vor allem aus der nicht greifba-

ren Intention eines Angreifers, die eine systematische Risikoermittlung und den Top-Down-Ansatz in dem hier betrachteten Einsatzszenario bzw. der Beispielanlage erschwert [VDI2011]. Daher erfolgt in diesem Fall eine Ausrichtung an einem Bottom-Up-Ansatz. Im folgenden Abschnitt 4.4 werden dafür zunächst die Auswirkungen von Bedrohungen auf die Assets des Betrachtungsgegenstands und die damit einhergehenden Risikofaktoren betrachtet. Im Anschluss erfolgt eine Bewertung des Gesamtrisikos für die jeweiligen Assets, welches sich aus der Betrachtung der Bedrohung für den Betrachtungsgegenstands ergibt.

4.4 Auswirkungen von Bedrohungen

Sofern eine Bedrohung existiert, die durch Ausnutzung einer Schwachstelle zu Stande kommt, können Folgen bzw. Risiken für die Assets einer Automatisierungsanlage entstehen. Im folgenden Abschnitt sollen generelle Angriffsszenarien und unmittelbare Folgen gezeigt werden, die durch die genannten Bedrohungen entstehen können. Die Folgen sollen Risiken für Automatisierungsanlagen herausstellen, die als Ausgangspunkt zur Auswahl relevanter Schutzziele und zur Risikobewertung dienen.

4.4.1 Eigenschaften von Bedrohungen

Neben den in Tabelle 4-1 genannten Top 10 Bedrohungen existiert eine Vielzahl weiterer Bedrohungen, die einen Bezug zur Automatisierungstechnik aufweisen. Mit Hilfe des von Microsoft entwickelten STRIDE-Ansatzes lassen sich systematisch Bedrohungen entsprechend deren Eigenschaften kategorisieren [MIC2002]. Diese sollen anschließend auf das Anlagenbeispiel übertragen werden.

Bedrohung		Beschreibung
S	Spoofing	Unter Spoofing versteht man das Vortäuschen einer falschen Identität um beispielsweise Zugriff auf vertrauliche Daten zu erlangen.
T	Tampering	Tampering bezeichnet die unbefugte Manipulation von Daten wie beispielsweise das Verändern von Netzwerkpaketinhalten.
R	Repudiation	Unter Repudiation versteht man das Abstreiten einer vollzogenen Handlung beziehungsweise die Nichtbeweisbarkeit der Handlung.
I	Information Disclosure	Die offene Verfügbarkeit von Daten, die nicht von Dritten einsehbar sein sollten wird als Information Disclosure bezeichnet. Beispiel dafür ist die unverschlüsselte Übertragung von vertraulichen Daten.
D	Denial of Service	Ziel des Angreifers bei einem „Denial of Service“-Angriff ist es, die Verfügbarkeit eines vom System angebotenen Dienstes einzuschränken.
E	Elevation of Privilege	Kann ein Angreifer seine Rechte erhöhen, wird dies als Elevation of Privilege bezeichnet. Endziel eines solchen Angriffs ist bspw. die volle Berechtigung über die Ressourcen eines Systems zu erlangen.

Tabelle 4-3: Bedrohungen im „STRIDE“-Modell

Das STRIDE-Modell ermöglicht eine systematische Betrachtung von Bedrohungen. Hierbei steht der Begriff „STRIDE“ mit seinen Einzelbuchstaben jeweils für eine typische Bedrohung bzw. ein Angriffsmuster. Diese typischen Bedrohungen können sowohl entfernt über die Kommunikation als auch lokal auf eine Komponente durchgeführt werden. Diese Angriffsmuster können auf jede der in Tabelle 4-1 aufgezeigten Bedrohungen übertragen werden, wobei dieser Zusammenhang in Tabelle 4-4 dargestellt ist.

Nr.	Bedrohung		S	T	R	I	D	E
1	Unberechtigte Nutzung von Fernwartungszugängen		●		●			●
2	Online-Angriffe über Büronetzwerk bzw. Leitebene					●	●	
3	Angriffe auf Standardkomponenten im Netzwerk							
4	(Distributed) „Denial of Service-“Angriffe / (D)DoS						●	
5	a)	Menschliches Fehlverhalten						
	b)	Sabotage					●	
6	Einschleusen von Schadcode über Wechseldatenträger und externe Hardware		●	●	●		●	●
7	Lesen und Schreiben von Nachrichten in ICS-Netzen		●	●	●	●	●	●
8	Unberechtigter Zugriff auf Ressourcen					●		●
9	Angriffe auf Netzwerkkomponenten		●	●			●	
10	Technisches Fehlverhalten / Höhere Gewalt							

Tabelle 4-4: Übertragung des „STRIDE“-Modells auf typische Bedrohungen

Auf diese Weise ist eine übersichtliche Bedrohungsanalyse möglich, da eine Zusammenfassung der Bedrohungen bzw. typische Angriffsmuster entsprechend dem STRIDE-Ansatz möglich ist. In der vorliegenden Bedrohungsanalyse einer beispielhaften Automatisierungsanlage, werden die im STRIDE-Modell genannten Bedrohungen bzw. Angriffsmuster betrachtet und deren unmittelbare Folgen aufgezeigt.

4.4.2 Übersicht zu Auswirkungen von Bedrohungen

Bedrohungen (bzw. ausgenutzte Schwachstellen) der Kommunikation und der Automatisierungskomponenten sollen anhand des vereinfachten Modells des Betrachtungsgegenstandes separat betrachtet werden. Die Abgrenzung zwischen beiden Bestandteilen des Betrachtungsgegenstands erfolgt anhand der Systemgrenze. Als generische Bedrohungen werden die einzelnen Kategorien des STRIDE-Modells herangezogen.

Unmittelbare Folgen und Risiken von Bedrohungen der Kommunikation

Getrieben durch die „Industrie 4.0“-Initiative nimmt die Offenheit von Automatisierungsanlagen zu. Offene Industrial Ethernet Standards, basierend auf Standard Ethernet, führen so dazu, dass Bedrohungen und Schwachstellen für Automatisierungsnetzwerke wie auch für die Standard-IT gelten. Nachfolgend sollen die wichtigsten Folgen aufgezeigt werden.

Spoofing als Bedrohung der Kommunikation („S“)

Das Vortäuschen einer Identität (Spoofing) erfolgt durch Versendung von Nachrichten mit gefälschten/nachgestellten Adressinformationen (MAC-Adresse oder IP-Adresse) und/oder Autorisierungsinformationen (Benutzernamen / Passwörtern). Die Informationen hierfür können durch Mitlesen von Nachrichten auf dem Netzwerk (Sniffing) erlangt werden. Da die Kommunikation zwischen den BNK und PNK üblicherweise unverschlüsselt erfolgt, kann ein Angreifer Zugriff auf diese Informationen erhalten. [YOR2010]

Mit Hilfe von gefälschten Datenpaketen ist die Etablierung einer unautorisierten Verbindung zu Automatisierungskomponenten möglich. Auch sogenannte „Replay-Angriffe“ sind denkbar, bei denen Kommunikationsabläufe nachgestellt werden. Das Vortäuschen einer Identität ermöglicht somit die Steuerung von Prozessen durch Angreifer aufgrund mangelhafter Maßnahmen zum Schutz und der Feststellung der Identitäten. [AKB2009a]

Tampering als Bedrohung der Kommunikation („T“)

Tampering einer Kommunikation beschreibt das Verfälschen von übertragenen Nachrichteninhalten. Dem gehen Spoofing- und Sniffing-Angriffe voraus, um Zugriff auf die Kommunikationsinformationen zu erhalten. In Folge dessen können Nachrichten auf dem Netzwerk nicht nur mitgelesen und zurückgehalten werden, sondern auch durch die angreifende Person verändert und danach weitergeleitet werden. Der Angreifer agiert damit als dritter Kommunikationspartner zwischen den eigentlichen Kommunikationspartnern wie SPS und dezentraler Peripherie. Aufgrund dieser Eigenschaft wird dieser Angriff auch als „Man in the Middle“-Angriff bezeichnet [AKB2009a], der Spoofing (Vortäuschen einer Identität) und Tampering (Verfälschen von Nachrichteninhalten) nutzt (vgl. Abbildung 3-9).

Durch die unzureichende Authentifizierung der Kommunikationspartner kann der Angriff nicht erkannt werden. Eingesetzte Prüfsummenverfahren (CRC) sind durch Angreifer reproduzierbar und bieten keine Erkennungsmöglichkeit für vorsätzlich, verfälschte Daten. Auf diese Weise kann ein Angreifer unbemerkt die direkte Steuerung des technischen Prozesses übernehmen, womit Folgen für die Sicherheit im Allgemeinen entstehen. [ZEL2011]

Repudiation als Bedrohung der Kommunikation („R“)

Die fehlende eindeutige Authentifizierungder Kommunikationspartner erlaubt es, dass durchgeführte Aktionen im Automatisierungsnetzwerk nicht eindeutig zugeordnet bzw. protokolliert werden können. Erlaubte Aktionen, aber insbesondere unerlaubte Aktionen wie Angriffe, können so nicht eindeutig zugeordnet und nachvollzogen werden.

Jede im Anlagenbeispiel aufgezeigte Automatisierungskomponente muss ein eindeutiges Identifikationsmerkmal erhalten, damit Vorgänge im Netzwerk zugeordnet werden können und potentielle Angriffe identifizierbar sind. [HAR2011]

Information Disclosure als Bedrohung der Kommunikation („I“)

Die Übertragung der Informationen im Automatisierungsnetzwerk erfolgt unverschlüsselt, lesbar für alle Teilnehmer des Netzwerkes, einschließlich eines potentiellen Angreifers. Somit kann aus der Kommunikation auf mögliche vertrauliche Informationen im Automatisierungsnetzwerk zugegriffen werden.

Relevante Informationen sind hierbei bspw. schützenswerte Prozessabläufe, die auf Rezepte schließen lassen, oder auch Informationen hinsichtlich des Aufbaus einer Automatisierungsanlage um Angriffe vorzubereiten. Ein Angreifer ist somit in der Lage über die Kommunikation nicht nur Einfluss auf den technischen Prozess zu nehmen, sondern auch unerlaubt Zugriff auf Know-How zu erlangen.

Denial of Service („DoS“) als Bedrohung der Kommunikation („D“)

„Denial of Service“-Angriffe haben zum Ziel, Dienste einer Komponente zu unterbinden. Hierfür wird der offene Dienst [DIG2013] einer Komponente über den Kommunikationsweg mit Anfragen überlastet, bis dieser Dienst nicht mehr verfügbar ist. Zudem erzeugen „Denial of Service“-Angriffe Überlastungen der Kommunikationsinfrastruktur und führen dadurch zu Störungen. Die fehlende Unterscheidung zwischen autorisierten und unautorisierten Vorgängen beim Datenverkehr ist der Ausgangspunkt für „Denial of Service“-Angriffe.

Elevation of Privilege als Bedrohung der Kommunikation („E“)

Elevation of Privilege, meint eine unerlaubte Rechteausweitung. Eine solche Bedrohung macht sich Schwachstellen zu Eigen, um Zugriff auf Informationen oder Kontrolle über das System zu erhalten, deren Zugriff durch Nutzerrechte beschränkt ist. Durch eine unzureichende Sicherung von Informationen und Identitäten im Netzwerk, besteht die Möglichkeit diese Informationen zur unerlaubten Rechteerlangung bspw. auf Automatisierungskomponenten zu nutzen. Diese unerlaubte Rechteerlangung kann dann als Ausgangspunkt für Angriffe auf Automatisierungskomponenten genutzt werden. [BEI2011]

Unmittelbare Folgen und Risiken von Bedrohungen der Komponenten

Entsprechend Abbildung 4-2 erfolgt in diesem Abschnitt die Betrachtung der Auswirkungen von Bedrohungen auf eine Komponente, welche durch die Systemgrenze dargestellt ist. Dieses System entspricht dem in Abschnitt 3.1.1 dargestellten Aufbau einer Automatisierungskomponente. Sowohl über physikalische Schnittstellen als auch durch direkten Zugriff auf die Komponente kann ein Angriff erfolgen, der die hinterlegten Daten inkl. der Anwendung betrifft. Nachfolgend sollen grundlegende Bedrohungen der Komponenten und daraus resultierende Risiken aufgezeigt werden.

Spoofing als Bedrohung der Komponente („S“)

Während Spoofing in der Kommunikation speziell das Vortäuschen einer Identität durch Manipulation von Nachrichten meint, so umfasst Spoofing auch allgemein das Untergraben von Identifikationsverfahren [YOR2010]. Ein Angreifer greift dazu auf vertrauenswürdige Identifikationsmerkmale zurück, um in diesem Fall Zugriff auf Automatisierungskomponenten zu erhalten. Die dafür notwendigen Informationen können bspw. über Ausspähung der Kommunikation im Automatisierungsnetzwerk oder der Anwender des Automatisierungssystems beschafft werden.

Ein Angriff auf die Komponente kann die Veränderung der Systemfunktion der Komponente (z.B. Übertragung einer manipulierten Firmware) oder der Systemdaten zur Folge haben. Die inzwischen zahlreichen Dienste auf den Automatisierungskomponenten (bspw. Web-Server) bieten hierfür einen möglichen Angriffspunkt [DIG2013].

Tampering als Bedrohung der Komponente („T“)

Tampering einer Komponente meint die unautorisierte Veränderung der Eigenschaften der Komponente. Sowohl die Systemfunktionen der Komponente [ZEL2011] als auch die Systemdaten der Komponente (vgl. Abbildung 4-2) sind dabei Ziel des Angriffs. Der Zugriff erfolgt über die Schnittstellen, sowie über direkten Zugriff zum Speicher der Komponente.

Repudiation als Bedrohung der Komponente („R“)

Fehlende Mechanismen zur Protokollierung sicherheitsrelevanten Vorgängen, wie potentiellen Angriffen über die Kommunikation, gescheiterte Anmeldeversuche oder unautorisierte Veränderungen der Software einer Komponente führen dazu, dass auf potentielle Bedrohungen nicht oder nicht rechtzeitig reagiert wird. Ein Nachvollziehen von Sicherheitsvorfällen, um Gegenmaßnahmen ergreifen zu können, ist so nicht möglich [NIS2008]. Mögliches Ergebnis sind längere Ausfallzeiten und finanzielle Verluste.

Information Disclosure als Bedrohung der Komponente („I“)

Ungeschützte Automatisierungskomponenten ermöglichen es Angreifern Zugriff auf die Gerätesoftware zu erlangen. Handelt es sich dabei um eine aktive Komponente, können zudem Informationen über deren Parametrierung ausgelesen werden. Hinsichtlich der Gerätesoftware besteht die Gefahr des Verlustes von Know-How. Hierzu muss jedoch eine Automatisierungskomponente nicht zwingend am Netzwerk angeschlossen sein. Ein Angreifer ist auch in der Lage nach Kauf der Komponente Zugriff auf die Gerätesoftware zu erlangen und diese zu analysieren (z.B. in einer Werkstatt).

Während die Gerätesoftware zur Erstellung von illegalen Nachbauten (Produktpiraterie) genutzt werden kann, so gibt die Parametrierung möglicherweise Rückschluss auf den Aufbau der Automatisierungsanlage und dient der Vorbereitung von Angriffen. Finanzielle Einbußen in Folge von Know-How Verlust sind das Ergebnis.

Denial of Service („DoS“) als Bedrohung der Komponente („D“)

Ein „Denial of Service“-Angriff und die dadurch erzeugte Überlastsituation bei der Kommunikation auf dem Netzwerk, können zu einem Ausfall der Komponente oder der Automatisierungsanlage führen. Die Komponente muss eine gewisse Überlast an der Kommunikationsschnittstelle abfangen können. Andernfalls ist ein Ausfall der Automatisierungsanlage möglich [RUN2008], mit evtl. daraus resultierenden finanzielle Verlusten.

Elevation of Privilege als Bedrohung der Komponente („E“)

Mit direktem Zugriff auf die Automatisierungskomponente sind Angriffe möglich, die es erlauben, ohne Kenntnisse von Identifikationsmerkmalen Zugriffsrechte auf die Software der Komponente zu erhalten, z.B. in Folge eines „Buffer Overflow“-Angriffs [ECK2009]. Dabei wird durch einen Angreifer ein Überlauf des Speicherbereichs provoziert, wodurch andere Speicherbereiche überschrieben werden und so schadhafte Software zur Ausführung gebracht wird. In einem zweiten Schritt werden erweiterte Zugriffsrechte etabliert, durch diese kann der Angreifer vollständige Kontrolle über die Komponente erlangen. Aufgrund fehlender Maßnahmen zur Erkennung von Manipulationen an den Komponenten kann auf diesem Weg die Funktion verändert werden.

Die dargestellten Bedrohungen (bzw. Schwachstellen) und deren Eigenschaften zeigen auf, dass sowohl die Kommunikation zwischen den Komponenten als auch die Komponenten selbst gefährdet sind. Auf Basis der Betrachtung der Bedrohungen kann nachfolgend eine Bewertung des Risikos für die Schutzziele erfolgen.

4.5 Risikobewertung und Darstellung der aktuellen Situation

Ausgehend von den vorherigen Definitionen, Betrachtungen und Erläuterungen ist das Gesamtrisiko für ein Automatisierungssystem zu ermitteln. Das Gesamtrisiko einer Bedrohung für das Automatisierungssystem setzt sich aus den in Abschnitt 2.2.1 dargestellten Risikofaktoren zusammen. Für jede der in Abschnitt 4.4 dargestellten Bedrohungen wird nachfolgend eine Bewertung des Risikos für den Betrachtungsgegenstand bzw. das Automatisierungssystems durchgeführt. Die Bewertung der Risikofaktoren erfolgt anhand der definierten Stufen aus Abschnitt 2.2.2 von gering bis hoch.

Tabelle 4-5 zeigt die definierten Werte der Risikogrößen für die Assets „Kommunikation“ und „Komponente“ auf. Dabei werden für die Assets und deren Bedrohungen die Risikogrößen ermittelt und das Gesamtrisiko berechnet. Das definierte akzeptable Risiko gibt dabei Aufschluss, ob eine Risikoreduzierung erforderlich ist und somit Schutzmaßnahmen für die IT-Sicherheit erforderlich sind. Im Allgemeinen werden diese Werte der Risikofaktoren im Rahmen von Risikobewertungsverfahren ermittelt, an dem ein interdisziplinär zusammengesetzter Personenkreis (z.B. Inbetriebnehmer, Planungsingenieur etc.) teilnimmt. Für die vorliegende Arbeit wurden die Werte der Risikogrößen vom Autor exemplarisch festgelegt, da primär das generelle Verfahren der Risikobewertung und dessen Ergebnis im Fokus steht und weniger das zahlenmäßige Ergebnis des Risikobewertungsverfahrens.

Asset	Bedrohung	Bewertung des Risikos				Akzeptables Risiko	Risikoreduzierung erforderlich?
		Ausmaß der Bedrohung	Wahrscheinlichkeit des Eintritts	Schadenspotential	Gesamtrisiko		
Kommunikation	**S**	5	5	5	125	40	<Ja>
	T	4	5	5	100	50	<Ja>
	R	4	4	4	64	50	<Ja>
	I	5	4	5	100	50	<Ja>
	D	5	5	4	100	40	<Ja>
	E	5	4	5	100	50	<Ja>
Komponente	**S**	5	4	4	80	40	<Ja>
	T	4	4	4	64	50	<Ja>
	R	4	4	4	64	50	<Ja>
	I	4	4	4	64	50	<Ja>
	D	5	5	4	100	40	<Ja>
	E	4	4	4	64	50	<Ja>

Tabelle 4-5: Gesamtbewertung des Risikos

Tabelle 4-5 zeigt auf, dass durch Multiplikation der Risikofaktoren schon ein einzelner hoher Faktor zu einem hohen Gesamtrisiko einer Bedrohung für das Automatisierungssystem führen kann. Die Reduzierung eines Faktors um eine Stufe würde bereits eine signifikante Reduzierung des potentiellen Risikos bewirken. Im Speziellen ist das Gesamtrisiko bei Bedrohungen der Kommunikation zumeist hoch. Dies erklärt sich mit der offenen Kommunikation auf Basis von Industrial Ethernet, bspw. durch Angriffe auf Fernwartungszugänge. Hinzu kommt die Verwendung dieser zumeist ungesicherten industriellen Kommunikation. Bezüglich des Risikos für die Komponente zeigt sich ein mittleres bis hohes Gesamtrisiko. Dies ist bedingt durch den benötigten direkten lokalen Zugriff auf die Komponente und daran geknüpfte lokale Angriffsmethoden. In Summe zeigt sich jedoch, dass Schutzmaßnahmen zur Risikoreduzierung zwingend erforderlich sind.

Kapitel 4 zeigte die Bedrohungen auf, denen eine Automatisierungsanlage ausgesetzt ist. Zur Verdeutlichung wurde hierfür eine exemplarische Bedrohungsanalyse anhand der VDI-Richtlinie 2182 [VDI2008] durchgeführt. Hierfür ist eine grundlegende Betrachtung der Top 10 Bedrohungen aus dem Jahr 2012 für industrielle Anlagen auf zwei definierte Assets erfolgt [BSI2014]. Das Ergebnis der Risikoanalyse zeigte, dass aufgrund der zahlreichen Folgen für Automatisierungsanlagen in jedem Fall Maßnahmen zu deren Schutz getroffen werden müssen.

Aktuelle Berichte aus dem Umfeld der IT-Sicherheit in der Automatisierungstechnik verdeutlichen, dass die Gefahr von Angriffen zunimmt, womit Risiken weiterhin steigen und sich verändern werden [MAT2011], [DHS2012]. Dieser Umstand zeigt sich bspw. durch die Aktualisierung der Top 10 Bedrohungen durch das BSI im Jahr 2014 nach nur zwei Jahren [BSI2014]. Trotz dieser zwischenzeitlichen Aktualisierung können Angriffe nach wie vor nach dem in Abschnitt 4.2 dargestellten Ansatz klassifiziert werden. Dies gilt ebenfalls für die evtl. auftretenden Auswirkungen für die Bedrohungen (siehe Abschnitt 4.4), was letztlich in der Risikobewertung zu einem ähnlichen Ergebnis führen würde.

5 Einsatz von Schutzmaßnahmen in der Automation

Kapitel 4 verdeutlichte, welches IT-Sicherheitsrisiko für Anlagen der Automatisierungstechnik besteht. Es zeigte sich, dass Schutzmaßnahmen in jedem Fall etabliert werden müssen. Kapitel 5 zeigt nun Schutzmaßnahmen auf, die zu einer Reduzierung des Risikos auf ein akzeptables Niveau führen sollen. Dabei sollen vor allem Maßnahmen betrachtet werden, die in der Praxis bereits Anwendung finden. Außerdem ist zu prüfen, inwiefern diese Maßnahmen gleichzeitig die Anforderungen der IT-Sicherheit und Automatisierungstechnik erfüllen.

Hierzu sind zunächst grundlegende Anforderungen zu definieren (►5.1). Ausgehend davon sollen verschiedene Schutzmaßnahmen hinsichtlich der Anforderungen betrachtet werden (►5.2). In Abschnitt 5.3 erfolgt dann anhand dieser Betrachtung eine zusammenfassende Bewertung der aktuellen Maßnahmen und die Darstellung der Defizite. Zusätzlich wird überprüft, ob die Maßnahmen eine Risikoreduzierung herbeiführen, wobei die Kriterien und Ergebnisse der Risikoanalyse (STRIDE) aus Kapitel 4 herangezogen werden. Weiterhin erfolgt die Darstellung grundlegender Anforderungen an erweiterte Schutzmaßnahmen.

5.1 Anforderungsanalyse an Schutzmaßnahmen

In Abschnitt 5.1 wird eine Anforderungsanalyse durchgeführt. Ziel ist die Erfassung von Anforderungen, die durch die IT-Sicherheit sowie die Automatisierungstechnik an Schutzmaßnahmen gestellt werden. Auf Basis dieser Anforderungen sollen Schutzmaßnahmen betrachtet und bewertet werden, um Defizite ermitteln zu können.

5.1.1 Anforderungen aus der IT-Sicherheit

Die Aufgabe der IT-Sicherheit ist es, die in Abschnitt 2.1.2 erläuterten Schutzziele für ein informationstechnisches System mit Hilfe von Schutzmaßnahmen zu erfüllen die zu einer Risikoreduzierung führen. Da eine Verletzung der Schutzziele zahlreiche Auswirkungen haben kann, ist eine Betrachtung der Schutzziele der IT-Sicherheit aus Sicht der Automatisierungstechnik erforderlich. Die Automatisierungstechnik stellt zusätzlich Anforderungen an die Schutzmaßnahmen für die IT-Sicherheit des informationstechnischen Systems (►5.1.2).

Im Zuge der Übersicht zu den Bedrohungen wurde deutlich, welche Gefährdung bzw. potentielle Risiken durch Bedrohungen entstehen. Tabelle 5-1 stellt die jeweiligen Bedrohungen direkt den assoziierten Schutzzielen gegenüber [MIC2002]. So wird bspw. im Falle des Spoofing direkt das Schutzziel Authentizität adressiert.

Bedrohung		Kurzbeschreibung der Bedrohung	Assoziiertes Schutzziel
S	Spoofing	Vortäuschen einer falschen Identität	Authentizität
T	Tampering	Unbefugte Manipulation von Daten	Integrität
R	Repudiation	Abstreiten einer vollzogenen Handlung	Verbindlichkeit
I	Information Disclosure	Offenlegung von Informationen	Vertraulichkeit
D	Denial of Service	Einschränken der Verfügbarkeit eines Dienstes	Verfügbarkeit
E	Elevation of Privilege	Unautorisierte Rechte- und Ressourcenerlangung	Autorisierung

Tabelle 5-1: STRIDE-Modell und assoziierte Schutzziele

Wie in Abschnitt 2.1.2 erläutert, können weitere Schutzziele in die Betrachtung mit einfließen. In diesem Fall betrifft dies die Autorisierung, da neben der Feststellung einer Identität sichergestellt sein muss, ob diese Identität zu Handlungen im informationstechnischen System autorisiert ist. Abschnitt 4.4.2 zeigte hierzu, dass die fehlende Identifikation von Kommunikationspartnern und deren Datenkommunikation ein Ausgangspunkt für Bedrohungen ist. Durch Vortäuschen einer Identität ist die Manipulation von übertragenen Daten, oder der Zugriff auf eine Automatisierungskomponente möglich. Weiterhin ist eine Unterscheidung zwischen autorisierten und unautorisierten Vorgängen nicht möglich. Bezogen auf den Betrachtungsgegenstand ist daher ein Schutzziel immer in Zusammenwirken mit anderen Schutzzielen zu betrachten.

Aus Tabelle 5-1 ergeben sich direkte Anforderungen an Schutzmaßnahmen, um entsprechende Schutzziele erreichen zu können. Ausgehend von den Bedrohungen und den assoziierten Schutzzielen, lassen sich entsprechend [BSI2014], [BSI2010b], [DHS2009], [DHS2011] wesentliche Anforderungen an Schutzmaßnahmen ableiten, die in Tabelle 5-2 aufgeführt sind.

Bedrohung		Kurzbeschreibung der Bedrohung	Anforderung an Schutzmaßnahmen
S	Spoofing	Vortäuschen einer falschen Identität	Sicherstellung der Identität von Netzwerkteilnehmern im Automatisierungssystem
T	Tampering	Unbefugte Manipulation von Daten	Schutz vor Manipulation von Informationen
R	Repudiation	Abstreiten einer vollzogenen Handlung	Zuordnung von Abläufen (z.B. Anmeldevorgängen) in einem Automatisierungssystem
I	Information Disclosure	Offenlegung von Informationen	Schutz vor unautorisiertem Zugriff auf vertrauliche Informationen
D	Denial of Service	Einschränken der Verfügbarkeit eines Dienstes	Schutz vor unautorisiertem oder unzulässiger Nutzung von Diensten
E	Elevation of Privilege	Unautorisierte Rechte- und Ressourcenerlangung	Schutz vor unautorisiertem Zugang mit Hilfe von Manipulationen des Systems

Tabelle 5-2: Abgeleitete Anforderungen an Schutzmaßnahmen aus dem STRIDE-Modell

So ist bspw. im Falle des Spoofing die Sicherstellung der Identität von Netzwerkteilnehmern erforderlich. In gleicher Weise können weitere Anforderungen durch die IT-Sicherheit bzw. assoziierten Schutzziele und Bedrohungen des STRIDE-Modells an die Schutzmaßnahmen gestellt werden. Bedrohungen, Schutzziele sowie Anforderungen an Schutzmaßnahmen stehen somit in direkter Beziehung zueinander. Die Anforderungen für Schutzmaßnahmen können damit auf ähnliche Weise auf die Schutzziele der IT-Sicherheit abgebildet werden.

Kapitel 4 zeigte, dass der Betrachtungsgegenstand in die Assets Kommunikationsinfrastruktur als auch Automatisierungskomponente separiert werden kann. Die Bedrohungsanalyse zeigt weiterhin, dass beide Assets durch die Bedrohungen des STRIDE-Modells betroffen sein können. Demzufolge gelten die Anforderungen an Schutzmaßnahmen für beide Assets. Bei der nachfolgenden Betrachtung von Schutzmaßnahmen werden daher stets beide Assets entsprechend der Anforderungen aus der IT-Sicherheit betrachtet. So ist im Falle des unbefugten Manipulierens von Daten („**T**“) eine Schutzmaßnahme notwendig, die sowohl die Manipulation der Daten einer Kommunikation als auch von Automatisierungskomponenten verhindern soll.

5.1.2 Anforderungen durch die Automatisierungstechnik

Die Automatisierungstechnik hat zur Aufgabe den unterbrechungsfreien produktiven Betrieb einer Automatisierungsanlage sicher zu stellen. Hauptfokus der Automatisierungstechnik liegt demnach nicht in der IT-Sicherheit einer Automatisierungsanlage. Doch auch beim Einsatz von Schutzmaßnahmen für die IT-Sicherheit sind wesentliche Anforderungen aus der Automatisierungstechnik zu berücksichtigen. Diese Anforderungen der Automatisierungstechnik sind:

- **Echtzeitanforderungen**

Der Begriff „Echtzeit“ betrifft die rechtzeitige Reaktion auf eintretende Ereignisse [REI2002]. In der Automatisierungstechnik muss dieses Kriterium erfüllt werden, um auf Ereignisse im System innerhalb der durch den Prozess vorgegebenen Reaktionszeit reagieren zu können. Je nach technischem Prozess existieren dabei unterschiedliche Zeitanforderungen. Während langsamere Vorgänge wie in der bspw. in der Prozessautomatisierung im Sekundenbereich ablaufen, so müssen in der Fertigungsautomatisierung kleinere Reaktionszeiten im Millisekunden-Bereich realisiert werden. Dies stellt hohe Anforderungen an das Zeitverhalten der Automatisierungskomponenten. Im Falle ressourcenbeschränkter Plattformen mit geringen Rechenkapazitäten ist dies eine besondere Herausforderung. Schutzmaßnahmen der IT-Sicherheit in der Automatisierungstechnik dürfen daher die Echtzeitfähigkeit des Automatisierungssystems nicht gravierend beeinträchtigen.

- Hohe **Verfügbarkeitsanforderungen** der Automatisierungsanlage

Der unterbrechungsfreie produktive Betrieb stellt hohe Anforderungen an die Verfügbarkeit der Automatisierungsanlage. Gemeint ist damit, dass ein Automatisierungssystem zu einem gegebenen Zeitpunkt bzw. Zeitraum eine geforderte Funktion erfüllen kann [DKE2013]. Die im Automatisierungssystem verwendeten Komponenten und Kommunikationslösungen müssen dieses Kriterium erfüllen.

Die dafür notwendigen Maßnahmen sind bspw. die Anpassung des Automatisierungssystem an raue Umgebungsbedingungen (z.B. mechanische und thermische Einwirkungen sowie starke elektromagnetische Einflüsse (EMV)). Diese als Robustheit bezeichnete Eigenschaft, ist für einen zuverlässigen Betrieb einer Automatisierungsanlage unerlässlich. Daher werden auch hohe Ansprüche an die Stör- und Ausfallsicherheit von Automatisierungssystemen gestellt. Sofern ein teilweiser Ausfall von Komponenten eintritt, muss die Überwachung und Steuerung des technischen Prozesses weiterhin möglich sein. Ein ungewolltes Einwirken von IT-Sicherheitsmaßnahmen in den produktiven Betrieb und damit in die Verfügbarkeit des Automatisierungssystems ist unerwünscht.

- **Lange Einsatzdauer** einer Automatisierungsanlage

Automatisierungssysteme sind für eine lange Einsatzdauer konzipiert. Im Vergleich zu typischen Büroumgebungen, in denen in Jahreszyklen sowohl Software als auch Hardware ersetzt bzw. erneuert werden, wird in Automatisierungsanlagen der Fokus auf einen möglichst unterbrechungsfreien Betrieb teils über Jahrzehnte gelegt. Dies gilt insbesondere für Aufgaben in der Prozessautomatisierung, wo ein Produktionsprozess über mehrere Jahrzehnte zu betreiben ist. Schutzmaßnahmen für die IT-Sicherheit von Automatisierungssystemen müs-

sen diesen Aspekt berücksichtigen. So sind Schutzmaßnahmen zu favorisieren, deren Einsatz weder die Verfügbarkeit noch Echtzeitfähigkeit eines Automatisierungssystems beeinflussen und darüber hinaus über einen langen Zeitraum einen ausreichenden Schutz bieten ohne in den Betrieb einzugreifen.

- Minimaler **Betriebsaufwand**

Der Aufwand zum Betrieb von Schutzmaßnahmen für die IT-Sicherheit ist minimal zu halten, da der produktive Betrieb im Vordergrund steht. Für den Anwender einer Automatisierungsanlage ist daher entscheidend, dass sich Schutzmaßnahmen für die IT-Sicherheit transparent in die Struktur der Automatisierungsanlage einbinden lassen. Auf diese Weise können Schutzmaßnahmen wirken, ohne den Anwender gravierend vom eigentlichen Betrieb der Anlage abzulenken.

- **Flexibilität** und **Skalierbarkeit** von Schutzmaßnahmen

Während Strukturveränderungen von Automatisierungssystemen in der Vergangenheit seltener der Fall waren, so ist im Zuge von „Industrie 4.0“ auch in der Automatisierungstechnik mit schnelleren Innovationszyklen zu rechnen, die eine flexible Umgestaltung eines Automatisierungssystems erforderlich machen. Um darüber hinaus den verschiedenen Sicherheitsanforderungen der Anwender gerecht werden zu können, müssen Schutzmaßnahmen skalierbar sein. Sowohl Flexibilität als auch Skalierbarkeit sind daher wichtige Anforderungen an Schutzmaßnahmen der IT-Sicherheit für die Automatisierungstechnik.

- **Umsetzbarkeit** der Schutzmaßnahmen

Das Bewusstsein für die IT-Sicherheit in der Automatisierungstechnik ist nicht im gleichen Maße vorhanden, wie für die funktionale Sicherheit. Im Bereich der funktionalen Sicherheit werden große (auch finanzielle) Anstrengungen unternommen, um Risiken zu minimieren, was nicht zuletzt durch die gesetzlichen Vorgaben notwendig ist. Im Falle der IT-Sicherheit ist aufgrund der nicht-fassbaren Bedrohungen eine Umsetzung von Schutzmaßnahmen der IT-Sicherheit schwierig, da der finanzielle Einsatz keinen offensichtlichen Vorteil bringt. So ist ersichtlich, dass die Etablierung und Entwicklung von Schutzmaßnahmen mit möglichst geringem finanziellem Aufwand erfolgen sollte, um die Umsetzbarkeit zu gewährleisten.

Zusätzlich ist die technische Umsetzbarkeit von Schutzmaßnahmen hervorzuheben. So ist auf ressourcen-beschränkten Systemen (z.B. dezentrale Peripherie) in der Automatisierungstechnik sicherzustellen, dass Schutzmaßnahmen mit geringem Ressourceneinsatz realisierbar sind. Nach wie vor besteht die Hauptaufgabe der Systeme darin, den technischen Prozess zu steuern und zu regeln, was durch Schutzmaßnahmen auf den Komponenten nicht gravierend beeinflusst werden darf. Allgemein ist daher auch bei der Umsetzung von Schutzmaßnahmen der Aufwand zu deren Implementierung seitens der Hersteller von Automatisierungslösungen zu betrachten.

Die zuvor gestellten Anforderungen bezüglich der Anwendung von Schutzmaßnahmen für die IT-Sicherheit in der Automatisierungstechnik werden in Tabelle 5-3 zusammengefasst und sollen bei der Betrachtung der möglichen Schutzmaßnahmen als Bewertungskriterium herangezogen werden.

Bezeichnung	Anforderung	Ziel der Anforderung an Schutzmaßnahme
A1	Hohe Echtzeitanforderungen	Schutzmaßnahmen dürfen die Echtzeitfähigkeit eines Automatisierungssystems nicht beeinflussen.
A2	Hohe Verfügbarkeitsanforderungen	Verfügbarkeit des Automatisierungssystems darf nicht verschlechtert werden.
A3	Lange Einsatzdauer	Schutzmaßnahmen müssen für die Einsatzdauern von Automatisierungssystemen ausgelegt sein.
A4	Minimaler Betriebsaufwand	Zum Betrieb der Schutzmaßnahmen sollte geringer Aufwand erforderlich sein.
A5	Flexibilität und Skalierbarkeit von Schutzmaßnahmen	Strukturänderungen eines Automatisierungssystems müssen durch Schutzmaßnahmen einfach handhabbar sein.
A6	Umsetzbarkeit der Schutzmaßnahmen	Der allgemeine finanzielle und technische Aufwand zur Umsetzung von Schutzmaßnahmen für die IT-Sicherheit sollte gering sein.

Tabelle 5-3: Anforderungen aus der Automatisierungstechnik an Schutzmaßnahmen

Die Anforderungsanalyse in Abschnitt 5.1 zeigt, dass der Einsatz von Schutzmaßnahmen neben den Anforderungen aus der IT-Sicherheit zusätzlich durch Anforderungen der Automatisierungstechnik geprägt ist. Sowohl Anforderungen der IT-Sicherheit sowie der Automatisierungstechnik müssen bei der Bewertung der Schutzmaßnahmen betrachtet werden.

5.2 Übersicht und Bewertung aktueller Schutzmaßnahmen

Abschnitt 5.2 zeigt aktuell eingesetzte Schutzmaßnahmen für die IT-Sicherheit in Automatisierungssystemen. Betrachtet werden aktuell eingesetzte organisatorische sowie technische Schutzmaßnahmen für die IT-Sicherheit. Anhand der in Abschnitt 5.1 gezeigten Anforderungen wird eine Bewertung der Schutzmaßnahmen vorgenommen.

Ausgangspunkt für alle IT-sicherheitsrelevanten Vorgänge, stellt das Information Security Management System (ISMS) dar [BSI2008b]. Durch das ISMS wird festgelegt, welche Maßnahmen über den gesamten Lebenszyklus des informationstechnischen Systems ergriffen, ausgerichtet bzw. verbessert werden müssen. Hierbei verfügt das ISMS über verschiedenste Ressourcen, die zum Einsatz kommen. Ziel ist eine Sicherheitsstrategie, welche sich aus Schutzzielen und der Bedrohungsanalyse ergibt. Diese dient als Hilfsmittel zur Umsetzung von Maßnahmen sowie von Sicherheitsleitlinien.

Ein Information Security Management System (ISMS) ist demnach ein mögliches Modell zur Einführung, Überwachung und ständigen Verbesserung von Schutzmaßnahmen der IT-Sicherheit [IEC2011]. Dabei sind Verfahrens- und Vorgehensweisen anzuwenden, die einen IT-Sicherheitsbeauftragten bei der Beurteilung und Umsetzung von Sicherheitsmaßnahmen unterstützen. Bestandteil hiervon ist bspw. die Vorgehensweise nach VDI 2182 [VDI2008] oder der IEC 62443 [IEC2012b]. Zum Einsatz kommen verschiedene organisatorische und technische Maßnahmen, die im Rahmen des ISMS zyklisch auf Ihre Wirksamkeit überprüft und ggf. verbessert werden. Die häufigsten dabei in der Automatisierungstechnik anzutreffenden organisatorischen und technischen Maßnahmen sollen nachfolgend, entsprechend den genannten Anforderungen, betrachtet werden.

5.2.1 Anwendung organisatorischer Maßnahmen

Organisatorische Maßnahmen sind Schutzfunktionen die durch Verfahrens- und Vorgehensweisen etabliert werden. Aktuelle Umsetzungen in der Automatisierungstechnik sind:

Sensibilisierung des Personals

Ein sicherheitskritischer Faktor in einer Automatisierungsanlage ist der Mensch. Die Sensibilisierung des Personals in der Anlage für sicherheitsrelevante Aspekte (z.B. Nutzung von Wechseldatenträgern oder Aufmerksamkeit gegenüber unautorisiertem Personal) ist daher als organisatorische Schutzmaßnahme zu verstehen. Hierfür müssen Schulungen der Mitarbeiter durchgeführt werden, die bspw. das Verhalten in sicherheitskritischen Umgebungen oder den sicheren Umgang mit IT-Technologien betreffen. Durch die Sensibilisierung der Mitarbeiter wird es einer angreifenden Person erschwert, Kenntnisse zu Zugangsdaten zu erhalten. Absichtlich herbeigeführte Beeinflussungen der Automatisierungsanlage werden durch diese Schutzmaßnahme jedoch nicht aufgehalten. An dieser Stelle müssen zusätzliche Maßnahmen greifen, indem z.B. Zugang zur Automatisierungsanlage nur bestimmten Personen erlaubt wird.

Die Schaffung eines Bewusstseins für das Thema IT-Sicherheit ist essentiell für dessen Gelingen. Ohne Darstellung der möglichen Auswirkungen wird der (Kosten-)Einsatz von weiteren IT-Sicherheitsmaßnahmen nicht als Mehrwert interpretiert. Hinsichtlich der Anforderungen durch die Automatisierungstechnik an Schutzmaßnahmen aus Tabelle 5-3 werden alle Anforderungen erfüllt. Die Sensibilisierung der Mitarbeiter hat jedoch nur eine begrenzte Schutzwirkung in Bezug auf die Schutzziele der Komponente →**I** und →**D**.

Benutzerauthentifizierung sowie Rollen- und Rechteverwaltung

Um Zugriff zu einer Automatisierungsanlage nur autorisiertem Personal zu ermöglichen, werden Zugangskontrollen etabliert, welche in Abbildung 5-1 dargestellt sind.

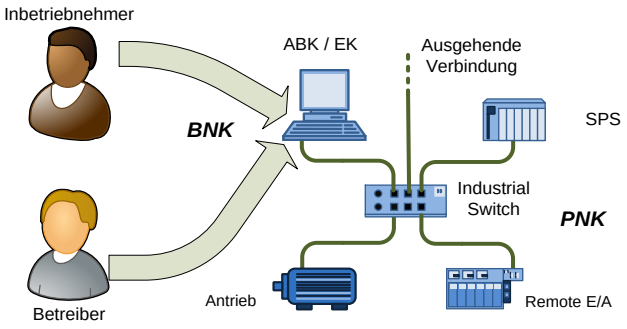


Abbildung 5-1: Benutzerauthentifizierung / Rollen- und Rechteverwaltung

Dabei wird eine Authentifizierung von Benutzern an benutzernahen Komponenten etabliert, die durch Kombination von Benutzermerkmalen (Namen / Passwörtern) erfolgt. Benutzern werden hierbei an den Stationen verschiedene Berechtigungen zur Bedienung eingeräumt, da diese z.B. einer bestimmten Rolle (z.B. Inbetriebnehmer, Betreiber) zugeordnet wurden. Hierfür ist vorab eine Festlegung in den Sicherheitsrichtlinien zu erstellen. Aktueller Fokus liegt auf der Benutzerauthentifizierung entsprechend ihrer Rollen lediglich an den benutzernahen Komponenten. Eine Authentifizierung an den Komponenten der Automatisierungsanlage erfolgt über diese Bedienstationen ebenso über Benutzernamen und Passwörter.

Da die Authentifizierung nur die BNK betrifft, wird die Verfügbarkeit und Echtzeitfähigkeit (→**A1** und →**A2**) der PNK nicht direkt beeinflusst. Die Umsetzung der Authentifizierung von Benutzern kann auf den jeweiligen BNK mit geringem Aufwand erfolgen (→**A6 und** →**A4**). Hinsichtlich **A3** und **A5** ist jedoch zu beachten, dass ein Ausschließen von Benutzern von der Rollen- und Rechteverwaltung ermöglicht werden muss, sofern diese bspw. den Betrieb verlassen haben bzw. ihnen die Berechtigung entzogen wurde. Dies erhöht den Verwaltungsaufwand für diese Schutzmaßnahme.

Die Wirksamkeit der Benutzerauthentifizierung bzw. Rollen- und Rechteverwaltung begrenzt sich auf die Anmeldung an ABK/EK und an einzelnen PNK und damit auf den Komponenten des Automatisierungssystems. Damit kann in erster Linie das Schutzziel **S** an einer Komponente adressiert werden. In begrenztem Maße können zusätzlich vollzogene Handlungen an Komponenten protokolliert werden (→**R**). Bei der Verwendung von Namen- / Passwortkombinationen besteht weiterhin die Gefahr des Spoofing. Nur durch Anwendung einer Mehrfaktor-Authentifizierung bspw. durch Einbeziehung kryptografische Hilfsmittel, kann dies wirksam verhindert werden.

5.2.2 Technische Verfahren und Maßnahmen zum Schutz der Anlage

Neben organisatorischen Maßnahmen erfolgt parallel der Einsatz von technischen Schutzmaßnahmen. Bei diesen Verfahren handelt es sich, im Gegensatz zu Verfahrens- und Vorgehensweisen, um solche Maßnahmen, die mit Hilfe technischer Mittel umgesetzt werden.

Physische Schutzmaßnahmen / Zutrittskontrolle

Physische Schutzmaßnahmen sind, im Gegensatz zur Zugangskontrolle zu Komponenten und Bedienstationen, eine Begrenzung des Zutritts zur Anlage. Hierzu gehören z.B. Maßnahmen wie Zäune, abschließbare Schränke, Schranken und Kameras. Unterstützend wird Sicherheitspersonal eingesetzt, welches den Zutritt kontrolliert oder technische Maßnahmen wie z.B. Drehkreuze mit Kartenlesern dessen Betrieb auch ohne Personal möglich ist.

Je nach Umfang der Zutrittskontrolle ist die Umsetzung (→**A6)** mit großem Aufwand verbunden. Hingegen erfolgt kein Einfluss der Automatisierungsanlage (→**A1** bis **A3)**, weshalb eine Zutrittskontrolle als Maßnahme sinnvoll ist, sofern der Aufwand zu deren Betrieb überschaubar bleibt (→**A4**). Darüber hinaus sind physische Schutzmaßnahme bzw. Zutrittskontrollen wenig flexibel oder skalierbar (→**A5**). Die Wirksamkeit von physischen Schutzmaßnahmen bzw. Zutrittskontrollen begrenzt sich auf den Schutz gegen unbefugten Zutritt. Zwar decken diese Schutzmaßnahmen zahlreiche Schutzziele entsprechend Tabelle 5-3 ab, bei Überwindung der Zutrittskontrolle besteht jedoch keine weitere Schutzwirkung [VID2008].

Einsatz von Firewalls

Zum Schutz von Teilen einer Automatisierungsanlage, werden Netzwerkbereiche über Firewalls geschützt bzw. abgeschottet. Netzwerkbereiche bilden hierbei Funktionseinheiten einer Automatisierungsanlage ab. Durch Firewalls wird die Kommunikation zwischen den Funktionseinheiten überwacht und unerlaubter Datenverkehr wird unterbunden. Realisiert werden Firewalls durch Software-Firewalls, bspw. auf einem Standard-PC oder in Form einer Hardware-Baugruppe für Hutschienenmontage in der Automatisierungstechnik. Die Komponenten

innerhalb dieses geschützten Netzwerkbereiches sind als vertrauenswürdig eingestuft, weshalb dieser Netzwerkbereich auch als „Trusted Zone“ bezeichnet wird. Ein zusätzlicher Schutz der Komponenten bzw. der Kommunikation in der „Trusted Zone“ besteht nicht. Das „Trusted Zone“-Prinzip wird in Abbildung 5-2 dargestellt.

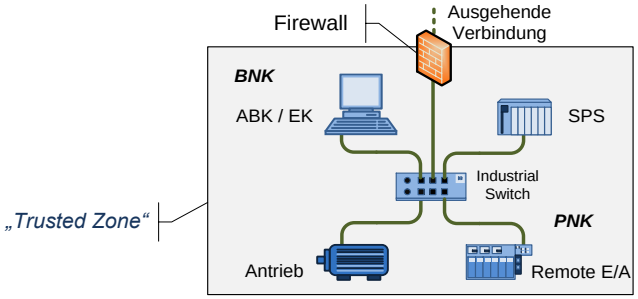


Abbildung 5-2: Einsatz einer Firewall und Aufbau einer „Trusted Zone“

Der Einsatz von Firewalls kann mit geringem Aufwand erfolgen (→**A6**). Zugriffe von außen können überwacht und minimiert werden. Doch geht dieser Schutzansatz von starren Automatisierungsstrukturen aus, was hinsichtlich Anforderung **A5** hinderlich ist. Sofern sich diese Systemstruktur des Automatisierungssystems nicht ändert, ist eine Firewall in seiner Einsatzdauer nicht begrenzt (→**A3**). Doch jede der Firewalls bedarf einer Konfiguration, was zu einem zusätzlichem Betriebsaufwand führt (→**A4**). Mit steigender Anzahl an Firewalls in einem Automatisierungssystem, bspw. zur Realisierung einer tiefengestaffelten Abschottung des Automatisierungsnetzwerks, erhöht sich zusätzlich der Betriebsaufwand. Da eine Firewall eine eigenständige Komponente darstellt, welche ein- und ausgehende Kommunikationen überwacht, kann sowohl die Verfügbarkeit eines Automatisierungssystems wie auch dessen Echtzeitfähigkeit negativ beeinflusst werden (→**A1** und →**A2**).

Wirksam sind Firewalls gegen Bedrohungen der Kommunikation. Ein Schutz der Komponenten wird nur indirekt adressiert. Die Kommunikation innerhalb der „Trusted Zone“ ist so lange geschützt, bis ein Angreifer die Firewall umgehen kann. Eine Firewall stellt damit auch ein mögliches Angriffsziel dar, um bspw. Zugriff auf den geschützten Bereich zu erlangen. Besteht durch einen Angreifer nach Umgehung der Firewall ein Zugriff auf die „Trusted Zone“, greifen keine weiteren Schutzmaßnahmen. Allgemein wirken Firewalls demnach auf die Schutzziele **I** und **D** der Kommunikation, solange der Schutz nicht umgangen wird.

Virtual Private Network (VPN)

Zu Wartungs- und Inbetriebnahmezwecken erfolgt der Aufbau (temporärer) Verbindungen zu Automatisierungskomponenten. Aufgrund der Verteiltheit von Automatisierungsanlagen erfolgt dies oft aus der Ferne (z.B. über das Internet). Dabei kann es sich um einen Servicemitarbeiter des eigenen Unternehmens oder um einen externen Dienstleister handeln. Erfolgt die Vernetzung von Produktionsanlagen über das Internet, so werden auch hier VPN-Verbindungen eingesetzt. Um nur autorisierte Kommunikation zu ermöglichen, werden Zugangspunkte (z.B. an einer Firewall) eingerichtet, an denen durch Nachweis der Authentizität eine (kryptografisch) gesicherte Verbindung etabliert wird. So kann über einen unsicheren Weg, wie z.B. das Internet, eine gesicherte Verbindung zu einem sicherheitskritischen Bereich eingerichtet werden. Diese Funktion wird als Virtual Private Network (VPN) bezeichnet.

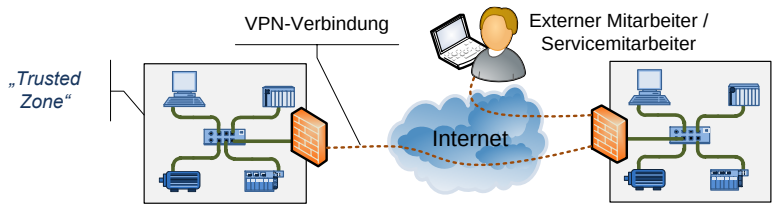


Abbildung 5-3: Gesicherte Verbindung (VPN)

Die Umsetzung von VPN-Lösungen kann auf Basis von IPSec [INT2004] oder SSL/TLS [RES2000] unter Nutzung von GnuTLS [GNU2013], OpenSSL [OPE2014] und OpenVPN [OPE2013] erfolgen (→**A6**). Gedacht sind VPN-Lösungen für einen gesicherten Kommunikationsaufbau von außerhalb mit der Automatisierungsanlage. Ein zusätzlicher Schutz der internen Kommunikation im abgeschotteten Bereich findet nicht statt. Folglich sind die Echtzeiteigenschaften der Kommunikation innerhalb des geschützten Bereichs wie auch die Verfügbarkeit der Komponenten in diesem Bereich nicht betroffen (→**A1** und **A2**). Die Flexibilität und Skalierbarkeit dieser Schutzmaßnahme (→**A5**) hängt maßgeblich von der Erreichbarkeit der Zugangspunkte und der Verwaltung der autorisierten Benutzer ab. Insbesondere die Nutzerverwaltung steigert den Betriebsaufwand (→**A4**). So sind aus Sicherheitsgründen regelmäßige Überprüfungen von Zugangsdaten durchzuführen, bspw. wenn Mitarbeiter den Betrieb verlassen und deren Zugangsrechte entzogen werden müssen. Andernfalls können VPN-Zugänge als ein Einfallstor und Angriffsmöglichkeit auf die Kommunikation im Automatisierungsnetzwerk genutzt werden [BSI2014].

Trotz des Betriebsaufwandes ist prinzipiell der Einsatz von VPN-Zugängen über den gesamten Lebenszyklus einer Automatisierungsanlage möglich (→**A3**). VPN-Technologien adressieren Schutzziele der Kommunikation und der Komponenten. Im Fokus steht die Kommunikation außerhalb des Automatisierungsnetzwerkes, bspw. beim Verbindungsaufbau zu einer Automatisierungsanlage. Eine Anwendung von VPN auf die interne Kommunikation in einem Automatisierungsnetzwerk wird nicht verfolgt, da insbesondere die Echtzeitfähigkeit der Kommunikation betroffen wäre. Bezüglich der Schutzziele der Komponente können durch den gesicherten Verbindungsaufbau die Schutzziele **S** und **R** sichergestellt werden.

“Härten” von Baugruppen

„Denial of Service“-Angriffe haben Einfluss auf die Verfügbarkeit von Komponenten. So kann schon bei größerem Kommunikationsaufkommen, inkl. Multicast und Broadcast, eine Automatisierungskomponente der Verarbeitung von Datenpaketen nicht gewachsen sein [RUN2008]. Dies gilt auch im Falle eines „Denial of Service“-Angriffs, bei dem eine angreifende Person Zugriff auf einen Switch (z.B. innerhalb Trusted Zone) erhalten kann, und gezielt das Kommunikationsaufkommen an Automatisierungskomponenten erhöht. Folge ist, dass die Komponenten ihre eigentliche Funktion nicht mehr erfüllen können. Dienste können nicht mehr bearbeitet werden oder Komponenten stellen ihre Funktion ein. Zu diesem Zweck werden Automatisierungskomponenten in Tests spezifizierten Lastsituationen ausgesetzt, um mögliche Auswirkungen von „Denial of Service“-Angriffen besser beurteilen zu können [ADH2010]. Ergebnisse der Tests werden genutzt, um Vorgaben zur Hardware bzw. Software der Automatisierungsplattform zu definieren, um so Lastsituation beherrschen zu können. Dieser Vorgang, der auch als „Härten“ bezeichnet wird, dient als Sicherheitsvorkehrung gegen „Denial of Service“-Angriffe (→**D**) und ist keine direkte Schutzmaßnahme.

So wird keine zusätzliche Funktion auf der Komponente etabliert, die eine Verbesserung des Schutzes der Komponente bewirkt, womit der Betriebsaufwand **A4** gering ist und die Flexibilität und Skalierbarkeit **A5** erhalten bleibt, da Tests der Komponenten nicht während des Betriebs der Automatisierungsanlage erfolgen. Dies bedeutet auch, dass kein Einfluss auf die Eigenschaften der Verfügbarkeit und Echtzeitfähigkeit des Automatisierungssystems während des Betriebes erfolgt (→**A1,** →**A2**). Jedoch kann durch diese Tests die Verfügbarkeit verbessert bzw. genauer bewertet werden. Die Umsetzung **A6** des „Härten“ erfolgt im Laborumfeld und zieht Anpassungen der Hard- bzw. Software der Komponenten nach sich. Diese Anpassung kann ggf. dazu führen, dass ein erhöhter Ressourcenbedarf entsteht. Die Wirksamkeit des Härtungsvorgangs ist dauerhaft, doch folgen späteren Verlauf des Lebenszyklus der Automatisierungsanlage keine zusätzlichen Verbesserungen der Komponenten (→**A3**).

Erkennung von Schadsoftware bzw. schadhaftem Verhalten

Die erhöhte Gefahr durch Schadsoftware in der Automatisierungstechnik erfordert Gegenmaßnahmen [KRE2013], bspw. durch Etablierung von Funktionen zur Erkennung bzw. Eindringen von Schadsoftware. Eingesetzt werden diese Funktionen z.B. auf Firewalls im Rahmen von Intrusion-Detection-, Intrusion-Prevention-Maßnahmen und Virenscannern. Beim Einsatz von Virenscannern wird nach auffälligem Verhalten von Schadsoftware (sogenannten Signaturen) gesucht, während durch Intrusion-Detection- und Intrusion-Prevention-Systeme Angriffe auf die Software eines Systems detektiert werden, um entsprechend reagieren zu können. Das Verhalten der schadhaften Software (engl. malware) wird dafür zuvor analysiert und als Definition bzw. Signatur in die Schadsoftwareerkennung integriert.

Sofern eine Schadsoftware-Erkennung auf Standard-PCs oder Firewall-Systemen eingesetzt wird, ist dies mit geringem Aufwand umsetzbar (→**A6**), da hierzu zahlreiche Lösungen auf dem freien Markt erhältlich sind. Anders ist dies im Falle von eingebetteten Systemen. Hier existieren nur wenige Lösungen zur Schadsoftware-Erkennung, da zum einen die eingesetzten Betriebssysteme der Automatisierungsplattformen weniger verbreitet sind und zum anderen wenig Schadsoftware bekannt ist. Da jedoch Rechnerplattformen der Automatisierungstechnik zunehmend auf Standard-Komponenten und Standard-Software basieren, besteht auch hier ein zukünftiger Bedarf an der Erkennung von schadhafter Software.

Die Erkennung von Schadsoftware benötigt Ressourcen auf den Rechnerplattformen. Dies kann insbesondere auf ressourcen-beschränkten Plattformen dazu führen, dass die Echtzeitfähigkeit und Verfügbarkeit der Kommunikation bzw. der Komponente negativ beeinflusst werden (→**A1,** →**A2**). Darüber hinaus benötigen Verfahren zur Erkennung von Schadsoftware ständige Aktualisierungen (Patches / Updates), was einen hohen Betriebsaufwand nach sich zieht (→**A4**). Im Gegensatz zur Standard-IT können zudem keine größeren Aktualisierungen während des Betriebs einer Automatisierungsanlage durchgeführt werden, da auch in diesem Falle die Verfügbarkeit bspw. durch Neustarts betroffen wäre, womit zusätzlich die Flexibilität bzw. Skalierbarkeit der Schutzmaßnahmen beschränkt ist (→**A5**). Die Einsatzdauer **A3** der Erkennung von Schadsoftware ist jedoch abhängig von der Aktualität der Definitionen für das Verhalten der schadhaften Software. Die Definitionen müssten ständig und regelmäßige aktualisiert werden. Letztlich ist die Wirksamkeit dieser Maßnahme zusätzlich auf einzelne Komponente begrenzt und zielt auf die Schutzziele **T**, **R**, **I** und **E** ab.

5.3 Defizite aktueller Schutzmaßnahmen

Die Umsetzung von Schutzmaßnahmen ist in der Automatisierungstechnik zwingend erforderlich, um den (sicheren) produktiven Betrieb aufrecht zu erhalten. Ein Automatisierungssystem wie auch die IT-Sicherheit stellen dazu unterschiedliche Anforderungen an Schutzmaßnahmen. Abschnitt 5.2 zeigte, dass die aktuellen Schutzmaßnahmen die in Abschnitt 5.1 gezeigten Anforderungen mit unterschiedlicher Effektivität und Effizienz erfüllen. In Tabelle 5-4 erfolgt eine zusammenfassende Bewertung[1] der Wirksamkeit der Schutzmaßnahmen basierend auf den Anforderungen bzw. Schutzzielen der IT-Sicherheit.

		Asset mit Schutzziel											
		Kommunikation						**Komponente**					
Schutzmaßnahme		**S**	**T**	**R**	**I**	**D**	**E**	**S**	**T**	**R**	**I**	**D**	**E**
Organisatorische Schutzmaßnahmen	Sensibilisierung der Mitarbeiter[2]				o	o					o	o	
	Benutzerauthentifizierung sowie Rollen- und Rechteverwaltung							+		o	o		o
	Physische Schutzmaßnahmen/ Zutrittskontrolle	-	-		o	o		o	o	o[3]	o	o	
Technische Schutzmaßnahmen	Einsatz von Firewalls				o	o					o	o	
	Virtual Private Network (VPN)	o	o	o	o		o	o		o			
	"Härten" von Baugruppen											o	
	Erkennung von Schadsoftware[4]								+	-	-		+
Gesamtbeurteilung		-	-	-	o	o	-	o	o	o	o	o	o

Tabelle 5-4: Bewertung der Wirksamkeit von Schutzmaßnahmen für Schutzziele

Die durchgeführte Beurteilung zeigt, dass durch die bisher beschriebenen Schutzmaßnahmen ein gewisser Schutz erreicht wird. Eine signifikante Reduzierung des Risikos (vgl. Risikobewertung in Tabelle 4-5) findet jedoch nicht statt. Somit verbleibt ein Restrisiko, welches eine weitere Risikoreduzierung durch weitere Schutzmaßnahmen erforderlich macht. Jede der organisatorischen und technischen Schutzmaßnahmen bietet für sich einen begrenzten Schutz für bestimmte Schutzziele bei den Assets Kommunikation und Komponente. Aus diesem Grund wird bei der Gesamtbeurteilung das sogenannte „Defense-in-Depth"-Schutzprinzip berücksichtigt, bei welchem verschiedene Schutzmaßnahmen gemeinsam wirken, um eine Erfüllung aller Schutzziele zu erreichen [DNH2005]. Dies unterstreicht nochmals, dass keine der aktuell eingesetzten Schutzmaßnahmen alleine einen ausreichenden Schutz bieten kann und daher die parallele Nutzung verschiedener Schutzmaßnahmen, die teilweise das gleiche Schutzziel adressieren, zwingend notwendig sind. Dieser Aspekt ist jedoch differenziert zu sehen, da die gleichzeitige Anwendung verschiedener unabhängiger Schutzmaßnahmen zu einer höheren Komplexität bei der Verwaltung der Schutzmaßnahmen für die IT-Sicherheit und einem höheren Betriebsaufwand führen kann.

Die allgemein ungünstige Bewertung der Schutzwirkung für die Kommunikation gemäß Tabelle 5-4 liegt in der Berücksichtigung des Wirkungsbereichs der Maßnahmen zum Schutz der Kommunikation, wie bspw. dem Einsatz von VPN-Lösungen oder Firewalls. Diese Lösungen zielen auf den Schutz oder die Absicherung gegen Angriffe auf die Automatisie-

[1] Legende zur Schutzwirkung: gut „+" , durchschnittlich „o", gering „-".

[2] Bezogen auf intentionale (vorsätzliche) Eingriffe durch Angriffsmethoden, aus Sicht der sensibilisierten Mitarbeiter.

[3] Sofern Zutrittskontrolle an Identitäten gebunden ist.

[4] Schadsoftware kann in Kommunikation erkannt werden, ist jedoch keine direkte Bedrohung der Kommunikation.

rungsanlage von außen ab. Innerhalb der Trusted Zone besteht kein weiterer Schutz, der eine positivere Beurteilung erlauben würde. Doch auch innerhalb der Trusted Zone sind Angriffe denkbar, die bspw. von Innentätern ausgeführt werden könnten [VER2014]. Im Falle des Schutzes der Komponente greifen zahlreiche Maßnahmen, die zum Teil direkt auf den Komponenten wirken. Insgesamt gesehen ist die Schutzwirkung bei den Komponenten als durchschnittlich anzusehen. Die Bewertung der Anforderungen der Schutzmaßnahmen durch die Automatisierungstechnik ist in Tabelle 5-5 aufgeführt.

		Anforderung der Automatisierungstechnik					
Schutzmaßnahme		A1	A2	A3	A4	A5	A6
Organisatorische Schutzmaßnahmen	Sensibilisierung der Mitarbeiter	+	+	+	o	+	+
	Benutzerauthentifizierung sowie Rollen- und Rechteverwaltung	+	+	+	-	o	+
	Physische Schutzmaßnahmen/ Zutrittskontrolle	+	+	+	-	-	-
Technische Schutzmaßnahmen	Einsatz von Firewalls	-	-	o	o	o	+
	Virtual Private Network (VPN)	-	-	o	o	o	+
	“Härten” von Baugruppen	+	+	o	o	-	+
	Erkennung von Schadsoftware	-	-	-	-	o	o
Gesamtbeurteilung		o	o	+	o	o	+

Tabelle 5-5: Bewertung der Anforderungen durch die Automatisierungstechnik

Die Umsetzbarkeit der aktuellen Schutzmaßnahmen sowie deren mögliche Einsatzdauer sind mit wenigen Ausnahmen positiv zu bewerten. Der Aufwand zu deren Betrieb wie auch die Flexibilität und Skalierbarkeit der Schutzmaßnahmen sind jedoch durchschnittlich. Bezüglich der Anforderungen Echtzeitfähigkeit und Verfügbarkeit zeigt sich, dass die organisatorischen Schutzmaßnahmen sowie das Härten die Anforderungen erfüllen. Allerdings weisen diese Maßnahmen eine vergleichsweise geringe Schutzwirkung, insbesondere bei der Kommunikation, auf. Die weiteren technischen Schutzmaßnahmen erfüllen die Anforderungen hinsichtlich Echtzeitfähigkeit und Verfügbarkeit nicht, weshalb insgesamt diese Anforderungen unterdurchschnittlich bewertet sind. Die Gesamtbeurteilung der Erfüllung aller Anforderungen ist als durchschnittlich zu sehen. Ausschlaggebend dafür ist auch, dass kein Schutz der Kommunikation innerhalb der Trusted Zone vorgesehen ist. Schutzmaßnahmen die innerhalb dieses Bereichs wirken (z.B. VPN-Lösungen) beeinflussen die Echtzeitfähigkeit des Automatisierungssystems. Firewalls wiederum schützen die Trusted Zone, jedoch nicht die Kommunikation innerhalb dieser Zone.

Allgemein sind die aktuellen Schutzmaßnahmen eine Adaption bzw. Übernahme von Maßnahmen aus der Standard-IT und somit nicht zwingend für die Automatisierungstechnik konzipiert. Daher werden die Anforderungen aus der Automatisierungstechnik auch nicht vollkommen erfüllt. Dies kann ein Grund für die zögerliche Umsetzung der Schutzmaßnahmen für die Automatisierungstechnik sein. Aus Sicht der Automatisierungstechnik ist die gesamtheitliche Betrachtung der Schutzziele (STRIDE-Modell) sinnvoll, welche an den Assets gespiegelt werden sollten. Erfolgt eine Betrachtung bzw. Konzeption von Schutzmaßnahmen ausgehend von diesem Ansatz, können gezielt die Anforderungen der Automatisierungstechnik betrachtet werden und somit eine effiziente Schutzwirkung erreicht werden, die zugleich die Komplexität zur Überwachung der IT-Sicherheit verringert und damit deren konsequente Umsetzung ermöglicht.

6 Maßnahmen für ein erweitertes Schutzkonzept

Kapitel 5 beschrieb aktuelle Schutzmaßnahmen, hinsichtlich der Erfüllung von Anforderungen aus der IT-Sicherheit und der Automatisierungstechnik. Die aus der Standard-IT entstammenden Maßnahmen werden zum Teil nur zögerlich umgesetzt. Die Anwendung voneinander unabhängiger Schutzmaßnahmen kann zudem zu erhöhter Komplexität für das Automatisierungssystem führen. Im folgenden Kapitel 6 werden Schutzmaßnahmen beschrieben, die eine effiziente Abdeckung der Schutzziele ermöglichen, wobei direkt die gestellten Anforderungen in Bezug auf die Automatisierungstechnik berücksichtigt werden sollen.

Zu Beginn erfolgt hierfür eine Erläuterung der Zielsetzung für die ergänzenden Schutzmaßnahmen (►6.1). Basierend darauf werden in Abschnitt 6.2 ergänzende Schutzmaßnahmen beschrieben, die eine Erreichung dieser Zielsetzung ermöglichen. In Abschnitt 6.3 folgt darauf eine zusammenfassende Bewertung der zuvor beschriebenen ergänzenden Schutzmaßnahmen. Abschließend wird aus den aktuellen sowie ergänzenden Schutzmaßnahmen ein Zwischenfazit für ein erweitertes Schutzkonzept gezogen.

6.1 Zielsetzung ergänzender Schutzmaßnahmen

Entsprechend Abschnitt 5.1.1 liegt die Zielsetzung der IT-Sicherheit in der Erfüllung von Schutzzielen, die in direktem Verhältnis zu Bedrohungen entsprechend des STRIDE-Modells stehen [MIC2002]. Mit Hilfe der IT-Sicherheitsempfehlungen für die Automatisierungstechnik aus [BSI2014] können notwendige Aufgaben und Funktionsweisen an Schutzmaßnahmen der Automatisierungstechnik aufgestellt werden. Tabelle 6-1 stellt diese Aufgaben und Funktionsweisen zur Übersicht zusammen.

Bedrohung		Aufgabe der Schutzmaßnahme	Funktionsweise bzw. Anforderung an die ergänzende Schutzmaßnahme
S	Spoofing	Sicherstellung der Identität von Netzwerkteilnehmern	Authentifizierung anhand (mehrerer) eindeutiger (kryptografischer) Identifikationsmerkmale
T	Tampering	Schutz vor Manipulation von Daten	Einsatz von kryptografischen Maßnahmen zur Verhinderung und Erkennung von Manipulationen
R	Repudiation	Erfassung (Kommunikations-)Beziehungen bzw. (Anmelde-)Vorgängen im Automatisierungssystem	Zuordnung durch Anwendung von eindeutigen Identifikationsmerkmalen
I	Information Disclosure	Schutz vor unautorisiertem Zugriff auf vertrauliche Informationen	Einsatz kryptografischer Maßnahmen zum Schutz vor Offenlegung von Daten
D	Denial of Service	Schutz vor unautorisiertem oder unzulässiger Nutzung von Diensten	Abblocken von Dienstanfragen ohne vorherige sichere Identitätsklärung
E	Elevation of Privilege	Schutz vor unautorisiertem Zugriff und/oder Zugang mit Hilfe von Manipulation	(Automatisierte) Rollen- und Rechteverwaltung im verteilten System anhand eindeutiger Identitäten

Tabelle 6-1: Aufgabe und Funktionsweise ergänzender Schutzmaßnahmen

Bei den in Tabelle 6-1 aufgeführten Schutzmaßnahmen bzw. deren Funktionsweise handelt es sich um Verfahren, die bisher beim Schutz von Automatisierungssystemen nur geringe Betrachtung finden. Insbesondere die Anwendung kryptografischer Verfahren in der Automatisierungstechnik wird nicht gezielt verfolgt, obgleich diese Verfahren bei der Erfüllung von Schutzzielen in der Standard-IT eine wichtige Rolle spielen. Der Einsatz von ergänzenden Schutzmaßnahmen, basierend auf den in Tabelle 6-1 gezeigten Funktionsweisen, ist für die Erarbeitung eines erweiterten Schutzkonzepts für die Automatisierungstechnik sinnvoll. Parallel dazu muss eine Berücksichtigung der Anforderungen aus der Automatisierungstechnik entsprechend Tabelle 5-3 erfolgen.

6.2 Beschreibung ergänzender Schutzmaßnahmen

In Abschnitt 6.2 werden relevante ergänzende Schutzmaßnahmen entsprechend der dargestellten Funktionsweisen in Tabelle 6-1 vorgestellt. Zur Beschreibung der ergänzenden Schutzmaßnahmen wird der vereinfachte Betrachtungsgegenstand aus Abbildung 4-2 genutzt. Im Gegensatz zu den einfachen aktuellen Schutzmaßnahmen aus Abschnitt 5.2 kann auf diese Weise eine vereinfachte Betrachtung der ergänzenden Schutzmaßnahmen erfolgen. Die Anforderungen aus der IT-Sicherheit sowie Automatisierungstechnik (vgl. Tabelle 5-2 und Tabelle 5-3) werden ebenfalls einbezogen. Im Anschluss an diese Beschreibung erfolgt abschließend die Bewertung der ergänzenden Schutzmaßnahmen.

6.2.1 Authentifizierung von Netzwerkteilnehmern

Die Authentifizierung zwischen Netzwerkteilnehmern beschreibt einen Prozess, bei dem die Identität gegenseitig verifiziert wird [INT2000]. Nur auf diese Weise wird die Echtheit eines Netzwerkteilnehmers (z.B. eine Automatisierungskomponente bzw. dessen Kommunikation) festgestellt. Die Durchführung des Authentifizierungs-Prozesses erfolgt in zwei Schritten:

1. ***Schritt: „Identifizierung“***

Im ersten Schritt wird ein Identifikationsmerkmal der Komponente zur Verfügung gestellt, an der eine Authentifizierung erfolgen soll. Dabei kann es sich um eine Zufallszahl bzw. kryptografisches Merkmal wie einen Schlüssel handeln.

2. ***Schritt „Verifikation“***

Im nächsten Schritt werden dem System, welches die Authentifizierung durchführt, Informationen bereitgestellt, durch welche die Echtheit des Identifikationsmerkmals festgestellt werden kann. Auf diese Weise wird sichergestellt, dass ein Identifikationsmerkmal auch zu der Komponente gehört, die eine Authentifizierung seiner Identität anfordert.

Eine Variante dieses Prozesses ist das „Challenge-Response“-Verfahren, welches einen gemeinsamen im Vorlauf verteilten Schlüssel (Pre-Shared Key (PSK)) verwendet. Dazu wird eine Anforderung (Challenge) gestellt, die bspw. eine Zufallszahl enthält. Antwortet der Empfänger mit der korrekt verschlüsselten Zufallszahl (Response), gilt die Authentifizierung als vollzogen. Durch die unverschlüsselte Übertragung der Anforderung und der verschlüsselten Antwort, gilt dieses Verfahren allgemein als unsicher, da mit Hilfe der Kryptoanalyse auf den gemeinsamen Schlüssel geschlossen werden könnte. Da aus Sicherheitsgründen zudem der Schlüssel in regelmäßigen Abständen zu erneuern ist, müsste dies auf unsicherem (unverschlüsseltem) Wege oder manuell erfolgen, was hohen Aufwand nach sich zieht.

Aus diesem Grund ist ein Authentifizierungs-Prozess sinnvoll, der zum einen keine sensiblen Informationen über das Netzwerk überträgt die auf das gemeinsame Geheimnis schließen lassen und zum anderen Identifikationsmerkmale geheim hält. An dieser Stelle haben sich asymmetrische kryptografische Verfahren etabliert [SCH2006a]. Ausgangspunkt hierfür ist ein miteinander verknüpftes Schlüsselpaar, bei dem die eine Hälfte des Schlüsselpaares geheim gehalten wird (Private Key) und die andere Hälfte nicht geheim gehalten werden muss (Public Key). Der nicht geheime Teil des Schlüsselpaares kann daher unverschlüsselt über das Netzwerk übertragen werden. Abbildung 6-1 zeigt die Anwendung eines asymmetrischen kryptografischen Verfahrens.

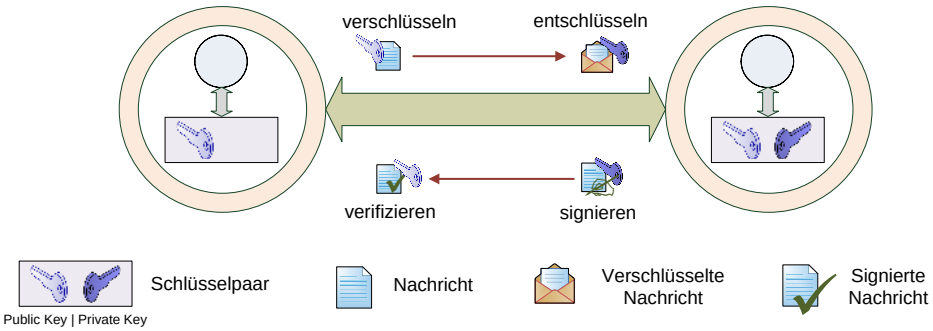


Abbildung 6-1: Asymmetrische kryptografische Verfahren

Die Kombination aus geheimem und nicht geheimem Schlüsselteil erlaubt zwei kryptografische Operationen. Wird mit Hilfe des Private Keys eine Nachricht verschlüsselt, so kann jeder Netzwerkteilnehmer, der im Besitz des nicht geheimen Public Key ist, die entsprechende Nachricht entschlüsseln. Dieser Vorgang entspricht einer digitalen Unterschrift (Signatur) die durch den Public Key verifiziert werden kann. So wird die Authentizität bzw. Vertraulichkeit einer Nachricht sichergestellt. Wird der vorliegende Public Key des Kommunikationspartners dazu genutzt eine Nachricht zu verschlüsseln, so kann nur der Besitzer des Private Keys diese Nachricht entschlüsseln. Wird eine (verschlüsselte) bidirektionale Kommunikation benötigt, so müssen beide Kommunikationspartner im Besitz des Public Key des Gegenübers sein. Damit können asymmetrische Verfahren nicht ausschließlich zur Authentifizierung, sondern auch zur verschlüsselten Kommunikation genutzt werden. Bekannte asymmetrische Verfahren sind das RSA-Kryptosystem [MVV2001] sowie die Elliptic Curve Cryptography (ECC) [HVM2004] und darauf basierende Verfahren zur Erstellung von Signaturen (ECDSA) [NIS2012d].

Aufgrund der dargestellten Eigenschaften bzw. Anwendungsmöglichkeiten eines asymmetrischen Schlüsselpaares kann dieses zur eindeutigen Authentifizierung von Netzwerkteilnehmern in einem (Automatisierungs-)netzwerk genutzt werden. Die Kombination aus Signatur und Public Key ermöglicht im Gegensatz zum Challenge Response Verfahren die zweifelsfreie Identifizierung, wobei keine potentiell sicherheitskritischen bzw. geheimen Informationen über das Netzwerk übertragen werden müssen. Da jedoch Signatur und Public Key alleine keinerlei Informationen über die Netzwerkteilnehmer liefern, die eine Authentifizierung bzw. Autorisierung wünschen, werden weitere Informationen bei der Authentifizierung benötigt. Public Key, Zusatzinformationen und Signatur sind Bestandteil eines (digitalen) Zertifikat, welches in Abbildung 6-2 dargestellt ist.

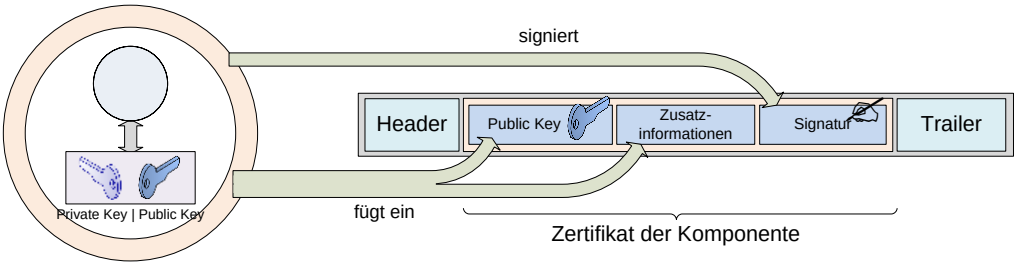


Abbildung 6-2: Aufbau eines Zertifikats bzw. Identifikationsmerkmals

Das Zertifikat dient im Netzwerk als Identifikationsmerkmal einer Komponente und wird bei einem Authentifizierungsvorgang zwischen zwei Kommunikationspartnern ausgetauscht. Zusatzinformationen im Zertifikat wie z.B. Seriennummer, Gültigkeitsdauer, Position und

Name des Teilnehmers werden dazu genutzt um eine Identität und ggf. Berechtigungen zuweisen zu können. Eine breite Verwendung findet bspw. das X.509-Format für Zertifikate [ITU2000]. Prinzipiell kann ein Zertifikat durch den Betreiber und/oder den Hersteller auf der Komponente hinterlegt werden. Um sicher zu stellen, dass jenes Zertifikat bzw. der Aussteller des Zertifikats vertrauenswürdig ist, muss bei der Überprüfung des Zertifikats neben der Signatur dessen Vertrauenswürdigkeit überprüft werden. Hierfür wird ein weiteres Zertifikat einer vertrauenswürdigen Zertifizierungsstelle (Stammzertifikat der Certification Authority (CA)) benötigt, die den Public Key des ersten (Komponenten-)Zertifikats signiert. Auf diese Weise entsteht eine Zertifikatskette bis hin zu einer vertrauenswürdigen Zertifizierungsstelle, die die Authentizität des Zertifikats der Komponente verifiziert und gegenüber dem Nutzer bestätigt. Die Verwaltung von Zertifikaten kann sowohl durch eine offene verteilte „Public Key Infrastructure“ (PKI) [HAH2012], als auch durch einen zentralen Server durchgeführt werden, welcher auf Basis des EAP-Protokolls arbeitet [INT2004]. Da zusätzliche (Server-)komponenten die Verfügbarkeit eines Automatisierungssystems negativ beeinflussen können, ist die PKI-Lösung zu favorisieren. Dabei kann, wie dargestellt, eine PKI seitens des Herstellers und/oder des Betreibers der Komponente etabliert werden.

Die Authentifizierung von Netzwerkteilnehmern mit Hilfe asymmetrischer Kryptografie erlaubt neben der eindeutigen Identifikation auch eine gesicherte und verschlüsselte Kommunikation. Daher kann mit Hilfe der asymmetrischen Verfahren eine weitreichende Abdeckung zahlreicher Schutzziele (vgl. STRIDE-Modell in Tabelle 6-1) erreicht werden. Bezüglich der Kommunikation tragen asymmetrische Verfahren dazu bei, dass eine vertrauliche und gesicherte Datenübertragung (→**T** und **I**) möglich wird und nicht authentifizierte bzw. nicht autorisierte Kommunikation verworfen wird (→**D**). Authentifizierungsmechanismen sehen zusätzliche Maßnahmen vor, welche die Schutzziele **S**, **R** und **E** der Kommunikation schützen. Beim Schutz der Komponente können die Schutzziele **S**, **R** und **D** adressiert werden. Das Zurückweisen von nicht authentifizierten Verbindungsanfragen verhindert, dass ein unerlaubter Zugriff auf die Komponente entsteht, die dessen Funktion beeinträchtigen könnte.

Bezüglich der Anforderungen aus der Automatisierungstechnik in Tabelle 5-3 existieren aktuell zahlreiche Lösungen um die sichere Authentifizierung durchführen zu können (→**A6**). Zu den bekanntesten Lösungen gehören SSL/TLS [RES2000] und IPSec [INT2004]. Bei SSL/TLS handelt es sich um eine Lösung auf der Anwendungsebene des ISO/OSI-Schichtenmodells, wohingegen IPSec auf Schicht 3 aufbaut. Implementierungen zu IPSec und SSL/TLS sind aufgrund der benötigten Speichergröße für ressourcen-beschränkte Automatisierungskomponenten weniger gut geeignet. Durch Implementation nur notwendiger Bestandteile dieser Lösungen, wie bspw. des Schlüsselaustauschverfahrens oder dem Schutz der Datenpakete, ist deren Anwendung auch in Automatisierungsnetzwerken begrenzt möglich.

Anwendungen in der Standard-IT zeigen, dass diese sowohl SSL/TLS- wie auch IPSec-Lösungen flexibel und skalierbar anwendbar sind (→**A5**). Jedoch kann erst nach Erarbeitung eines Schutzkonzeptes für Automatisierungssysteme in Kapitel 7 und der Evaluierung der asymmetrischen Kryptoverfahren in Kapitel 8 festgestellt werden, welche der Lösungen zum Verbindungsaufbau in der Automatisierungstechnik geeignet ist. Dies betrifft in erster Linie die Anforderungen der Automatisierungstechnik **A1** bis **A4** gemäß Tabelle 5-3.

Die mathematisch aufwändigen asymmetrischen Verfahren sind zur Authentifizierung von Netzwerkteilnehmern konzipiert. Im Allgemeinen wird daher im Anschluss an die Authentifizierung eine gesicherte bzw. verschlüsselte Kommunikation auf Basis eines Verfahrens eingerichtet, welches einen gemeinsamen (symmetrischen) Schlüssel verwendet. Diese sogenannten symmetrischen Verfahren werden im nachfolgenden Abschnitt 6.2.2 erläutert.

Der gemeinsame Schlüssel wird bei Authentifizierung über ein Schlüsselaustauschverfahren (z.B. „Diffie-Hellman“-Schlüsselaustauschverfahren [DIH1976]) ausgehandelt. Durch Schlüsselaustauschverfahren kann anhand unverschlüsselter Parameter ein gemeinsamer Schlüssel erstellt werden, ohne diesen über das Netzwerk übertragen zu müssen. Der ausgehandelte Schlüssel ist anschließend auf Sender und Empfängerseite geheim zu halten. So wird bei jedem Verbindungsaufbau ein neuer Schlüssel auf geheime Weise ausgehandelt oder kann zwischenzeitlich erneuert werden (vgl. PSK). Sowohl SSL/TLS als auch IPSec unterstützen entsprechende Schlüsselaustauschverfahren. Zur sicheren Identitätsfeststellung sind jedoch nach wie vor Zertifikate zu verwenden, da nur diese die Identität der Kommunikationspartner eindeutig wiederspiegeln.

6.2.2 Sichere Übertragung von Daten

Die in Abschnitt 6.2.1 beschriebenen asymmetrischen Kryptoverfahren sind primär für eine Authentifizierung von Netzwerkteilnehmern gedacht, wohingegen symmetrische Verfahren primär für die schnelle und sichere Übertragung von Daten konzipiert sind. Zusätzlich sind symmetrische Kryptoverfahren für ressourcen-beschränkte Plattformen mit geringer Rechenkapazität aufgrund Ihres geringen Ressourcenbedarfs besonders geeignet. Abbildung 6-3 zeigt die prinzipielle Funktionsweise von symmetrischen kryptografischen Verfahren.

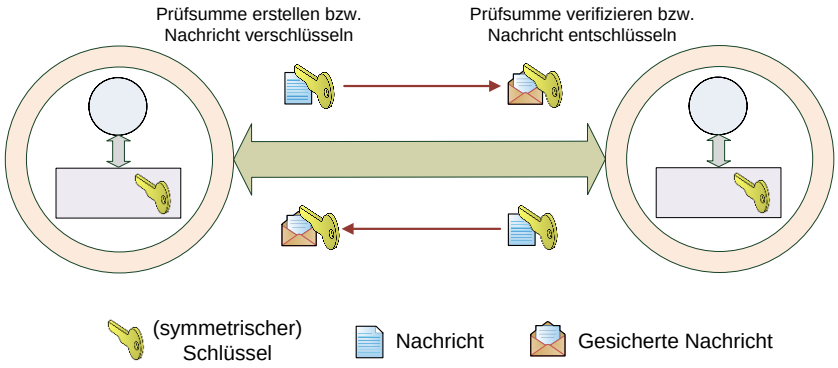


Abbildung 6-3: Symmetrische kryptografische Verfahren

Bei symmetrischen Verfahren verwenden Netzwerkteilnehmer einen gemeinsamen (geheimen) Schlüssel. Da nur bestimmte (authentifizierte) Netzwerkteilnehmer über diesen gemeinsamen Schlüssel verfügen, kann der gemeinsame symmetrische Schlüssel auf verschiedene Art zur sicheren Übertragung von Informationen bzw. zur Erfüllung zahlreicher Schutzziele bspw. bei der Kommunikation, genutzt werden. Dabei kann grundlegend zwischen der vertraulichen Übertragung bzw. den kryptografischen Prüfsummenverfahren unterschieden werden.

Vertrauliche Übertragungen, die das Schutzziel **I** adressieren, setzen eine Ver- bzw. Entschlüsselung von Daten voraus. Wird eine bitweise Ver- bzw. Entschlüsselung von Daten durchgeführt, wird von stromorientierten Verfahren gesprochen. Dafür wird aus dem gemein-

samen Schlüssel fester Länge ein beliebig langer Schlüsselstrom generiert mit dem die unverschlüsselten Daten bitweise verknüpft werden. Ergebnis der stromorientierten Verfahren ist ein verschlüsselter (vertraulicher) Datenstrom beliebiger Länge. Stromorientierte kryptografische Verfahren können effizient in Hard- und Software implementiert werden und ermöglichen einen hohen Datendurchsatz. Bekannte stromorientierte Verfahren sind der inzwischen als unsicher erkannte RC4-Algorithmus [MVV2001] sowie spezielle Varianten, die zusätzlich das Schutzziel **T** adressieren, wie bspw. Helix [FWS2003].

Blockorientierte Verfahren verschlüsseln eine festgelegte Datenmenge (Block) entsprechend der genutzten Schlüssellänge. Da ein Block eine festdefinierte Größe darstellt, sind zu verschlüsselnde Eingangsdaten ggf. auf eine Mindestlänge aufzufüllen (engl. padding). Um beiden blockorientierten Verfahren sicherzustellen, dass eine beliebige Anzahl zusammenhängender Blöcke reihenfolgerichtig verschlüsselt werden kann, ermöglichen Betriebsmodi der blockorientierten Verfahren die reihenfolgerichtige Verkettung der verschlüsselten Blöcke [SCH2006a]. Auf diese Weise sind zudem die verschlüsselten Blöcke nicht beliebig austauschbar. Der blockorientierte AES-Algorithmus findet weite Verwendung [NIS2001a]. So kommt der Betriebsmodi CBC zum Einsatz [NIS2001b], oder der (hybride) GCM-Modus, welcher zusätzlich den Schutz der Integrität (→**T**) ermöglicht. CBC und GCM unterscheiden sich zusätzlich in ihrer Parallelisierbarkeit. Während bei CBC die Blöcke einzeln nacheinander ver- und entschlüsselt, ermöglicht GCM die parallele Ver- und Entschlüsselung von Daten bzw. Blöcken [NIS2012e].

Sowohl strom- als auch blockorientierte Verfahren sind für die vertrauliche Übertragung von Daten gedacht (→**I**). Wie Abschnitt 3.3.2 aufzeigte, ist nicht in jedem Fall eine vertrauliche Übertragung von Daten notwendig. Der Schutz der Integrität der Daten hat in einem Automatisierungsnetzwerk eine höhere Priorität (→**T**) und kann unabhängig vom Schutzziel der Vertraulichkeit realisiert werden. Hierfür wird eine kryptografisch sichere Prüfsumme den zu übertragenden Nachrichten angefügt, welche auch als Message Authentication Code (MAC) bezeichnet wird. Ausgangspunkt dafür ist bspw. die Bildung einer kryptografischen Prüfsumme über eine beliebige Menge an Daten, bei welcher durch Kryptoanalyse der Prüfsumme nicht auf die Eingangsdaten des Prüfsummenverfahrens geschlossen werden kann. Bekannteste genutzte Prüfsummenverfahren sind die Secure Hash Algorithmen (SHA) [NIS2012c]. Da der SHA-1 inzwischen als unsicher gilt [WYY2005], wird stattdessen der SHA-2 Algorithmus verwendet. Die „(Keyed)-Hash-Based“ Message Authentication Codes (HMAC) basieren auf einem sicheren Prüfsummenverfahren, in deren Erstellung ein (symmetrischer) Schlüssel eingebunden ist [NIS2002]. Der HMAC wird anschließend dem Nachrichtenpaket beigefügt und kann durch den Empfänger verifiziert werden, sofern dieser im Besitz des dazugehörigen Schlüssels ist.

Prinzipiell ist auch eine Nutzung der blockorientierten Verfahren als MAC möglich. Entsprechende Verfahren werden als „cipher-based“ MAC bezeichnet. Dazu wird das Prinzip der verketteten Blöcke genutzt, indem der letzte verschlüsselte Block als MAC genutzt wird. Verwendet wird dazu bspw. der genannte blockorientierte AES-Algorithmus, mit den zur Verfügung stehenden Betriebsmodi CBC oder GCM. Entsprechend werden diese MAC-Verfahren als CMAC (AES-CBC-MAC) [NIS2012a] und GMAC (AES-GCM-MAC) [NIS2012b] bezeichnet.

Abhängig von den zu erfüllenden Schutzzielen bei der Kommunikation, können die dargestellten symmetrischen kryptografischen Verfahren zur Absicherung der Daten der Kommunikation verwendet werden. Der Datenpaketaufbau entsprechend dem Standard Ethernet Format (vgl. Abbildung 3-6) bedarf jedoch einer Anpassung, um eine sichere Übertragung zu ermöglichen. Zusätzlich müssen Sender und Empfänger einer sicheren Kommunikation die geschützten Informationen verarbeiten. Sowohl die Anpassung des Datenpakets als auch die Verarbeitung sollen nachfolgend dargestellt werden.

- **Anwendung von Message Authentication Codes (MAC)**

Die Übertragungen in einem Automatisierungsnetzwerk erfolgt unverschlüsselt. Hierdurch ist ein Angreifer nicht nur in der Lage an vertrauliche Informationen zu gelangen, sondern kann auch eine Manipulation der Kommunikation durchführen (vgl. „Man in the Middle“-Angriff, siehe Abbildung 3-9). Dieser Angriff wird nur dadurch ermöglicht, dass lediglich das allgemein bekannte CRC-Prüfsummenverfahren des Standard Ethernets angewendet wird, welches im Wesentlichen zur Erkennung von beschädigten Datenpaketen auf Grund von Übertragungsstörungen dient. Ein ergänzender Schutz der Daten in einem Automatisierungsnetzwerk ist demnach zwingend notwendig. Dieser Schutz kann durch Anwendung der erläuterten MAC-Verfahren erreicht werden. Abbildung 6-4 zeigt die Anwendung von MACs zur Erfüllung des Schutzziels **T** bei der Übertragung von Informationen in einem Datenpaket. Dargestellt sind ein sicherer Sendevorgang und die Verarbeitung beim Empfänger.

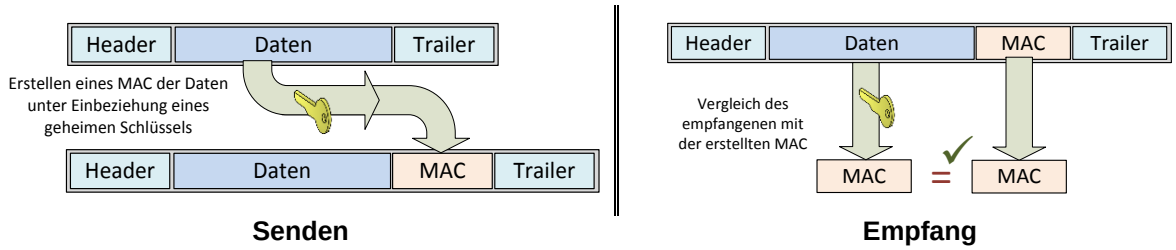


Abbildung 6-4: Anwendung von Message Authentication Codes (MAC)

Aus den Daten wird auf der Senderseite unter Verwendung eines symmetrischen Schlüssels ein MAC berechnet, der dem Paket beigefügt wird. Empfängt der Sender ein solches Paket, ist der darin enthaltene MAC zu überprüfen. Dazu nutzt der Empfänger den ausgehandelten symmetrischen Schlüssel und erstellt seinerseits einen MAC aus den zugesendeten Daten. Abschließend ergibt eine Überprüfung des empfangenen und eigens erstellten MACs, ob eine unverfälschte Übertragung vorliegt (→**T**). Die Authentizität der Daten wird ebenso sichergestellt (→**S**), da nur der korrekt authentifizierte Kommunikationspartner über den entsprechenden symmetrischen Schlüssel verfügen kann.

Wie im Falle der CRC-Prüfsumme des Standard Ethernets, muss der MAC dem Datenpaket beigefügt werden, wie Abbildung 6-4 zeigt. Dies erhöht je nach verwendetem MAC-Verfahren die zusätzlich zu übertragene Datenmenge (Overhead). Da es sich bei MACs um eine kryptografische Prüfsumme handelt, und nicht um ein Verfahren zur geheimen (verschlüsselten) Übertragung, sind die Informationen die durch die MAC abgesichert werden, weiterhin lesbar. Ist eine vertrauliche Übertragung erforderlich, muss zusätzlich ein Ver- bzw. Entschlüsselungsverfahren angewendet werden.

- **Verschlüsselte Kommunikation**

Um vertrauliche Daten im Automatisierungsnetzwerk zu schützen, ist der Einsatz einer Ver- bzw. Entschlüsselung notwendig. Hierdurch kann die Erfüllung des Schutzziels **I** der Kommunikation erreicht werden. Da eine Verschlüsselung jedoch nur die Vertraulichkeit der Informationen schützt, ist zusätzlich ein MAC beizufügen, um unautorisierte Veränderungen am verschlüsselten Inhalt erkennen zu können. Andernfalls würde der veränderte verschlüsselte Inhalt beim Empfänger der Nachricht mit besagter Veränderung entschlüsselt werden und die inhaltliche Integrität der Nachricht wäre verletzt (→**T**). Abbildung 6-5 zeigt die Ver- und Entschlüsselung einer Kommunikation bei einem Sende- und Empfangsvorgang mit zusätzlicher Absicherung durch einen MAC.

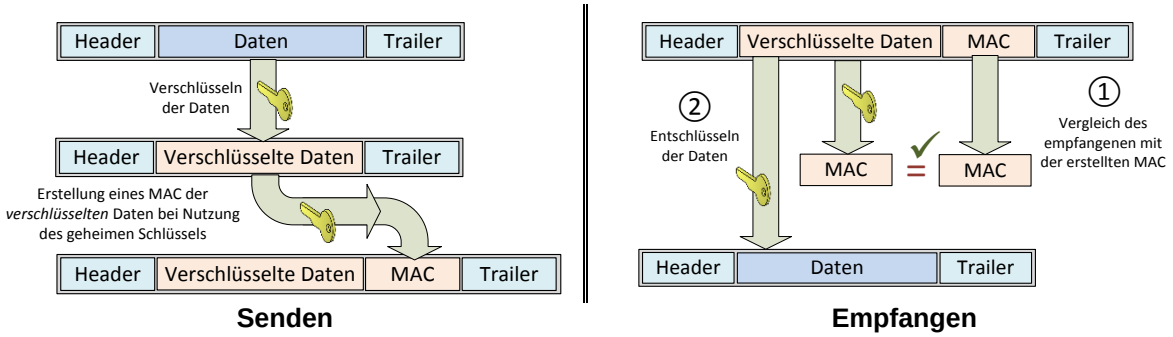


Abbildung 6-5: Anwendung einer verschlüsselten Kommunikation

In einem ersten Schritt werden die vertraulichen Informationen mit Hilfe des gemeinsamen ausgehandelten Schlüssels durch ein kryptografisches Verfahren verschlüsselt. Anschließend wird ein MAC der verschlüsselten Daten erstellt und dem Datenpaket beigefügt. Der Empfänger überprüft bei Ankunft des Paketes zunächst den MAC der verschlüsselten Daten ①. Hat keine Veränderung der verschlüsselten Daten stattgefunden, wird anschließend die Entschlüsselung durchgeführt ②. Sollte hingegen die Prüfung des MACs eine Veränderung anzeigen, so wird auf die anschließende Entschlüsselung verzichtet. Liegen die Daten im Paket verschlüsselt und durch einen MAC abgesichert vor, sind nur die authentifizierten Kommunikationspartner in der Lage die Informationen wiederzugewinnen und deren Integrität zu überprüfen. Eine angreifende Person im Netzwerk ist weder in der Lage die Nachricht zu lesen, um daraus Informationen zu gewinnen, noch diese zu verändern. Somit kann die Integrität sowie die Vertraulichkeit der Informationen bewahrt werden und eine unerlaubte Rechteerlangung über die Kommunikation unterbunden werden (→**T**, **I** und **E**).

Hinsichtlich der Anforderungen aus der Automatisierungstechnik ist die Umsetzbarkeit der sicheren Kommunikation aufgrund der zahlreichen verfügbaren Lösungen gegeben (→**A6)**. Flexibilität und Skalierbarkeit der sicheren Kommunikation kann durch verschiedene symmetrische Kryptoverfahren und deren Anwendungsweise beeinflusst werden. Bezüglich der Anforderungen **A1** bis **A4** gemäß Tabelle 5-3 kann eine endgültige Beurteilung erst nach Evaluierung und Erarbeitung eines erweiterten Schutzkonzepts erfolgen. Dies gilt insbesondere für die benötigte Rechenleistung zur Berechnung der kryptografischen Verfahren.

6.2.3 Zustandsüberwachung von Automatisierungskomponenten

Mit Zugriff auf eine Automatisierungskomponente, bspw. über das Automatisierungsnetzwerk oder eine lokale Schnittstelle, kann eine angreifende Person eine unautorisierte Veränderung sowohl der Systemfunktion als auch der Systemdaten durchführen. Die aus dieser Bedrohung resultierenden Folgen für ein Automatisierungssystem sind in Abschnitt 4.4.2 dargestellt worden. Zur Abwendung dieser Bedrohung ist der Einsatz einer Zustandsüberwachung sinnvoll. In Abbildung 6-6 ist das Prinzip einer Zustandsüberwachung dargestellt.

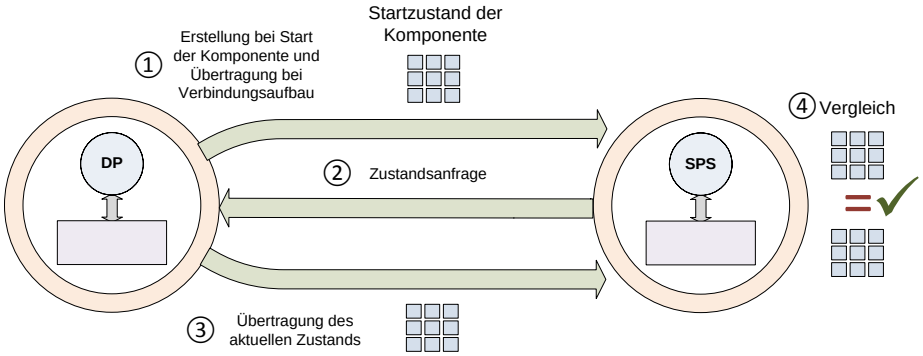


Abbildung 6-6: Zustandsüberwachung der Komponente

Nach Start der Komponente (z.B. dezentrale Peripherie) übernimmt die Zustandsüberwachung die Erfassung des Zustands der Komponente. Der Zustand wird durch Berechnung des aktuellen Abbildes der Systemfunktion sowie der Systemdaten der Komponente erstellt. Hierfür wird ein kryptografisches Prüfsummenverfahren (z.B. SHA-2 Algorithmus) verwendet. Das Prüfsummenverfahren berechnet aus den vorliegenden Systemdaten (z.B. Parametrierungs- und Konfigurationsdaten) sowie der Systemfunktion (z.B. die lokale Anwendung der Komponente) eine Prüfsumme. Diese Prüfsumme repräsentiert den aktuellen Zustand der Komponente bei Start der Komponente [RTN2012b].

Die Zustandsüberwachung wird lokal ausgeführt, um Manipulationen an der Komponente während des Betriebes erkennen zu können. Hat bspw. ein Angriff stattgefunden, können lokale Maßnahmen (z.B. sicheres Herunterfahren, Absetzen von Alarmen) ergriffen werden. Als Erweiterung der lokalen Überwachung kann der Startzustand der Komponente bspw. bei Authentifizierung mit übertragen werden ①. So kann der Kommunikationspartner (bspw. die SPS) die Überwachung des Zustands der dezentralen Peripherie übernehmen. Sind in der Zwischenzeit (autorisierte) Veränderungen an den Komponenten durchzuführen, so muss eine Übertragung des erneuerten Zustands erfolgen, bspw. durch erneute Authentifizierung.

Im Gegensatz zu anderen Vorschlägen, wie bspw. in [HAH2011], so erfolgt in Abbildung 6-6 eine regelmäßige Zustandsüberprüfung. Zustandsanfragen ② an die zu überwachenden Komponente sollen sicherstellen, dass zwischenzeitlich keine Manipulation der Komponente stattgefunden haben. Auf die Anfrage erfolgt die Übertragung eines aktualisierten Zustandswertes ③. Ergibt die Überprüfung des aktualisierten Zustands mit dem Startzustand ④, dass keine Veränderung an der Komponente stattgefunden hat, so liegt ein normales Verhalten vor. Eine (unautorisierte) Manipulation der Komponente führt zu einem negativen Überprüfungsergebnis. Auch in diesem Fall können Maßnahmen ergriffen werden, wie bspw. eine Trennung der Verbindung.

Sowohl die lokale als auch entfernte Zustandsüberwachung können dazu beitragen die Schutzziele **T** und **E** zu erfüllen. Da eine Authentifizierung der Netzwerkteilnehmer durchgeführt wird, können Veränderungen an den Komponenten nur durch entsprechend autorisierte Netzwerkteilnehmer durchgeführt werden. Die Zustandsüberwachung erkennt unautorisierte Veränderungen an der Systemfunktion und den Systemdaten während des Betriebes. Sind Aktualisierungen an den Komponenten (z.B. der Systemfunktion) durchzuführen, muss dies auf authentifiziertem bzw. autorisiertem Weg erfolgen. In diesem Fall ist die Zustandsüberwachung, z.B. nach erneutem Verbindungsaufbau, zu aktualisieren

Die Anwendung der Zustandsüberwachung erhält die Flexibilität und Skalierbarkeit des Automatisierungssystems (→**A5**), da eine Schutzmaßnahme etabliert wird, die sich der (Netzwerk-)Struktur des Automatisierungssystems anpasst. Die Umsetzbarkeit ist durch die zahlreich verfügbaren kryptografischen Prüfsummenverfahren gegeben (→**A6**). Wie im Falle der ergänzenden Schutzmaßnahmen aus den Abschnitten 6.2.1 bis 6.2.2, erfolgt die abschließende Beurteilung der Anforderungen **A1** bis **A4** im nachfolgenden Kapitel 7.

6.2.4 Sichere Verwahrung sensibler Informationen

Die in den Abschnitten 6.2.1 bis 6.2.3 genannten Schutzmaßnahmen basieren auf kryptografischen Verfahren. Die Verfahren verwenden zu diesem Zweck kryptografische Merkmale wie Zertifikate und Schlüssel. Üblicherweise liegen diese Merkmale im Speicher der jeweiligen Komponente. Damit wäre eine angreifende Person potentiell in der Lage, diese kryptografischen Merkmale auszulesen. Dieser Umstand würde dazu führen, dass die gezeigten Schutzmaßnahmen aus den Abschnitten 6.2.1 bis 6.2.3 umgangen werden könnten.

Da die Aufbewahrung der kryptografischen Merkmale, insbesondere des Private Key, im Speicher der Komponente nicht sicher ist, empfiehlt sich der Einsatz eines sicheren Speichers auf der Komponente, der ein unautorisiertes Auslesen der sensiblen Informationen verhindert. Bei diesen sicheren Speichern handelt es sich um Halbleiterbausteine, welche speziell für die Handhabung sensibler kryptographischer Informationen gedacht sind. Diese Handhabung erfordert einen speziellen Aufbau des sicheren Speichers, der in Abbildung 6-7 gezeigt wird. Oft wird diese Technologie als „Security Token“ bezeichnet. Abbildung 6-7 zeigt den grundlegenden Aufbau eines Security Token.

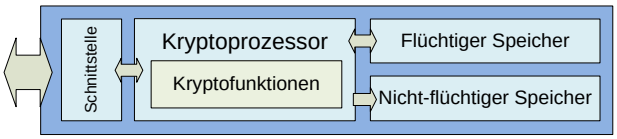


Abbildung 6-7: Aufbau eines Security Token

Die hardware-seitige Anbindung des Security Token kann auf verschiedene Weise erfolgen (z.B. I^2C, LPC, USB). Der Zugriff auf das Token erfolgt über eine definierte Software-Schnittstelle. Auf Vorgänge und Daten (z.B. sensible kryptografische Informationen) innerhalb des Token besteht kein direkter Zugriff.

Wird eine kryptografische Operation mit sensiblen Informationen seitens der Schnittstelle angefordert, so führt diese Operationen das Security Token selbständig aus. Nur das Ergebnis der Operation wird über die Schnittstelle mitgeteilt. Damit das Token diese Funktion selbständig durchführen kann, verfügt es über einen eignen Kryptoprozessor, der die Verarbei-

tung der Anfragen über die Schnittstelle übernimmt. Verschiedene symmetrische und asymmetrische kryptografische Funktionen sind dafür im Kryptoprozessor vorgesehen. Dies stellt sicher, dass die kryptografischen Operationen bei Nutzung von sensiblen Informationen unbeeinflusst von angreifenden Personen arbeiten können. Das Token stellt weiterhin flüchtige und nicht-flüchtige Speicher zur Verfügung. Der nicht-flüchtige Speicher hält Informationen vor, die zur Identifikation des Token bzw. der Komponente mit dem Token dienen. Diese Identifikationsmerkmale verlassen das Token niemals (z.B. der Private Key). Im Gegensatz dazu hält der flüchtige Speicher des Security Token Daten während der Laufzeit der Plattform vor, wie bspw. temporär genutzte Schlüssel auf die ein stark begrenzter Zugriff über den Kryptoprozessor besteht. Zusätzlich verfügen Security Token über konstruktive Maßnahmen, die das physische Auslesen von Informationen aus dem Token verhindern sollen. Trotzdem sind Fälle bekannt, in denen die Informationen ausgelesen werden konnten [TAR2010]. Dieses Verfahren ist jedoch aufwändig, setzt eine spezielle Ausrüstung voraus und adressiert lediglich ein einzelnes Security Token bzw. eine Komponente.

Abbildung 6-8 zeigt die Anwendung eines Security Token auf einer Automatisierungskomponente als ergänzende Schutzmaßnahme für sensible kryptografische Informationen. Das Token übernimmt dabei speziell die Verwahrung des privaten Teils des Public-/Private Key-Schlüsselpaares zum Schutz vor unautorisierten Zugriffen.

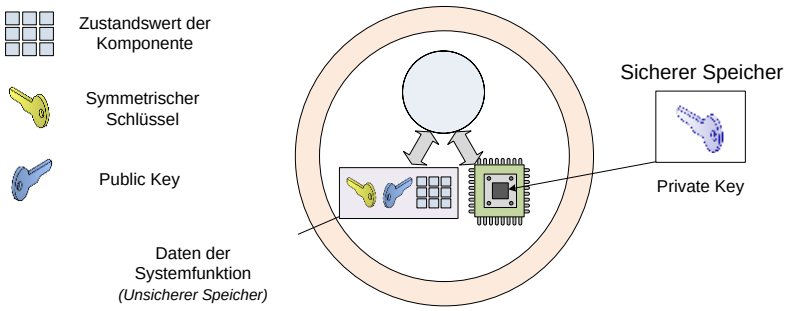


Abbildung 6-8: Erweiterung der Komponente um ein Security Token

Gewisse kryptografische Informationen, wie symmetrische Schlüssel oder der Zustandswert der Komponente, müssen während der Laufzeit der Komponente ggf. im unsicheren Speicher der Komponente aufbewahrt werden. Auch hier sieht das Token einen Schutz vor. Durch lokale Verschlüsselung von Informationen mit dem Public Key kann nur mit dem entsprechenden geheimen Private Key der Komponente deren Entschlüsselung erfolgen. Die so verschlüsselten Informationen sind an den lokalen Private Key gebunden (engl. bind) und können nur lokal entschlüsselt werden.

Derzeit werden verschiedene Security Token Technologien auf dem Markt vertrieben. Die meist verbreitete Variante sind die sogenannten Smartcards [RAN2010], wie sie z.B. für den elektronischen Zahlungsverkehr oder für den neuen Personalausweis verwendet werden. Hierbei können die Smartcards mit unterschiedlichen Funktionen beliebig ausgestattet werden. Neben diesen tragbaren Token werden seit einigen Jahren auch Security Token in Chip-Form verwendet. Ein Beispiel hierfür ist das sogenannte „Trusted Platform Module“ (TPM) [TRU2007], welches zu einer Smartcard vergleichbare Funktionen bereitstellt, jedoch in Form eines elektronischen Bauelementes zum direkten Einbau zur Verfügung steht. Abbildung 6-9 zeigt sowohl Smartcard als auch TPM.

Abbildung 6-9: Token Technologien (links: Smartcard | rechts: TPM)

Neben diesen beiden Security Token Technologien gibt es zahlreiche weitere Ausprägungen die eine ähnliche Funktionalität aufweisen. Jedoch zeigen diese eine geringe Relevanz für Anwendungen in der Automatisierungstechnik auf [TEB2011]. Tabelle 6-2 zeigt die Gegenüberstellung der beiden Security Token Technologien anhand relevanter Kriterien.

Auswahlkriterien	**Smartcard**	**TPM**
Herstellerunabhängigkeit	+	+
Eindeutige Identifizierbarkeit	o	+
Austauschbarkeit	+	-
Anwendung in Automatisierungskomponenten	o	+
Anwendungsentwicklung	o	+
Komplexität der Integration	-	+
Kosten	-	+
Datentransferrate	o	+
Kryptografische Funktionen	+	-
Bewertung	o / +	+

Tabelle 6-2: Gegenüberstellung von Smartcard und TPM [RNT2012]

Ein maßgeblicher Grund zur Wahl von TPM und Smartcard ist die herstellerunabhängige Bezugsmöglichkeit der beiden Technologien. Beide Technologien ermöglichen die eindeutige Identifizierung der Komponenten anhand eines asymmetrischen Schlüsselpaares in Kombination mit einem Zertifikat. Das TPM ist im Gegensatz zur Smartcard jedoch mit der Plattform verlötet und auch durch weitere Maßnahmen an die Komponente gebunden. Dies verstärkt die eindeutige Identifizierung einer Komponente, da das TPM sich nicht mit einfachen Mitteln austauschen lässt. Im Falle eines Defektes ist daher im Zweifelsfall die Komponente inklusive des TPMs zu tauschen. Smartcards sind aufgrund ihrer Kontaktierung für den industriellen Einsatz (z.B. aggressive Atmosphäre) nicht geeignet. Trotzdem ist eine Anwendung zur personengebunden Benutzerauthentifizierung bspw. an BNK sinnvoll.

Im Gegensatz zum fest vorgegebenen Funktionsumfang eines TPM in Form eines elektronischen Bauelements, erlaubt der Aufbau einer Smartcard eine spezifische Erweiterung des Funktionsumfangs, bspw. um eine gewünschte Anzahl an kryptografischen Funktionen. Diese Flexibilität führt bei den Smartcards aber ggf. zu einem größeren Entwicklungsaufwand und erschwert letztlich auch die einfache Integration in Automatisierungskomponenten. Allgemein ist daher die Integration von Smartcards mit höheren Kosten verbunden, da ggf. zusätzliche Schnittstellen zur Anbindung von Smartcards benötigt werden. Hier kann das TPM direkt über Bussysteme (z.B. I^2C oder LPC) mit der Hardware einer Komponente verbunden werden, was die Integration erleichtert und hohe Datentransferraten ermöglicht.

Der Funktionsumfang des TPM wird durch die „Trusted Computing Group“ (TCG) definiert und umfasst aktuell grundsätzlich nur das RSA-Kryptosystem und eine Zufallszahlenerzeu-

gung für die Erstellung der Schlüssel. Zusätzliche kryptografische Funktionen können nur durch die Hersteller der TPM integriert werden. Mit der zukünftigen erscheinenden Nachfolgerversion des TPM in der Version 2.0 [TRU2011] werden jedoch grundlegende Erweiterungen von kryptografischen Funktionen erfolgen. Eine weitere besondere Eigenschaft des TPM ist die integrierte Funktion zur Erfassung des Systemzustandes auf Basis einer SHA-Prüfsumme der Komponente, mit der das TPM verbunden ist. Dieser Zustandswert der Komponente kann ebenfalls im sicheren Speicher verwahrt werden. Damit ist das TPM in der Lage die Zustandsüberwachung der jeweiligen Komponente zu unterstützen. Wird dieser sicher gespeicherte Zustandswert der Komponente bspw. als Schlüssel genutzt, so muss die Komponente zur Verschlüsselung in eben diesem unveränderten Zustand vorliegen. So wird sichergestellt, dass nur vertrauenswürdige (nicht-manipulierte) Komponenten Systemfunktion ausführen oder Zugriff auf Systemdaten haben [RTN2012b]. Diese Funktion wird als „sealing“ bezeichnet und kann als Softwarelizensierungsmechanismus genutzt werden. TPM bilden den Grundstein des „Trusted Computing“, wobei eine vertrauenswürdige Rechnerplattform ausgehend vom Start der Komponente bis hin zur Anwendung („Secure oder Trusted Boot“) etabliert wird [MUE2008].

Eine Komponente mit Security Token, inkl. der darin enthaltenen kryptografischen Informationen, ist eindeutig identifizierbar. Insbesondere die sichere Speicherung des Private Key und das beiliegende Zertifikat auf der Komponente bewirkt, dass die Identität einer Komponente fest an diese gebunden ist. So können illegale Nachbauten von Komponenten erkannt werden, da (kopierte) Nachbauten nicht über dieses Identifikationsmerkmal verfügen können [RNH2012]. Damit schützen Security Token die Komponente bezüglich der Schutzziele **T** sowie **I** und **E** in Zusammenwirken mit der Zustandsüberwachung. Hinsichtlich der Beurteilung der Anforderungen **A1** bis **A6** der Automatisierungstechnik sind weitere Betrachtungen notwendig, da eine Bewertung der Anforderungen erst nach Anwendung der Token im Betrieb in einem erweiterten Schutzkonzept erfolgen kann.

6.3 Bewertung der ergänzenden Schutzmaßnahmen

In Abschnitt 6.2 sind die ergänzenden Schutzmaßnahmen eines erweiterten Schutzkonzepts beschrieben worden. Diese haben zum Ziel die Anforderungen der IT-Sicherheit entsprechend der in Abschnitt 6.1 geforderten Zielsetzung von ergänzenden Schutzmaßnahmen zu erfüllen. Die ergänzenden Schutzmaßnahmen wirken je nach Maßnahme auf verschiedene Schutzziele der Assets Kommunikation und Komponente. Betrachtet werden die Schutzziele entsprechend des STRIDE-Modells (vgl. Tabelle 6-1). Tabelle 6-3 zeigt, durch welche Maßnahmen ein jeweiliges Schutzziel erreicht wird und wie die Schutzwirkung zu bewerten ist.

Ausgangspunkt für die ergänzenden Schutzmaßnahmen ist die eindeutige gegenseitige Authentifizierung der Komponenten auf dem Netzwerk, mit Hilfe der mathematisch aufwändigen asymmetrischen Kryptografie. Durch Anwendung der symmetrischen MAC- bzw. Ver- und Entschlüsselungsverfahren im Anschluss, kann so ein wirksamer und effektiver Schutz der (echtzeitfähigen) Kommunikation erreicht werden. Im Besonderen sind für MAC- und Ver- bzw. Entschlüsselungsverfahren weitere Betrachtungen im Datenpaketaufbau notwendig, um das Schutzziel **R** erfüllen zu können. Die Betrachtung dazu erfolgt in Kapitel 7 bei der Erarbeitung des erweiterten Schutzkonzepts.

	Asset bzw. Schutzziele											
	Kommunikation						Komponente					
Schutzmaßnahme	**S**	**T**	**R**	**I**	**D**	**E**	**S**	**T**	**R**	**I**	**D**	**E**
Gegenseitige Authentifizierung von Komponenten	+	+	+	+	+[1]	+	+		+		+ 1	
Einsatz von MACs bei der Kommunikation	+	+	o									
Ver- bzw. Entschlüsselung der Kommunikation			o	+		+						
Durchführung einer Zustandsüberwachung der Komponenten								+		o		+
Einsatz von Security Token auf den Komponenten[2]								o		+		o
Gesamtbeurteilung	+	+	+	+	+	+	+	+	+	+	+	+

Tabelle 6-3: Bewertung der Wirksamkeit der erweiterten Schutzmaßnahmen

Die Komponente wird durch den Einsatz eines Security Token erweitert, welches eine sichere Verwahrung von sensiblen Informationen ermöglicht. Eine Zustandsüberwachung soll sicherstellen, dass unautorisierte Manipulationen an den Komponenten erkannt werden. So können weitere Schutzmaßnahmen ergriffen werden, bspw. lokal durch sicheres Herunterfahren, oder entfernt durch Umschalten auf eine redundante Komponente. Das Zusammenwirken von Zustandsüberwachung und Security Token in Kombination mit der gegenseitigen Authentifizierung ermöglicht einen effektiven Schutz der Komponente.

Obwohl sensible Informationen (z.B. Schlüssel, Zustandswert der Komponente) oder Anwendungen wie Zustandsüberwachung im unsicheren Speicher ausgeführt bzw. gespeichert werden, so sind die ergänzenden Schutzmaßnahmen trotzdem eine Verbesserung der IT-Sicherheit gegenüber den gegenwärtigen Schutzmaßnahmen. Wesentliches Merkmal der hier ergänzten Schutzmaßnahmen ist das sicher verwahrte Identifikationsmerkmal, welches an ein Gerätezertifikat geknüpft wird. Die sichere Speicherung im TPM und die Verknüpfung mit einem Zertifikat erlaubt so eine zweifelsfreie Identifikation der Komponente, womit Produktpiraterie wirksam verhindert werden kann. Sind alle (IT-)sicherheitsrelevanten Operationen zu sichern, so ist kryptografische Hardware mit einem erweiterten Funktionsumfang einzusetzen. Die kryptografische Hardware muss nicht nur in der Lage sein kryptografische Funktionen auszuführen und sensible Informationen zu speichern, sondern gleichermaßen anwenderspezifische Anwendungen in der kryptografischen Hardware auszuführen. Proprietäre Lösungen für sichere Speicher und kryptografische Erweiterungen wie ARM „TrustZone“ [ARM2009] stellen diesen Funktionsumfang zur Verfügung. Das ARM „TrustZone-Konzept“ ermöglicht die sichere Ausführung von Systemfunktionen und stellt sicheren Speicher bereit. Die Leistungsfähigkeit und Einsetzbarkeit für die Automatisierungstechnik ist jedoch zunächst zu belegen. Insbesondere der mögliche Datendurchsatz dieses Konzepts bzw. dessen Echtzeitfähigkeit ist zu überprüfen.

In der Gesamtbeurteilung zeigt sich, dass alleine durch die Anwendung der ergänzenden Schutzmaßnahmen eine Erfüllung der Schutzziele für die Assets möglich ist. Eine parallele Anwendung bestehender aktueller Schutzmaßnahmen ist jedoch weiterhin möglich und wird durch die ergänzenden Schutzmaßnahmen nicht eingeschränkt.

[1] Nicht authentifizierte bzw. autorisierte Kommunikation wird verworfen.

[2] Durch gemeinsamen Einsatz mit Zustandsüberwachung.

6.4 Zwischenfazit für ein erweitertes Schutzkonzept

Die in der Automatisierungstechnik eingesetzten Schutzmaßnahmen für die IT-Sicherheit kommen gemeinsam im sogenannten „Defence-in-Depth“-Schutzansatz zum Einsatz. Aktuelle Schutzmaßnahmen entsprechend Abschnitt 5.2 zeigen auch in gemeinsamer Anwendung Defizite hinsichtlich eines wirksamen Schutzes. Darüber hinaus werden die Anforderungen an Schutzmaßnahmen der IT-Sicherheit durch die Automatisierungstechnik nicht hinreichend erfüllt. Auf die flexible und skalierbare Gestaltung eines Automatisierungssystems wird ebenso wenig Rücksicht genommen, wie auf den Schutz der Kommunikation zwischen den Komponenten. Dies fällt besonders bezüglich des „Trusted Zone“-Konzepts auf. Dieses Konzept geht nicht nur von starren Strukturen aus, die im starken Gegensatz zu offenen verteilten Systemen im Sinne von „Industrie 4.0“ stehen, sondern sieht keine Kommunikationsschutzmaßnahmen innerhalb der Trusted Tone vor.

Die in Abschnitt 6.2 aufgezeigten ergänzenden Schutzmaßnahmen, die für ein erweitertes Schutzkonzept zum Tragen kommen, bieten eine verbesserte Schutzwirkung. Diese Schutzmaßnahmen können zu einer signifikanten Reduzierung des potentiellen Risikos führen. Die hohe Wirksamkeit wird dadurch erreicht, dass alle ergänzenden Schutzmaßnahmen auf Basis der kryptografischen Verfahren zusammenarbeiten, im Unterschied zu den aktuell eingesetzten Maßnahmen, die jeweils als Einzelmaßnahmen zu sehen sind. Da zusätzlich die ergänzenden Schutzmaßnahmen direkt auf den Komponenten und deren Kommunikationsbeziehungen aufbauen, kann flexibel auf Strukturänderungen eines Automatisierungssystems reagiert werden. Dabei ist unerheblich ob Kommunikation innerhalb oder außerhalb der „Trusted Zone“ stattfindet, womit die ergänzenden Schutzmaßnahmen mit dem „Defence-in-Depth“-Schutzansatz in Einklang gebracht werden können, da keine starren Strukturvorgaben existieren, die die Schutzmaßnahmen behindern könnten.

Ein wesentlicher Unterschied zwischen ergänzenden und aktuellen Schutzmaßnahmen ist weiterhin, dass es sich bei den ergänzenden Schutzmaßnahmen um integrierbare Maßnahmen auf den Komponenten handelt, die zugleich einen Schutz der Kommunikation bewirken [RUN2013]. Damit kann die Umsetzung der ergänzenden Schutzmaßnahmen bereits beim Entwicklungsprozess von Automatisierungskomponenten erfolgen. Dieses Konzept wird als „Security by Design“ bezeichnet. Im Gegensatz dazu handelt es sich bei den aktuellen Schutzmaßnahmen um additive Maßnahmen, die zusätzlich während des Aufbaus eines Automatisierungssystems berücksichtigt oder nachgerüstet werden müssen.

Unabhängig von den angewendeten Schutzmaßnahmen, sind die Anforderungen **A1** bis **A6** aus der Automatisierungstechnik zu berücksichtigen. Da jedoch die ergänzenden Schutzmaßnahmen miteinander (kryptografisch) verknüpft sind, ist eine Bewertung der Anforderungen aus der Automatisierungstechnik erst nach Erarbeitung eines erweiterten Schutzkonzepts sinnvoll, welches alle ergänzenden Schutzmaßnahmen miteinander kombiniert. Die Bewertung des Gesamtkonzepts erfolgt abschließend im folgenden Kapitel.

7 Erstellung eines erweiterten Schutzkonzepts

Kapitel 6 beschreibt ergänzende Schutzmaßnahmen eines erweiterten Schutzkonzepts. Ziel ist der Schutz von Komponenten sowie der Kommunikation in Automatisierungssystemen. Da die Schutzwirkung der ergänzenden Schutzmaßnahmen nachgewiesen wurde, erfolgt in Kapitel 7 die Kombination der Maßnahmen in einem erweiterten Schutzkonzept, wobei speziell die Anforderungen der Automatisierungstechnik berücksichtigt werden sollen.

Das erweiterte Schutzkonzept wird in Form einer sogenannten IT-Sicherheitsschicht am Beispiel des PROFINET-Protokolls erarbeitet (►7.1). In Abschnitt 7.2 werden dazu verschiedene Realisierungsalternativen vorgestellt, die gegenübergestellt und bewertet werden. Nach Auswahl eines Konzepts wird die Einbindung bzw. Realisierung der ergänzenden Schutzmaßnahmen beschrieben (►7.4). Das realisierte Schutzkonzept wird dann abschließend dargestellt und anhand der Anforderungen aus der Automatisierungstechnik betrachtet.

7.1 Konzept einer IT-Sicherheitsschicht

In den vorgegangen Kapiteln wurde aufgezeigt, dass aktuelle Schutzmaßnahmen Defizite hinsichtlich der Schutzwirkung aufweisen. Diese Defizite können durch Anwendung von ergänzenden Schutzmaßnahmen auf Basis kryptografischer Verfahren beseitigt werden. In Abschnitt 7.1 wird daher ein erweitertes Schutzkonzept erarbeitet. Zunächst sollen die Aufgaben des erweiterten Schutzkonzepts in einer Übersicht dargestellt werden. Eine IT-Sicherheitsschicht kombiniert diese Aufgaben, wobei die Notwendigkeit der Schicht begründet werden soll. Die IT-Sicherheitsschicht hat dabei Anforderungen zu erfüllen, damit dessen Einsatz in Automatisierungssystemen möglich ist.

7.1.1 Aufgaben eines erweiterten Schutzkonzepts

Die Aufgaben des erweiterten Schutzkonzepts beziehen sich auf den Schutz der Assets Komponente und Kommunikation. Hierzu erfolgt eine Übertragung der dafür notwendigen Schutzmaßnahmen aus Abschnitt 6.2 auf die Assets. Weiterhin sind Zusatzaufgaben durch das erweiterte Schutzkonzept zu erfüllen, dessen Darstellungen ebenso folgen.

Schutz der Kommunikation

Zwischen Automatisierungskomponenten (bspw. SPS und DP) wird bei Inbetriebnahme des Automatisierungssystems eine Kommunikationsbeziehung etabliert. Dazu stellen die Komponenten über Schnittstellen (z.B. Industrial Ethernet) eine Verbindung über die Systemgrenze her. Zunächst sind für den Verbindungsaufbau benötigte Informationen wie Adress-, Parametrierungs- sowie Konfigurationsdaten zu übertragen, gefolgt von der eigentlichen Prozessdatenkommunikation. Die Übertragung aller Informationen erfolgt dabei ungeschützt und kann durch einen Angreifer mitgelesen als auch verändert werden. Aus diesem Grund sind ergänzende Schutzmaßnahmen so einzusetzen, dass Schwachstellen der Kommunikation geschlossen werden. Angriffe auf die Kommunikation sind durch Alarmmeldungen mitzuteilen. Sowohl ein sicherer Verbindungsaufbau, wie auch eine gesicherte (echtzeitfähige) Kommunikation über die Systemgrenze werden benötigt, wie Abbildung 7-1 zeigt.

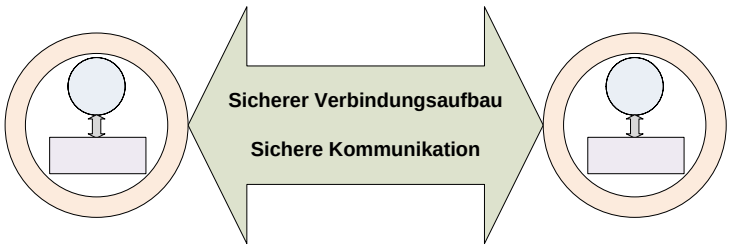


Abbildung 7-1: Schutz der (echtzeitfähigen) Kommunikation

Die Aufgaben zum Schutz der Kommunikation lassen sich zwischen dem sicheren Verbindungsaufbau und der daran anschließenden sicheren Kommunikation differenzieren. Die sichere Kommunikation bezieht sich neben der Prozessdatenkommunikation dabei auch auf die Kommunikation zur Parametrierung und Konfiguration der Komponenten.

- **Sicherer Verbindungsaufbau**

Zu Beginn erfolgt der Verbindungsaufbau mit Hilfe von initialen Verbindungsparametern. Da diese Informationen für angreifende Personen wertvoll sein können, sollten die Informationen geschützt bzw. verschlüsselt kommuniziert werden. Zu diesem Zweck muss eine gegenseitige Authentifizierung anhand des in Abschnitt 6.2.1 gezeigten Verfahren erfolgen. Zur Vereinfachung des sicheren Verbindungsaufbaus sollten die dafür notwendigen Zertifikate in der Automatisierungskomponente vorliegen bzw. bei Inbetriebnahme erstellt werden. Erst nach Authentifizierung kann im Anschluss die sichere Kommunikation stattfinden.

- **Sichere Kommunikation**

Die sichere Kommunikation in einem Automatisierungsnetzwerk muss anhand der in Abschnitt 6.2.2 gezeigten kryptografischen Verfahren erfolgen. Dazu ist je nach Sicherheitsbedarf durch den Betreiber des Automatisierungssystems festzulegen, welches Verfahren zur sicheren Übertragung erforderlich ist. Der Betreiber hat dazu die Wahlmöglichkeit zwischen Anwendung von MAC-Verfahren und der Vollverschlüsselung der Kommunikation

  - *Anwendung von MAC-Verfahren*

Das bei Industrial Ethernet angewendete CRC-Prüfsummenverfahren des Standard Ethernet bietet keinerlei Schutz gegen intentionale Beeinflussungen der Kommunikation. Es ist daher aus Gründen der IT-Sicherheit zusätzlich ein MAC-Verfahren zum Schutz der (echtzeitfähigen) Kommunikation anzuwenden. Dieser Basisschutz ermöglicht, dass Manipulationen an den übertragenen Daten erkannt werden können und verhindert so eine mögliche Beeinflussung des Automatisierungssystems durch eine angreifende Person. Die angreifende Person ist jedoch weiterhin in der Lage, die übertragenen Daten zu lesen, weshalb im Fall von sensiblen Daten weitere Schutzmaßnahmen zu ergreifen sind.

  - *Anwendung von Verschlüsselungen*

Sind bei der Kommunikation vertrauliche Informationen zu übertragen, so sind die zu übertragenen Daten zusätzlich zu verschlüsseln. Erst auf diese Weise wird verhindert, dass eine angreifende Person Zugriff auf diese Informationen erhält. Wie in Abschnitt 6.2.2 dargestellt, schützt die Verschlüsselung lediglich die Vertraulichkeit (→**I**) der Daten, weshalb zusätzlich ein MAC-Verfahren benötigt wird, um das Schutzziel **T** erfüllen zu können. Die Berechnung einer Verschlüsselung zusätzlich zum MAC ist mit zusätzlichem Rechenaufwand verbunden und sollte nur (optional) bei erhöhtem Sicherheitsbedarf angewendet werden.

Schutz der Komponenten (Zustandsüberwachung)

Der Schutz der Kommunikation meint den Schutz der Kommunikationsbeziehung von Automatisierungskomponenten über ihre Systemgrenze hinweg. Abbildung 7-2 zeigt die prinzipielle Position einer Schutzmaßnahme für eine Komponente um seine Systemgrenze.

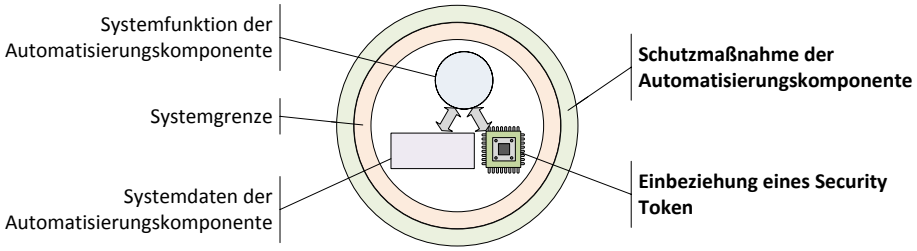


Abbildung 7-2: Schutz der Komponente

Entsprechend Abschnitt 4.1.2 werden innerhalb der Systemgrenze zum einen die Systemfunktion (z.B. Anwendung zur Messdatenauswertung) und zum anderen Daten der Systemfunktion (z.B. Parametrierungs- und Konfigurationsdaten) bereitgestellt. Beide Bestandteile der Komponente sind durch Schutzmaßnahmen innerhalb dieser Systemgrenze unter Einbeziehung von Security Token zu schützen. Erfolgt die Manipulation durch eine angreifende Person, müssen Maßnahmen ergriffen werden, wie bspw. die Versendung von Alarmen.

Da die Systemfunktion einer Automatisierungskomponente durch eine angreifende Person verändert werden kann, sind Maßnahmen vorzusehen, die dies verhindern. Durch Zustandsüberwachung der Systemfunktionen zur Aufdeckung von Manipulationen an den Funktionen der Automatisierungskomponente können Angriffe erkannt werden. In einem verteilten Automatisierungssystem können so zusätzlich Maßnahmen ergriffen werden, die das System in Folge eines Angriffes in einen sicheren Zustand überführen. Dadurch ist sichergestellt, dass das Automatisierungssystem durch einen Angriff keinen unkontrollierbaren Zustand annimmt. Ziel des Konzeptes ist die dauerhafte verteilte Zustandsüberwachung wie in Abschnitt 6.2.3 beschrieben, bspw. durch Überwachung der Anwendung einer Automatisierungskomponente während dessen Laufzeit.

Weiterhin können die Systemdaten der Komponente ein mögliches Angriffsziel darstellen. Zu diesen Systemdaten gehören neben den Echtzeitdaten, den Parametrier- und Konfigurationsdaten auch die in Abschnitt 6.2 genannten kryptografischen Merkmale und Schlüssel. Aus diesem Grund sollten Schutzmaßnahmen eingesetzt werden, die die (relevanten) Systemdaten schützen. Insbesondere die kryptografischen Merkmale sind vor unautorisiertem Auslesen oder einer Veränderung durch eine angreifende Person zu schützen, da mit Hilfe dieser kryptografischen Informationen die hier beschriebenen ergänzenden Schutzmaßnahmen ausgehebelt werden könnten. Ein Schutz der Systemdaten kann durch Anwendung der in 6.2.4 beschriebenen Einbindung eines Security Token erfolgen. [RNT2012]

Weitere notwendige Funktionen des erweiterten Schutzkonzepts

Die ergänzenden Schutzmaßnahmen benötigen und nutzen Funktionen, die durch das Schutzkonzept zur Verfügung gestellt werden müssen. Da der Schutz der Komponente und Kommunikation auf ähnliche Funktionen zurückgreifen, sind sie als eigenständige Funktionen des erweiterten Schutzkonzepts zu sehen.

- **Einbindung der kryptografischen Verfahren**

Kryptografische Funktionen werden für die Funktionen des erweiterten Schutzkonzepts benötigt. Das erweiterte Schutzkonzept übernimmt die Aufgabe, kryptografische Funktionen den ergänzenden Schutzmaßnahmen zur Verfügung zu stellen. Zu diesem Zweck kann die Einbindung einer kryptografischen Bibliothek wie bspw. OpenSSL erfolgen [OPE2014], die zahlreiche kryptografische Funktionen bereithält.

- **Einbindung der Security Token**

Das erweiterte Schutzkonzept benötigt eine Software-Schnittstelle über die Zugriff auf ein Security Token besteht. Auf diese Weise können anderen Funktionen des erweiterten Schutzkonzepts auf sicher gespeicherte Informationen auf dem Token zurückgreifen.

- **Schlüssel- und Zertifikatsverwaltung**

Die verwendeten Schlüssel und Zertifikate zum sicheren Verbindungsaufbau und der sicheren Kommunikation müssen durch das erweiterte Schutzkonzept verwaltet werden. Die Aufgabe kann durch Anwendung einer bereits geforderten Public Key Infrastructure (PKI) erfüllt werden, die Zertifikats- und Schlüsselverwaltung übernimmt (siehe auch Abschnitt 6.2.1).

- **Alarmbehandlung**

Sowohl der Schutz der Kommunikation als auch der Schutz der Komponente muss in der Lage sein, Alarme im Automatisierungsnetzwerk zu versenden. So wird bspw. im Falle eines fehlgeschlagenen Authentifizierungsvorgangs, einem erkannten Angriff auf Komponente oder Kommunikation ein Alarm versendet, auf welchen das Automatisierungssystem reagiert.

Gemeinsame Anwendung der Aufgaben des erweiterten Schutzkonzepts

Um die in Abschnitt 6.1 erläuterte Anforderung bezüglich der Abdeckung aller Schutzziele erreichen zu können, sind die Schutzmaßnahmen für die Komponente und die Kommunikation gemeinsam anzuwenden, was Abbildung 7-3 zeigt.

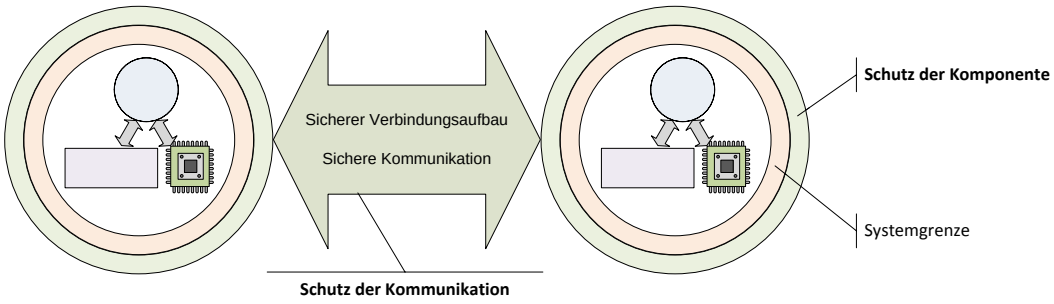


Abbildung 7-3: Gemeinsame Anwendung der ergänzenden Schutzmaßnahmen

Der Schutz der Komponente bezieht sich entsprechend Abbildung 7-2 auf die Systemgrenze der Komponente. Die geschützte Kommunikation wird über die Systemgrenze zwischen den Komponenten etabliert. Durch das Vorhandensein des Schutzes der Komponente setzt die Absicherung der Kommunikation auf einer geschützten Komponente auf. Sowohl der Schutz der Komponente als auch der Kommunikation interagieren auf Basis der kryptografischen Funktionen. Die gemeinsame Anwendung der ergänzenden Schutzmaßnahmen erlaubt so eine größtmögliche Abdeckung der Schutzziele.

7.1.2 Begründung für eine IT-Sicherheitsschicht

Um die IT-Sicherheit eines informationstechnischen Systems beurteilen zu können, sind Analysen des Systems notwendig. Trotz der Analyse eines vereinfachten Betrachtungsgegenstandes in Kapitel 4 konnte deutlich gemacht werden, dass mit einem stark vernetzten und komplexen System auch die Analyse des Systems größere Dimensionen annimmt. Auch die Anwendung von Schutzmaßnahmen für die IT-Sicherheit nimmt mit dem Ausmaß des Systems zu. Folglich steigt die Komplexität in der Beherrschung des Systems und auch der IT-Sicherheit gleichermaßen [SCH1999]. Steigt die Komplexität weiter an, ist ein Verlust der Wirksamkeit von Schutzmaßnahmen denkbar, da Schutzmaßnahmen der IT-Sicherheit nicht mehr sicher beherrscht werden können [DIT2013].

Gegenwärtig eingesetzte und in Abschnitt 5.3 beschriebene Schutzmaßnahmen sind als Einzelmaßnahmen zu sehen, wobei für jede der Schutzmaßnahme zusätzlicher Aufwand zu erbringen ist und damit die Komplexität der IT-Sicherheit steigt. Im Gegensatz dazu, basieren die die aufgezeigten ergänzenden Schutzmaßnahmen auf gemeinsam genutzten kryptografischen Funktionen, wie in Abschnitt 7.1.1 dargestellt. Da die ergänzenden Schutzmaßnahmen darüber hinaus um integrierbare bzw. integrierte Funktionen in den Komponenten handelt, wird die Komplexität für den Nutzer der Automatisierungsanlage verringert, da integrierte Maßnahmen in das Engineering des Automatisierungssystems mit einbezogen werden können, und nicht wie bei aktuellen Schutzmaßnahmen zusätzlich zu planen sind.

Die ergänzenden Schutzmaßnahmen, auf Basis der kryptografischen Funktionen machen die Zusammenführung der ergänzenden Schutzmaßnahmen sinnvoll. Dies kann die Komplexität für die Sicherstellung der IT-Sicherheit insgesamt reduzieren und den Betriebsaufwand für die Schutzmaßnahmen (→**A4**) minimieren. Aus diesem Grund ist die Einführung einer IT-Sicherheitsschicht sinnvoll. Die IT-Sicherheitsschicht koordiniert die ergänzenden Schutzmaßnahmen und ist prinzipiell in Abbildung 7-4 dargestellt.

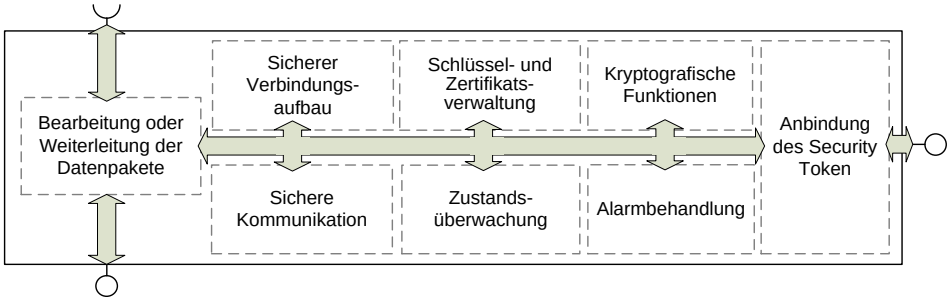


Abbildung 7-4: Funktionen der IT-Sicherheitsschicht

Die IT-Sicherheitsschicht kann in eine Automatisierungskomponente integriert werden. Dazu muss eine Anpassung der Software der Komponente wie bspw. der Kommunikations-Protokollsoftware so erfolgen, dass sicherheitsrelevante Vorgänge nur über die IT-Sicherheitsschicht laufen. Werden keine Schutzmaßnahmen benötigt, können die Daten direkt ohne Verarbeitung durch die IT-Sicherheitsschicht weiter geleitet werden. Die Platzierung der IT-Sicherheitsschicht kann an verschiedenen Stellen der Automatisierungskomponente anhand des ISO/OSI-Schichtenmodells erfolgen. Für die Platzierung der IT-Sicherheitsschicht sind zunächst allgemeine Anforderungen aufzustellen. Die Diskussion dieser Anforderungen hinsichtlich der Platzierung erfolgt im nächsten Abschnitt.

7.1.3 Anforderungen an die IT-Sicherheitsschicht

Wie in Abschnitt 7.1.2 erläutert, ist die Einführung einer IT-Sicherheitsschicht notwendig um die Komplexität bei der Anwendung der ergänzenden Schutzmaßnahmen zu minimieren. Um die Effektivität der IT-Sicherheitsschicht beurteilen zu können, werden zuvor Anforderungen an die IT-Sicherheitsschicht definiert. Diese Anforderungen betreffen sowohl den allgemeinen Betrieb als auch Aspekte der Automatisierungstechnik.

- **Betriebsaufwand** für den Anwender

Die Einführung der IT-Sicherheitsschicht reduziert den Betriebsaufwand für die ergänzenden Schutzmaßnahmen. Diese Reduzierung ist allerdings auch abhängig von der Platzierung der IT-Sicherheitsschicht. Daher wird der Betriebsaufwand für den Anwender bei der Betrachtung der Realisierungsalternativen getrennt betrachtet.

- **Implementierungsaufwand** für die IT-Sicherheitsschicht

Je nach Platzierung der IT-Sicherheitsschicht ergibt sich ein unterschiedlich hoher Implementierungsaufwand. Der Aufwand sollte dem Nutzen des Schutzes entsprechen und möglichst gering sein. Entsprechend sollten bestehende Vorgaben wie Standards und Normen durch die Implementierung der IT-Sicherheitsschicht berücksichtigt werden.

- **Transparente Integration** der IT-Sicherheitsschicht

Eine transparente Einbindung der Schicht ist zu bevorzugen, da so Anpassungen an Anwendungsprofilen nicht erforderlich sind. Dies gilt insbesondere für die Absicherung von sicherheitsgerichteter Kommunikation (im Sinne von Safety) durch die IT-Sicherheitsschicht.

- **Vollständiger Schutz der Kommunikation**

Der Schutz muss die gesamte Kommunikation erfassen und alle sicherheitsrelevante Kommunikationsparameter mit einbeziehen. Weiterhin darf keine Beschränkung der Echtzeitfähigkeit durch die IT-Sicherheitsschicht erfolgen.

- **Vermeidung zusätzlichen Overheads**

Die Übertragung der kryptografischen Parameter wie MAC nimmt in den Datenpaketen zusätzlichen Platz in Anspruch. Die Bearbeitung des Overheads nimmt weiterhin zusätzliche Rechenzeit in Anspruch. Aus diesen Gründen ist der Overhead minimal zu halten.

- **Erweiterbarkeit auf andere Industrial Ethernet Protokolle**

Die Anwendbarkeit der IT-Sicherheitsschicht sollte nicht auf ein Industrial Ethernet Protokoll begrenzt sein und sich demnach auf andere Protokolle übertragen lassen. Die Lage der Sicherungsschicht im OSI-Protokollstack muss gewährleisten, dass dies möglich ist.

Anhand der dargestellten Anforderungen erfolgt eine Betrachtung verschiedener Realisierungsalternativen zur Platzierung der IT-Sicherheitsschicht. Alle Anforderungen an die IT-Sicherheitsschicht müssen bei der Auswahl einer sinnvollen Realisierungsalternative berücksichtigt werden, da nur so ein wirksamer und ressourcenschonender Schutz möglich ist. In Abschnitt 7.2 folgt die Gegenüberstellung der Realisierungsalternativen.

7.2 Realisierungsalternativen für eine IT-Sicherheitsschicht

Die Platzierung der IT-Sicherheitsschicht kann an verschiedenen Stellen des ISO/OSI-Schichtenmodells erfolgen. Während der Schutz der Komponente weitestgehend unabhängig von der Platzierung der IT-Sicherheitsschicht ist, so hat die Platzierung für den Schutz der Kommunikation größere Auswirkungen, da ggf. nicht alle Schichten des ISO/OSI-Modells ausreichend durch die IT-Sicherheitsschicht geschützt werden. Die Betrachtung der Realisierungsalternativen erfolgt anhand der in Abschnitt 7.1.3 aufgestellten Anforderungen.

Wie in Abschnitt 3.2.3 dargestellt, wird in der vorliegenden Arbeit beispielhaft die Absicherung des PROFINET-Protokolls durchgeführt. Dafür werden in Ergänzung zu den Beschreibungen des Industrial Ethernet in Abschnitt 3.2 wesentliche Zusatzeigenschaften des PROFINET-Protokolls betrachtet, die für die Realisierung der IT-Sicherheitsschicht notwendig sind. Anhand dieser Eigenschaften werden drei Realisierungsalternativen zur Platzierung der IT-Sicherheitsschicht in der PROFINET-Protokollsoftware dargestellt. Abschließend erfolgt die Bewertung und Auswahl einer Realisierungsalternative.

7.2.1 Vorbetrachtung des PROFINET-Protokolls für die IT-Sicherheitsschicht

Wie im Falle anderer Industrial Ethernet Ausprägungen (vgl. Abschnitt 3.2), stellt das PROFINET-Protokoll sowohl eine echtzeitfähige als auch nicht-echtzeitfähige Kommunikation bereit. Daher wird für die Vorbetrachtung eine Differenzierung anhand dieser beiden Kommunikationsdienste durchgeführt. Ausgangspunkt für die Vorbetrachtung sind die in Abschnitt 3.2 erläuterten Grundlagen zu Industrial Ethernet und dessen Protokollaufbau.

Der Aufbau der Datenpakete des PROFINET-Protokolls basiert grundlegend auf dem Standard Ethernet Paket (vgl. Abbildung 3-6). Zur Unterscheidung zwischen echtzeitfähiger rund nicht-echtzeitfähiger Kommunikation wird der sogenannte EtherType dem Datenpaket im Header hinzugefügt. So weist der Wert **0x8892** des EtherType auf eine (echtzeitfähige) PROFINET-Kommunikation hin. Weitere von PROFINET unterstützte Standard-Protokolle, insbesondere nicht-echtzeitfähige Kommunikation, verwenden einen anderen EtherType, z.B. **0x0800** für IP-basierte Kommunikation. Das Datenfeld sowie die weitere Adressierung der PROFINET-Komponenten unterscheiden sich zusätzlich nach Kommunikationsform.

Echtzeitfähige Kommunikation

Abbildung 7-5 zeigt den Aufbau eines PROFINET-Datenpakets.

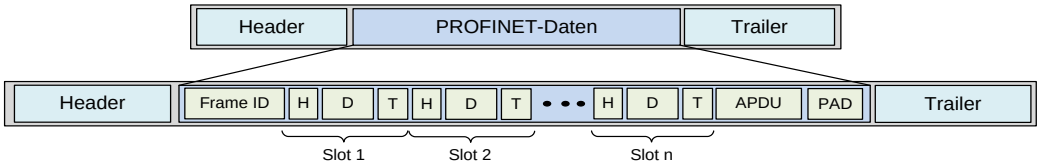


Abbildung 7-5: Prinzipieller Aufbau eines PROFINET-Datenpakets

Um die Echtzeitfähigkeit der Kommunikation zu erhalten, entfallen die Informationen wie IP-Adresse und TCP/UDP-Daten. Die entsprechenden Layer fehlen in dem Teil des Kommunikationsstacks. Die Adressierung erfolgt auf Basis der MAC-Adresse einer PROFINET-Komponente, womit die Kommunikation auf eine Broadcast-Domäne begrenzt ist. Sofern anhand des EtherType eine PROFINET-Kommunikation erkannt wurde, übernimmt die

PROFINET-Protokollsoftware eine weitere Differenzierung der Kommunikation anhand der FrameID. Die FrameID erlaubt zwischen verschiedenen echtzeitfähigen Kommunikationsformen des PROFINET-Protokolls zu unterscheiden. [POP2005]

Sowohl kompakte als auch modulare PROFINET-Komponenten verwenden das Datenfeld des PROFINET-Datenpakets auf gleiche Weise. Der physikalische Aufbau des Geräts definiert Slots, über die eine direkte Adressierung der E/A-Daten einer PROFINET-Komponente erfolgen kann. Jeder der Slots führt zusätzlich Header und Trailer-Informationen als Datenstatus mit sich. Weiterhin befinden sich im PROFINET-Datenfeld zusätzliche Informationen wie die APDU zur Kommunikationssteuerung und das Padding (PAD) zum Auffüllen des Datenpakets auf die Mindestlänge. Die APDU beinhaltet weiterhin einen PROFINET-Paketzähler (engl. counter) zur Sicherstellung der Reihenfolgerichtigkeit von Datenpaketen, sowie Datenfelder für den Daten- sowie Kommunikationsstatus. Das Padding (engl. auffüllen) dient dazu die PROFINET-Daten auf eine Mindestlänge aufzufüllen, welche das Ethernet-Protokoll vorgibt. Für den Anwender des PROFINET-Protokolls besteht nur Zugriff auf den Datenstatus des APDU-Feldes sowie die Daten der jeweiligen Slots. Auf die FrameID und den PROFINET-Counter besteht durch den Anwender kein direkter Zugriff.

Die PROFINET-Spezifikation in der Version 2.3 definiert Zykluszeiten von 31,25 µs für die bidirektionale Kommunikation, also der Behandlung einer Kommunikationsverbindung mit sowohl ein- als auch ausgehenden Datenpaketen [PNO2010]. Damit ist eine echtzeitfähige isochrone PROFINET-(IRT)-Kommunikation (engl. isochronous real-time) möglich, bspw. zur Antriebssynchronisierung. Diese Zykluszeiten setzen jedoch eine spezielle Umsetzung des PROFINET-Protokollstacks in Hardware wie z.B. einem ASIC voraus. Typische echtzeitfähige PROFINET-(RT)-Kommunikation (engl. real-time) liegt im Bereich von Zykluszeiten von 1 bis 2 ms bei einer bidirektionalen Kommunikation [FFV2011].

Nicht-Echtzeitfähige Kommunikation

Das PROFINET-Protokoll nutzt, neben der echtzeitfähigen Kommunikation, zahlreiche Standardprotokolle wie SNMP, http oder ARP. Diese werden für die Parametrierung und Konfiguration der PROFINET-Komponenten verwendet. Die nicht-echtzeitfähige Kommunikation unterscheidet sich nicht nur im EtherType, der das verwendete Protokoll anzeigt, sondern zusätzlich in der Form der Adressierung. Neben der MAC-Adresse werden zusätzlich TCP- bzw. UDP-Daten sowie ggf. eine IP-Adresse zur Adressierung verwendet. Dieser Umstand ermöglicht die Kommunikation mit Komponenten außerhalb der Broadcast-Domäne, kann aber letztlich zum Verlust der Echtzeitfähigkeit führen.

Wie in Abschnitt 4.4 dargestellt, kann auch die nicht-echtzeitfähige Kommunikation das Ziel einer angreifenden Person sein. Besonders dann, wenn aus dieser Kommunikation Informationen hinsichtlich des Aufbaus des Automatisierungssystems geschlossen werden kann. Da das PROFINET-Protokoll sich an übliche Standards bei der Verwendung der nicht-echtzeitfähigen Kommunikation hält und keinen speziellen Aufbau des Datenfeldes vorsieht und nicht die Echtzeitfähigkeit der Kommunikation betrifft, ist bei der Absicherung dieser Kommunikation lediglich darauf zu achten, dass die Platzierung der IT-Sicherheitsschicht die in Abschnitt 7.1.3 gestellten Anforderungen erfüllt.

7.2.2 Darstellung der Realisierungsalternativen

Ziel der IT-Sicherheitsschicht ist die größtmögliche Schutzwirkung für das PROFINET-Netzwerk und die daran angebunden Komponenten. Nachfolgend soll anhand des ISO/OSI-Modells die Einbindung der IT-Sicherheitsschicht (siehe Abschnitt 7.1) im PROFINET-Protokoll erfolgen. Die Bewertung verschiedener Realisierungsalternativen soll anhand der Anforderungen an die IT-Sicherheitsschicht in Abschnitt 7.1.3 erfolgen. Aus dieser Bewertung gehen Vor- und Nachteile hervor, die dargestellt werden. Im Anschluss wird die Auswertung und Auswahl einer Realisierungsalternative durchgeführt.

Realisierungsalternative 1

Realisierungsalternative 1 beschreibt die Erweiterung des PROFINET-Protokolls auf Basis eines sogenannten Anwendungsprofils. Dies bedeutet, dass die IT-Sicherheitsschicht in Form einer anwenderspezifischen Erweiterung in das PROFINET-Protokoll eingebunden wird. Abbildung 7-6 zeigt die Platzierung der IT-Sicherheitsschicht nach diesem Konzept.

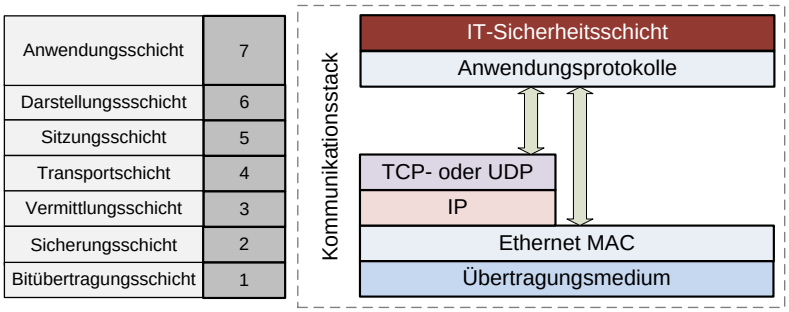


Abbildung 7-6: Protokollaufbau bei Realisierungsalternative 1

Eine auf den Anwendungsprotokollen aufbauende IT-Sicherheitsschicht ist direkt vergleichbar zur Safety-Lösung für das PROFINET-Protokoll, welche als PROFIsafe bezeichnet wird. Bezogen auf die echtzeitfähige Kommunikation besteht durch die IT-Sicherheitsschicht daher als Anwendungsprofil nur Zugriff auf die Daten aus der Anwendung. Durch diese Eigenschaft ergibt sich ein spezieller Aufbau des PROFINET-Datenpakets bei Anwendung der IT-Sicherheitsschicht, welcher in Abbildung 7-7 dargestellt ist.

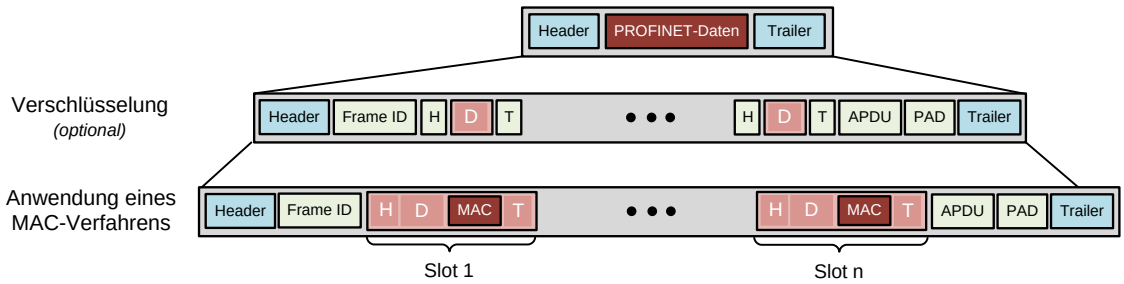


Abbildung 7-7: PROFINET-Datenpaketaufbau bei Realisierungsalternative 1

Durch die IT-Sicherheitsschicht als Anwendungsprofil besteht lediglich Zugriff auf die Daten der Slots. Jeder der Slots kann (optional) verschlüsselt werden, wobei Header und Trailer unverschlüsselt bleiben, um die Erkennung der Slots weiter zu ermöglichen. Anschließend erfolgt die Berechnung eines MAC für jeden Slot. Die Parameter des PROFINET-Protokolls wie FrameID, und das Padding des Datenpakets liegen außerhalb der ergänzenden Schutzmaßnahmen. Auch Bestandteile der APDU wie der PROFINET-Counter und der Datenstatus des gesamten PROFINET-Pakets bleiben ungeschützt. Dieser Sachverhalt gilt

ebenso bei der nicht-echtzeitfähigen Kommunikation. Während die Daten der Anwendung durch die ergänzenden Schutzmaßnahmen abgesichert werden können, so sind die Parameter zur Steuerung der Anwendungsprotokolle sowie die TCP- und UDP-Daten ungesichert.

Bewertung

Der Betriebsaufwand bei der Anwendung der IT-Sicherheitsschicht nach Realisierungsalternative 1 bedarf lediglich der Berücksichtigung im Engineering des Automatisierungssystems. Da alle Vorgänge der ergänzenden Schutzmaßnahmen, wie bspw. die Authentifizierung, automatisiert im Hintergrund arbeiten, ist der Betriebsaufwand minimal. Die Erweiterung in Form eines Anwendungsprofils hält ebenso den Implementierungsaufwand minimal, da das PROFINET-Protokoll entsprechende Schnittstellen für anwenderspezifische Erweiterungen vorsieht. Damit sind Veränderungen am PROFINET-Standard [IEC2008a] nicht notwendig, um die ergänzenden Schutzmaßnahmen zu integrieren. Eine transparente Integration der IT-Sicherheitsschicht kann jedoch nicht erfolgen, da die anwenderspezifische Erweiterung mit anderen Anwendungsprofilen konkurriert. So wären zwingend Anpassungen an der PROFIsafe-Lösung und/oder der IT-Sicherheitsschicht notwendig, wenn beide (Schutz-)Maßnahmen gleichzeitig ergriffen werden sollen. Eine entsprechend angepasste Lösung wäre nicht mehr auf andere Industrial Ethernet Ausprägungen übertragbar.

Ein vollständiger Schutz der Kommunikation auf Basis von Realisierungsalternative 1 ist nicht gegeben. Zwar können sämtliche Daten aus der Anwendung durch die IT-Sicherheitsschicht geschützt werden, Informationen unterhalb der IT-Sicherheitsschicht können jedoch nicht abgedeckt werden. Parameter der Anwendungsprotokolle sowie TCP-und UDP-Daten bleiben daher ungesichert. Eine angreifende Person kann demnach keinen Zugriff auf die geschützten Daten der Anwendung erhalten, aber das Verhalten der Anwendungsprotokolle manipulieren. Ungeschützte UDP- und TCP-Daten ermöglichen weitere Angriffe auf die nicht-echtzeitfähige Kommunikation.

Ein wesentlicher Punkt ist der entstehende Overhead bei der Übertragung der PROFINET-Datenpakete nach Alternative 1. Da jeder Slot des PROFINET-Datenpakets mit einem MAC versehen wird, steigt mit der Anzahl an Slots nicht nur die Menge an zu übertragenden Daten sondern auch der Rechenaufwand, da jeder MAC einzeln zu erstellen ist. Die Vor- bzw. Nachteile der Realisierungsalternative sind in Tabelle 7-1 aufgeführt.

Vorteile	Nachteile
• Als Anwendungsprofil ist eine Integration der IT-Sicherheitsschicht auf jedem PROFINET-Kommunikationsstack möglich. • Der Bestehende PROFINET-Standard wird nicht verändert.	• Prüfsummen für jeden Slot führen zu erhöhtem Overhead da mehrere Prüfsummen pro Paket. • Anzahl an Prüfsummen erhöht Rechenaufwand. Einfluss auf die Echtzeitfähigkeit vergrößert. • Weitere Anwendungsprofile arbeiten mit der IT-Sicherheitsschicht nicht ohne Anpassungen. • Parameter der Anwendungsprotokolle ungeschützt. • Ungeschützte nicht-echtzeitfähige Kommunikation

Tabelle 7-1: Vor- und Nachteile der Realisierungsalternative 1

Realisierungsalternative 2

Bei Realisierungsalternative 2 handelt es sich ebenso um eine anwendungsspezifische Erweiterung des PROFINET-Protokolls. Die Einbindung erfolgt jedoch unterhalb des Anwendungsprotokolls, womit Daten aus der Anwendung bereits durch das Anwendungsprotokoll interpretiert wurden. Damit ist Realisierungsalternative 2 vergleichbar zu SSL/TLS [RES2000]. Abbildung 7-8 zeigt diese Platzierung der IT-Sicherheitsschicht.

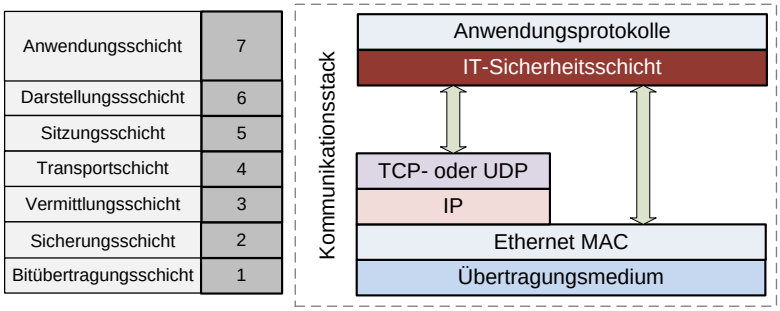


Abbildung 7-8: Protokollaufbau bei Realisierungsalternative 2

Durch die Platzierung der IT-Sicherheitsschicht entsprechend Realisierungsalternative 2 wird im Gegensatz zu einer Absicherung pro Slot nach Realisierungsalternative 1 ein übergreifender Schutz des PROFINET-Datenpakets möglich. Die so geartete Platzierung der IT-Sicherheitsschicht hat maßgeblich Einfluss auf den PROFINET-Datenpaketaufbau bei der echtzeitfähigen Kommunikation. Abbildung 7-9 zeigt die notwendigen Anpassungen am PROFINET-Datenpaketaufbau durch die Platzierung unterhalb der Anwendungsprotokolle.

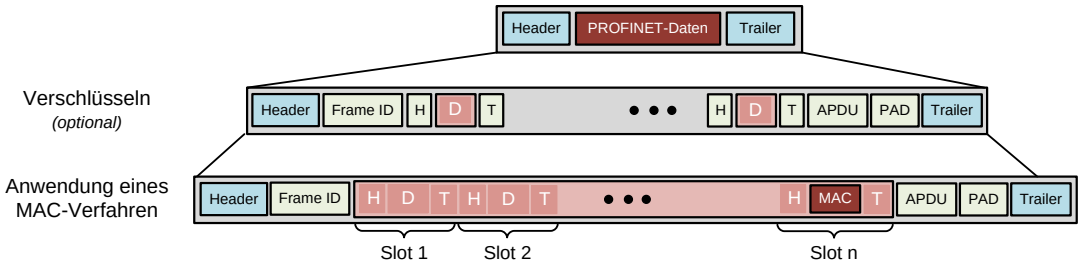


Abbildung 7-9: PROFINET-Datenpaketaufbau bei Realisierungsalternative 2

In Ergänzung zu Realisierungsalternative 1 besteht ein gesamter Zugriff auf die Daten der Anwendung, nach Verarbeitung durch die Anwendungsprotokolle. In einem ersten Schritt können die Daten aus der Anwendung verschlüsselt werden. Header und Trailer eines jeden Slots bleiben weiterhin unverschlüsselt, damit die Struktur des Datenpakets zur Verarbeitung durch die IT-Sicherheitsschicht interpretierbar bleibt.

Aus den gesamten verschlüsselten oder unverschlüsselten Daten wird anschließend ein MAC erstellt. Die MAC-Prüfsumme befindet sich anschließend in einem eigenen Slot der Anwendungsdaten [AKB2009b], [AKB2009c]. Die Realisierungsalternative 2 orientiert sich damit an dem allgemeinen (modularen) PROFINET-Datenpaketaufbau, da die IT-sicherheitsrelevanten Informationen in einem eigenen PROFINET-typischen Slot versendet werden. Alternative 1 und 2 teilen aufgrund ihrer Platzierung in der Anwendungsschicht jedoch die Eigenschaft, dass kein Zugriff auf Daten der APDU, FrameID, Padding usw. besteht. Damit bleiben diese Übertragungsparameter weiterhin einem Angriff ausgesetzt. In gleicher Weise gilt dies für die nicht-echtzeitfähige Kommunikation, die nur unzureichend durch die IT-Sicherheitsschicht abgedeckt ist (siehe TCP- und UDP-Daten).

Bewertung

Der Aufwand zum Betrieb der IT-Sicherheitsschicht ist identisch zu Realisierungsalternative 1. Da es sich weiterhin im Falle von Alternative 2 ebenso um ein Anwendungsprofil handelt, bleibt ebenfalls der Implementierungsaufwand der Schicht minimal. Dies führt wie in Alternative 1 dazu, dass parallel arbeitende Anwendungsprofile angepasst werden müssen, weshalb die transparente Integration der IT-Sicherheitsschicht erschwert ist und sich die Lösung nach Realisierungsalternative 2 nicht auf andere Feldbusse und Industrial Ethernet Protokolle übertragen lässt.

Eine gleichzeitige Anwendung von SSL/TLS-Funktionen und dem dargestellten Schutz der PROFINET-Kommunikation in Abbildung 7-9 erlaubt den Schutz der Anwendungsdaten und der Informationen der Anwendungsprotokolle. Der vollständige Schutz der Kommunikation ist damit jedoch weiterhin nicht möglich. Nach wie vor besteht kein Zugriff auf die Kommunikationsparameter der echtzeitfähigen Kommunikation (z.B. APDU) und der nicht-echtzeitfähigen Kommunikation (TCP- und UDP-Daten). Trotzdem wird durch Alternative 2 der Overhead zur Übertragung der IT-sicherheitsrelevanten Informationen verringert, da nur ein MAC pro Datenpaket zu übertragen ist. Die wesentlichen Eigenschaften bzw. Vor- und Nachteile der zweiten Realisierungsalternative sind in Tabelle 7-2 zusammengefasst.

Vorteile	Nachteile
• Geringer Aufwand zur Implementation der IT-Sicherheitsschicht als Anwendungsprofil. • PROFINET-Standard wird nicht verändert. • Eine kryptografische Operation (Prüfsumme bzw. zusätzliche Verschlüsselung) für ein Datenpaket.	• Paralleler Betrieb von Anwendungsprofilen zur IT-Sicherheitsschicht nur mit vorheriger Anpassung. (Veränderung von Standards und Integrationsaufwand für Anwender) • Kein vollständiger Schutz der Kommunikation.

Tabelle 7-2: Vor- und Nachteile der Realisierungsalternative 2

Realisierungsalternative 3

Realisierungsalternative 3 beschreibt die Einbindung der IT-Sicherheitsschicht in der Sicherungsschicht als Erweiterung der Zugriffsmechanismen auf das Medium. Abbildung 7-10 zeigt die Platzierung der IT-Sicherheitsschicht entsprechend der Alternative 3.

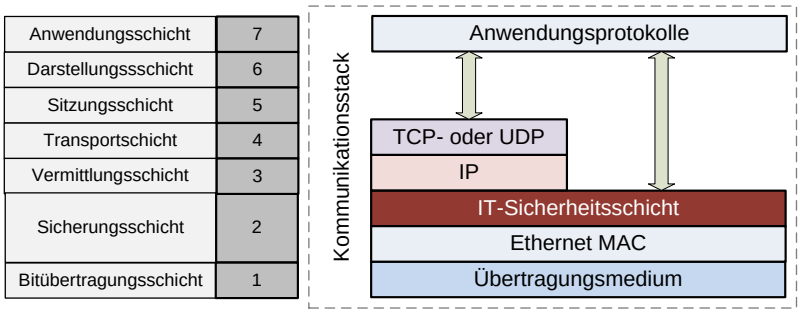


Abbildung 7-10: Protokollaufbau bei Realisierungsalternative 3

Durch diese Platzierung können alle Kommunikationsverbindungen bezüglich der ergänzenden Schutzmaßnahmen betrachtet werden. Dazu übernimmt die IT-Sicherheitsschicht die Daten aus der Anwendung inklusive möglicher Parameter darüber liegender Schichten. Für die Absicherung eines PROFINET-Datenpakets ergibt sich für die echtzeitfähige Kommunikation der in Abbildung 7-11 dargestellte Paketaufbau.

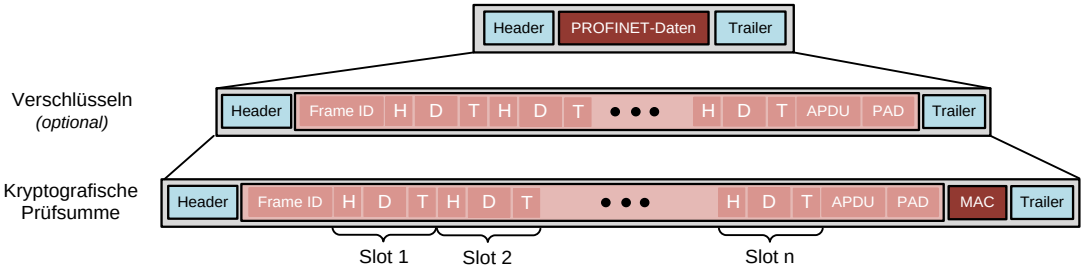


Abbildung 7-11: PROFINET-Datenpaketaufbau bei Realisierungsalternative 3

Zunächst können die Daten vollständig verschlüsselt werden. Anschließend wird die Prüfsumme errechnet und angehängt. Da die Absicherung des PROFINET-Datenpakets damit identisch zur Absicherung eines Standard Ethernet Pakets ist, kann auf identische Weise die nicht-echtzeitfähige Kommunikation geschützt werden.

Bewertung

Wesentlicher Nachteil besteht in der notwendigen, begrenzten Veränderung des PROFINET-Standards, da IT-Sicherheitsschicht in dieser Position Veränderungen des PROFINET-Stacks auf Schicht 2 erfordert und nicht als Anwendungsprofil erfolgen kann. Dies erhöht gleichzeitig den Aufwand zur Implementierung der IT-Sicherheitsschicht, da nicht auf gegebene Schnittstellen zurückgegriffen werden kann. Andererseits erfolgt die Einbindung der Schicht nahe am Zugriff auf das Medium und schließt darüber liegende Anwendungsprofile (z.B. PROFIsafe) mit ein. Alternative 3 erlaubt damit eine transparente Einbindung der IT-Sicherheitsschicht, die in gleicher Weise auch auf weitere Industrial Ethernet Protokolle übertragen werden kann [RTN2012a].

Die Einbindung der IT-Sicherheitsschicht an Schicht 2 des ISO/OSI-Schichtenmodells zeigt, dass neben den Anwendungsprotokollen auch ein Schutz der TCP- oder UDP-Daten wie auch der IP-Adresse möglich ist. Alternative 3 bewirkt auf diesem Weg eine Absicherung der echtzeitfähigen wie auch der nicht-echtzeitfähigen Kommunikation. Bei der nicht-echtzeitfähigen Kommunikation können Ansätze und Verfahren des IPSec-Protokolls angewendet werden, während der Schutz der echtzeitfähigen Kommunikation unabhängig vom Aufbau der Daten aus der Anwendung ist. Eine Berücksichtigung des Aufbaus der PROFINET-Datenpakete entsprechend der Slots ist nicht notwendig und es besteht voller Zugriff auf alle Kommunikationsparameter der darüber liegenden Schichten, die damit auch vollständig geschützt werden können. Weiterhin ist der Overhead der abgesicherten Kommunikation minimal, da z.B. nur ein MAC zusätzlich zu den Nutzdaten zu übertragen ist. Tabelle 7-3 fasst die Vor- und Nachteile der Realisierungsalternative 3 zusammen.

Vorteile	Nachteile
• Gesamte PROFINET-Kommunikation inklusive aller Zusatzparameter können geschützt werden. • Alle Anwendungsprofile können auf erweiterte Schutzmaßnahmen aufbauen. • Absicherung der nicht-echtzeitfähigen Kommunikation für Parametrierung und Konfiguration möglich.	• Es sind Anpassungen am PROFINET-Standard notwendig. • Höherer Implementierungsaufwand für die erweiterten Schutzmaßnahmen im PROFINET-Kommunikationsstack

Tabelle 7-3: Vor- und Nachteile der Realisierungsalternative 3

7.2.3 Auswertung und Auswahl einer Realisierungsalternative

Die Platzierung der IT-Sicherheitsschicht hat Einfluss auf Sicherheitseigenschaften bei der Anwendung der ergänzenden Schutzmaßnahmen, wie Abschnitt 7.2.2 gezeigt hat. Die Realisierungsalternativen werden in Tabelle 7-4 gemäß den Anforderungen aus Abschnitt 7.1.3 nach deren Schutzwirkung bewertet.

	Konzept 1	**Konzept 2**	**Konzept 3**
Betriebsaufwand für Anwender	o	o	o
Implementierungsaufwand der IT-Sicherheitsschicht	+	+	o
Transparente Integration der IT-Sicherheitsschicht	-	-	+
Schutz der echtzeitfähigen Kommunikation			
• Schutz der Daten aus der Anwendung bzw. Prozessdaten	+	+	+
• Schutz der PROFINET-Parameter (z.B. APDU, FrameID)	-	-	+
Schutz der nicht-echtzeitfähige Kommunikation	-	o	+
Erweiterung auf andere Feldbusse	-	-	+
Zusätzlicher Overhead	-	o	o
Schutzwirkung	**o**	**o**	**+**

Tabelle 7-4: Gegenüberstellung und Bewertung der Realisierungsalternativen

Die zusammenfassende Bewertung der Realisierungsalternativen aus Abschnitt 7.2.2 zeigt, dass zwischen den Alternativen im Wesentlichen kein Unterschied im Betriebsaufwand für den Anwender besteht. Der Implementierungsaufwand für die IT-Sicherheitsschicht ist jedoch unterschiedlich, was sich vor allem durch den Grad der notwendigen Anpassungen am der PROFINET-Protokollstack zeigt. Realisierungsalternative 3 erlaubt die optimale transparente Einbindung der erweiterten Schutzmaßnahmen für Hersteller und Anwender bspw. im Engineering des Automatisierungssystems. Dies zeigt sich z.B. durch die Möglichkeit der Einbindung von Anwendungsprofilen (z.B. PROFIsafe) in die Schutzmaßnahmen der IT-Sicherheitsschicht. So kann für funktional sichere Kommunikation zusätzlich die IT-Sicherheit gewährleistet werden, wenn diese benötigt wird [WIS2012].

Ein Schutz der Daten aus der Anwendung ist durch jedes der drei Konzepte gegeben, doch zeigen sich bei den Alternativen 1 und 2 Defizite bezüglich der Schutzwirkung der PROFINET-Parameter und der nicht-echtzeitfähige Kommunikation. Dieser Aspekt und die begrenzte Erweiterbarkeit von Alternative 1 und 2 auf andere Industrial Ethernet Protokolle sowie der durch diese Lösungsvorschläge entstehende Overhead führen dazu, dass insgesamt die Schutzwirkung durchschnittlich bewertet sind.

Trotz des Implementierungsaufwandes wiegt die Schutzwirkung von Realisierungsalternative 3 stärker, als der Aufwand zu deren Realisierung. Nur Alternative 3 erlaubt einen Schutz der gesamten PROFINET-Kommunikation und die transparente Integration der IT-Sicherheitsschicht sowie die Ausweitung auf andere Industrial Ethernet Protokolle. Realisierungsalternative 3 ist vergleichbar mit MACsec [IEE2009]. MACsec ist jedoch nicht für den Einsatz in der Automatisierungstechnik entwickelt worden und kann nur in Verbindung mit speziellen Netzwerkkomponenten verwendet werden. Dies würde voraussetzen, dass Netzwerkkomponenten wie Switches die Datenpakete bezüglich ihrer Sicherheitsmerkmale prüfen, was Laufzeiten im Netzwerk vergrößert und daher die Einsetzbarkeit von MACsec in einem Automatisierungsnetzwerk nicht sinnvoll macht.

7.3 Notwendige Anpassungen für das PROFINET-Protokoll

Auf Basis der Realisierungsalternative 3 sind weitere Betrachtungen für das PROFINET-Protokoll notwendig, um den Schutz der Kommunikation vervollständigen zu können. Sowohl in Bezug auf die echtzeitfähige als auch die nicht-echtzeitfähigen Kommunikation bedarf es zusätzlicher Festlegungen hinsichtlich der gewählten Realisierungsalternative. Echtzeitfähige sowie die nicht-echtzeitfähige Kommunikation sollen daher separat betrachtet werden.

7.3.1 Echtzeitfähige Kommunikation

Zur Kommunikationssteuerung der IT-Sicherheitsschicht und Differenzierung zwischen nicht-abgesicherter oder abgesicherter Kommunikation ist ein Unterscheidungsmerkmal einzusetzen, welcher als Security Header bezeichnet wird (SEC_H). Der Security Header ist in Abbildung 7-12 dargestellt und setzt sich aus der SEC FrameID, dem Frame Control Identifier (FCI) und dem Security Counter (SEC Counter) zusammen. Der Security Header wird in dem PROFINET-Datenpaketaufbau entsprechend Realisierungsalternative 3 eingesetzt.

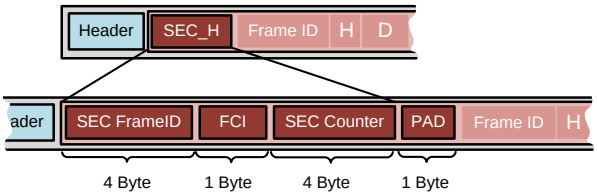


Abbildung 7-12: Aufbau des Security Header

Standard Ethernet Datenpakete ermöglichen die Übertragung von maximal 1500 Byte Nutzdaten. Der PROFINET-Standard nutzt jedoch nicht den gesamten Teil des Nutzdatenfeldes, weshalb hier bis zu 58 Byte für spätere Erweiterungen genutzt werden können [PIM2005]. Dieser Platz wird dazu genutzt, die Informationen des Security Header zur Steuerung der IT-Sicherheitsschicht (und auch den MAC bzw. das Padding für die Verschlüsslung) zu übertragen. Nachfolgend werden die Bestandteile des Security Headers erläutert.

- **SEC FrameID** (Security FrameID)

Zur Identifizierung eines abgesicherten Datenpakets werden die PROFINET-eigenen FrameIDs verwendet. Der PROFINET-Standard [IEC2008c] ermöglicht dazu die freie Verwendung von benutzerspezifischen FrameIDs zur Implementierung eigener Erweiterungen. Auf lange Sicht ist der Einsatz eines eigenen EtherType für abgesicherte Datenpakete sinnvoll, an dem eine Unterscheidung erfolgen kann. So kann unabhängig vom verwendeten Industrial Ethernet Protokoll eine Absicherung der Kommunikation erfolgen. Der EtherType ist jedoch bei der IEEE zu beantragen und zieht ein Genehmigungsverfahren nach sich. Durch das Voranstellen des Security Header ist die Abwärtskompatibilität zum PROFINET-Standard für Komponenten gewährleistet, die über keine IT-Sicherheitsschicht verfügen.

- **FCI** (Frame Control Identifier)

Ein Schlüssel für kryptografische Operationen muss in regelmäßigen Abständen erneuert werden. Andernfalls kann durch Aufzeichnung von verschlüsselten Paketen sowie Analyse der verschlüsselten Inhalte ein Angreifer nach endlicher Zeit auf den Schlüssel schließen. Zu diesem Zweck wird der FCI verwendet, um die Gültigkeit von Schlüsseln zu steuern. Bei Verbindungsaufbau wird einer Kommunikationsbeziehung ein FCI zugeordnet. Erfolgt nach

Ablauf einer bestimmten Zeit die Umschaltung auf einen erneuerten Schlüssel, erkennt der Empfänger anhand des FCI im Datenpaket welcher Schlüssel gültig ist. Der Ablauf bzw. die Erneuerung von Schlüsseln wird über einen separaten Security-Counter gesteuert.

- **SEC Counter** (Security-Counter)

PROFINET verwendet zur Sicherstellung der Reihenfolgerichtigkeit einen (PROFINET-) Counter, der mit jedem ausgehenden Datenpaket erhöht und durch den Empfänger geprüft wird. Die Bindung des Counters an die Taktzyklen der Kommunikation ermöglicht darüber hinaus eine Zeitmessung. Aufgrund der geringen Größe des PROFINET-Counter (2 Byte im APDU-Feld) und der sehr kleinen Zykluszeiten, kommt es in kurzen regelmäßigen Zeiten zu einem Überlauf des Counters. Würde dieser Counter zur Steuerung der Schlüsselgültigkeit genutzt werden, so wäre die Schlüsselgültigkeit auf wenige Minuten begrenzt. Dies zieht jedoch erheblichen Mehraufwand bei der Verwaltung der Schlüssel nach sich.

Da aus oben genannten Gründen die Verwendung permanenter Schlüssel nicht sinnvoll ist, sollte ein Security-Counter verwendet werden, der eine längere Schlüsselgültigkeit ermöglicht. Ansonsten könnte ein Angreifer aufgrund der immer wiederkehrenden Überläufe verschlüsselte Inhalte wieder einspielen und damit sogenannten „Replay-Angriff“ durchführen, womit das Schutzziel **R** verletzt wäre. Aus diesem Grund beinhaltet der Security Header einen separaten Security-Counter. Abbildung 7-12 zeigt die Erweiterung des Security Headers um dem separaten Security-Counter, der eine Größe von 4 Byte aufweist und längere Schlüsselgültigkeiten erlaubt.

	Taktzeit		**Counter**	**Abgelaufene Zeit**	**Schlüsselgültigkeit**	
	31,25 µs	1 ms			Aktueller Schlüssel	Folgender Schlüssel
1	0 s	0 s	0x000000000	0 %	Key_n	Nicht vorhanden
2	32 h	43 d	0xDFFFFFFF	85 %	Key_n	Key_n+1 ermitteln
3	35 h	46 d	0xEFFFFFFF	93 %	Key_n	Key_n+1
4	37 h	49 d	0xFFFFFFFF	100 %	Key_n abgelaufen	Key_n+1
5/1	0 s	0 s	0x00000000	0 %	Key_n nicht gültig	Key_n+1

Tabelle 7-5: Definition des Security-Counters und der Schlüsselgültigkeit

Der dargestellte Ablauf teilt sich in vier (bzw. fünf) Zeiträume ein. Während der Gültigkeit des ersten Schlüssels, wird ein zweiter Schlüssel ermittelt, bspw. durch Ableitung aus dem vorherigen Schlüssel [NIS2009a] oder durch Neuaushandlung eines Schlüssels zwischen den Kommunikationspartnern. Zwischen der Ermittlung eines neuen Schlüssels und dem Ablauf des alten Schlüssels besitzen beide Schlüssel eine Gültigkeit. Ist der erste Schlüssel abgelaufen, kann übergangslos auf den erneuerten Schlüssel umgeschaltet werden. Der erste Schlüssel verliert seine Gültigkeit und wird gelöscht. Da der Counter durch eine Prüfsumme abgesichert ist und verschlüsselt werden kann, ist ein Angreifer nicht in der Lage „Replay-Angriffe“ durchzuführen. Auch kann durch die verschlüsselten Daten nicht auf den Schlüssel geschlossen werden. Als Erweiterung ist eine Aushandlung der Schlüsselgültigkeit denkbar, mit der anwenderseitig die Einsatzdauer eines Schlüssels definiert werden kann.

- **PAD** (Padding für optionale Verschlüsselung)

Wird eine Verschlüsselung durchgeführt, wird ggf. ein Auffüllen der Nutzdaten auf die Mindestlänge durchgeführt (engl. padding). Damit der Empfänger dies erkennen kann, beinhaltet der Security Header ggf. ein Datenfeld welches die Anzahl an hinzugefügten Bytes angibt.

7.3.2 Nicht-Echtzeitfähige Kommunikation

Realisierungsalternative 3 setzt auf Schicht 2 (bzw. in Schicht 3) des ISO/OSI-Referenzmodells an. Diese gewählte Alternative erlaubt die Absicherung der nicht-echtzeitfähigen IP-basierten Kommunikation durch das IPSec-Protokoll, welches auf derselben Schicht zu finden ist [INT2005d]. Das IPSec-Protokoll wird in zahlreichen RFCs spezifiziert und bietet einen großen Umfang an umsetzbaren Schutzmaßnahmen. Die vollständige Umsetzung würde daher umfangreiche Ressourcen in Anspruch nehmen. Aus diesem Grund wird die Umsetzung nur notwendiger Maßnahmen angestrebt, die im Rahmen der in dieser Arbeit vorgestellten ergänzenden Schutzmaßnahmen benötigt werden. Dabei handelt es sich zum einen um die Authentifizierung bzw. den Schlüsselaustausch über das IKEv2-Protokoll [INT2005a] sowie die Absicherung der Datenpakete nach Vorgaben durch IPSec.

Zur gegenseitigen Authentifizierung wird durch das IPSec-Protokoll das IKEv2-Verfahren genutzt. IPSec baut mit Hilfe von IKEv2 sogenannte Security Association (SA) zwischen Kommunikationspartnern auf, über die weitere Parameter der Verbindung ausgehandelt werden. Dazu gehören bspw. Parameter zum Schlüsselaustausch (z.B. Diffie-Hellman-Verfahren), Sitzungsinformationen oder das zu verwendende kryptografische Verfahren. Zur Authentifizierung der Kommunikationspartner werden bei IKEv2 die digitalen Zertifikate der Komponenten ausgetauscht. Zur Absicherung der Datenpakete erlaubt IPSec zwei Ansätze, wobei zwischen dem Tunnel-Modus und dem Transport-Modus unterschieden wird. Das als Tunnel-Modus bezeichnete Verfahren ermöglicht primär die geheime Übertragung, in Form von Punkt-zu-Punkt Verbindungen über das Internet (VPN-Tunnel). Dazu werden die Ursprungsdaten in ein neues Datenpaket gekapselt. Der Transport-Modus erweitert die Datenpakete vergleichbar zum Ansatz in Abbildung 7-11. Gleichzeitig werden die TCP/IP bzw. UDP/IP-Daten mit geschützt.

Neben den Modi zur Übertragung werden zwei Ansätze zur Paketerweiterung in IPSec definiert, welche als Authentication Header (AH) [INT2005b] und als Encapsulated Security Payload (ESP) [INT2005c] bezeichnet werden. Die Verwendung von AH ermöglicht den Schutz von nicht-veränderbaren Daten des IP-Headers. Da jedoch in Netzwerken ggf. Verfahren wie NAT (Network Address Translation) verwendet werden, ist die Verwendung von AH nicht sinnvoll, da bspw. durch NAT die nicht-veränderbaren Daten geändert werden. Demnach könnte ein AH-gesichertes Datenpaket nach einer NAT-Operation nicht mit authentifiziert werden. Zudem sieht der AH-Modus keinen Schutz der Vertraulichkeit (→**I**) der zu übertragenden Daten vor, sondern ausschließlich die Authentizität (→**S**) und Integrität (→**T**) der Daten ab. Im Falle von ESP erfolgt der Schutz der Vertraulichkeit sowie der Integrität und der Authentizität der Daten. ESP ist darüber hinaus kompatibel zu NAT. Die dabei anwendbaren Verfahren zur Absicherung der Daten sind für den Nutzer wählbar und werden, wie bei AH, zu Beginn der Kommunikation ausgehandelt.

Während primär die Verwendung des Transport-Modus sinnvoll ist und optional der Tunnel-Modus angewendet werden kann (bspw. bei anlagenübergreifender Kommunikation), ist zwischen den Kommunikationspartnern während des sicheren Verbindungsaufbaus via IKEv2 auszuhandeln, welche Paketerweiterung (AH oder ESP) verwendet werden soll.

7.4 Realisierung der IT-Sicherheitsschicht

In Abschnitt 6 sind die die ergänzenden Schutzmaßnahmen eines erweiterten Schutzkonzepts beschrieben worden. Diese ergänzenden Schutzmaßnahmen erlauben einen gemeinsam verknüpften Schutz, der in Abschnitt 7.1 in einer sogenannten IT-Sicherheitsschicht vereint wird. In Abbildung 7-4 sind die Funktionen der IT-Sicherheitsschicht dargestellt worden. Entsprechend Realisierungsalternative 3 wird die IT-Sicherheitsschicht im Kommunikationsstack nahe dem Zugriffsmedium platziert. Für die Platzierung der IT-Sicherheitsschicht in einer Komponente ergibt sich nach Abbildung 3-1 die in Abbildung 7-13 dargestellte Form.

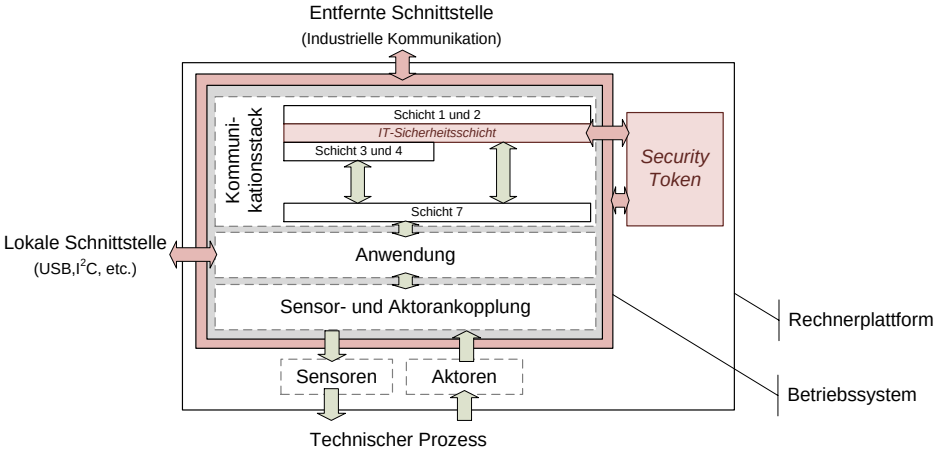


Abbildung 7-13: Einbindung der IT-Sicherheitsschicht in der Komponente

Wie erläutert, vereint die IT-Sicherheitsschicht die ergänzenden Schutzmaßnahmen. Die Abbildung 7-13 zeigt die IT-Sicherheitsschicht als Bestandteil des Kommunikationsstack als Zwischeninstanz zwischen Anwendung und Zugriff auf das Übertragungsmedium. Das Security Token ist als passives Bauteil an die IT-Sicherheitsschicht angebunden und dient der Unterstützung zur Zustandsüberwachung (z.B. zur Erkennung unautorisierter Veränderungen über die lokale Schnittstelle) sowie zur sicheren Verwahrung kryptografische Informationen wie Schlüsseln.

Die Umsetzung der IT-Sicherheitsschicht erfolgt im Zuge des durch das Bundesministerium für Bildung und Forschung (BMBF) geförderten Projekts „SEC_PRO“[1]. Aufgrund des großen Umfanges der Arbeiten zur Erstellung der Schicht, wird die Protokollerweiterung in Teilaufgaben gegliedert und an den projektausführenden Hochschulen bearbeitet. Die Hochschule Hannover (HsH) sowie das „Institut für Industrial IT“ (InIT) an der Hochschule Ostwestfalen-Lippe (HS OWL) bearbeiten dazu schwerpunktmäßig Teilaufgaben, wobei die Hochschulen durch industrielle Partner unterstützt werden.

Schwerpunkt der Hochschule Ostwestfalen-Lippe liegt in der Implementierung der gegenseitigen Authentifizierung sowie der lokalen Schlüsselverwaltung und des globalen Public Key Management. An der Hochschule Hannover fokussieren sich die Arbeiten auf die Absicherung der Kommunikation und der Implementation der kryptografischen Funktionen. Zusätzlich erfolgt die Einbindung der Zustandsüberwachung sowie der Alarmsteuerung an der Hochschule Hannover. Gemeinsam durch beide Hochschulen wird die Anbindung der Security Token und der lokalen Schlüssel- und Zertifikatsspeicherung realisiert.

[1] SEC_PRO – Sichere Produktion mit verteilten Automatisierungssystemen | FKZ: 17060A10

Ein weiteres Aufgabengebiet der Hochschule Hannover ist die Einbindung der IT-Sicherheitsschicht in die PROFINET-Protokollsoftware. Die Protokollsoftware wird seitens der KW Software GmbH zur Verfügung gestellt. Die IT-Sicherheitsschicht wird in Form eines Sende- und Empfangspuffers eingebunden. Bei ein- und ausgehenden Datenpaketen erfolgt eine Meldung an die Schicht. Ist die IT-Sicherheitsschicht inaktiv, so werden die Pakete ohne Bearbeitung freigegeben bzw. durchgeleitet. Ist die Protokollerweiterung aktiv, wird seitens der Schicht eine Verarbeitung der Datenpakete entsprechend der ergänzenden Schutzmaßnahmen durchgeführt.

Gemäß den Anforderungen in Tabelle 5-3 durch die Automatisierungstechnik an Schutzmaßnahmen für die IT-Sicherheit, ist eine direkte Beurteilung der Anforderungen für die (einzelnen) ergänzenden Schutzmaßnahmen erschwert, da die ergänzenden Schutzmaßnahmen gemeinsam (kryptografisch) verknüpft sind. Die Zusammenfassung der ergänzenden Schutzmaßnahmen in einer IT-Sicherheitsschicht erlaubt eine gemeinsame Bewertung hinsichtlich der gestellten Anforderungen aus der Automatisierungstechnik.

Die Umsetzbarkeit **A6** der IT-Sicherheitsschicht hängt zusammen mit der Verfügbarkeit von Lösungen zu den ergänzenden Schutzmaßnahmen, welche in Abschnitt 6.2 erläutert wurden. Hierzu existieren zahlreiche frei verfügbare Implementierungen, die jedoch nicht für eine Anwendung in der Automatisierungstechnik konzipiert sind. Eine Anpassung bzw. Umsetzung der Lösungen für die Automatisierungstechnik ist jedoch grundsätzlich möglich. Deutlich wurde zudem, dass die IT-Sicherheitsschicht durch die ihr zugrunde liegenden ergänzenden Schutzmaßnahmen an zukünftige Strukturveränderungen eines Automatisierungssystems anpassbar ist, weshalb die Flexibilität und Skalierbarkeit der Lösung gegeben ist (→**A5)**. Zwar entsteht durch die Verwaltung der IT-Sicherheitsschicht ein gewisser Betriebsaufwand **A4**, doch ist dieser durch die transparente Integration der Schicht nach Realisierungsalternative 3 überschaubar. Auch im Hinblick auf die Verfügbarkeit **A2** kann so trotz der zusätzlichen ergänzenden Schutzmaßnahmen gewährleistet werden, dass diese die Verfügbarkeit nicht gravierend beeinflussen.

Bezüglich der Echtzeitanforderungen **A1** und der Einsatzdauer **A3** der IT-Sicherheitsschicht, ist eine Betrachtung der kryptografischen Funktionen notwendig, die die Basis der ergänzenden Schutzmaßnahmen bilden. Die teils aufwändigen mathematischen Verfahren können einen erheblichen Einfluss auf die Echtzeitfähigkeit des Automatisierungssystems haben. Die Einsatzdauer der kryptografischen Funktionen hängt von der Sicherheit der verwendeten kryptografischen Verfahren ab. Es muss gewährleistet sein, dass die gewählten kryptografischen Verfahren eine Einsatzdauer ermöglichen, die den Lebenszyklen von Automatisierungssystemen entsprechen und über diesen Zeitraum ein ausreichendes Maß an Sicherheit bieten sowie die Echtzeitfähigkeit des Automatisierungssystems nicht beeinflussen.

Um die Anforderungen **A1** und **A3** der Automatisierungstechnik endgültig bewerten zu können, ist eine Evaluierung der IT-Sicherheitsschicht bzw. von relevanten kryptografischen Funktionen durchzuführen, welche in Kapitel 8 erfolgt.

8 Evaluierung der IT-Sicherheitsschicht

Die in Kapitel 6 beschriebenen ergänzenden Schutzmaßnahmen, wurden in Kapitel 7 in einer IT-Sicherheitsschicht zusammengefasst und am Beispiel von PROFINET integriert. Die IT-Sicherheitsschicht verwendet kryptografische Verfahren, die einen Einfluss auf die Echtzeitfähigkeit sowie Einsatzdauer der IT-Sicherheitsschicht bzw. das Automatisierungssystem haben können. Kapitel 8 dient der konkreten Auswahl und Evaluierung von relevanten kryptografischen Funktionen und deren Einfluss in der IT-Sicherheitsschicht.

In Abschnitt 8.1 werden zunächst kryptografische Funktionen und verschiedenen Rechnerplattformen zur Evaluierung ausgewählt. Es folgt in Abschnitt 8.2 die Messung und Evaluierung der Ausführungszeiten der verschiedenen kryptografischen Funktionen, mit und ohne IT-Sicherheitsschicht. Abschließend wird die Evaluierung zusammenfassend bewertet.

8.1 Auswahl kryptografischer Funktionen und Messverfahren

In Abschnitt 8.1.1 erfolgt eine detaillierte Auswahl von kryptografischen Verfahren, wobei die mögliche Einsatzdauer und Sicherheit der Verfahren im Vordergrund stehen. Zur späteren Messung werden Rechnerplattformen ausgewählt, die das Leistungsspektrum von Komponenten der Automatisierungstechnik widerspiegeln sollen. Zudem wird das Messverfahren zur Evaluierung der IT-Sicherheitsschicht erläutert.

8.1.1 Relevante kryptografische Funktionen

Aufgrund der großen Bandbreite verfügbarer symmetrischer sowie asymmetrischer Verfahren ist zu evaluieren, welche Verfahren im Rahmen der gegebenen Aufgabenstellung verwendet werden können. Dabei soll vor allem die Akzeptanz und Verbreitung der jeweiligen Verfahren als Auswahlkriterium herangezogen werden. Zusätzlich werden nationale bzw. internationale Empfehlungen seitens des NIST [NIS2011], BSI [BSI2008c], NSA [NSA2013] sowie ENISA [ENI2013] herangezogen. Diese Empfehlung berücksichtigt einen sicheren Einsatz der jeweiligen Kryptofunktion über das Jahr 2030 hinaus. Tabelle 8-1 führt die empfohlenen kryptografischen Funktionen auf.

Voraussichtliche Einsatzdauer	Minimale Schlüssellänge	Ver- bzw. Entschlüsselungs-verfahren	Asymmetrische kryptografische Verfahren		Prüfsummen für MAC bzw. Signaturerstellung
			RSA	ECC	
2030+	*128*	*AES-128*	*3072*	*256*	*SHA-256*
2030++	192	AES-192	7680	284	SHA-384
2030+++	256	AES-256	15360	512	SHA-512

Tabelle 8-1: Empfohlene kryptografische Verfahren und Schlüssellängen in Bit

Grundlegende Vorgabe ist die minimale Schlüssellänge der Verfahren und die voraussichtliche Einsatzdauer der kryptografischen Verfahren. Vertreten sind der AES-Algorithmus als Ver- bzw. Entschlüsselungsverfahren, ECC und RSA als asymmetrische Verfahren sowie der SHA-2-Algorithmus zur Erstellung von MACs bzw. Signaturen sowie zur Zustandsüberwachung (siehe Abschnitt 6.2). Grundlage dieser Empfehlungen ist die jeweilige kryptografische Stärke der Verfahren. Die kryptografische Stärke wird anhand des Rechenaufwandes zum Brechen (Kryptoanalyse) des kryptografischen Verfahrens bzw. des zu Grunde liegenden

mathematischen Problems und der dabei verwendeten Schlüssellänge definiert. Da mit steigender kryptografischer Stärke der Aufwand zur Berechnung der kryptografischen Funktionen steigt, ist aus Effizienzgründen für ressourcen-beschränkte Automatisierungskomponenten ein Kompromiss aus kryptografischer Stärke und möglicher Einsatzdauer zu treffen. Aus diesem Grund kommen die in Zeile „2030+“ genannten Verfahren zum Einsatz. Allgemein handelt es sich bei den in Tabelle 8-1 gezeigten kryptografischen Funktionen um akzeptierte Kryptofunktionen, die eine weite Verbreitung finden. Entsprechend stehen diese Kryptofunktionen unter ständiger Beobachtung von Kryptoanalytikern (vgl „Kerckhoffs‘ Prinzip“ [SCH2006a]). Sowohl die Akzeptanz bzw. Verbreitung der kryptografischen Verfahren und die mögliche Einsatzdauer heben die Bedeutung der Empfehlungen für die kryptografischen Verfahren aus Tabelle 8-1 für die Automatisierungstechnik hervor.

Aus diesem Grund stellen die in Tabelle 8-1 gezeigten kryptografischen Verfahren die Grundlage für die weitere Betrachtung dar. Auffällig ist, dass derzeit keine stromorientierten Verfahren empfohlen werden, was durch [BSI2008c] unterstrichen wird. Einzig die Stromchiffre Rabbit [BVP2003] findet Erwähnung, jedoch keine weite Verbreitung. Arbeiten bezüglich der Verwendung von Stromchiffren in der Automatisierungstechnik [WKS2012], sind daher als kritisch zu sehen, da deren Sicherheit nicht endgültig bewertet wurde. Aktuelle Arbeiten zur Verwendung der Quantenkryptografie in der Automatisierungstechnik sind vielversprechend und bieten ein hohes Maß an kryptografischer Sicherheit [SCH2011]. Jedoch befindet sich die Quantenkryptografie noch in einem experimentellem Zustand.

8.1.2 Evaluierungsplattformen und -verfahren

Zur Evaluierung der kryptografischen Funktionen werden drei Plattformen herangezogen. Die drei Plattformen decken ein breites Leistungsspektrum der einsetzbaren Komponenten im Umfeld der Automatisierungstechnik ab. Tabelle 8-2 zeigt die grundlegenden Eigenschaften der drei Plattformen sowie deren mögliches Einsatzgebiet und das Messverfahren.

	Plattform 1	**Plattform 2**	**Plattform 3**
System-konfiguration	Raspberry-PI (ARM1176JZF-S) 150 MHz (getaktet) 256 MByte RAM Linux (Kernel 3.6.11)	PowerPC-Plattform (Freescale MPC 8313e) 330 MHz 64 MByte RAM Linux (Kernel 2.6.27.57)	Standard-PC (Intel x86) 1,4 GHz 512 MByte RAM Windows XP
Referenz für:	(stark) ressourcen-beschränkte dezentrale Peripherie	Ressourcen-beschränkte dezentrale Peripherie, lokale Steuerungs- und Regelungsaufgaben	SPS, zentrale Steuerungs- und Regelungsaufgaben
Messung der Ausführungszeit der Verfahren	Messung mit Hilfe der Linux-Systemfunktion *gettimeofday()* mit einer Auflösung von 1 µs.		Windows-Funktion *QueryPerformanceCounter()* und einer Auflösung unter 1 µs

Tabelle 8-2: Evaluierungsverfahren und Messplattformen

Das breite Leistungsspektrum der drei gewählten Systemkonfigurationen erlaubt die Beurteilung der Einsatzfähigkeit von kryptografischen Funktionen in den unterschiedlichen Einsatzgebieten. Die Plattformen decken zusätzlich verschiedene Prozessorarchitekturen und Betriebssysteme ab, und damit ein breites Feld an verwendeter Software im Umfeld der Automatisierungstechnik. Die kryptografischen Funktionen selbst werden durch die Softwarebibliothek „OpenSSL“ [OPE2014] zur Verfügung gestellt, weshalb die Messung software-basiert

erfolgt. Basis der Evaluierung ist die Ausführungszeit der kryptografischen Funktionen auf den Plattformen.

Zur Messung der Ausführungszeit bearbeiten die Plattformen die kryptografischen Funktionen bzw. die IT-Sicherheitsschicht, wobei verschiedene zu verarbeitende Datenpaketgrößen in Abhängigkeit der zu bearbeitenden kryptografischen Funktion zur Verarbeitung vorgegeben werden. Um die Ausführungszeit ermitteln zu können, werden Systemfunktionen der Betriebssysteme als Zeitstempel genutzt, die eine Auflösung von 1 µs ermöglichen. Die Genauigkeit der Systemfunktionen hängt zwar von der verwendeten Plattform bzw. dessen Hardware ab, trotzdem kann eine Genauigkeit von ca. 1 µs erreicht werden [MIC2014], [THÜ2006], [KOC2011]. Die Differenz der Zeitstempel zwischen Beginn und Ende der Ausführung der kryptografischen Funktionen bildet die Ausführungszeit t_{crypto}. Diese Zeit stellt die Dauer dar, in der eine Plattform ein ein- bzw. ausgehendes Datenpaket kryptografisch verarbeitet hat. Ausgewertet werden die in Zeile 1 von Tabelle 8-1 aufgeführten kryptografischen Verfahren, wobei für die blockorientierten kryptografischen Verfahren die in Abschnitt 6.2.2 genannten Betriebsmodi verwendet werden. Da es sich bei den Plattformen nicht um Echtzeitbetriebssysteme handelt, treten Schwankungen in der Ausführungszeit auf. Um Schwankung berücksichtigen zu können, wird zum Mittelwert der Ausführungszeit aus 500 Messungen dessen Standardabweichung als Bewertungsgrundlage hinzugezogen.

Wie in Abschnitt 7.2.1 beschrieben, ermöglicht das PROFINET-Protokoll Zykluszeiten bis zu 31,25 µs bei einer taktsynchronen (IRT)-Kommunikation. Die typische minimale echtzeitfähige PROFINET-(RT)-Kommunikation liegt hingegen im Bereich zwischen 1 ms und 2 ms [FFV2011]. In Anbetracht der software-basierten Umsetzung der IT-Sicherheitsschicht wird daher die minimal zu erfüllende Zykluszeit für eine bidirektionale Kommunikation zu 1 ms definiert. Da die folgenden Messungen sich auf eine unidirektionale Verarbeitung der Kommunikationsbeziehung (entweder Senden oder Empfangen) beziehen, halbiert sich die minimal zu erfüllende Ausführungszeit.

$$t_y = t_{krypto} + t_{it-sicherheitsschicht} + t_{anwendung} \leq \frac{1ms}{2}$$

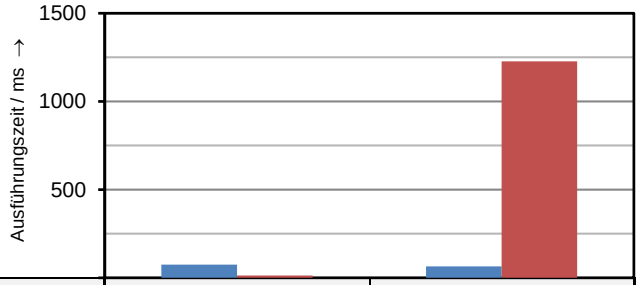
Die Addition der Ausführungszeit der kryptografischen Funktion sowie der IT-Sicherheitsschicht zuzüglich einer Anwendung auf der jeweiligen Plattform, sollte daher geringer sein als 500 µs. Da für die Anwendung und die Verwaltungsaufgaben seitens der IT-Sicherheitsschicht eine Reserve von 20 % angenommen wird, reduziert sich die maximale Ausführungszeit der kryptografischen Funktionen um weitere 100 µs auf $t_x = t_y \cdot 0{,}8$ (400 µs). Ziel der Messung ist die Feststellung der Echtzeitfähigkeit (siehe Tabelle 5-3 Anforderung **A1**) der in Abschnitt 6.2 vorgestellten kryptografischen Funktionen zum Schutz der Kommunikation durch die IT-Sicherheitsschicht unter Berücksichtigung der zu erfüllenden bzw. definierten Zykluszeit nach gezeigter Formel. Bei der Messung werden die in Abschnitt 8.1.1 gezeigten relevanten symmetrischen und asymmetrischen kryptografischen Funktionen auf diese Vorgabe für die echtzeitfähige Kommunikation überprüft.

8.2 Messung und Evaluierung der IT-Sicherheitsschicht

Die Messung ist zunächst auf die Ausführungszeit t_{krypto} der symmetrischen sowie asymmetrischen kryptografischen Funktionen ohne IT-Sicherheitsschicht und ohne Anwendung fokussiert (→8.2.1 und 8.2.2), da zunächst die rechenzeitintensiven kryptografischen Funktionen im Fokus stehen sollen. Im Anschluss an diese Messung erfolgt die Festlegung auf geeignete kryptografische Funktionen für die echtzeitfähige Kommunikation. Anhand dieser Festlegung folgt anschließend deren Anwendung und Messung in der IT-Sicherheitsschicht des erweiterten PROFINET-Protokollstacks und anschließender Bewertung.

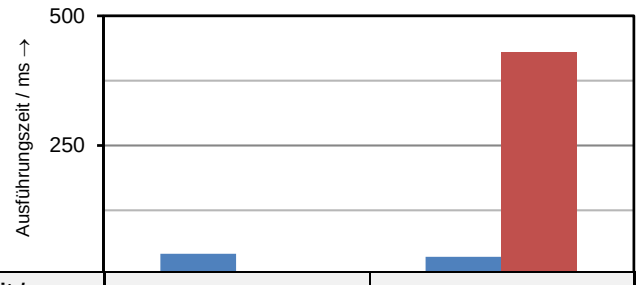
8.2.1 Messung und Bewertung der asymmetrischen Verfahren

Asymmetrische Verfahren verwenden ein sogenanntes Schlüsselpaar (siehe Abschnitt 4.1). Während mit dem Public-Key Daten verschlüsselt bzw. verifiziert werden, so erlaubt der Private-Key, Daten zu signieren oder zu entschlüsseln. Da beide Teile des Schlüsselpaares für verschiedene Aufgaben eingesetzt werden können und die Algorithmen RSA und ECC spezifische Eigenschaften in der Implementierung aufweisen, die eine Vergleichbarkeit der Ausführungszeiten beeinträchtigen würden, wird lediglich das Signieren (Private-Key-Operation) und das Verifizieren (Public-Key-Operation) der Algorithmen gemessen. Signiert bzw. verifiziert wird die SHA-256-Prüfsumme (also 32 Byte) beliebiger Daten. Obwohl die Messung sich lediglich auf das Signieren und Verifizieren bezieht, so sind die Ausführungszeiten doch auf das Ver- und Entschlüsseln übertragbar. Die Ausführungszeiten sind Angaben der Standardabweichung für den gemittelten Wert aus einer Anzahl von 500 Messungen.



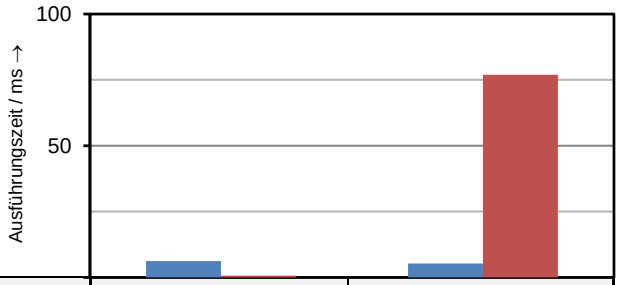
Ausführungszeit / ms N = 500	Public-Key Operation	Private-Key Operation
ECC-256	74,98 ± 1,86	64,61 ± 1,45
RSA-3072	13,38 ± 0,47	1227,35 ± 4,84

Tabelle 8-3: Asymmetrische Verfahren / Plattform 1



Ausführungszeit / ms N = 500	Public-Key Operation	Private-Key Operation
ECC-256	41,15 ± 0,38	35,52 ± 0,34
RSA-3072	4,26 ± 0,06	429,30 ± 1,17

Tabelle 8-4: Asymmetrische Verfahren / Plattform 2



Ausführungszeit / ms N = 500	Public-Key Operation	Private-Key Operation
ECC-256	6,22 ± 0,20	5,30 ± 0,33
RSA-3072	0,70 ± 0,04	76,94 ± 1,72

Tabelle 8-5: Asymmetrische Verfahren / Plattform 3

Wie die Tabellen 8-3 bis 8-5 zeigen, ist die Ausführung einer Public-Key Operation auf Basis von RSA um ein vielfaches schneller als eine Private-Key Operation. Das Ungleichgewicht bei den Ausführungszeiten zwischen beiden Operationen schränkt den Einsatz von RSA für die echtzeitfähige bidirektionale Kommunikation ein, da dafür auch die langsamere Private-Key Operationen benötigt wird. Der ECC-Algorithmus weist dieses Ungleichgewicht der Ausführungszeiten zwischen Public- und Private-Key Operation nicht auf.

Allgemein liegen die Ausführungszeiten in den Tabellen 8-3 bis 8-5 im Bereich mehrerer Millisekunden. Asymmetrische Verfahren sind demnach nicht geeignet für die echtzeitfähige Kommunikation in einem PROFINET-Netzwerk, da die in Abschnitt 8.1.2 definierte minimale Zykluszeit von 400 µs nicht unterschritten wird. Da darüber hinaus die Anwendung der Plattform (bspw. Mess- und Stellwertbearbeitung) und die IT-Sicherheitsschicht auszuführen sind, würde sich die Ausführungszeit weiter vergrößern. Primär sind asymmetrische Verfahren zur gegenseitigen Authentifizierung konzipiert und wie in Abschnitt 6.2.1 gezeigt notwendig. Allgemein zeigt sich zusätzlich, dass die ECC-Verfahren bei gleicher kryptografischer Stärke und kleinerer Schlüssellänge eine geringere Ausführungszeit benötigen, weshalb ECC dem RSA-Algorithmus vorzuziehen ist.

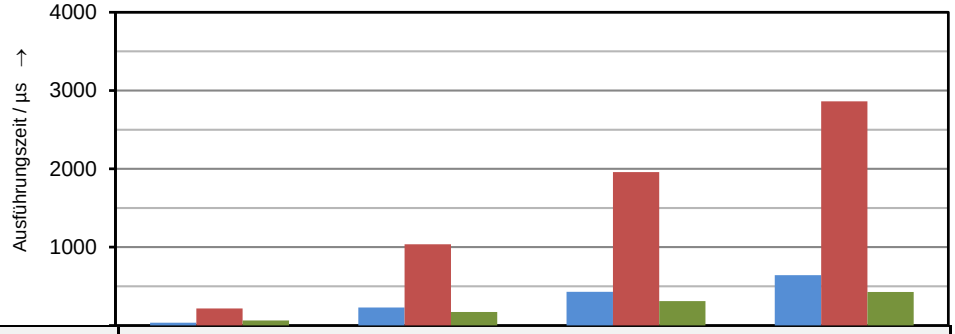
8.2.2 Messung und Bewertung der symmetrischen Verfahren

Bei den symmetrischen Verfahren verwenden beide Kommunikationspartner einen gemeinsamen Schlüssel. Mit Hilfe dieses symmetrischen Schlüssels können Daten ver- bzw. entschlüsselt und/oder für ein MAC-Verfahren genutzt werden (vgl. Abschnitt 6.2.2). Da die Rechenoperationen für Ver- und Entschlüsselung bzw. Erstellung und Überprüfung eines MACs in etwa gleiche Rechenzeit benötigen, wird zur Evaluierung der symmetrischen Verfahren für die echtzeitfähige Kommunikation nur eine (unidirektionale) Kommunikationsrichtung betrachtet (Entschlüsselung bzw. Überprüfung eines MACs bei Empfang eines Datenpakets).

Die Messungen der symmetrischen Verfahren werden getrennt nach MAC-Verfahren und Ver- bzw. Entschlüsselung durchgeführt. Da das primäre Anwendungsfeld der symmetrischen Verfahren der Schutz großer zusammenhängender Datenmengen ist, werden bei der Evaluierung der symmetrischen Verfahren im Gegensatz zu den asymmetrischen Verfahren typische Prozessdatengrößen (40 Byte, 480 Byte, 960 Byte, 1440 Byte) als zusätzliche Bewertungsgrundlage herangezogen.

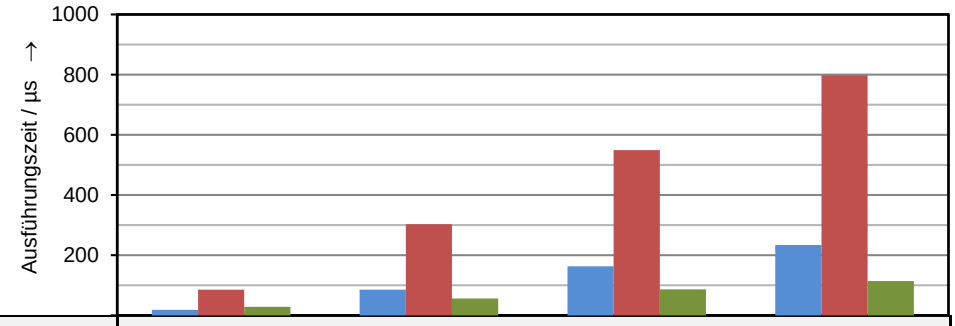
Gegenüberstellung der MAC-Verfahren

Tabelle 8-6 bis Tabelle 8-8 zeigen die Zusammenfassung der Messung der MAC-Verfahren auf den verschiedenen Plattformen. Die Ausführungszeiten sind in µs angegeben und stellen den Mittelwert sowie die Standardabweichung aus 500 Messungen dar.



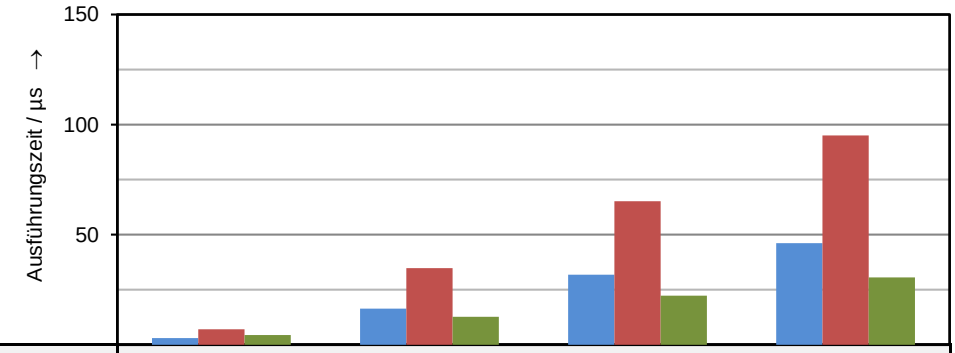
Ausführungszeit / µs N = 500	Prozessdatengröße			
	40 Byte	480 Byte	960 Byte	1440 Byte
CMAC (AES-128)	34,07 ± 10,10	230,12 ± 57,37	429,09 ± 54,42	643,04 ± 73,66
GMAC (AES-128)	216,99 ± 46,63	1036,12 ± 91,99	1958,52 ± 184,63	2863,01 ± 218,80
HMAC (SHA-256)	64,06 ± 19,48	171,53 ± 24,63	310,16 ± 59,32	426,54 ± 72,79

Tabelle 8-6: Symmetrische Verfahren / MAC-Verfahren / Plattform 1



Ausführungszeit / µs N = 500	Prozessdatengröße			
	40 Byte	480 Byte	960 Byte	1440 Byte
CMAC (AES-128)	18,87 ± 9,31	85,50 ± 10,86	163,23 ± 15,89	234,22 ± 16,79
GMAC (AES-128)	85,87 ± 13,73	303,16 ± 22,83	549,55 ± 31,81	798,57 ± 35,30
HMAC (SHA-256)	28,49 ± 4,41	56,30 ± 7,64	86,89 ± 9,49	114,18 ± 10,83

Tabelle 8-7: Symmetrische Verfahren / MAC-Verfahren / Plattform 2



Ausführungszeit / µs N = 500	Prozessdatengröße			
	40 Byte	480 Byte	960 Byte	1440 Byte
CMAC (AES-128)	3,05 ± 1,68	16,43 ± 4,66	31,81 ± 10,50	46,15 ± 6,17
GMAC (AES-128)	7,00 ± 0,18	34,79 ± 8,77	65,19 ± 9,55	95,09 ± 6,33
HMAC (SHA-256)	4,42 ± 0,51	12,70 ± 0,66	22,30 ± 4,99	30,58 ± 5,86

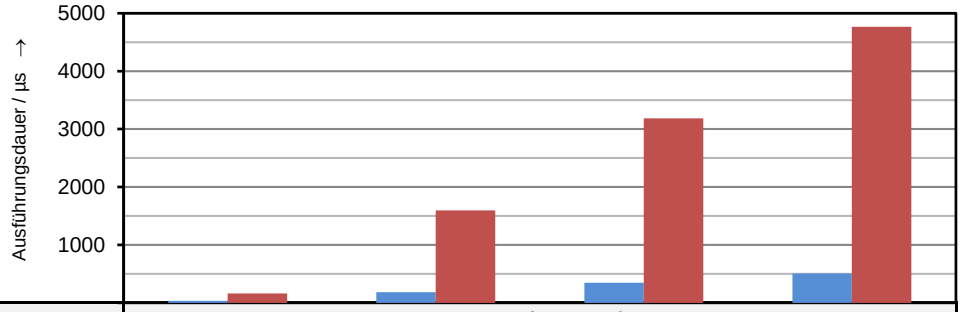
Tabelle 8-8: Symmetrische Verfahren / MAC-Verfahren / Plattform 3

Der CMAC-Algorithmus zeigt bei kleinen Prozessdatengrößen (40 Byte) in den Tabellen 8-6 bis 8-8 allgemein die geringste Ausführungszeit auf. Mit zunehmender Prozessdatengröße unterschreitet der HMAC-Algorithmus die Ausführungszeit des CMAC-Algorithmus, wie den Tabellen entnommen werden kann. Der GMAC-Algorithmus weist auf den Testplattformen insgesamt die größte Ausführungszeit auf, die um ein vielfaches größer als die des HMAC- und CMAC-Algorithmus ist. Im Vergleich ist mit zunehmender Prozessdatengröße die Ausführungszeit beim HMAC-Algorithmus auf Basis des SHA-256 insgesamt am geringsten.

Da die überwiegende Prozessdatengröße in der Automatisierungstechnik im Bereich kleiner Datenmengen unter 480 Byte liegt (siehe [FFV2011]), ist der Einsatz eines MACs auf allen Plattformen möglich. Dies lässt sich am aufgestellten Kriterium in Abschnitt 8.1.2 überprüfen. So ist bspw. selbst die stark-ressourcenbeschränkte Plattform 1 in Tabelle 8-6 in der Lage 480 Byte an Daten mit Hilfe des HMAC-Algorithmus in 171,53 µs abzusichern, was unterhalb der definierten Grenze von 400 µs liegt. Den Messungen kann zudem ein linearer Anstieg der Ausführungszeit mit zunehmender Prozessdatengröße entnommen werden.

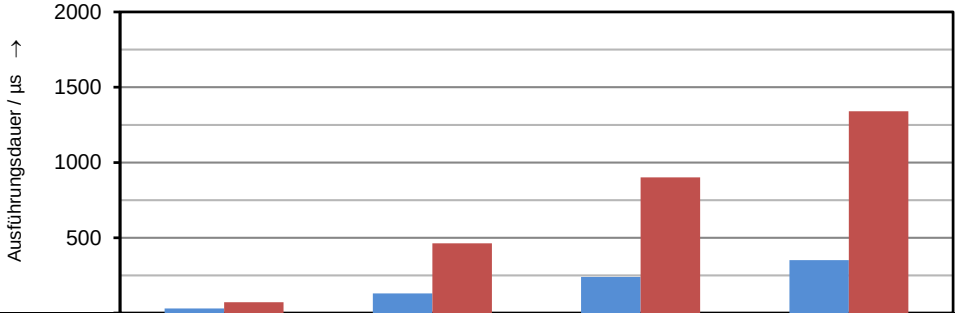
Gegenüberstellung der Ver- bzw. Entschlüsselungsverfahren

Für die vertrauliche Übertragung von Informationen ist eine Ver- bzw. Entschlüsselung notwendig. Tabelle 8-9 bis Tabelle 8-11 zeigen die Messung der Ver- bzw Entschlüsselungsverfahren. Die Ausführungszeiten sind in µs angegeben und stellen den Mittelwert sowie die Standardabweichung aus 500 Messungen dar. Die AES-128-GCM-Implementierung weist gegenüber der AES-128-CBC-Implementierung eine allgemein höhere Ausführungszeit auf.



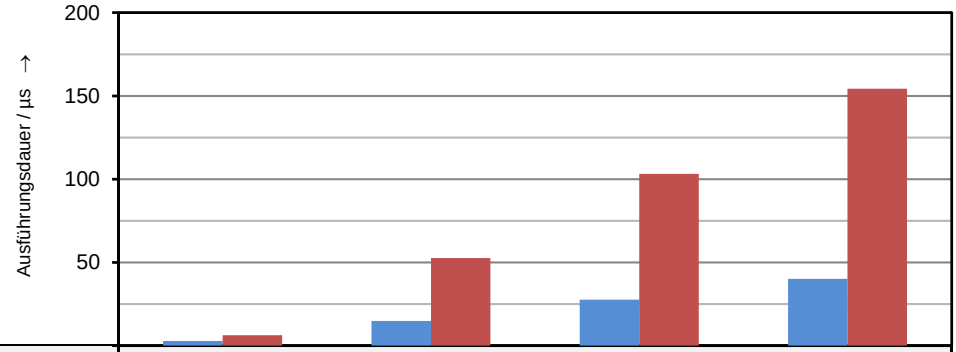
Ausführungszeit / µs N = 500	Prozessdatengröße			
	40 Byte	480 Byte	960 Byte	1440 Byte
AES-128-CBC	34,55 ± 13,93	183,34 ± 34,10	346,08 ± 46,83	507,85 ± 63,05
AES-128-GCM	161,85 ± 32,38	1595,36 ± 126,54	3186,02 ± 118,96	4765,32 ± 158,72

Tabelle 8-9: Symmetrische Verfahren / Ver. bzw. Entschlüsselung / Plattform 1



Ausführungszeit / µs N = 500	Prozessdatengröße			
	40 Byte	480 Byte	960 Byte	1440 Byte
AES-128-CBC	30,42 ± 6,98	129,87 ± 10,47	240,07 ± 14,51	351,70 ± 29,20
AES-128-GCM	72,36 ± 9,00	463,67 ± 30,53	901,22 ± 39,63	1340,77 ± 55,19

Tabelle 8-10: Symmetrische Verfahren / Ver. bzw. Entschlüsselung / Plattform 2



Ausführungszeit / µs N = 500	Prozessdatengröße			
	40 Byte	480 Byte	960 Byte	1440 Byte
AES-128-CBC	2,86 ± 0,40	14,82 ± 4,49	27,64 ± 3,97	40,09 ± 3,11
AES-128-GCM	6,29 ± 0,52	52,62 ± 3,63	103,24 ± 2,20	154,31 ± 4,05

Tabelle 8-11: Symmetrische Verfahren / Ver. bzw. Entschlüsselung / Plattform 3

Da die Ver- und Entschlüsselung ausschließlich der Sicherung der Vertraulichkeit dient, ist zusätzlich ein MAC zu erstellen (siehe Abschnitt 6.2.2). Der MAC wird nach der Verschlüsselung der Daten errechnet, um beim Empfänger vor Entschlüsselung der Daten die Integrität der verschlüsselten Daten prüfen zu können. Daraus ergibt sich bspw. bei einer verschlüsselten und gesicherten Übertragung die Kombination: „AES-128-CBC + HMAC (SHA-256)“. Obwohl der AES-GCM-Algorithmus diese Eigenschaft parallel erfüllt und zusätzlich für hohe Datendurchsätze und geringe Ausführungszeiten konzipiert ist, so ist die Kombination von AES-128-CBC mit HMAC (SHA-256) trotzdem um ein Vielfaches schneller als die AES-GCM-Lösung. Ein Grund für diesen Nachteil liegt möglicherweise in der Optimierung des AES-GCM-Algorithmus für eine Ausführung in Hardware. Daher ist in der vorliegenden softwarebasierten Evaluierung der AES-CBC- dem AES-GCM-Algorithmus vorzuziehen.

Bezogen auf den AES-CBC-Algorithmus in den Tabellen 8-10 und 8-11 zeigt sich allgemein eine Ausführungszeit, die das Kriterium von 400 µs aus Abschnitt 8.1.2 erfüllt. Einzig Plattform 1 in Tabelle 8-9 erfüllt das Kriterium nicht. Wird jedoch davon ausgegangen, dass die typische Prozessdatengröße unterhalb von 480 Byte liegt, so erfüllt auch Plattform 1 das Kriterium hinsichtlich der minimalen Ausführungszeit von 400 µs. Es ist jedoch zu beachten, dass ein zusätzliches Verfahren zur Integritätssicherung (MAC) bei der Ver- und Entschlüsselung mit einbezogen werden muss.

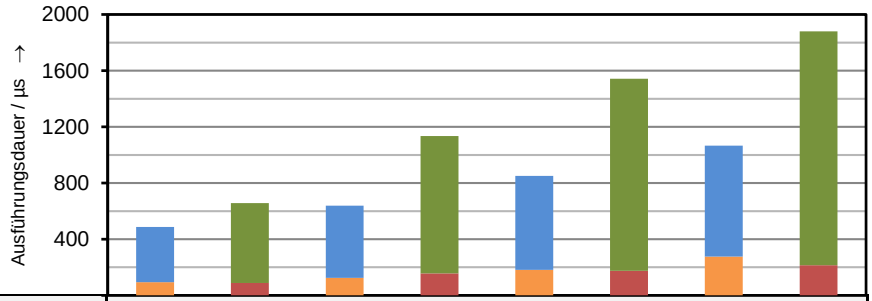
Wie im Falle der MAC-Verfahren ist auch bei den Ver- und Entschlüsselungsalgorithmen mit zunehmender Prozessdatengröße ein linearer Anstieg der Ausführungszeit zu erkennen. Damit zeigt sich allgemein auch hier ein ansteigender Ressourcenbedarf auf den Plattformen bei steigender zu verarbeitender Prozessdatengröße. Im direkten Vergleich zu den asymmetrischen Verfahren zeigt sich zudem, dass die symmetrischen Verfahren eine um ein vielfaches kleinere Ausführungszeit aufweisen. Während bspw. die asymmetrischen Verfahren auf Plattform 2 (siehe Tabelle 8-4) im Bereich von mehreren Millisekunden liegen, so haben die symmetrischen Verfahren auf Plattform 2 (siehe Tabelle 8-7 und Tabelle 8-10) Ausführungszeiten im zwei- bis dreistelligen Mikrosekunden-Bereich. Diese Eigenschaft hebt die Eignung der symmetrischen Verfahren für die (abgesicherte) echtzeitfähige PROFINET-Kommunikation nochmals hervor. Die asymmetrischen Verfahren können und werden daher primär im Bereich der Authentifizierung verwendet.

8.2.3 Messung der Durchlaufzeit der gesamten IT-Sicherheitsschicht

Die Messungen der symmetrischen und asymmetrischen kryptografischen Verfahren in den Abschnitten 8.2.1 und 8.2.2 zeigen auf, dass die jeweiligen kryptografischen Verfahren für einen speziellen Anwendungsfall konzipiert sind. Während die asymmetrischen Verfahren bei der Authentifizierung bspw. im Rahmen des IKEv2-Protokolls Anwendung finden, so können die symmetrischen Verfahren aufgrund der geringen Ausführungszeit zur sicheren (echtzeitfähigen) PROFINET-Kommunikation eingesetzt werden. Im weiteren Verlauf werden die symmetrischen Verfahren in der IT-Sicherheitsschicht des PROFINET-Protokollstacks zum Schutz der Kommunikation angewendet und die gemeinsame Ausführungszeit gemessen. Basis ist eine prototypische PROFINET-Protokollsoftware, welche der aktuellen PROFINET-Spezifikation entspricht [PNO2010].

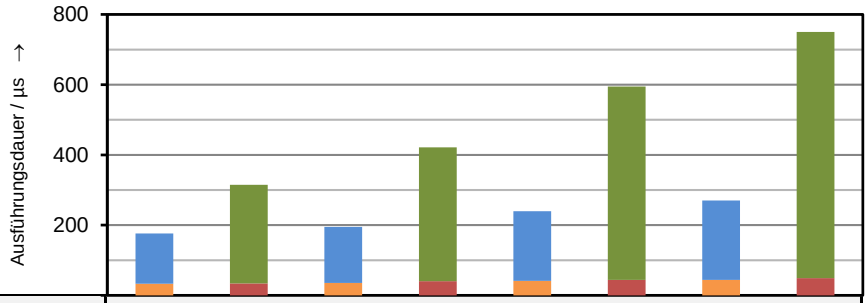
Wie in Abschnitt 6.2.2 erläutert, kann die sichere Übertragung von Daten in einem Netzwerk auf zwei Arten erfolgen. Der Basisschutz stellt die Integritätssicherung der Daten mit Hilfe eines MAC-Verfahrens dar. Bei einem höheren Sicherheitsbedarf ist eine vertrauliche Übertragung zu etablieren, die zusätzlich zum MAC-verfahren eine Ver- bzw. Entschlüsselung der Daten erfordert. In beiden Fällen übernimmt der PROFINET-Protokollstack inkl. der IT-Sicherheitsschicht die Verarbeitung der gesicherten Daten. Da bei einer (optionalen) vertraulichen Übertragung die Ausführungszeit des PROFINET-Protokollstacks aufgrund des zusätzlichen Aufwands der Verarbeitung der gesicherten Daten entstehen kann, erfasst die Messung die Ausführungszeit des PROFINET-Protokolls für beiden Arten separat.

Die Tabellen 8-12 bis 8-14 zeigen die Messung des PROFINET-Protokollstacks (inkl. der IT-Sicherheitsschicht) und dem jeweiligen symmetrischen kryptografischen Verfahren zur sicheren Übertragung. Die angewendeten symmetrischen Verfahren sind der HMAC-SHA-256 zur Integritätssicherung sowie der AES-128-CBC-Verschlüsselungsalgorithmus, da diese Verfahren in den vorherigen Messungen in Abschnitt 8.2.2 über dem gesamten Bereich der Prozessdatengröße die geringste Ausführungszeit zeigten. Angaben sind Mittelwerte und Standardabweichungen aus 500 Messungen, wobei wie im Falle der Messung der symmetrischen kryptografischen Funktionen (vgl Abschnitt 8.2.2) nur eine Kommunikationsrichtung betrachtet wird.



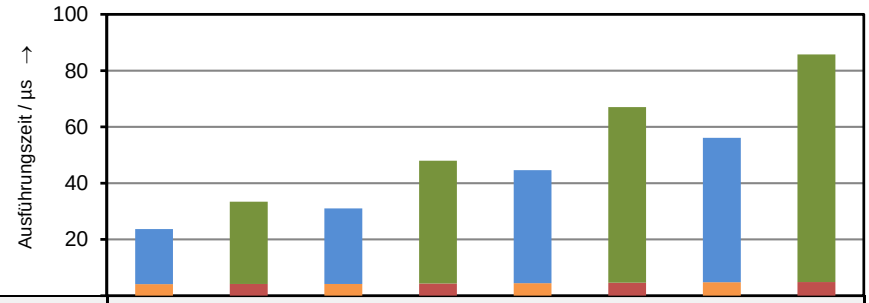
Ausführungszeit / µs N = 500	Prozessdatengröße			
	40 Byte	480 Byte	960 Byte	1440 Byte
PROFINET-Stack *(inkl. IT-Sicherheitsschicht)*	94,04 ± 43,29	124,33 ± 46,66	181,87 ± 81,87	276,04 ± 110,89
HMAC-SHA-256	393,47 ± 109,28	514,07 ± 114,41	669,47 ± 126,17	789,92 ± 149,43
PROFINET-Stack *(inkl. IT-Sicherheitsschicht)*	87,82 ± 40,45	156,33 ± 73,73	175,42 ± 60,10	214,32 ± 64,81
AES-128-CBC + HMAC-SHA-256	569,02 ± 114,65	978,18 ± 172,26	1367,79 ± 136,68	1665,37 ± 147,21

Tabelle 8-12: PROFINET-Stack + Kommunikationsabsicherung / Plattform 1



Ausführungszeit / µs N = 500	Prozessdatengröße			
	40 Byte	480 Byte	960 Byte	1440 Byte
PROFINET-Stack *(inkl. IT-Sicherheitsschicht)*	32,88 ± 7,98	35,28 ± 1,93	41,23 ± 4,58	43,86 ± 0,97
HMAC-SHA-256	143,49 ± 16,13	159,83 ± 0,80	198,38 ± 14,76	226,47 ± 1,62
PROFINET-Stack *(inkl. IT-Sicherheitsschicht)*	33,77 ± 0,42	40,15 ± 14,86	43,85 ± 9,59	48,90 ± 15,51
AES-128-CBC + HMAC-SHA-256	281,26 ± 23,08	381,39 ± 21,74	550,69 ± 51,32	701,50 ± 55,08

Tabelle 8-13: PROFINET-Stack + Kommunikationsabsicherung / Plattform 2



Ausführungszeit / µs N = 500	Prozessdatengröße			
	40 Byte	480 Byte	960 Byte	1440 Byte
PROFINET-Stack *(inkl. IT-Sicherheitsschicht)*	4,11 ± 1,61	4,20 ± 0,96	4,47 ± 0,88	4,77 ± 1,16
HMAC-SHA-256	19,57 ± 4,83	26,85 ± 2,50	40,17 ± 3,24	51,33 ± 3,33
PROFINET-Stack *(inkl. IT-Sicherheitsschicht)*	4,19 ± 1,33	4,32 ± 1,15	4,60 ± 1,79	4,88 ± 1,32
AES-128-CBC + HMAC-SHA-256	29,22 ± 5,60	43,67 ± 4,44	62,43 ± 5,37	80,86 ± 6,43

Tabelle 8-14: PROFINET-Stack + Kommunikationsabsicherung / Plattform 3

Der PROFINET-Protokollstack (inkl. IT-Sicherheitsschicht), nimmt in den Tabellen 8-12 bis 8-14 einen geringen Teil der Ausführungszeit in Anspruch und ist weitestgehend unabhängig vom jeweils verwendeten kryptografischen Verfahren. Den größeren Teil der Ausführungszeit benötigen die kryptografischen Verfahren, deren Ausführungszeit sich aufgrund der parallelen Nutzung des PROFINET-Protokollstacks inkl. der IT-Sicherheitsschicht im vgl. zu den Messungen der symmetrischen Verfahren in Abschnitt 8.2.2 stark erhöht hat. Wird auf den Schutz der Vertraulichkeit verzichtet (nur HMAC-SHA-256), so ist Fall von Plattform 2 und Plattform 3 in den Tabellen 8-13 und 8-14 das Kriterium aus Abschnitt 8.1.2 ($t_x \leq$ 400 µs) erfüllt. Bei Plattform 1 ist das Kriterium nicht erfüllt, da selbst bei kleinen Prozessdatengrößen die Ausführungszeit größer als 400 µs ist. Bei Anwendung einer vertraulichen Datenübertragung (AES-128-CBC + HMAC-SHA-256) erhöht sich die Ausführungszeit auf allen drei Plattformen. Plattform 3 in Tabelle 8-14 erfüllt dabei weiterhin das Kriterium. Plattform 2 hingegen nur dann, wenn die Prozessdatengröße kleiner als 480 Byte ist. Plattform 3 in Tabelle 8-12 zeigt bei der Messung bereits sehr große Ausführungszeiten oberhalb der 400 µs bei Prozessdatengrößen um 40 Byte. Aus der Messung der IT-Sicherheitsschicht ergeben sich die in Tabelle 8-15 dargestellten Einsatzszenarien für gesicherte Kommunikationsverbindungen in einem Automatisierungsnetzwerk für die drei Plattformen.

	Plattform 1	Plattform 2	Plattform 3
Referenz für:	(stark) ressourcen-beschränkte dezentrale Peripherie	Ressourcen-beschränkte dezentrale Peripherie, lokale Steuerungs- und Regelungsaufgaben	SPS, zentrale Steuerungs- und Regelungsaufgaben
Mögliche Zykluszeiten	< 2 bis 4 ms	< 1 ms / > 1 ms	< 1 ms in Abhängigkeit der Anzahl der Kommunikationspartner
Typische Prozessdatengrößen	< 100 Byte	< 480 Byte / > 480 Byte	40 bis 1440 Byte

Tabelle 8-15: Einsatzszenarien der evaluierten Plattformen

Plattform 1 kann zur Absicherung von geringen Prozessdatengrößen verwendet werden. Jedoch sind keine Zykluszeiten von 1 ms möglich, bedingt durch das vorgegebene Kriterium aus Abschnitt 8.1.2. Plattform 2 erlaubt diese Zykluszeit, auch bei einer vertraulichen Übertragung, wenn die Prozessdatengröße nicht größer als 480 Byte ist. Andernfalls sind andere Zykluszeiten zu wählen. Plattform 3 hingegen kann zur vollständigen gesicherten Kommunikation angewendet werden. Die Zykluszeit ist jedoch abhängig von der Anzahl zu schützender Kommunikationsverbindungen der zentralen Steuerung bzw. SPS. Dieser Sachverhalt wird nachfolgend betrachtet.

Extrapolation mehrerer bidirektionaler Kommunikationsverbindungen

Während die durch Plattform 1 und 2 repräsentierten Automatisierungskomponenten oftmals nur eine bidirektionale Kommunikationsbeziehung unterhalten müssen, so muss eine SPS (Plattform 3) mehrere bidirektionale (sichere) Verbindungen gleichzeitig aufrechterhalten, weil in der Regel mehrere E/A-Systeme an eine SPS angeschlossen sind. Auf Plattform 3 ist daher wegen der höheren Anzahl der Kommunikationsbeziehungen mit einem höheren Ressourcenbedarf aufgrund der kryptografischen Funktionen zu rechnen.

In der vorangegangenen Messung der IT-Sicherheitsschicht ist die unidirektionale gesicherte Kommunikation bewertet worden. Ausgehend von den Messungen zu Plattform 3 in Tabelle 8-14 soll nachfolgend eine Extrapolation der möglichen Zykluszeiten für mehrere gesicherte Kommunikationsverbindungen durchgeführt werden, da zum Zeitpunkt der Messungen keine größere Anzahl an Komponenten mit dem erweiterten Schutzkonzept zur Verfügung standen. Die Extrapolation erfolgt unter Annahme eines linear ansteigenden Ressourcenbedarfs mit steigender Anzahl an bidirektionalen gesicherten Kommunikationsbeziehungen. Die extrapolierte Ausführungszeit für eine bidirektionale gesicherte Kommunikation ergibt sich durch folgende Berechnung, wobei der Faktor 2 für die Verdopplung der Ausführungszeit der unidirektionalen Messungen aus Tabelle 8-14 steht.

$$t_A = 2 \cdot t_y \cdot n \quad \text{(n = Anzahl der Kommunikationsverbindungen)}$$

Abbildung 8-1 zeigt die Extrapolation der Ausführungszeit der PROFINET-Protokollsoftware inkl. der IT-Sicherheitsschicht und den kryptografischen Funktionen mit steigender Anzahl abzusichernder Kommunikationsverbindungen. Gegenübergestellt werden die minimale und maximale Prozessdatengröße (40 Byte … 1440 Byte), wobei jeweils das HMAC-Verfahren mit oder ohne vorhergehende Verschlüsselung der Daten (+ AES-128-CBC) zum Schutz der Vertraulichkeit der Daten zum Einsatz kommt.

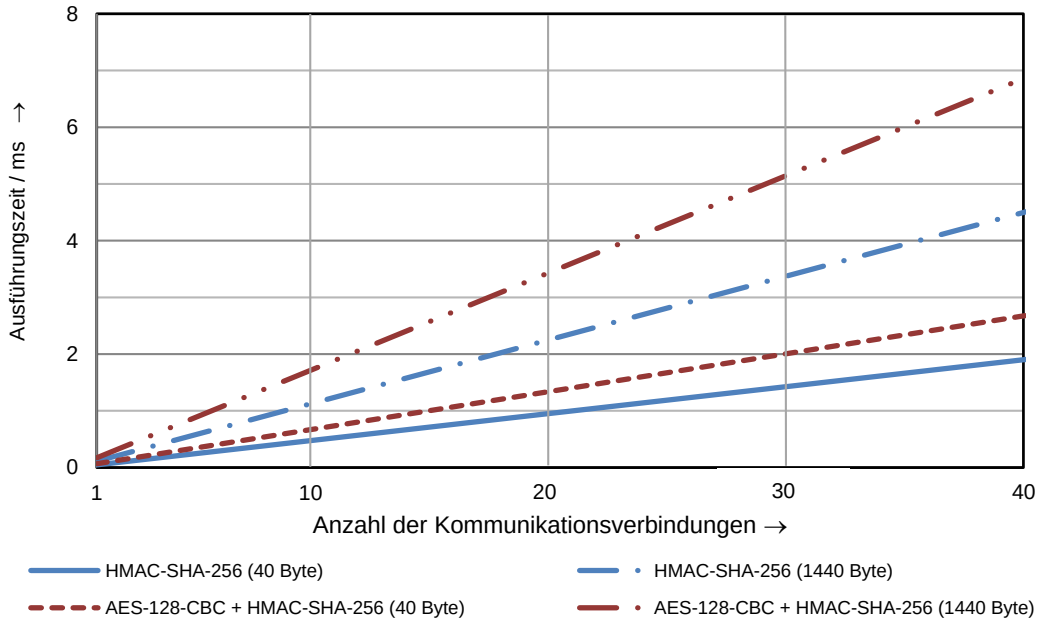


Abbildung 8-1: Absicherung mehrerer Kommunikationsverbindungen auf Plattform 3

(Extrapolation | IT-Sicherheitsschicht + kryptografische Funktion für bidirektionale Kommunikation)

Die Extrapolation in Abbildung 8-1 zeigt, dass Plattform 3 in der Lage ist, eine verschlüsselte bidirektionale Kommunikation (AES-128-CBC + HMAC-SHA-256) von 40 Kommunikationsverbindungen in einem Zeitraum von unter 8 ms zu bearbeiten. Die Prozessdaten haben dabei die Maximalgröße von 1440 Byte. Bei Verzicht auf den Schutz der Vertraulichkeit (nur HMAC-SHA-256) und 40 Kommunikationsverbindungen, sind Zykluszeiten unter 5 ms möglich. Verringert sich die Prozessdatengröße so können kleinere Zykluszeiten erreicht werden.

8.3 Zusammenfassung der Evaluierung der IT-Sicherheitsschicht

Die kryptografischen Funktionen bilden die Basis des erweiterten Schutzkonzepts, welches die Verwendung einer IT-Sicherheitsschicht vorschlägt. Die teils rechenaufwändigen kryptografischen Verfahren der IT-Sicherheitsschicht können einen erheblichen Einfluss auf die Echtzeitfähigkeit und den Ressourcenbedarf der jeweiligen Automatisierungskomponente haben. Die Evaluierung in Kapitel 8 zeigte diesen Einfluss auf. Hierfür erfolgte die Auswahl relevanter symmetrischer und asymmetrischer kryptografischer Verfahren. Verschiedene Evaluierungsplattformen stellen ein breites Anwendungsspektrum von Komponenten in der Automatisierungstechnik dar. Evaluierungsgrundlage ist die Ausführungszeit der kryptografischen Funktionen auf den jeweiligen Plattformen für eine unidirektionale Verbindung. Damit eine Absicherung der Kommunikation in kleinen Zykluszeiten möglich ist, wurde ein Kriterium festgelegt, anhand dessen die Bewertung der Ausführungszeiten erfolgt.

Aufgrund der großen Ausführungszeiten der asymmetrischen Verfahren, ist deren Anwendung in der echtzeitfähigen Kommunikation nicht möglich. Bei der Messung des RSA-Kryptosystems zeigt sich zusätzlich ein Ungleichgewicht in der Ausführungszeit zwischen Public- und Private-Key Operation. Dieses Verhalten weist das ECC-Verfahren nicht auf. Da darüber hinaus das ECC-Verfahren bei kleinerer Schlüssellänge eine größere kryptografische Stärke aufweist und die Ausführungszeiten auf einem niedrigerem Niveau liegen, ist

das ECC-Verfahren dem RSA-Kryptosystem zu vorzuziehen. Die Messungen zeigen, dass die symmetrischen Verfahren für eine schnelle Ausführung optimiert sind, die deren Verwendung zum Schutz der PROFINET-Kommunikation ermöglichen. Auftretende Schwankungen in den Ausführungszeiten sind auf Basis der Standardabweichungen berücksichtigt. Das HMAC-Verfahren zur Erstellung einer kryptografischen Prüfsumme wie auch das Verschlüsselungsverfahren AES-CBC sind die geeignetsten symmetrischen kryptografischen Verfahren, aufgrund der niedrigeren Ausführungszeiten über den gesamten Bereich der Prozessdatengröße. Mit Hilfe dieser symmetrischen Verfahren können niedrige Ausführungszeiten erreicht werden, die kleine Zykluszeiten bei einer gesicherten echtzeitfähigen PROFINET-Kommunikation ermöglichen [RCT2013], [RTN2013]. Abhängig sind die erreichbaren Zykluszeiten von der zu übertragenden Prozessdatengröße und dem angewendeten kryptografischen Algorithmus der Plattform. Die Anwendung der symmetrischen kryptografischen Verfahren in der IT-Sicherheitsschicht des prototypischen PROFINET-Protokollstacks zeigt eine allgemeine Erhöhung der Ausführungszeit der kryptografischen Verfahren, die sich mit der parallelen Anwendung des PROFINET-Protokollstacks inkl. der IT-Sicherheitsschicht erklärt. Insgesamt ergibt sich durch die Evaluierung eine bestimmte Einsatzmöglichkeit der jeweiligen Plattformen, welche sich durch die mögliche Zykluszeit, die mögliche Prozessdatengröße und der Anzahl zu verarbeitenden Kommunikationsverbindungen ergibt.

Die Eigenschaften der symmetrischen und asymmetrischen Verfahren machen eine Kombination beider Verfahren sinnvoll. Asymmetrische Verfahren sind primär zur Authentifizierung von Kommunikationspartnern konzipiert. Ein neben der Authentifizierung ausgehandelter symmetrischer Schlüssel wird für ein anschließendes symmetrisches Verfahren verwendet. Der allgemeine zweistufige Ansatz ist Abbildung 8-2 dargestellt.

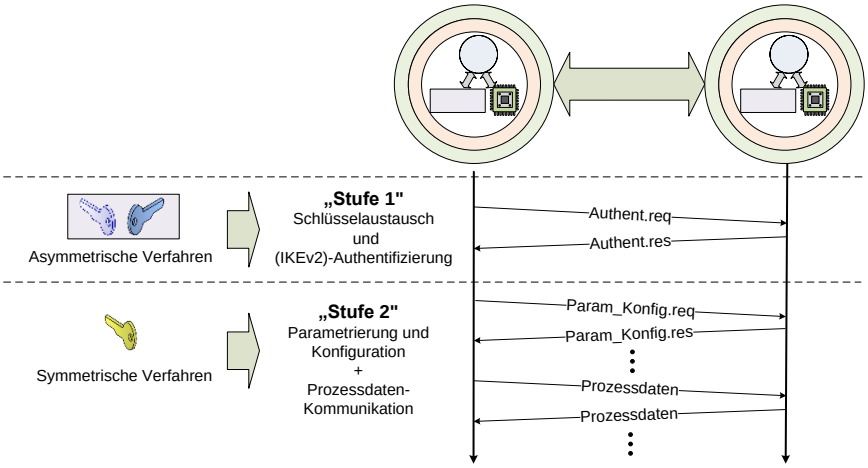


Abbildung 8-2: Zweistufiger Kommunikationsaufbau

Der zweistufige Kommunikationsaufbau ermöglicht eine sichere Authentifizierung auf Basis eines asymmetrischen kryptografischen Verfahrens, bspw. unter Verwendung des IKEv2-Protokolls, in dessen Folge eine geschützte Kommunikation zur Parametrierung bzw. Konfiguration sowie (echtzeitfähige) Prozessdatenkommunikation etabliert wird. Das asymmetrische Verfahren kommt nur beim ersten Verbindungsaufbau der Automatisierungskomponente zum Einsatz, wohingegen ein symmetrisches Verfahren nachfolgend verwendet wird. Ein vergleichbarer Ansatz findet sich bei OPC UA [DIN2008], SSL/TLS [INT2008] und IPSec

[INT2004], wobei keiner der zuvor genannten Ansätze den Schutz einer echtzeitfähigen Kommunikation adressiert, was ein maßgebliches Ziel dieser Arbeit ist.

In Abschnitt 8.1.1 erfolgte die Festlegung auf die in Tabelle 8-1 gezeigten kryptografische Verfahren. Um künftig neue kryptografische Verfahren einsetzen zu können, sieht die IT-Sicherheitsschicht anwenderspezifische Erweiterungsmöglichkeiten vor. Um dann weiterhin die Kompatibilität zwischen den Kommunikationspartnern gewährleisten zu können, erfolgt bei Authentifizierung zwischen den Partnern die Aushandlung eines gemeinsamen kryptografischen Verfahrens, welches beide Partner unterstützen. Ein (H)MAC ist erforderlich, da nur so eine unautorisierte Veränderung der zu übertragenen Daten einer Kommunikation zwischen Komponenten erkannt werden kann. Der HMAC nutzt dazu ein sicheres Prüfsummenverfahren (SHA-Algorithmen), welches zugleich bei der Zustandsüberwachung der Komponenten verwendet wird. Muss über den (H)MAC hinaus die Vertraulichkeit der Kommunikation gesichert werden, so sind die Daten zusätzlich zu verschlüsseln, bspw. auf Basis des AES-CBC-Algorithmus, wodurch sich die Ausführungszeit jedoch weiter erhöht. Da die Vertraulichkeit nur bei erhöhtem Sicherheitsbedarf benötigt wird und nicht zwingend erforderlich ist, kann die Verschlüsselung optional eingesetzt werden. Diesen optionalen Einsatz sieht die IT-Sicherheitsschicht vor, wobei der Anwender den Schutz der Kommunikation nach den jeweiligen Sicherheitsanforderungen skalieren kann.

Aufgrund der Skalierbarkeit der kryptografischen Maßnahmen der IT-Sicherheitsschicht, wird die Anforderung **A5** gemäß Tabelle 5-3 hinsichtlich eines flexiblen und skalierbaren Einsatzes der ergänzenden Schutzmaßnahmen zusätzlich sichergestellt. Diese flexible Wahlmöglichkeit sowie die Vorauswahl relevanter der kryptografischen Verfahren gewährleistet, dass eine lange Einsatzdauer **A3** der ausgewählten kryptografischen Verfahren über das Jahr 2030 und darüber hinaus möglich ist. Die Messungen der relevanten kryptografischen Funktionen haben darüber hinaus gezeigt, dass die Echtzeitanforderungen **A1** eines Automatisierungssystems, im Speziellen bei einem PROFINET-Netzwerk, erfüllt werden können.

Um die Ausführungszeiten weiter verbessern zu können, ist der Einsatz von optimierten Plattformen notwendig, bspw. unter Verwendung einer hardware-basierten Berechnung der kryptografischen Funktionen oder eines dedizierten Kryptobeschleunigers auf der jeweiligen Plattform. Auch Multicore-Prozessoren können verwendet werden, wobei die Anwendung der Plattform und die kryptografischen Verfahren auf separaten Prozessoren berechnet werden könnten. Erste Messungen zum dedizierten hardware-basierten Kryptobeschleuniger „Freescale - Security Engine“ [FRE2010] auf Plattform 2 sowie einer hardware-basierten Berechnung von kryptografischen Funktionen [CHH2013] zeigen, dass deren Nutzung vielversprechend ist, jedoch weiterer Optimierungen bedarf [RTN2012a]. Security Token sind ebenso wenig zur Beschleunigung von kryptografischen Funktionen geeignet, da der Kryptoprozessor des Token im Vergleich zum Hostsystem über geringe Ressourcen verfügt und zudem nur über ein relativ langsames serielles Interface angebunden ist [RNT2012]. Die großen Ausführungszeiten von kryptografischen Funktionen auf den Security Token ermöglichen keine echtzeitfähige Kommunikation mit kleinen Zykluszeiten. Das Security Token kann jedoch zur Unterstützung bei der Authentifizierung verwendet werden, da dieser Vorgang auf Basis der asymmetrischen kryptografischen Verfahren nicht der Vorgabe der echtzeitfähigen Kommunikation unterliegt (vgl. Abschnitt 8.2.1).

9 Funktion des erweiterten Schutzkonzepts

Kapitel 7 beschreibt ein erweitertes Schutzkonzept in Form einer IT-Sicherheitsschicht, welches sich ergänzender Schutzmaßnahme auf Basis kryptografischer Verfahren bedient. In Kapitel 8 ist dahingehend die Echtzeitfähigkeit und Einsatzdauer der IT-Sicherheitsschicht nachgewiesen worden, indem relevante kryptografische Verfahren ausgewählt und bewertet wurden. Das nun folgende Kapitel beschreibt die Funktion der IT-Sicherheitsschicht. Die Beschreibung der Funktion des Schutzkonzepts bzw. der IT-Sicherheitsschicht wird anhand von Aktivitätsdiagrammen durchgeführt. Diese Beschreibung soll die (sichere) Kommunikationsbeziehung von SPS und dezentraler Peripherie aufzeigen, wobei die Beschreibung auch auf andere Kommunikationsbeziehungen, bspw. zwischen ABK/EK und SPS, übertragbar ist. Abbildung 9-1 zeigt die Kommunikationsbeziehung, anhand derer die Beschreibung erfolgt.

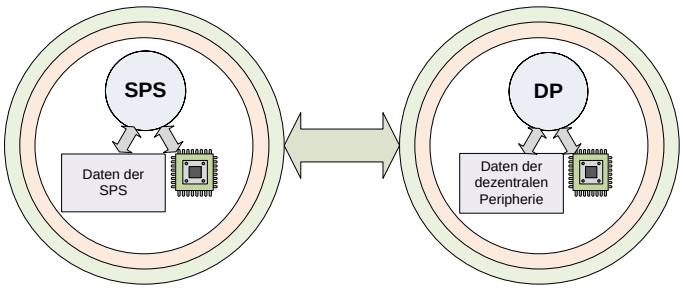


Abbildung 9-1: Betrachtete (sichere) Kommunikationsbeziehung

SPS und die dezentrale Peripherie nehmen unterschiedliche Aufgaben in einem Automatisierungssystem war, wie Abschnitt 3.1.1 zeigte. Dieser Aspekt macht eine getrennte Betrachtung der Anwendung des erweiterten Schutzkonzepts für SPS und dezentrale Peripherie notwendig. Weiterhin ist durch das PROFINET-Protokoll vorgegeben, welcher Kommunikationspartner den Kommunikationsaufbau initiiert und damit den Authentifizierungsvorgang, die Zustandsüberwachung sowie die Alarmsteuerung startet oder lediglich E/A-Signale verarbeitet, wie die dezentrale Peripherie.

Abschnitt 9.1 stellt den grundsätzlichen Ablauf der Implementierung der IT-Sicherheitsschicht dar. Danach folgt eine Beschreibung der Funktionsweise des Schutzkonzepts am Beispiel des Kommunikationsablaufs. Eine Validierung des Schutzkonzepts soll den Nachweis über die Wirksamkeit des Schutzkonzepts bzw. die IT-Sicherheitsschicht auf der Komponente und der Kommunikation erbringen (►9.3).

9.1 Ablaufsteuerungen des Schutzkonzepts

Die Ablaufsteuerung der SPS sowie der DP wird anhand von Aktivitätsdiagrammen erläutert. Diesen Aktivitätsdiagrammen liegen tiefergehende Zustandsdiagramme zu Grunde. Während die Aktivitätsdiagramme lediglich die grundlegenden Funktionen der Protokollerweiterung erfassen, zeigen die Zustandsdiagramme die internen Vorgänge der Protokollerweiterung. Diese internen Vorgänge beziehen sich dabei vor allem auf die parallel arbeitenden Funktionen, die in ähnlicher Art und Weise sowohl auf SPS als auch auf der DP ausgeführt werden. In Anhang A.1 sind die Zustandsdiagramme der Authentifizierung, der (sicheren) Kommunikation in Sende- und Empfangsrichtung dargestellt. Weiterhin zeigt der Anhang Zustandsdiagramme der Zustandsüberwachung und Schlüsselerneuerung.

9.1.1 Ablaufsteuerung der dezentralen Peripherie

Die (dezentrale) Peripherie einer Automatisierungsanlage dient als Schnittstelle zum technischen Prozess, der automatisiert wird, wobei eine Umsetzung der digitalen bzw. analogen Signale erfolgt. Die Peripherie setzt daher lediglich Stellwertbefehle der SPS um und/oder sendet aktuelle Messwerte an die Steuerung in der SPS. Bezüglich der Umsetzung des erweiterten Schutzkonzepts unterscheidet sich daher der funktionale Ablauf der dezentralen Peripherie von dem einer SPS. Abbildung 9-3 zeigt den funktionalen Ablauf für die dezentrale Peripherie am Beispiel eines Aktivitätsdiagramms.

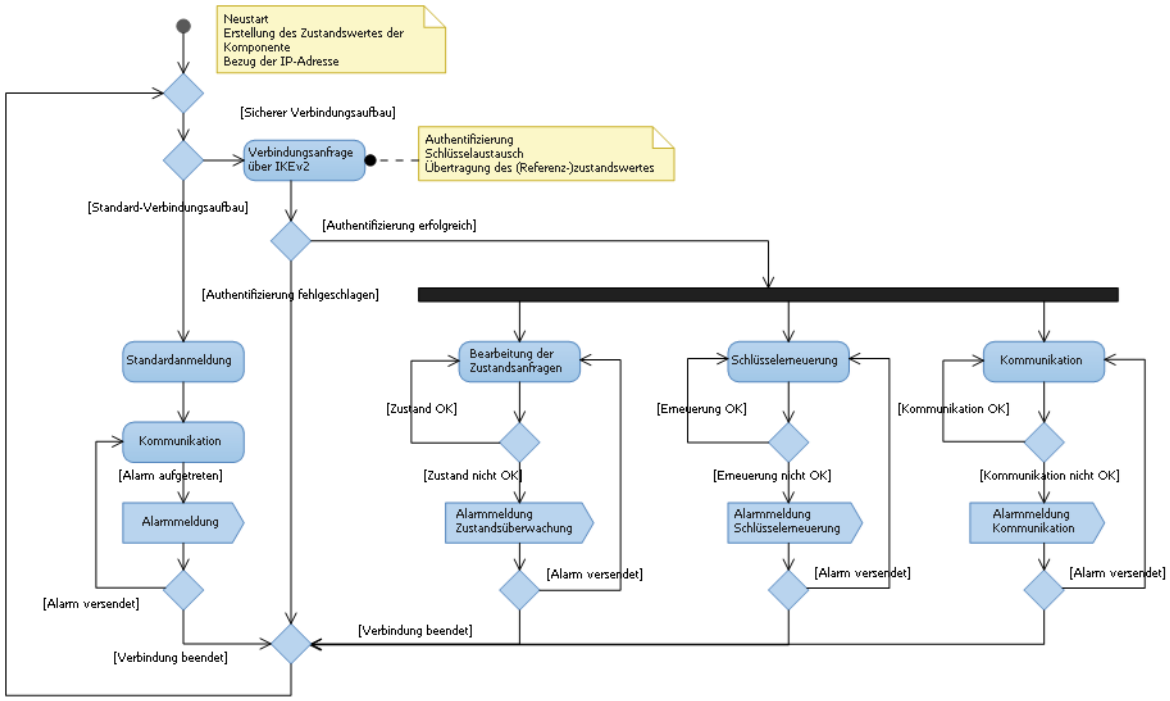


Abbildung 9-2: Aktivitätsdiagramm / Erweitertes Schutzkonzept (DP)

Bei Gerätestart werden zunächst Parameter zum Verbindungsaufbau bezogen sowie der Zustandswert der Komponente ermittelt. Während die Parameter zum Verbindungsaufbau über das Industrial Ethernet Protokoll versendet werden, wird der Zustandswert der Komponente lokal berechnet (siehe auch Abschnitt 6.2.3). Ab diesem Zeitpunkt kann eine Verbindung zur dezentralen Peripherie aufgebaut werden, wobei eine Anmeldung auf regulärem oder sicherem Weg erfolgen kann. Bei sicherem Verbindungsaufbau wird eine Authentifizierung durchgeführt, in deren Verlauf ein Schlüsselaustausch sowie der Zustandswert (Referenzwert) der Komponente übermittelt werden. Liegt eine Autorisierung für die Verbindungsanfrage vor, so starten parallel die Funktionen der Protokollerweiterung.

Eine Aufgabe der dezentralen Peripherie liegt in der Bearbeitung regelmäßig eintreffender Zustandsanfragen. Der zu Beginn übermittelte Referenzwert des Zustands wird seitens der SPS erfragt und gegen den aktuellen Wert verglichen. So wird sichergestellt, dass keine unautorisierten Veränderungen an der dezentralen Peripherie stattgefunden haben. Im Zuge der sicheren Kommunikation werden die abgesicherten bzw. geschützten Daten der ein- und ausgehenden Datenpakete überprüft. Die Schlüsselerneuerung übernimmt die Aktualisierung des (symmetrischen) Schlüssels, bspw. durch Ableitung eines neuen Schlüssels aus dem vorhergehenden oder durch Neuaushandlung zwischen den Kommunikationspartnern ent-

sprechend des Schlüsselaustausches beim IKEv2-Protokoll, wie in Abschnitt 7.3.2 eingeführt. Der Ablauf der Authentifizierung und des Schlüsselaustausches wird nachfolgend in Abschnitt 9.2.1 näher erläutert.

Tritt bei einer der parallel arbeitenden Funktionen ein Fehler auf, z.B. da die Schlüsselerneuerung fehlgeschlagen bzw. der Security Counter abgelaufen ist, so erfolgt das Versenden einer Alarmmeldung. Ist seitens der SPS eine größere Anzahl an Alarmen registriert worden, so übernimmt die SPS die Alarmbehandlung, z.B. in Form eines regulären Verbindungsabbaus. Die Alarmbehandlung bzw. ein mögliches Ausschalten der Komponente hat dann zur Folge, dass nach einem Neustart ein erneuter Verbindungsaufbau erfolgt.

9.1.2 Ablaufsteuerung der SPS

Wie Abschnitt 3.1.1 aufzeigte, nimmt die SPS unterschiedliche Aufgaben in einer Automatisierungsanlage war. Die SPS baut zu diesem Zweck Verbindungen zu dezentralen Peripherien auf. Im Falle des hier vorgestellten Schutzkonzepts übernimmt die SPS die Überwachung der ergänzenden Schutzmaßnahmen. Daher erfolgt im Gegensatz zur dezentralen Peripherie die Einbindung der Schutzmaßnahmen in veränderter Form. Abbildung 9-3 zeigt den Ablauf des erweiterten Schutzkonzepts für die SPS.

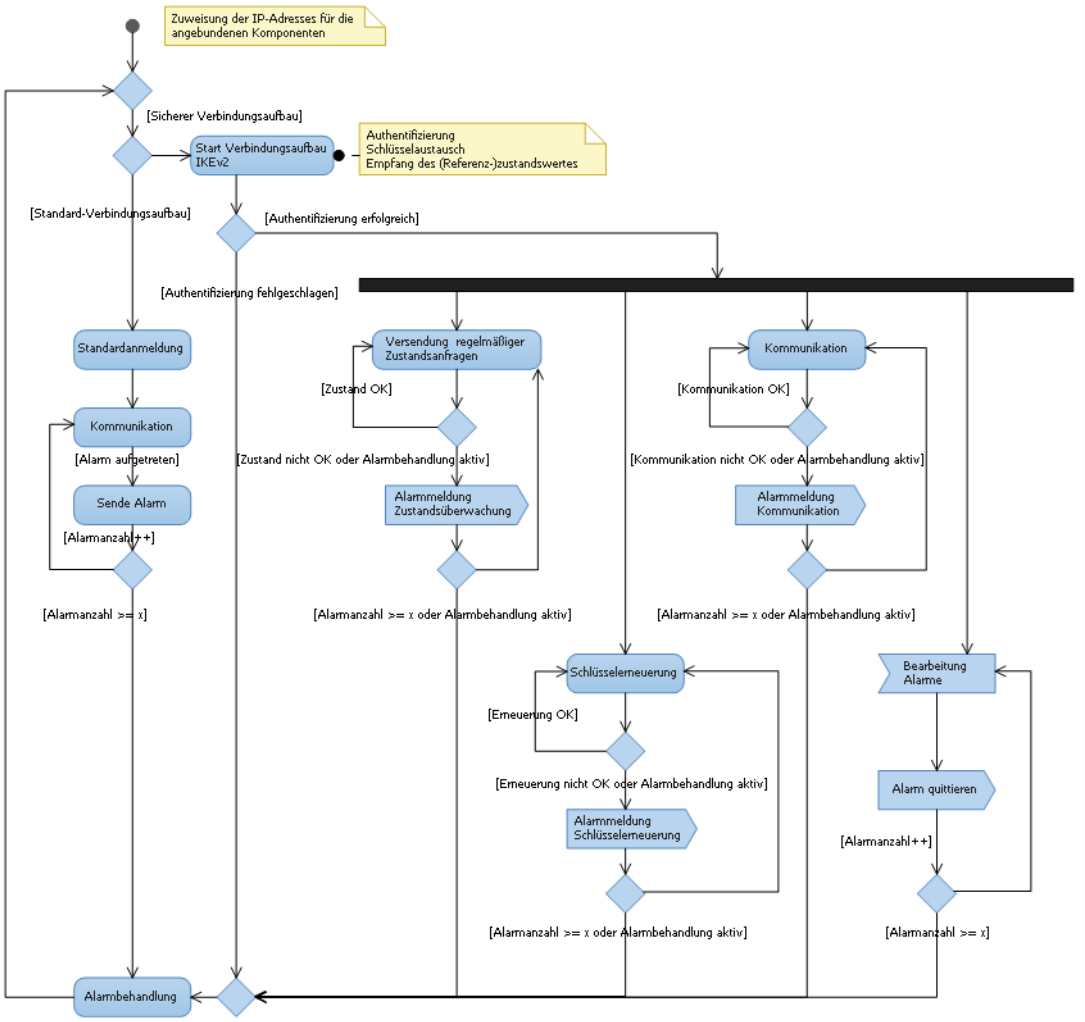


Abbildung 9-3: Aktivitätsdiagramm / Erweitertes Schutzkonzept (SPS)

Die SPS initiiert den Verbindungsaufbau. Das Engineering der Automatisierungsanlage entscheidet, ob ein sicherer oder ein konventioneller Verbindungsaufbau eingeleitet wird. Ist die Authentizität des Kommunikationspartners (z.B. der dezentralen Peripherie) sichergestellt, so werden die Funktionen des erweiterten Schutzkonzepts ausgeführt.

Der Unterschied zwischen SPS und der DP liegt in der Initiierung des Verbindungsaufbaus, welcher von der SPS ausgeht, und der Behandlung eingehender Alarme sowie der Zustandsüberwachung. Die SPS kann in regelmäßigen Abständen eine Anfrage des Zustands des Kommunikationspartner stellen und daraus ggf. Maßnahmen ableiten. Selbiges gilt für eingehende Alarme, die durch Kommunikationspartner oder lokal abgesetzt wurden.

9.2 Kommunikationsablauf des Schutzkonzepts

Während Abschnitt 9.1 den Funktionsablauf des Schutzkonzepts beschreibt, soll nun der Kommunikationsablauf zwischen diesen Automatisierungskomponenten dargestellt werden.

9.2.1 Authentifizierung und Übertragung des Referenzwertes

Abbildung 9-4 zeigt den Authentifizierungsvorgang zwischen SPS und der dezentralen Peripherie. Die Initiierung ① der Authentifizierung erfolgt ausgehend von der SPS mit der dezentralen Peripherie mit Hilfe des IKEv2-Protokolls. Wie in Abschnitt 6.2 erläutert, verfügen die Kommunikationspartner jeweils über ein asymmetrisches Schlüsselpaar sowie ein Zertifikat, welches als Nachweis über die Echtheit des Schlüsselpaares dient. Zum Zweck der Zustandsüberwachung stellt die dezentrale Peripherie einen (Start-)zustandswert zur Verfügung, welcher durch die SPS überwacht wird.

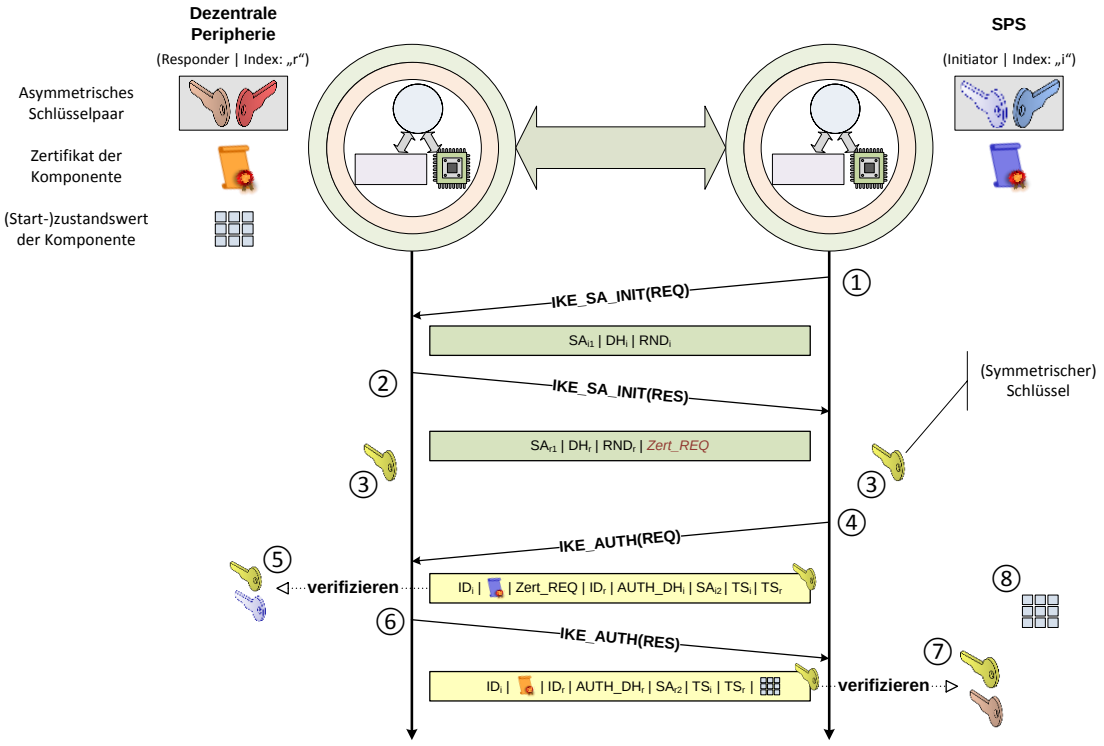


Abbildung 9-4: Authentifizierungsvorgang basierend auf dem IKEv2-Protokoll

Die Authentifizierung mit Hilfe des IKEv2-Protokolls erfolgt in zwei Schritten. Die Initiierung der Authentifizierung beginnt mit Hilfe der IKE_SA_INIT-Nachrichten, wobei direkt darauf die gegenseitige Authentifizierung anhand der IKE_AUTH-Nachrichten durchgeführt wird. Zu

Beginn ① überträgt der Initiator der Authentifizierung ungesichert den Vorschlag einer Security Association (SA) sowie Diffie-Hellman-Parameter (DH) und eine Zufallszahl (RND), die für das Diffie-Hellman-Verfahren benötigt wird. Als Reaktion ② darauf überträgt die Gegenstelle (engl. responder) entsprechend ungesichert eigene Parameter hinsichtlich SA, DH und RND. Weiterhin wird eine Zertifikatsanforderung (CERTREQ) gestellt, welche anzeigt, dass eine Authentifizierung anhand von Zertifikaten gewünscht ist. Diese beinhaltet Prüfsummen öffentlicher Schlüssel bereits vertrauenswürdiger Zertifizierungsstellen (vgl. Abschnitt 6.2.1). Dadurch ist die Gegenstelle bereits mit der nächsten Antwort in der Lage Zertifikate zu übertragen, dessen Vertrauenswürdigkeit sofort festgestellt werden kann. Dabei ist nicht zwingend eine Online-Verbindung zu einer CA notwendig, um die Identität der Gegenstelle zu überprüfen, sofern das Zertifikat der CA bereits in der Komponente vorliegt. Durch das IKE_SA_INIT sind nun beide Kommunikationspartner in der Lage mit Hilfe des Diffie-Hellman-Verfahrens einen gemeinsamen symmetrischen Schlüssel auszuhandeln. Dieser gemeinsame Schlüssel dient als Basis die nachfolgende Kommunikation mit Hilfe symmetrischer Verfahren zu sichern. Um „Denial of Service“-Angriffe bei der Authentifizierung zu verhindern (in Form einer Vielzahl IKE_SA_INIT(REQ) auf die keine IKE_AUTH-Nachricht folgt), wird bei Bedarf seitens des IKEv2-Protokolls eine sogenannte Cookie-Challenge durchgeführt [INT1999].

Da durch die Initiierung der Verbindung lediglich der Austausch eines gemeinsamen geheimen Schlüssels erfolgte, muss als nächster Schritt die gegenseitige Authentifizierung erfolgen (IKE_AUTH). Die Authentifizierungs-Nachrichten ④ und ⑥ werden durch den gemeinsam ausgehandelten Schlüssel (symmetrisch) verschlüsselt und durch einen MAC abgesichert. Inhalt der Nachrichten sind Vorschläge zu Identifikatoren (ID) von Initiator und Responder, das jeweilige Zertifikat sowie Zertifikatsanforderungen mit entsprechenden Vorschlägen für vertrauenswürdige CAs. Weiterhin befinden sich mit Hilfe eines asymmetrischen Verfahrens erstellte Signaturen (AUTH_DH) in den Nachrichten, welche über die eigene beim IKE_SA_INIT-Vorgang erstellte Zufallszahl (RND) sowie der eigenen ID gebildet werden. Der Empfänger der jeweiligen Nachricht überprüft diese mit Hilfe der symmetrischen Verfahren und verifiziert die Signaturen sowie das Zertifikat durch asymmetrische Kryptografie (⑤ und ⑦). Weiterhin wird die SA beider Seiten festgelegt und durch die Traffic-Selektoren (TS) definiert, womit die Festlegung auf ein zu verwendendes kryptografisches Verfahren je Richtung erfolgt. Letztlich erfolgt die Eintragung der ausgehandelten Parameter in eine lokale Security Police Database (SPD).

Am Ende des Authentifizierungsvorgangs ist die Identität der Kommunikationspartner sichergestellt. Zusätzlich verfügt die SPS über den (Start-)zustandswert der dezentralen Peripherie, mit dessen Hilfe eine Zustandsüberwachung der dezentralen Peripherie durchgeführt werden kann ⑧. Gleichzeitig ist mit der Authentifizierung ein gemeinsamer (symmetrischer) Schlüssel ausgehandelt worden mit dessen Hilfe die anschließende Kommunikation abgesichert wird. Ist eine Schlüsselerneuerung erforderlich, so kann ein neuer Schlüssel aus dem alten abgeleitet werden oder es erfolgt die Neuaushandlung eines (symmetrischen) Schlüssels mit Hilfe des IKEv2-Protokolls.

9.2.2 Sichere Kommunikation und Zustandsüberwachung

Im Anschluss an die Authentifizierung der Kommunikationspartner finden unter Verwendung eines ausgehandelten symmetrischen kryptografischen Verfahrens die sichere Kommunikation inkl. der Alarmmitteilungen und die azyklische Zustandsüberwachung statt. Abbildung 9-5 zeigt zunächst die azyklische Zustandsüberwachung der dezentralen Peripherie.

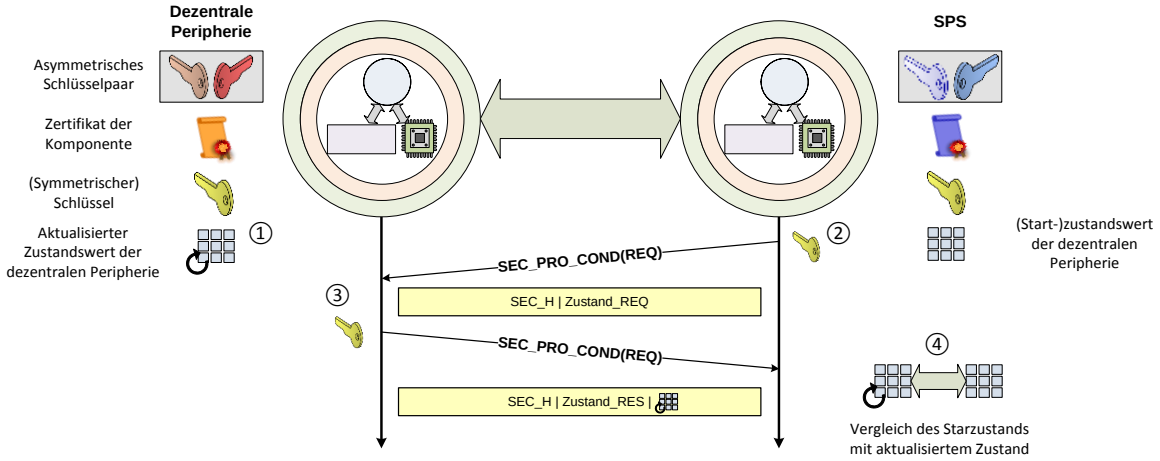


Abbildung 9-5: Azyklische Zustandsüberwachung

Während der Laufzeit der dezentralen Peripherie erfolgt in regelmäßigen Abständen eine Aktualisierung des lokalen Zustandswerts durch die Zustandsüberwachung ①. Wird seitens der SPS eine Anfrage ② über einen aktualisierten Zustands gestellt, so sendet die dezentrale Peripherie den aktualisierten Zustandswert ③ an die SPS. Diese vergleicht den (Start-)zustandswert mit dem aktualisierten Wert und kann dadurch ermitteln, ob unautorisierte Veränderungen an der dezentralen Peripherie stattgefunden haben ④. Auf diese Weise kann die SPS geeignete Maßnahmen ergreifen um Schäden an Mensch und/oder Maschine zu verhindern, bspw. in Form eines ordnungsgemäßen Verbindungsabbaus. Im Gegensatz zu [PHK2013] wird bei dem hier dargestellten Ansatz eine Zustandsüberwachung auch auf den prozessnahen Komponenten möglich. Weiterhin zielt der hier gezeigte Ansatz nicht ausschließlich auf sicherheitsgerichtete Kommunikation ab, sondern auf jegliches Anwendungsprotokoll unter Anwendung von Security Token. Dies wird durch die in Abschnitt 7.2.3 definierte Platzierung der IT-Sicherheitsschicht ermöglicht. Die regelmäßige Überprüfung des Zustands hat zusätzlich den Vorteil, dass der Aufwand zur Ausführung der Zustandsüberwachung auf niedrig-performanten Plattformen möglich bleibt.

Wie die Aktivitätsdiagramme in Abbildung 9-2 und 9-3 zeigen, findet parallel zur Zustandsüberwachung die gesicherte Kommunikation, die Alarmbehandlung sowie Schlüsselerneuerung statt. Wie in Abschnitt 7.3.1 beschrieben, erfolgt die Schlüsselerneuerung lokal durch Ableitung eines neuen symmetrischen Schlüssels aus dem alten symmetrischen Schlüssel oder durch Neuaushandlung. Die gesicherte Kommunikation wie auch die Alarmbehandlung (bzw. Alarmkommunikation) sind in Abbildung 9-6 dargestellt. Entsprechend Kapitel 7 wird durch die IT-Sicherheitsschicht die zu übertragende Kommunikation gesichert ①, wobei ein symmetrisches kryptografisches Verfahren angewendet wird, um ggf. die Echtzeitfähigkeit der Kommunikation erhalten zu können. Bestandteil der gesicherten Kommunikation ist der Security Header (SEC_H), die ein- und ausgehenden Daten zwischen den Kommunikationspartnern (DATA_E bzw. DATA_A) sowie die Bestätigung der ein- und ausgehenden Daten

für die Gegenrichtung (DATA_E_ACK bzw. DATA_A_ACK). Auf diesem Wege wird ebenso die gesamte Alarmkommunikation ② geschützt, um auch hier einen möglichen Angriff auf die Alarmnachrichten zu verhindern.

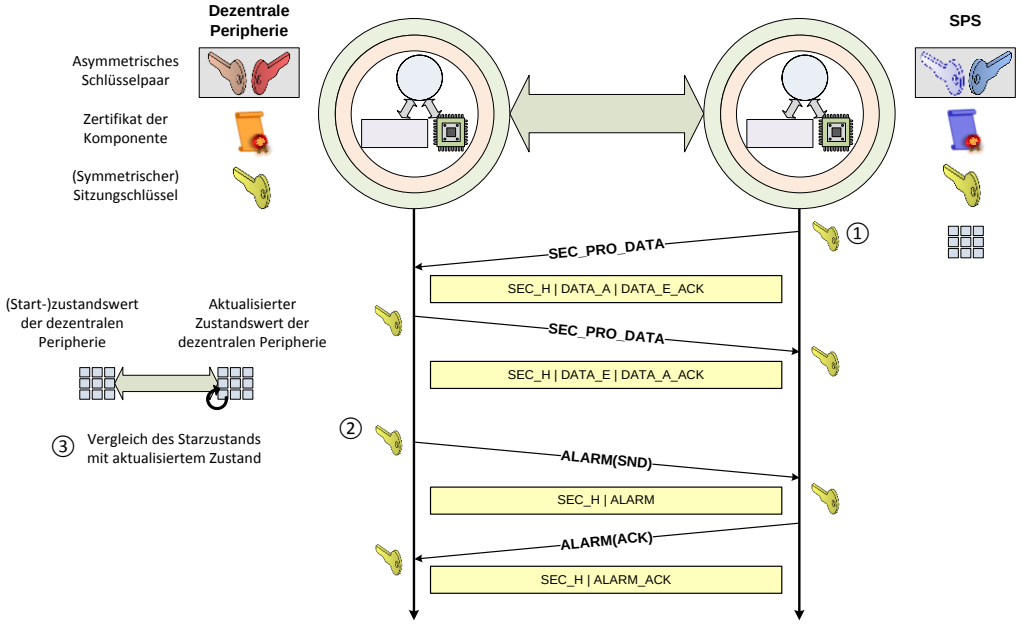


Abbildung 9-6: Sichere Kommunikation

Bestandteil der Alarmbehandlung ist neben der entfernten Zustandsüberwachung über die Kommunikation (siehe Abbildung 9-5) die lokale Zustandsüberwachung ③. Im Falle eines Angriffes auf die Komponente, bei welchem eine Manipulation der dezentralen Peripherie stattfinden kann, wird bei Erkennen eines solchen Angriffs ebenfalls ein Alarm ② an den jeweiligen Kommunikationspartner (hier die SPS) versendet und entsprechend quittiert. Auch hier können Schutzmaßnahmen ergriffen werden, um Schäden am Automatisierungssystem und dessen Umfeld zu verhindern. Entsprechend kann die lokale Zustandsüberwachung auch auf anderen Komponenten – z.B. der SPS – durchgeführt werden, die wiederum von anderen Komponenten des Automatisierungssystems überwacht werden kann.

9.3 Validierung des erweiterten Schutzkonzepts

Das erweiterte Schutzkonzept ist in Form einer Demonstrationsanlage, am Beispiel des PROFINET-Protokolls, zusammenfassend implementiert und validiert worden (►9.3.1). Hierbei kommen die in Abschnitt 8.1.2 gezeigten Plattformen, die bereits zur Evaluierung der kryptografischen Funktionen herangezogen wurden, zum Einsatz.

Ziel der Validierung ist der Nachweis der Wirkung des erweiterten Schutzkonzepts für Automatisierungssysteme. Der Nachweis soll durch beispielhafte Angriffe auf die Assets Kommunikation (►9.3.2) und Komponente (►9.3.3) erbracht werden. Der Nachweis gilt als erbracht, wenn das System trotz Angriff operabel bleibt oder einen definierten (sicheren) Zustand annimmt. Darüber hinaus können durch die Validierung Verbesserungsmöglichkeiten bzw. Schwachstellen des erweiterten Schutzkonzepts identifiziert werden.

9.3.1 Validierungsumgebung des erweiterten Schutzkonzepts

Abbildung 9-7 zeigt die schematische Darstellung des Demonstrators zur Validierung des erweiterten Schutzkonzepts. Der Aufbau des Demonstrators ist im Anhang A.2 erläutert. Aufgabe des Demonstrators ist die Steuerung einer Lauflichtanwendung auf dezentral angeordneten Komponenten PNK als dezentrale Peripherien (DP).

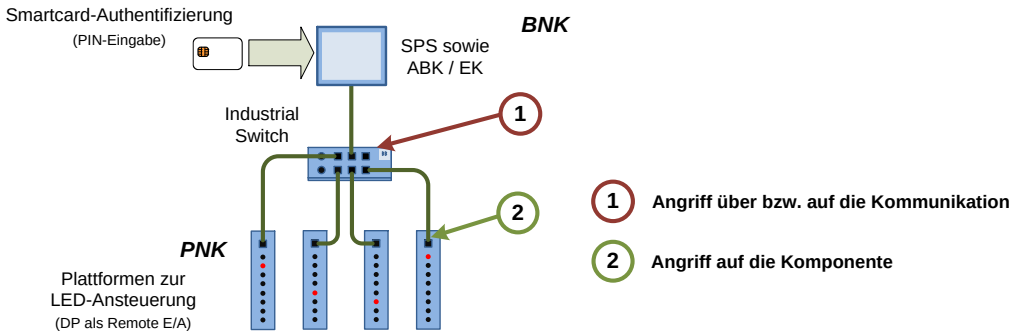


Abbildung 9-7: Angriffe auf die Validierungsumgebung

Die BNK des Demonstrators wird in Form einer HMI-Bedienstation in Hutschienenausführung bereitgestellt und entspricht der evaluierten Plattform 3 (Standard-PC). Zur Anmeldung eines Benutzers an der BNK ist eine Authentifizierung mit Hilfe einer Smartcard-/PIN-Kombination erforderlich. Über die Bedienoberfläche der BNK (siehe Anhang A.2, Abbildung A-13) erfolgt die Bedienung des Demonstrators (ABK). Die Bedienstation fungiert gleichzeitig als SPS sowie als EK zur Konfiguration und Parametrierung des Demonstrators. Die SPS führt die Berechnung der Ausgabewerte der LED-Lauflichtanwendung durch, wobei die BNK die Ausgabewerte auf der Bedienoberfläche visualisiert.

Die über die SPS-Funktion berechneten LED-Ausgabewerte werden über das PROFINET an die PNK übertragen. Die Übertragung erfolgt unter Verwendung des prototypischen PROFINET-Protokollstacks, welcher das erweiterte Schutzkonzept beinhaltet. Die PNK stellen letztendlich die empfangenen Ausgabewerte der Lauflichtanwendung dar. Als PNK werden die in Abschnitt 8.1.2 genannten (stark-)ressourcen-beschränkten Plattformen 3 verwendet. Diese Plattformen repräsentieren die dezentrale Peripherie (DP).

Ausgehend von Abbildung 4-3 in Abschnitt 4.1.1 werden auf den Demonstrator zwei exemplarische Angriffe auf die (geschützten) Kommunikationsverbindungen und (überwachten) Komponenten durchgeführt.

- **Angriff auf die Kommunikation**

Der in Abbildung 3-9 gezeigte „Man in the Middle“-Angriff wird auf die Kommunikation durchgeführt, wobei der Zugriff auf das Netzwerk über den Industrial Switch erfolgt. Um die Wirksamkeit des Schutzes für die Kommunikation nachweisen zu können, werden einzelne Verbindungen ungesichert und andere gesichert aufgebaut. Im Falle der gesicherten Verbindung können mögliche Angriffe auf die Kommunikation erkannt und dem Benutzer an der BNK als Alarm gemeldet werden, womit eine mögliche Alarmbehandlung folgen kann.

- **Angriff auf die Komponenten**

Per Zugriff über eine lokale USB-Schnittstelle an der PNK, soll im Rahmen der Validierung eine unautorisierte Veränderung der Komponente (z.B. der Software) durchgeführt werden.

Die ergänzenden Schutzmaßnahmen des erweiterten Schutzkonzepts machen den Angriff erkennbar und ermöglichen die Ausgabe entsprechender Alarmmeldungen an der Bedienoberfläche der BNK. Auch in diesem Fall kann eine mögliche Alarmbehandlung folgen.

Die Wirksamkeit des erweiterten Schutzkonzepts gilt als erbracht, wenn die Komponenten des Demonstrators keinen undefinierten (unsicheren) Zustand einnehmen.

9.3.2 Validierung des Kommunikationsschutzes

Abbildung 9-8 zeigt den Angriff auf die geschützte Kommunikation des Demonstrators unter Verwendung eines „Man in the Middle“-Angriffs.

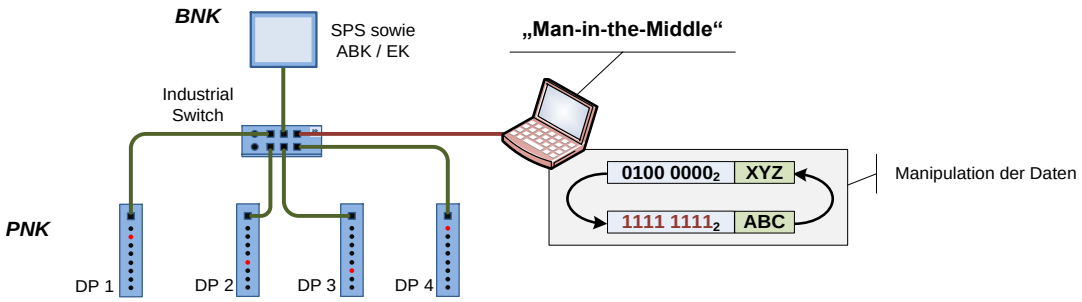


Abbildung 9-8: Angriff auf die geschützte Kommunikation

Ziel des Angriffs ist die Umleitung der Kommunikation und Veränderung der Ausgabewerte für die LED-Lauflichtanwendung. Der Angriff soll sowohl auf eine geschützte als auch eine ungeschützte Kommunikation erfolgen, um die Auswirkungen des Angriffes zeigen zu können. Während Komponente DP 1 über eine gesicherte Verbindung verfügt, wird die Komponente DP 2 auf ungesichertem Wege kommunizieren.

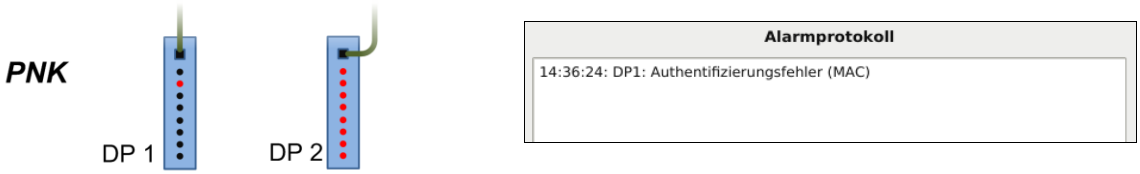


Abbildung 9-9: Auswirkung des Angriffs auf die Kommunikation

Im Falle der ungesicherten Kommunikation von Komponente DP 2 führt der Angriff dazu, dass alle LED der Komponente vom Angreifer unkontrolliert eingeschaltet werden können. Eine entsprechende Meldung über diesen Vorfall an die BNK bzw. SPS erfolgt nicht. Komponente DP 1 hingegen erkennt durch die Nutzung des erweiterten Schutzkonzeptes die Manipulation an den empfangenen und veränderten Datenpaketen und meldet diesen an die SPS und die Bedienoberfläche, wie Abbildung 9-9 zeigt. Die Meldungen zeigen an, dass bei mehreren Datenpaketen in Folge der MAC nicht korrekt war, weshalb die darin gefälschten Ausgabewerte für die LED nicht ausgegeben wurden (siehe Abbildung 9-9 links, Komponente DP 1). Treten entsprechende Meldungen auf, ist von einem Angriff auszugehen und ggf. die Komponente ist in einen sicheren Zustand zu bringen. Da darüber hinaus die nicht-authentifizierte Kommunikation zwischen der SPS und unterlagerten Komponenten verworfen wird, können Einflüsse, wie bspw. „Denial of Service“-Angriffe auf die Komponenten über die Kommunikation, reduziert werden, da die IT-Sicherheitsschicht ein Weiterreichen korrupter Datenpakete an höhere Protokollschichten unterbindet.

9.3.3 Validierung des Komponentenschutzes

Wie in Abschnitt 4.2 erläutert, besteht durch einen Angriff auf die lokalen Schnittstellen der Automatisierungskomponenten ggf. unautorisierter Zugriff auf dessen Systemfunktionen (Software) und Systemdaten (Konfiguration). Als Folge dessen sind unautorisierte Veränderungen an der Komponente möglich. Die im Zuge des erweiterten Schutzkonzepts implementierte lokale bzw. (regelmäßige) entfernte Überwachung des Zustands der Komponenten dient der Erkennung derartiger Veränderungen. Aus der Erkennung lokaler Angriffe können anschließende Maßnahmen zum Schutz des Automatisierungssystems folgen, wie bspw. die Trennung der Verbindung zu einer angegriffenen Komponente. Um die Wirkung des Schutzes für die Komponente nachweisen zu können, wird ein Angriff auf die BNK bzw. DP über eine ungesicherte Schnittstelle, wie bspw. USB nachgestellt. Mit Zugriff auf die Komponente erfolgt die Veränderung der Software und der Plattformkonfiguration. In Abbildung 9-10 ist der Angriff auf die kombinierte BNK über ihre lokalen Schnittstellen zum Zweck der Validierung des Schutzes dargestellt.

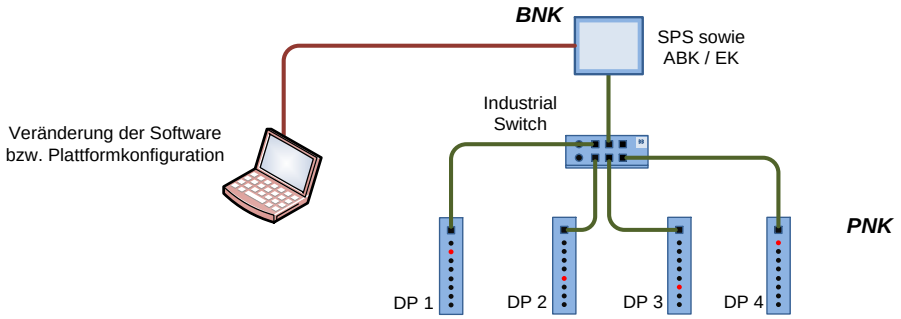


Abbildung 9-10: Angriff auf die SPS-Funktion der BNK

Abbildung 9-11 zeigt die Alarmmeldungen, die in Folge des Angriffs auf SPS bzw. ABK/EK auf der Bedienoberfläche des Demonstrators ausgegeben werden.

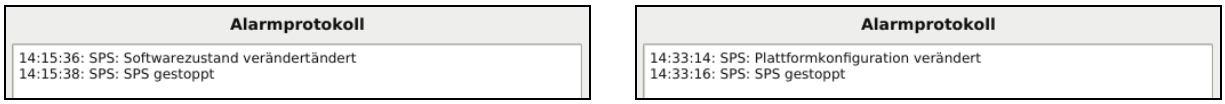


Abbildung 9-11: Alarmmeldungen der SPS-Überwachung an der ABK

Sowohl bei Veränderung der Software der Plattform als auch bei Veränderung der Konfiguration erscheint eine entsprechende Alarmmeldung im Alarmprotokoll der ABK. Da diese Meldungen einen möglichen Angriff aufzeigen, beendet die SPS aus Sicherheitsgründen ihre Funktion und Verbindung zu den unterlagerten Komponenten. Abbildung 9-12 zeigt den Angriff auf die lokalen Schnittstellen der Komponente DP 1 der dezentralen Peripherie.

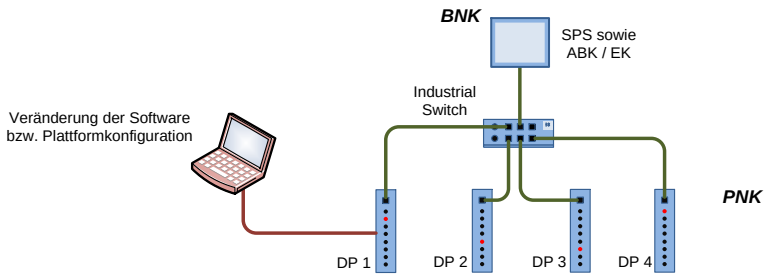


Abbildung 9-12: Angriff auf die Komponente DP 1

Abbildung 9-13 zeigt die Alarmmeldungen der ABK nach Angriff auf die Komponente DP 1.

Abbildung 9-13: Alarmmeldungen der DP-Überwachung an der ABK

Die Veränderung der Software, wie auch der Konfiguration, der Komponente DP 1 bewirkt das Absetzen entsprechender Alarme, die auf der ABK zur Anzeige gebracht werden. Da darüber hinaus, die SPS in regelmäßigen Zeitabständen den Zustand der dezentralen Peripherie abfragt, ergibt der Vergleich mit dem (Start-)Zustandswert der Komponente DP 1, welcher bei Authentifizierung bzw. Verbindungsaufbau übertragen wurde, dass eine (unautorisierte) Veränderung stattgefunden hat bzw. ein Angriff auf die Komponente erfolgt ist.

9.4 Risikobewertung des erweiterten Schutzkonzepts

Die Anwendung von Schutzmaßnahmen für die IT-Sicherheit hat eine Reduzierung des Risikos für das Automatisierungssystem zum Ziel. Tabelle 4-5 in Abschnitt 4.5 zeigte, dass eine Risikoreduzierung erforderlich ist. Die gezeigte Wirksamkeit des erweiterten Schutzkonzepts führt zu dieser Reduzierung. Tabelle 9-1 zeigt die Neubewertung des Risikos für die Assets „Kommunikation“ und „Komponente“ nach Anwendung des erweiterten Schutzkonzepts.

Asset	Bedrohung	Bewertung des Risikos				Akzeptables Risiko	Risikoreduzierung erforderlich?
		Ausmaß der Bedrohung	Wahrscheinlichkeit des Eintritts	Schadenspotential	Gesamtrisiko		
Kommunikation	**S**	3	4	3	36	40	<Nein>
	T	3	3	3	27	50	<Nein>
	R	3	3	3	27	50	<Nein>
	I	3	2	3	18	50	<Nein>
	D	3	4	4	48	40	<Ja>
	E	3	2	3	18	50	<Nein>
Komponente	**S**	3	3	3	27	40	<Nein>
	T	3	2	3	18	50	<Nein>
	R	4	4	3	48	50	<Nein>
	I	3	2	3	18	50	<Nein>
	D	3	4	4	48	40	<Ja>
	E	4	3	4	48	50	<Nein>

Tabelle 9-1: Risikobewertung nach Anwendung des erweiterten Schutzkonzepts

Tabelle 9-1 zeigt im Vergleich zur eingehenden Risikobewertung in Tabelle 4-5 eine Reduzierung des Risikos für ein Automatisierungssystem. Hinsichtlich des Schutzes vor Angriffen auf die Verfügbarkeit (**D**), in Form von „Denial of Service“-Angriffen auf das Automatisierungssystem, verbleibt jedoch ein Restrisiko, was eine weitere Risikoreduzierung erfordert.

Korrupte Datenpakete (z.B. als Folge eines „Denial of Service“-Angriffs) können vor einer Weiterleitung an höher liegende Schichten durch die IT-Sicherheitsschicht erkannt bzw. verworfen werden. Diese Erkennung benötigt Ressourcen auf der jeweiligen Plattform, womit bei einer großen Anzahl an korrupten Datenpaketen die Verfügbarkeit beeinträchtigt sein könnte. Die Bedrohung **D** kann nur dann wirksam abgewehrt werden, wenn lediglich authentifizierte Teilnehmer am Netzwerk zugelassen werden. So können bspw. Switche die Authentizität eines angeschlossenen Teilnehmers überprüfen und damit den Zugang zur Kommunikationsinfrastruktur begrenzen (siehe Ausblick in Abschnitt 10.2).

10 Fazit und Ausblick

Kapitel 10 gibt ein kurzes inhaltliches Fazit zur vorliegenden Arbeit und gibt einen Ausblick auf mögliche anschließende Forschungs- und Entwicklungsvorhaben.

10.1 Fazit

Die vorliegende Arbeit hat gezeigt, dass die Sicherheit in der Automatisierungstechnik von besonderer Bedeutung ist. Der Begriff wird im Sinne von funktionaler Sicherheit und auch für die IT-Sicherheit mit unterschiedlicher Bedeutung verwendet. Insbesondere die funktionale Sicherheit genießt besondere Beachtung, da Mensch und Maschine bzw. die Umwelt vor Einflüssen des Automatisierungssystems geschützt werden. Die IT-Sicherheit hat heute noch einen geringeren Stellenwert und beschreibt den Schutz des Automatisierungssystems vor unerwünschter Einflussnahme. Um diese Einflussnahme zu unterbinden sind Schutzziele der IT-Sicherheit für ein (Automatisierungs-)system zu erfüllen.

Die zunehmende Vernetzung im Umfeld der Automatisierungstechnik und die damit einhergehende Bedrohungssituation für Automatisierungssysteme erfordert Schutzmaßnahmen für dessen IT-Sicherheit. Bei genauerer Betrachtung der aktuellen Bedrohungssituation und der zukünftigen Entwicklung in der Automatisierungstechnik stellt sich jedoch heraus, dass aktuelle Schutzmaßnahmen unzureichend auf diese Bedrohungssituation ausgerichtet sind. Es erfolgt lediglich eine Anpassung von Schutzmaßnahmen der IT-Sicherheit aus der Standard-IT unter der Annahme starrer Automatisierungsstrukturen. Dieser Aspekt bietet Möglichkeiten zur Optimierung des Schutzes der IT-Sicherheit von Automatisierungssystemen.

An diesem Punkt greifen ergänzende Schutzmaßnahmen für ein erweitertes Schutzkonzept. Ausgangspunkt ist die Betrachtung der Schutzziele der IT-Sicherheit unter gezielter Berücksichtigung der Anforderungen aus der Automatisierungstechnik. Ziel ist der vollständige Schutz der Kommunikation und Komponenten des Automatisierungssystems. Die vorliegende Arbeit wendet dabei ergänzende Schutzmaßnahmen auf Basis kryptografischer Verfahrensweisen an, da so eine vollständige Abdeckung aller gesetzten Schutzziele möglich ist. Erreicht wird dies vor allem dadurch, dass die ergänzenden Schutzmaßnahmen im Gegensatz zu den aktuellen Schutzmaßnahmen keine Einzelmaßnahmen darstellen, sondern eine gemeinsame kryptografische Basis nutzen.

Das erweiterte Schutzkonzept vereint die ergänzenden Schutzmaßnahmen in einer sogenannten IT-Sicherheitsschicht. Die IT-Sicherheitsschicht übernimmt die gesamte Verwaltung der ergänzenden Schutzmaßnahmen. Die Schicht reduziert die Komplexität zur Handhabung der ergänzenden Schutzmaßnahmen und macht eine einfache Umsetzung der Maßnahmen, auch für andere industrielle Kommunikationsprotokolle, möglich. Im Zuge einer Evaluierung konnte nachgewiesen werden, dass der Einsatz von kryptografischen Verfahren auf den Komponenten des Automatisierungssystems zu deren Schutz möglich ist. Mit Hilfe von Messungen relevanter kryptografischer Verfahren ist gezeigt worden, dass auch durch Anwendung kryptografischer Verfahren der Schutz einer authentifizierten (echtzeitfähigen) Kommunikation möglich ist. Eine Zustandsüberwachung der Komponenten vervollständigt das erweiterte Schutzkonzept.

Die Validierung des erweiterten Schutzkonzepts ist an einer beispielhaften Automatisierungsanlage erfolgt. Die Validierung des Schutzkonzepts zeigte, dass durch die vorliegende Arbeit ein Beitrag zum verbesserten Schutz von Automatisierungssystemen erreicht wird. Sowohl die Automatisierungskomponenten wie auch die Kommunikation verfügen über einen wirksamen Schutz gegen Angriffe.

10.2 Ausblick

Aus der Validierung in Abschnitt 9.3 und den Ergebnissen dieser Arbeit ergeben sich weitere Aufgaben, die nachfolgend dargestellt werden sollen. Diese Aufgaben bauen direkt auf den Ergebnissen dieser Arbeit auf und sind direkte Weiterentwicklungen bzw. neue Forschungs- und Entwicklungsarbeiten im Bereich der IT-Sicherheit für die Automatisierungstechnik.

- **Erprobung des Einsatzes von hardware-basierten Kryptolösungen zur Beschleunigung von kryptografischen Funktionen.**

In Kapitel 8 ist eine software-basierte Evaluierung von kryptografischen Funktionen durchgeführt worden. Insbesondere die symmetrischen kryptografischen erwiesen sich dabei als geeignet für die Kommunikation mit kleinen Zykluszeiten. Um die Ausführungszeiten der kryptografischen Funktionen weiter zu verringern und die Ressourcen der Komponenten zu schonen, ist eine gezielte Erprobung von zusätzlichen hardware-basierten Kryptolösungen sinnvoll. Erste Ergebnisse dazu sind vielversprechend. [RTN2012a], [RCT2013], [CHH2013]

- **Einbindung von kryptografischen Maßnahmen zum Schutz der Kommunikationsinfrastruktur.**

Der angenommene Betrachtungsgegenstand definiert den Switch als Bestandteil der Kommunikationsinfrastruktur. Da zunehmend Switches Aufgaben einer Automatisierungskomponente übernehmen, können diese ebenfalls in die gesicherte Kommunikation und die Zustandsüberwachung als eigenständige Komponente eingebunden werden. Dazu sind die Maßnahmen des erweiterten Schutzkonzepts auf Switches zu übertragen, womit der Schutz des Automatisierungssystems weiter verbessert werden kann. So können sich bspw. nur authentifizierte Netzwerkteilnehmer am Switch anmelden und an der Kommunikation teilnehmen.

- **Einsatz von Software-Werkzeugen zur Vereinfachung der Schwachstellen- und Bedrohungsanalyse in Form eines (teil-)automatisierten Ansatzes.**

Die in dieser Arbeit beispielhaft durchgeführte Bedrohungsanalyse zeigt auf, dass je nach Umfang des zu untersuchenden Betrachtungsgegenstandes eine große Menge an Informationen gewonnen wird, die auszuwerten ist. Um diesen Prozess wesentlich zu vereinfachen, um damit auch nachhaltig die IT-Sicherheit zu verbessern, können (teil-)automatisierte Software-Werkzeuge eingesetzt werden, die die Schwachstellen- und Bedrohungsanalyse in einem Automatisierungssystem unterstützen.

- **Gezielter Einsatz von sicheren Laufzeitumgebungen zur weiteren Verhinderungen von Manipulationen an den Automatisierungskomponenten.**

Die Ausführung von Systemfunktionen im unsicheren Speicher der Komponenten stellt eine potentielle Schwachstelle dar, da ein Angreifer auf diese Funktionen Zugriff erhalten kann. Diese Schwachstelle betrifft auch die in dieser Arbeit implementierten erweiterten Schutzmaßnahmen. Durch Anwendung einer sicheren Laufzeitumgebung, wie bspw. dem ARM „TrustZone“-Konzept [ARM2009], kann eine direkte Manipulation der Systemfunktionen durch Angreifer verhindert werden und ist daher weiter zu betrachten.

- **Implementierung des erweiterten Schutzkonzepts in weitere Kommunikationsprotokolle der Automatisierungstechnik.**

Das in dieser Arbeit erstellte Schutzkonzepts ist am Beispiel des Industrial Ethernet Protokoll PROFINET implementiert worden. Die Einbindung der erarbeiteten IT-Sicherheitsschicht nach der gewählten Realisierungsalternative erlaubt prinzipiell die Übertragung des erweiterten Schutzkonzepts auf andere Industrial Ethernet Protokolle und Feldbustechnologien.

- **Erarbeitung einer IT-Sicherheitsinfrastruktur für Automatisierungssysteme im Kontext von „Industrie 4.0“.**

Die zunehmende Vernetzung im Umfeld der Automatisierungstechnik bringt neue (übergreifende) Infrastrukturen von Automatisierungssystemen hervor, bspw. in Form der „Industrie 4.0“-Initiative. Dieser Umstand erfordert neuartige erweiterte Schutzmaßnahmen, wie sie in dieser Arbeit erarbeitet wurden. Der Schutz der Kommunikation und der Komponenten ist dabei nicht auf einen abgeschlossenen Bereich eines Automatisierungssystems begrenzt.

Aufgabe weiterer Forschungs- und Entwicklungsarbeiten ist jedoch die Untersuchung der Handhabbarkeit komplexer Automatisierungssysteme mit zahlreichen Komponenten zur Erarbeitung einer IT-Sicherheitsinfrastruktur, wobei Schutzmaßnahmen nach dem Vorbild dieser Arbeit zum Einsatz kommen sollten.

Literaturverzeichnis

[ADH2010] Adamczyk, H.; Döhring, T.; Heiss, S.: Verfahren zur Identifikation und Analyse von IT-Security Schwachstellen für Automatisierungsgeräte. In: Kommunikation in der Automation (KOMMA 2010), Lemgo, Deutschland, November 2010.

[AKB2009a] Akerberg, J.; Bjorkman, M.: Exploring Security in PROFINET IO. In: Computer Software and Applications Conference (COMPSAC 09). Seattle, Washington, USA, Juli 2009.

[AKB2009b] Akerberg, J.; Bjorkman, M.: Introducing security modules in PROFINET IO. In: IEEE Conference on Emerging Technologies & Factory Automation (ETFA 2009), Palma de Mallorca, Spanien, September 2009.

[AKB2009c] Akerberg, J.; Björkman, M.: Exploring Network Security in PROFIsafe. In: 28th International Conference on Computer Safety, Reliability, and Security (SAFECOMP 2009). Hamburg, Deutschland, September 2009; S. 67-80.

[ALL2013] Allerkamp, A.: Die versteckte Gefahr. IT-Sicherheit in der Produktion. http://testlab.sit.fraunhofer.de/content/output/article/0605Produktionssicherheit.php, 15.05.2013.

[AND2001] Anderson, R.: Security engineering. A guide to building dependable distributed systems. Wiley, New York, 2001.

[ARM2009] ARM: ARM Security Technology. Building a Secure System using TrustZone Technology, 14.01.2014.

[BEI2011] Beirer, S.: Tanzende Affen und andere Schwachstellen in SIMATIC S7-Steuerungen - All-About-SECURITY. http://www.all-about-security.de/security-artikel/organisation/security-management/artikel/12758-tanzende-affen-und-andere-schwachstellen-in-simatic-s7-steue/, 24.10.2012.

[BEM2007] Bettenhausen, K.; Morr, W.: Informationssicherheit in der Automatisierung. Mehr als eine technologische Herausforderung. In: atp - Automatisierungstechnische Praxis. Ausgabe 4, Jg. 49, Oldenbourg Industrieverlag, München, 2007; S. 76–79.

[BLE2005] Bless, R.: Sichere Netzwerkkommunikation. Grundlagen, Protokolle und Architekturen ; mit 12 Tabellen. Springer Verlag, Berlin [u.a.], 2005.

[BVP2003] Boesgaard, M.; Vesterager, M.; Pedersen, T.; Christiansen, J.; Scavenius, O.: Rabbit. A New High-Performance Stream Cipher. In: 10th International Workshop on Fast Software Encryption (FSE 2003). Lund, Schweden, Februar 2003.

[BOH2006] Bormann, A.; Hilgenkamp, I.: Industrielle Netze. Ethernet-Kommunikation für Automatisierungsanwendungen. Hüthig-Verlag, Heidelberg, 2006.

[BSI2008a] BSI: BSI-Standard 100-3 - Risikoanalyse auf der Basis von IT-Grundschutz, 2008.

[BSI2008b] BSI: BSI-Standard 100-1 - Managementsysteme für Informationssicherheit (ISMS), 2008.

[BSI2008c] BSI: BSI TR-02102. 1.0: Kryptographische Verfahren: Empfehlungen und Schlüssellängen, 2008.

[BSI2010a] BSI: BSI Lagebericht: 3. Quartal 2010, 2010.

[BSI2010b] BSI: IT-Grundschutz-Kataloge. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html, 07.05.2013.

[BSI2013a] BSI: Gefährdungskataloge. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/Gefaehrdungskataloge/gefaehrdungskataloge_node.html, 11.07.2013.

[BSI2013b] BSI: M 5.150: Durchführung von Penetrationstests, 2013.

[BSI2014] BSI: Industrial Control System Security. Top 10 Bedrohungen und Gegenmaßnahmen 2014, 2014.

[BUN2013] Bundesministerium des Innern: "IT-Sicherheitsgesetz" (Entwurf), http://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/Entwuerfe/Entwurf_it-sicherheitsgesetz.pdf;jsessionid=DD7C8E211F44CA4095A6E7113FC61CC9.2_cid295?__blob=publicationFile, 14.12.2013.

[CHA2009] ChannelPartner: Schon wieder Ausfall in einem LCD-Glaswerk von Corning. http://www.channelpartner.de/knowledgecenter/displays_beamer/283614/, 11.06.2013.

[CHH2013] Czybik, B.; Hausmann, S.; Heiss, S.; Jasperneite, J.: Performance Evaluation of MAC Algorithms for Real-Time Ethernet Communication. In: IEEE International Conference on Industrial Informatics (INDIN 2013). Bochum, Deutschland, Juli 2013.

[COM2009] Common Criteria CCMB-2009-07-001 Rev 3. 3.1: Common Methodology for Information Technology Security Evaluation - Part 1: Introduction and general model (IEC 15408-1), 2009.

[COR2012] Corporate Trust: Studie: Industriespionage 2012. Aktuelle Risiken für die Wirtschaft durch Cyberwar, München, 2012.

[DHS2009] DHS/CERT: Catalog of Control Systems Security. Recommendations for Standards Developers, 2009.

[DHS2011] DHS/CERT: Catalog of Control Systems Security. Recommendations for Standards Developers, 2011.

[DHS2012] DHS/CERT: ICS-CERT Incident Response Summary Report. 2009-2011, 2012.

[DIE2004] Dierstein, R.: Sicherheit in der Informationstechnik. Der Begriff IT-Sicherheit. In: Informatik Spektrum. Ausgabe 4, Springer, 2004; S. 343–353.

[DIH1976] Diffie, W.; Hellman, M.: New Directions in Cryptography. In: IEEE Transactions on Information Theory. Ausgabe 6, Jg. 22, IEEE, 1976; S. 644–654.

[DIG2013] Digital Bond: Project “Basecamp”. http://www.digitalbond.com/tools/basecamp/, 08.05.2013.

[DIN2008] DIN 62541-2: OPC Unified Architecture – Teil 2: Modell für die IT-Sicherheit. 2008.

[DIT2013] Ditting, S.: Die Zukunft der Sicherheit in Industrie 4.0. In: AUTOMATION 2013 (VDI/GMA-Kongress). Baden-Baden, Deutschland, Juli 2013.

[DKE2012] DKE: Referenzmodel – Gerätemodell (Generische Kernmodelle als gemeinsame Basis für die Normungsarbeit im FB9). DKE, 2012.

[DKE2013] DKE-IEV: DKE-IEV Online Wörterbuch. www.dke.de/dke-iev, 22.10.2013.

[DOY1983] Dolev, D.; Yao, A.: On the security of public key protocols. In: IEEE Transactions on Information Theory. Ausgabe 2, Jg. 29, IEEE, 1983; S. 198–208.

[DNH2005] Dzung, D.; Naedele M.; Hoff, T. P. von; Crevatin, M.; Naedele, M.; Hoff, T. von: Security for industrial communication systems. In: Proceedings of the IEEE. Ausgabe 6, Jg. 93, IEEE, 2005; S. 1152–1177.

[ECK2009] Eckert, C.: IT-Sicherheit. Konzepte - Verfahren - Protokolle. Oldenbourg Industrieverlag, München, 2009.

[ENI2013] ENISA: Algorithms, Key Sizes and Parameters Report. 2013 recommendations. October 2013, 2013.

[ESC2010] ESCoRTS Consortium: Survey of Existing Methods, Procedures and Guidelines. European Netowrk For the Secuirty of Control and Real Time Systems. Survey of Existing Methods, Procedures and Guidelines Deliverable, 2010.

[FWS2003] Ferguson, N.; Whiting D.; Schneier B.; Kelsey J.; Lucks S.; Kohno T.: Helix. Fast Encryption and Authentication in a Single Cryptographic Primitive. In: 10th International Workshop on Fast Software Encryption (FSE 2003). Lund, Schweden, Februar 2003.

[FFV2011] Ferrari, P.; Flammini, A.; Venturini, F.; Augelli, A.: Large PROFINET IO RT networks for factory automation: a case study. In: IEEE Conference on Emerging Technologies and Factory Automation (ETFA 2011). Toulouse, Frankreich, September 2011.

[FOA2013] Forschungsunion acatech: Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0. Abschlussbericht des Arbeitskreises Industrie 4.0. Deutschlands Zukunft als Produktionsstandort sichern. http://www.plattform-i40.de/sites/default/files/Bericht_Industrie%204.0_0.pdf, 25.04.2013.

[FRA2014] Fraunhofer: Herausforderungen für die IT-Sicherheitsforschung. Strategie- und Positionspapier Cyber-Sicherheit 2020, 2014.

[FRE2010] Freescale Semiconductor: MPC8313E PowerQUICC II Pro Integrated Processor Family Reference Manual. Supports MPC8313E MPC8313. http://www.freescale.com/files/32bit/doc/ref_manual/MPC8313ERM.pdf.

[FUR2003] Furrer, F. J.: Industrieautomation mit Ethernet-TCP/IP und Web-Technologie. Hüthig-Verlag, Heidelberg, 2003.

[GDR2007] Gang, C.; Dong, Y.; Rensheng, C.: Developing Trend of Industrial Fieldbus Control System. In: International Conference on Electronic Measurement and Instruments (ICEMI 2007). Xian, China, September 2007; S. 765–768.

[GEG2006] Gevatter, H.-J.; Grünhaupt, U.: Handbuch der Mess- und Automatisierungstechnik in der Produktion. Springer, Berlin [u.a.], 2006.

[GNU2013] GnuTLS: GnuTLS. The GnuTLS Transport Layer Security Library. http://www.gnutls.org/, 13.08.2013.

[GRA2003] Grams, T.: Risikooptimierung kontra Risikobegrenzung. Analyse eines alten und andauernden Richtungsstreits. In: Automatisierungstechnische Praxis. Ausgabe 8, Jg. 45, Oldenbourg Industrieverlag, München, 2003; S. 50–57.

[GUT2010] Gutbrodt, F.: Effizienter Schutz der IT-Sicherheit auf der Feldebene von Automatisierungssystemen. Dissertation. Shaker, Stuttgart, 2010.

[GUG2006] Gutbrodt, F.; Göhner, P.: IT-Sicherheit auf der Feldebene von Automatisierungssystemen. In: Entwurf komplexer Automatisierungssysteme (EKA 2006). Braunschweig, Deutschland, Mai 2006.

[HVM2004] Hankerson, D. R.; Vanstone, S. A.; Menezes, A. J.: Guide to elliptic curve cryptography. Springer-Verlag, Berlin [u.a.], 2004.

[HAH2011] Harris, J.; Hill, R. L.: StaticTrust. A Practical Framework for Trusted Networked Devices. In: 44th Annual Hawai'i International Conference on System Sciences (HICSS 2011). Koloa, Hawaii, USA, Januar 2011.

[HAR2011] Harsch, M.: Schwachstellenanalyse sowie Konzeption und prototypische Implementierung einer PROFINET-Protokollerweiterung. Bachelorarbeit, Hochschule Hannover, Hannover, 2011.

[HAU2006] Hauf, T.: Prozessleitsysteme: Lebenszyklus und Qualität. In: Automatisierungstechnische Praxis. Ausgabe 2, Jg. 48, 2006; S. 34–42.

[HAH2012] Hausmann, S.; Heiss, S.: Usage of Public Key Infrastructures in Automation Networks. In: IEEE Conference on Emerging Technologies and Factory Automation (ETFA 2012). Krakau, Polen, September 2012; S. 1069–1075.

[HEN2012] Hensel, R.: Industrie 4.0 revolutioniert die Produktion. In: VDI Nachrichten. Ausgabe 49. 2012.

[IEC1999] IEC 61508-5: Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 5: Examples of methods for the determination of safety integrity levels, 1999.

[IEC2001] IEC 61882: Hazard and operability studies (HAZOP studies) – Application guide, 2001.

[IEC2006a] IEC 60812 Ed. 2.0: Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA), 2006.

[IEC2006b] IEC 61025 Ed. 2.0: Fault Tree Analysis (FTA), 2006.

[IEC2007] IEC 62351-1. 1.0: Communication network and system security – Part 1 Introduction to security issues, 2007.

[IEC2008a] IEC 61158-5-10: Industrial communication networks - Fieldbus specifications - Part 5-10: Application layer service definition, 2008.

[IEC2008b] IEC 61784-1: Industrial communication networks – Profiles – Part 1: Fieldbus profiles, 2008.

[IEC2008c] IEC 61784-2: Industrial communication networks – Profiles – Part 2: Additional fieldbus profiles for real-time networks based on ISO/IEC 8802-3, 2008.

[IEC2011] IEC 27000: Information technology – Security techniques – Information security management systems, 2011.

[IEC2012a] IEC 27000: Information technology – Security techniques – Information security management systems – Overview and vocabulary, 2012.

[IEC2012b] IEC 62443-1-1: Security for industrial automation and control systems - Part 1.1: Terminology, Concepts, and Models, 2012.

[IEE2008] IEEE 802.3-2008: Part 3: Carrier sense multiple access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications. IEEE Computer Society, New York, 2008.

[IEE2009] IEEE 802.1AE: Secure Device Identity, 2009.

[INT1999] Internet Engineering Task Force RFC 3766: Photuris: Session-Key Management Protocol. Network Working Group, 1999.

[INT2000] Internet Engineering Task Force RFC 2828: Internet Security Glossary. Network Working Group, 2000.

[INT2004] Internet Engineering Task Force RFC 3748: Extensible Authentication Protocol (EAP). Network Working Group, 2004.

[INT2005a] Internet Engineering Task Force RFC 4306: Internet Key Exchange (IKEv2) Protocol. Network Working Group, 2005.

[INT2005b] Internet Engineering Task Force RFC 4302: IP Authentication Header (AH). Network Working Group, 2005.

[INT2005c] Internet Engineering Task Force RFC 4303: IP Encapsulating Security Payload (ESP). Network Working Group, 2005.

[INT2005d] Internet Engineering Task Force RFC 4301: Security Architecture for the Internet Protocol. Network Working Group, 2005.

[INT2008] Internet Engineering Task Force RFC 5246: The Transport Layer Security (TLS) Protocol. Network Working Group, 2008.

[ISO2008] ISO 9001: Quality Manangement Systems, 2008.

[ISO1996] ISO/IEC 7498-1: Information technology - Open Systems Interconnection - Basic Reference Model: The Basic Model, 1996.

[ISO1998] ISO/IEC 2382-8: Information technology - Vocabulary - Security, 1998.

[ITU2000] ITU X.509: Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks, 2000.

[JAH2003] Jahnke, M.: Schutz von verteilten Intrusion-Detection-Systemen gegen DoS-Angriffe. In: 10. Workshop Sicherheit in Vernetzten Systemen (DFN-CERT). Hamburg, Deutschland, Februar 2003.

[JAS2012] Jasperneite, J.: Was hinter Begriffen wie Industrie 4.0 steckt. Internet und Automation. http://www.computer-automation.de/steuerungsebene/steuernregeln/fachwissen/article/93559/?type=99, 25.04.2013.

[KKW2012] Kersten, H.; Klett, G.; Wolfenstetter, K.-D.: Der IT Security Manager. Aktuelles Praxiswissen für IT Security Manager und IT-Sicherheitsbeauftragte in Unternehmen und Behörden. Vieweg+Teubner, Wiesbaden, 2012.

[KOC2011] Koch, R.: Systemarchitektur zur Ein- und Ausbruchserkennung in verschlüsselten Umgebungen. Books on Demand, Norderstedt, 2011.

[KRE2013] Kreuzer, M.: Kraftwerke durch Malware lahm gelegt. http://www.energie-und-technik.de/automatisierung/news/article/94110/, 14.06.2013.

[MAM2006] Mana, A.; Munoz, A.: Protected Computing vs. Trusted Computing. In: International Conference on Communication System Software and Middleware (COMSWA 2006). Neu Dehli, Indien, Januar 2006; S. 1–7.

[MAT2011] Matzer, M.: Hackerangriffe immer raffinierter und gezielter. In: VDI Nachrichten. Ausgabe 22, 2011.

[MVV2001] Menezes, A. J.; van Oorschot, Paul C.; Vanstone, Scott A.: Handbook of applied cryptography. http://cacr.uwaterloo.ca/hac/, 12.10.2013.

[MIC2002] Microsoft: The STRIDE Threat Model. http://msdn.microsoft.com/en-US/library/ee823878(v=CS.20).aspx, 06.06.2013.

[MIC2014] Microsoft: Acquiring high-resolution time stamps. QueryPerformanceCounter (QPC). http://msdn.microsoft.com/en-us/library/aa915073.aspx, 25.03.2014.

[MOR2012] Morse, J.: The world market for Industrial Ethernet components. In: The Industrial Ethernet Book. Ausgabe 69, 2012.

[MUE2008] Mueller, T.: Trusted Computing Systeme. Konzepte und Anforderungen. In: Trusted Computing Systeme, Springer-Verlag, Berlin [u.a.], 2008.

[NAM2004] NAMUR 103: Einsatz von Internettechnologien in der Prozessautomatisierung, 2004.

[NAM2006] NAMUR 115: IT-Sicherheit für Systeme der Automatisierungstechnik, 2006.

[NJW2004] Ning, P.; Jajodia, S.; Wang, S.: Intrusion detection in distributed systems. An abstraction-based approach. Kluwer Academic Publishers, Boston, 2004.

[NIS2001a] NIST 197: Advanced Encryption Standard (AES), 2001.

[NIS2001b] NIST 800-38A: Recommendation for Block Cipher Modes of Operation- Methods and Techniques, 2001.

[NIS2002] NIST 198: The Keyed-Hash Message Authentication Code (HMAC), 2002.

[NIS2008] NIST: Malicious Control System Cyber Security Attack Case Study Maroochy Water Services, Australia. http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf, 29.11.2011.

[NIS2009a] NIST 800-108: Recommendation for Key Derivation Using Pseudorandom Functions (Revised), 2009.

[NIS2009b] NIST: Recommended Security Controls for Federal Information Systems and Organizations. 800-53 - Rev3. http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf, 24.09.2010.

[NIS2011] NIST 800-571 Part 1. Rev. 3: Recommendation for Key Management - Special Publication 800-57, 2011.

[NIS2012a] NIST 800-38B: Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, 2012.

[NIS2012b] NIST 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, 2012.

[NIS2012c] NIST 180-4: Secure Hash Standard, 2012.

[NIS2012d] NIST FIPS 186-3: Digital Signature Standard (DSS) - ECDSA, 2012.

[NIS2012e] NIST: The Galois/Counter Mode of Operation (GCM), 2012.

[NSA2013] NSA: NSA Suite B Cryptography - NSA/CSS. http://www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml, 31.05.2013.

[ODV2011] ODVA: Securing EtherNet/IP Networks. http://www.odva.org/Portals/0/Library/Publications_Numbered/PUB00269R0_ODVA_Securing_EtherNetIP_Networks.pdf, 11.11.2011.

[OPE2014] OpenSSL: OpenSSL. The Open Source toolkit for SSL/TLS. http://www.openssl.org/, 10.04.2014.

[OPE2013] OpenVPN: OpenVPN - Open Source VPN. http://openvpn.net/, 13.08.2013.

[PIM2005] Pigan, R.; Metter, M.: Automatisieren mit PROFINET. Industrielle Kommunikation auf Basis von Industrial Ethernet. Publicis Corp. Publ., Erlangen, 2005.

[PNO2007] PNO: PROFIsafe Specifiation. Systembeschreibung, Karlsruhe, 2007.

[PNO2010] PNO: PROFINET Specification v.2.3.. PROFIBUS Nutzerorganisation e.V., Karlsruhe, 2010.

[PNO2014] PNO: PROFINET Security Guideline. PROFIBUS Nutzerorganisation e.V., Karlsruhe, 2014.

[POR2008] Pohlmann, N.; Reimer, H.: Trusted Computing. Ein Weg zu neuen IT-Sicherheitsarchitekturen. Vieweg-Verlag, Wiesbaden, 2008.

[POP2005] Popp, M.: Das PROFINET-IO-Buch. Grundlagen und Tipps für Anwender. Hüthig-Verlag, Berlin, 2005.

[PHK2013] Preschern, C.; Hormer, A. J.; Kajtazovic, N.; Kreiner, C.: Software-Based Remote Attestation for Safety-Critical Systems. In: IEEE Conference on Software Testing, Verification and Validation Workshops (ICSTW 2013). Luxemburg, Luxemburg, März 2013; S. 8–12.

[RAN2010] Rankl, W.: Smart card handbook. Wiley, Chichester, U.K, 2010.

[RCT2013] Runde, M.; Czybik, B.; Tebbe, C.; Hausmann, S.; Niemann, K.-H.; Heiss, S.: Performanceevaluation eines Security-Layers für die Echtzeitkommunikation mit PROFINET auf ressourcenbeschränkten Plattformen. In: AUTOMATION 2013 (VDI/GMA-Kongress). Baden-Baden, Deutschland, Juni 2013.

[REI2002] Reissenweber, B.: Feldbussysteme zur industriellen Kommunikation. Oldenbourg Industrieverlag, München, 2002.

[RES2000] Rescorla, E.: SSL and TLS. Building and designing secure systems. Addison-Wesley, Harlow, 2000.

[RUN2008] Runde, M.: Coexistence of Different Ethernet-Based Fieldbus Systems on a single Ethernet Network. Diplomarbeit, Hochschule Hannover, Hannover, 2008.

[RNH2012] Runde, M.; Niemann, K.-H.; Hausmann, S.; Heiss, S.: Anwendung komponentenbezogener IT-Sicherheitsmaßnahmen in Automatisierungsnetzwerken. In: AUTOMATION 2012 (VDI/GMA-Kongress). Baden-Baden, Deutschland, Juni 2012.

[RNT2012] Runde, M.; Niemann, K.-H.; Tebbe, C.: Hardware-basierte IT-Sicherheitstechnologien in der Automatisierungstechnik. In: atp edition - Automatisierungstechnische Praxis. Ausgabe 3, Jg. 54, Oldenbourg Industrieverlag, München, 2012; S. 42–49.

[RTN2013] Runde, M.; Tebbe, C.; Niemann, K.-H.: Performance evaluation of an IT security layer in real-time communication. In: IEEE Conference on Emerging Technologies and Factory Automation (ETFA 2013). Cagliari, Italien, September 2013.

[RTN2012a] Runde, M.; Tebbe, C.; Niemann, K.-H.; Börgmann, A.: IT-Security in Automatisierungsnetzwerken unter Verwendung kryptografischer Maßnahmen. In: Kommunikation in der Automation (KOMMA 2012). Lemgo, Deutschland, November 2012; S. 156–165.

[RTN2012b] Runde, M.; Tebbe, C.; Niemann, K.-H.; Toemmler, J.: Automated Decentralized IT Security Supervision in Automation Networks. In: IEEE International Conference on Industrial Informatics (INDIN 2012). Beijing, China, Juli 2012.

[RUN2013] Runde, M.; Niemann, K.-H.: Security in der Komponente. In computer&AUTOMATION. Ausgabe 3, WEKA Fachmedien, München. 2013; S. 28-31.

[SCH2011] Schleupner, L.: Sichere Kommunikation in der Automatisierungstechnik. Dissertation, Fernuniversität Hagen, Hagen, 2011.

[SCH1999] Schneier, B.: A Plea For Simplicity. You can't secure what you don't understand. https://www.schneier.com/essay-018.html, 20.03.2014.

[SCH2006a] Schneier, B.: Angewandte Kryptographie. Protokolle, Algorithmen und Sourcecode in C. Pearson Studium, München [u.a.], 2006.

[SCH2006b] Schwarz, A. Hrsg.: Industrial Ethernet. Ethernet-basierte Automatisierungsprotokolle ; Volume Deutsch-Englisch. Vogel Industrie Medien, Würzburg, 2006.

[SEC2013] Security Insider: Wirtschaft sieht steigende Gefahren durch Cybercrime. http://www.security-insider.de/themenbereiche/sicherheits-management/risk-management/articles/404211/, 13.06.2013.

[TAR2010] Tarnovsky, C.: How to Crack a Smartcard Chip. In: BlackHat DC Conference, 2010.

[TEB2011] Tebbe, C.: Auswahl und Erprobung einer Security-Token Technologie für den Einsatz in Windows-basierten Automatisierungskomponenten. Masterarbeit, Hochschule Hannover, Hannover, 2011.

[THÜ2006] Thürmann, U.: Die Software-Uhr. https://www.ibr.cs.tu-bs.de/users/thuerman/time/kernel.html, 25.03.2014.

[TRU2007] Trusted Computing Group: Trusted Platform Module (TPM) Main Specification. Part 1: Architecture. v1.2, 2007.

[TRU2011] Trusted Computing Group: Trusted Platform Module (TPM) Main Specification. Part 1: Architecture. v2.0, 2011.

[VDI2008] VDI 2182 - Blatt 1. ICS 35.240.50: Informationssicherheit in der industriellen Automatisierung - Allgemeines Vorgehensmodell. VDI, 2008.

[VDI2009] VDI: Automation 2020. Bedeutung und Entwicklung der Automation bis zum Jahr 2020. Thesen und Handlungsfelder, 2009.

[VDI2011] VDI 2182 - Blatt 2.1. ICS 35.240.50: Informationssicherheit in der industriellen Automatisierung - Anwendungsbeispiel des Vorgehensmodells in der Fabrikautomation für Hersteller - Speicherprogrammierbare Steuerung (SPS). VDI, 2011.

[VDI2013] VDI: Thesen und Handlungsfelder - Cyber-Physical Systems. Chancen und Nutzen aus Sicht der Automation. http://www.vdi.de/uploads/media/Stellungnahme_CPS_2013-03-28_final_01.pdf, 25.04.2013.

[VER2014] Verizon: 2014 Data Breach Investigations Report, 2014.

[VID2008] Vidal, J.: No new coal - the calling card of the 'green Banksy' who breached fortress Kingsnorth | Environment | The Guardian. http://www.guardian.co.uk/environment/2008/dec/11/kingsnorth-green-banksy-saboteur, 27.06.2011.

[WYY2005] Wang, X.; Yin, L.; Yu, H.: Collision search attacks on SHA-1. In: International Cryptology Conference (CRYPTO 2005). Santa Barbara, California, USA, August 2005.

[WFS2013] Wieczorek, F.; Fiat, R.; Schiller, F.; Störtkuhl, T.: Zusammenhang von Security und Funktionaler Sicherheit. In: atp edition - Automatisierungstechnische Praxis. Ausgabe 6, Jg. 55, Oldenbourg Industrieverlag, München, 2013; S. 40–47.

[WKS2012] Wieczorek, F.; Krauß, C.; Schiller, F.; Eckert, C.: Towards secure fieldbus communication. In: 31th International Conference on Computer Safety, Reliability and Security (SAFECOMP 2012). Magdeburg, Deutschland, September 2012; S. 149–160.

[WIS2012] Wieczorek, F.; Schiller, F.: Safety und Security für Feldbus-Anforderungen. Architektur ermöglicht Nachweisbarkeit und Echtzeit. In: atp edition - Automatisierungstechnische Praxis. Ausgabe 10, Jg. 54, Oldenbourg Industrieverlag, München, 2012; S. 44–51.

[YOR2010] York, D.: Seven Deadliest Unified Communications Attacks. Syngress, Burlington, MA, USA, 2010.

[ZEL2011] Zeller, M.: Myth or Reality. Does the Aurora Vulnerability Pose a Risk to My Generator? In: Proceedings of the 6th International Conference on Availability, Reliability and Security (ARES 2011). Wien, Österreich, August 2011; S. 130–136.

A. Anhang

A.1 Zusammenstellung der Zustandsdiagramme

Die Zustandsdiagramme beschrieben die verschiedenen Funktionen des erweiterten Schutzkonzepts. Ausgangspunkt ist die Authentifizierung, welche nachfolgend dargestellt ist. Unterschieden wird zwischen Initiator und Responder der Authentifizierung.

Zustandsdiagramme der Authentifizierung

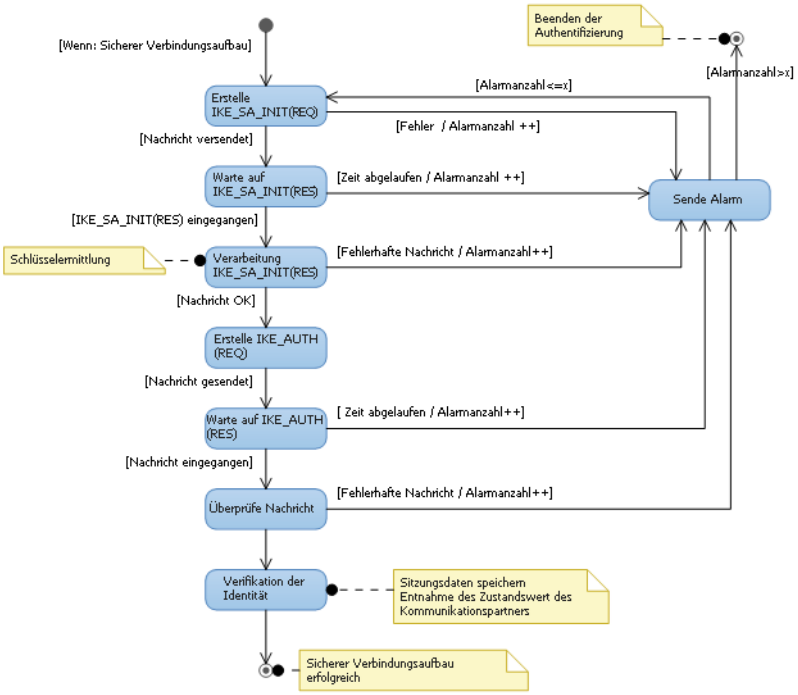


Abbildung A-1: Zustandsdiagramm „Authentifizierung (Initiator)“

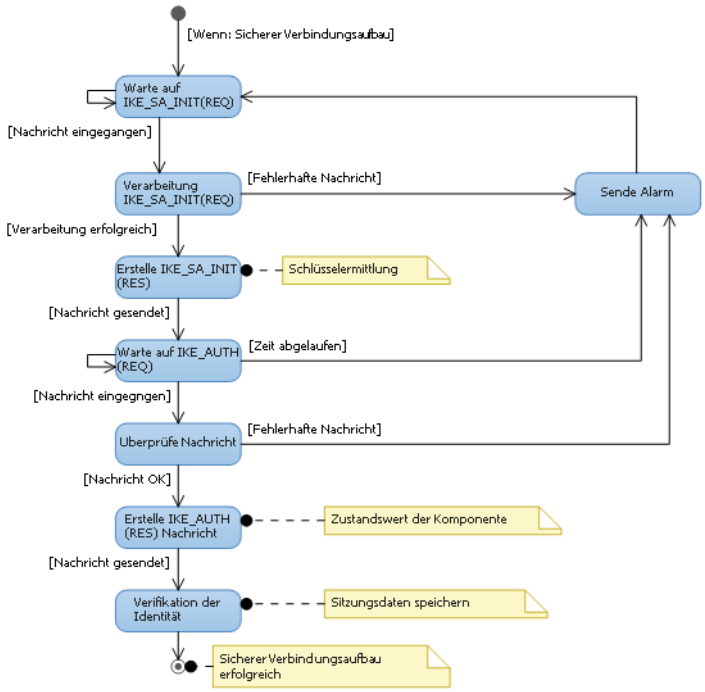


Abbildung A-2: Zustandsdiagramm „Authentifizierung (Responder)“

Nach erfolgter Authentifizierung (bzw. sicherem Verbindungsaufbau) starten die verschiedenen Funktionen des erweiterten Schutzkonzepts. Die Kommunikation zur Durchführung der Funktionen erfolgt dabei stets auf abgesichertem Wege. Je nachdem, ob eine SPS oder dezentrale Peripherie vorliegt bzw. Daten gesendet oder empfangen werden, unterscheiden sich die Zustandsdiagramme für die einzelnen Funktionen.

Zustandsdiagramme der (abgesicherten) Kommunikation

Die Abbildungen A-3 und A-4 zeigen die Zustandsdiagramme für das Senden und Empfangen der (gesicherten) (Prozessdaten-)kommunikation sowie der Übertragung von Konfigurations- und Parametrierdaten.

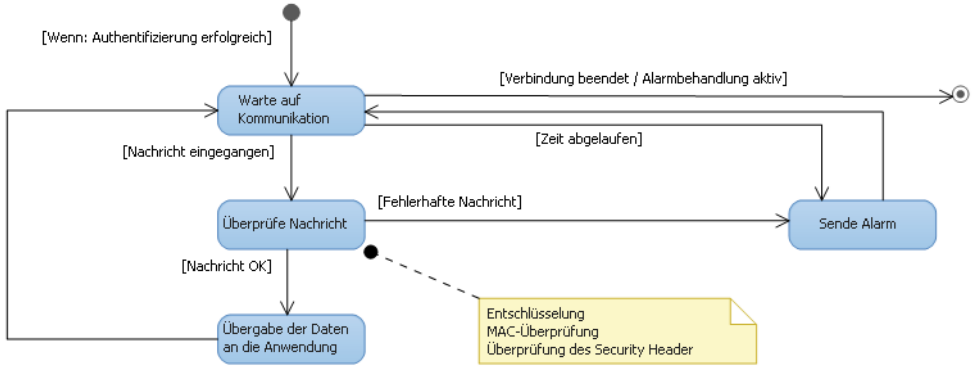


Abbildung A-3: Zustandsdiagramm „Kommunikation Empfang“

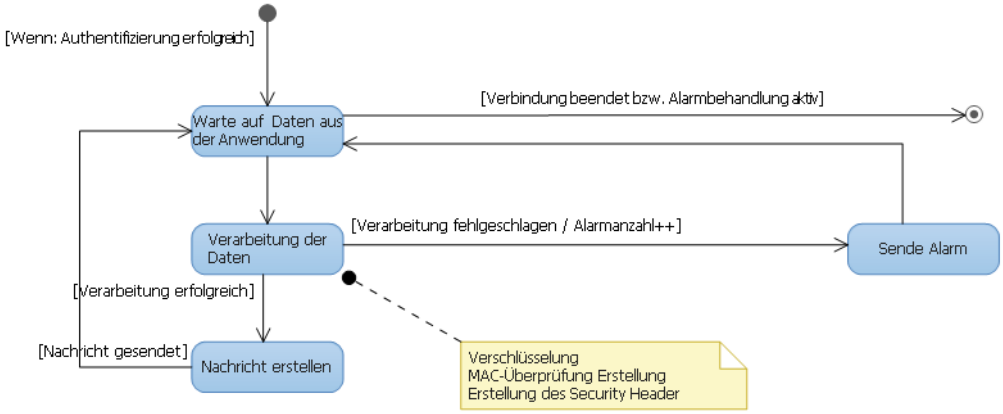


Abbildung A-4: Zustandsdiagramm „Kommunikation Senden“

Zustandsdiagramme der Zustandsüberwachung

In den Abbildungen A-5 und A-6 sind die Zustandsdiagramme der Zustandsüberwachung dargestellt. Die zu überwachende dezentrale Peripherie beantwortet mögliche Zustandsanfragen und führt zusätzlich in regelmäßigen Abständen eine eigens initiierte lokale Zustandsüberprüfung durch. Die SPS versendet im Gegenzug in regelmäßigen Zeitabständen Zustandsanfragen an die dezentralen Peripherien und leitet ggf. Maßnahmen zum Schutz des Automatisierungssystems ein, sofern mehrere Anfragen nicht beantwortet werden oder eine größere Anzahl an Alarmen aufgetreten ist.

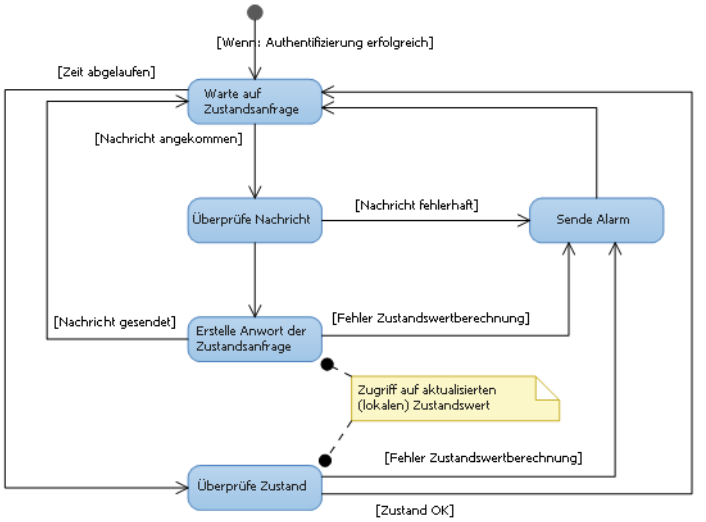


Abbildung A-5: Zustandsdiagramm „Zustandsüberwachung / dezentrale Peripherie“

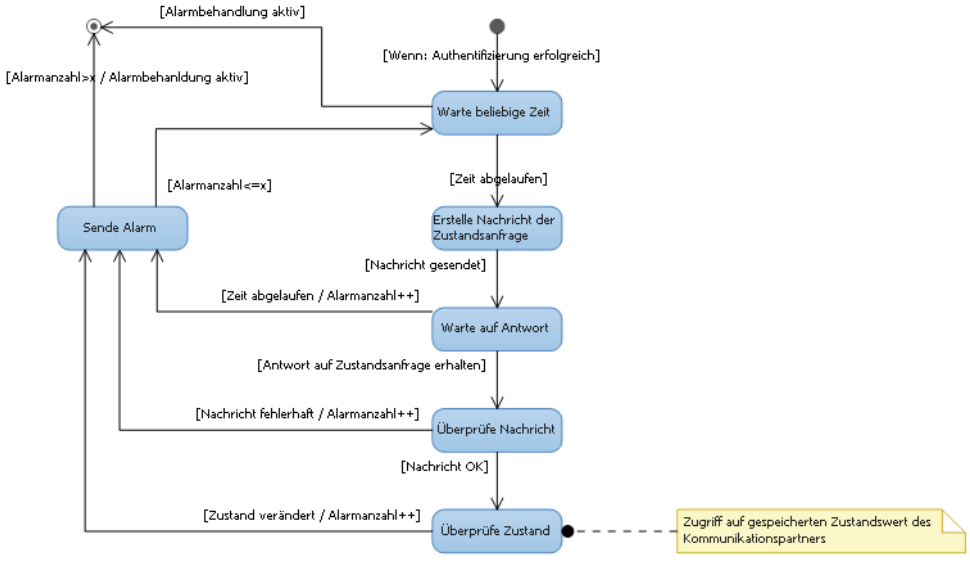


Abbildung A-6: Zustandsdiagramm „Zustandsüberwachung / SPS“

Zustandsdiagramme der Schlüsselerneuerung

Sowohl SPS als auch dezentrale Peripherie führen in regelmäßigen Abständen eine Erneuerung der für eine Kommunikationsbeziehung geltenden (symmetrischen) Schlüssel durch. Dies kann per Ableitung aus gemeinsamen vorhergehenden Schlüsseln oder durch Neuaushandlung erfolgen. Der Vorgang der Schlüsselerneuerung ist auf SPS und dezentraler Peripherie identisch. Jedoch ist im Gegensatz zur Schlüsselableitung, die von beiden Seiten unabhängig durchgeführt wird, die SPS der Initiator der Schlüsselneuaushandlung. Die Neuaushandlung erfolgt dann in Form des gezeigten Authentifizierungsvorgangs. Die parallelen Funktionen werden zu diesem Zweck nicht unterbrochen, sofern der Security Counter nicht abgelaufen ist.

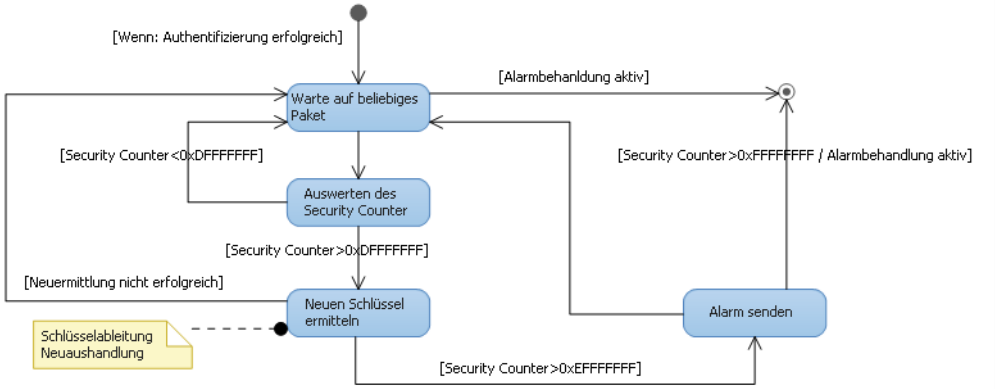


Abbildung A-7: Zustandsdiagramm „Schlüsselerneuerung / SPS“

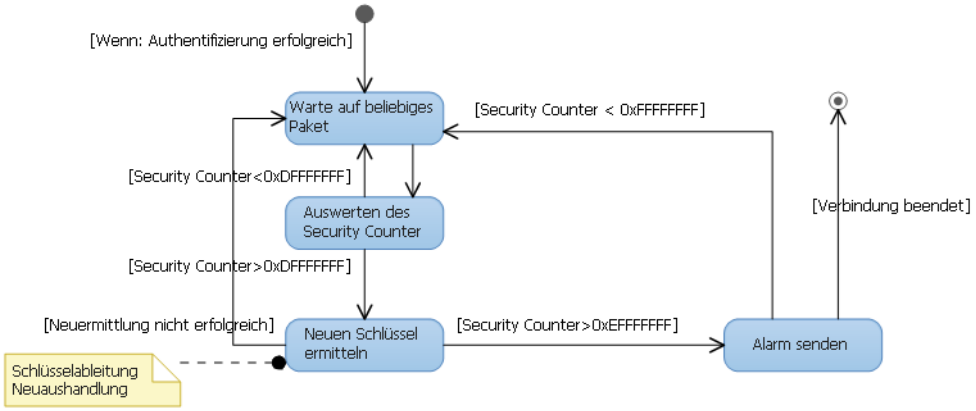


Abbildung A-8: Zustandsdiagramm „Schlüsselerneuerung / dezentrale Peripherie“

Zustandsdiagramme der Alarmsteuerung

SPS als auch dezentrale Peripherie sind in der Lage Alarme abzusetzen oder zu versenden. Abbildung A-9 zeigt diesen Vorgang anhand eines Zustandsdiagramms. Die SPS in Abbildung A-10, oder eine andere überwachende Komponente (z.B. ABK), registriert entsprechende Alarme und leitet ggf. Schutzmaßnahmen für das Automatisierungssystem aus den Alarmmeldungen ab.

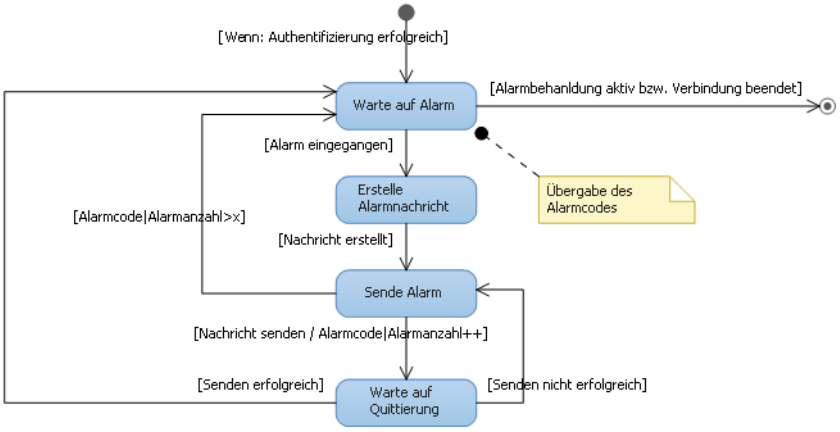


Abbildung A-9: Zustandsdiagramm „Alarmsteuerung / Alarme Auslösen und Senden“

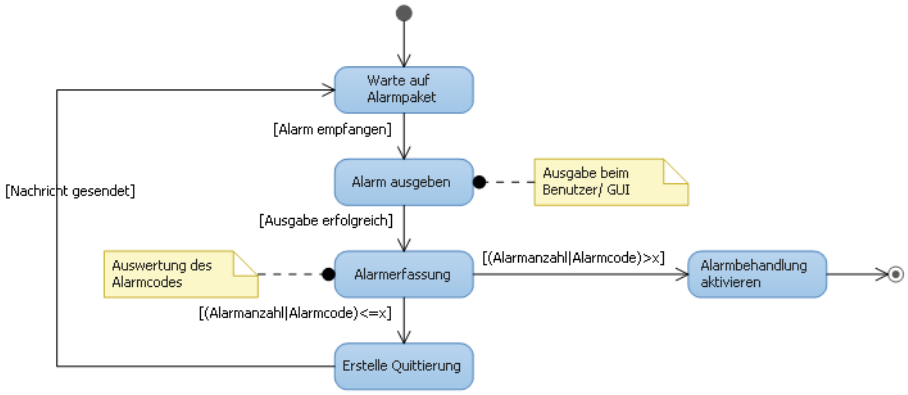


Abbildung A-10: Zustandsdiagramm „Alarmsteuerung / Alarme anzeigen und quittieren“

Das erweiterte Schutzkonzept sieht verschiedene Alarmmeldungen vor. Dabei erfolgt die Unterscheidung der Alarmmeldungen (neben der Absenderadresse) anhand des Alarmcodes. Beispielhafte Alarmcodes[1] sind in Abbildung A-11 dargestellt.

```
…
#define ALARM_COULD_NOT_INITIALIZE_PKI                    0x01
#define ALARM_CONNECTION_ABORT                            0x02
#define ALARM CONNECTION TIMEOUT                          0x03
#define ALARM CERTIFICATE JUST BEFOR EXPIRED              0x04
#define ALARM DEVICE CERTIFICATE EXPIRED                  0x05
#define ALARM IKE CONNECTION TIMEOUT                      0x06
#define ALARM_IKE_MESSAGE_ERROR                           0x07
#define ALARM_IKE_RES_ERROR                               0x08
#define ALARM MAC INCORRECT                               0x09
#define ALARM MAC CALCULATION FAILED                      0x10
#define ALARM ENCRYPTION FAILED                           0x11
#define ALARM DECRYPTION FAILED                           0x12
#define ALARM_ERROR_RECEIVED_PACKET                       0x13
#define ALARM_SECURITY_COUNTER_ERROR                      0x14
#define ALARM KEY RENEW FAILED                            0x15
#define ALARM KEY BEFOR EXPIRED                           0x16
#define ALARM CONDIT CALCULATION ERROR                    0x17
#define ALARM PLATTFORM CONFIG CHANGED                    0x18
#define ALARM_PLATTFORM_SOFTWARE_CHANGED                  0x19
…
```

Abbildung A-11: Benutzerdefinierte Alarmbehandlung (bsp. Alarmcodes)

[1] Alarmcodes in englischer Sprache aufgrund unterliegender Programmierung in selbiger Sprache.

A.2 Darstellung des Demonstrators

In Abschnitt 9.3 ist ein beispielhaftes Automatisierungssystem zur Demonstration und Validierung des erweiterten Schutzkonzepts eine beispielhafte Demonstrator verwendet worden. Anhang A.2 zeigt den Aufbau und die Bedienoberfläche des Demonstrators.

Aufbau des Demonstrators

Abbildung A-12 zeigt den Aufbau des Demonstrators des erweiterten Schutzkonzepts. Tabelle A-1 nimmt Bezug auf die Abbildung und stellt die Bestandteile des Demonstrators vor.

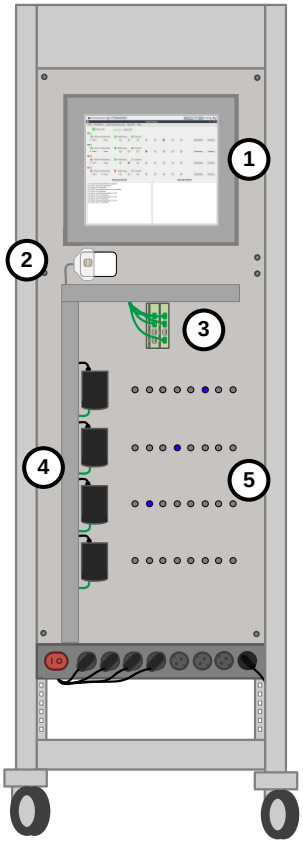


Abbildung A-12: Aufbau des Demonstrators

Bezeichnung		Beschreibung
①	HMI-Bedienstation	BNK als HMI-Bedienstation (ABK) mit berührungsempfindlichem Bildschirm, welche gleichzeitig als SPS und EK fungiert. Bedienung der lokalen SPS und der Verbindung mit den dezentralen Peripherien (DP) sowie Steuerung der Ausgabewerte für die LED-Lauflichtanwendung zur Übertragung an die DP. (Details zur Bedienoberfläche siehe Abbildung A-13 bzw. Tabelle A-2)
②	Smartcard-Lesegerät	USB-Smartcard-Lesegerät zur Benutzerauthentifizierung an der HMI-Bedienstation unter Verwendung einer Smartcard/PIN-Kombination.
③	Industrial Switch	Nicht-konfigurierbarer 8-Port Industrial Switch (10/100Mbit/s) zur Verbindung der verschiedenen Komponenten des Demonstrators.
④	DP 1 bis DP 4	(Stark-)ressourcen-beschränkte Komponenten gemäß der Definition in Tabelle 8-2 (Plattform 1) zur Ansteuerung von 8 LED-Leuchtelemente bzw. zur Darstellung der Ausgabewerte der LED-Lauflichtanwendung aus der SPS.
⑤	LED-Leuchtelemente	LED-Leuchtelemente zur Anzeige der empfangenen Ausgabewerte aus der SPS.

Tabelle A-1: Bestandteile des Demonstrators

Bedienoberfläche des Demonstrators

Abbildung A-13 zeigt die laufende Bedienoberfläche des Demonstrators, welche in der kombinierten SPS sowie ABK/EK des Demonstrators zu finden ist. Tabelle A-2 erläutert die Bedienelemente der Oberfläche bzw. deren Aufgaben.

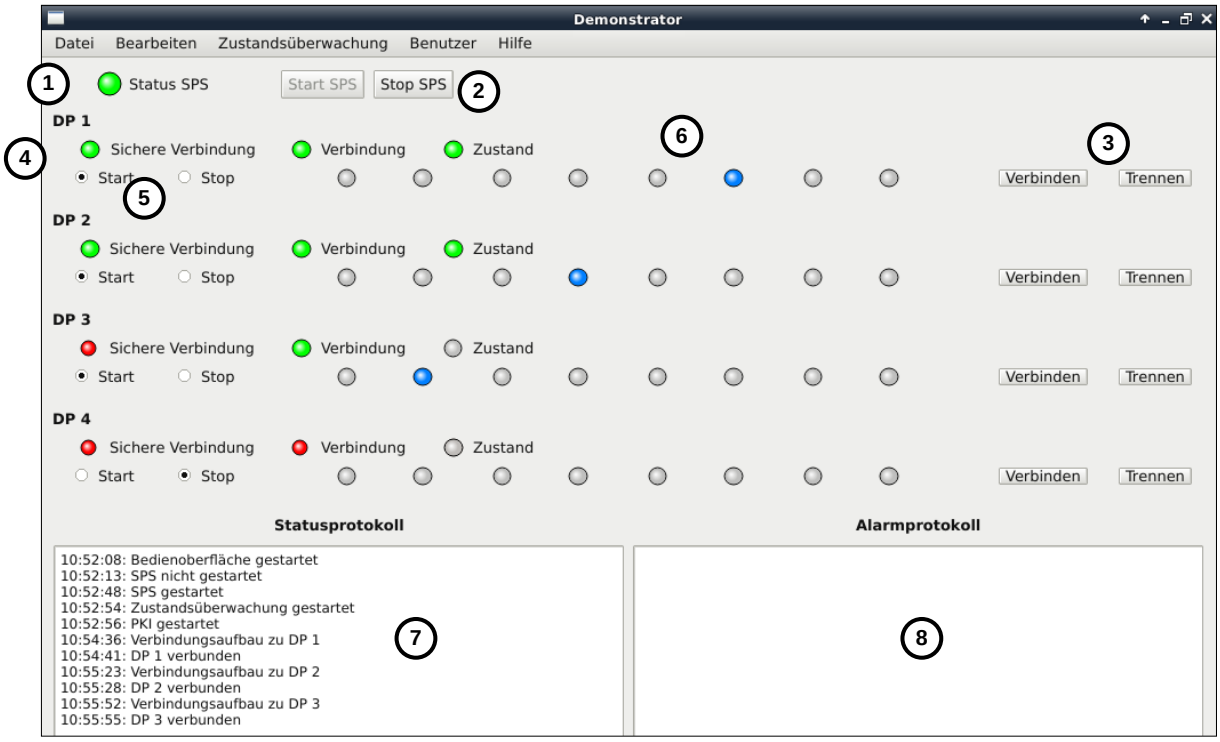


Abbildung A-13: Darstellung der Bedienoberfläche

Bezeichnung		Beschreibung
①	Status SPS	Anzeige über den Status der Software der SPS (Aktiv / Inaktiv)
②	Start/Stop der SPS	Schaltflächen zum Starten und Stoppen der SPS-Software und des dahinter liegenden Protokollstacks zur Kommunikation sowie der PKI.
③	Aufbau und Trennen der Verbindung zur DP	Schaltflächen zum Aufbau oder zur Trennung der Verbindung zur jeweiligen DP nach Start der SPS-Software.
④	Statusanzeige der DP	Die Anzeigen über den Status der DP geben Aufschluss über die Verbindung bzw. den Zustand der jeweiligen DP. So wird angezeigt, ob eine Verbindung besteht und ob diese abgesichert oder ungesichert ist. Weiterhin wird der aktuelle Zustand der DP angezeigt.
⑤	Start der Anwendung der DP	Starten und Stoppen der LED-Lauflichtanwendung auf der DP nach erfolgtem (sicherem) Verbindungsaufbau mit der SPS.
⑥	Soll-Status des LED-Lauflichts	8 LED Statusanzeigen als Soll-Zustandsanzeige der LED-Lauflichtanwendung.
⑦	Statusprotokoll	Anzeige von Meldungen über den Status des Demonstrators.
⑧	Alarmprotokoll	Anzeige von Meldungen zu lokal oder entfernt aufgetretenen Alarmen.

Tabelle A-2: Elemente der Bedienoberfläche

In Abbildung A-13 kommunizieren die Komponenten DP 1 und DP 2 über eine sichere Verbindung mit der SPS. Der Zustand der beiden DP ist gegenüber dem Verbindungsaufbau identisch und daher in Ordnung. Weiterhin werden die Ausgabewerte der LED-Lauflichtanwendung auf der Bedienoberfläche angezeigt. Die Kommunikation mit der Komponente DP 3 erfolgt über eine unsichere Verbindung. Aus diesem Grund ist der aktuelle Zustand von DP 3 unbekannt bzw. nicht verfügbar, jedoch ist die Lauflichtanwendung aktiv. Komponente DP 4 ist nicht mit der SPS verbunden und inaktiv.

Lebenslauf

Persönliche Daten

Name	Markus Runde
Geburtsort	Papenburg
Geburtsdatum	10. Mai 1984

Berufsausbildung

09/2000 – 06/2003	Ausbildung zum IT-Systemelektroniker, Meyer Werft, Papenburg

Schulausbildung

08/2003 – 07/2004	Fachoberschule Technik Klasse 12, Papenburg

Studium

09/2004 – 10/2008	Diplomstudium an der Fachhochschule Hannover Fakultät I - Elektro- und Informationstechnik Studiengang - Informationstechnik Vertiefungsrichtung - Prozessinformatik und Automatisierungstechnik
03/2009 – 08/2010	Masterstudium an der Fachhochschule Hannover Fakultät I - Elektro- und Informationstechnik Studiengang Sensor- und Automatisierungstechnik

Studienbegleitende Tätigkeiten

03/2006 – 08/2006	Praxissemester bei der VB Autobatterie GmbH & Co KGaA (VARTA / Johnson Controls), Hannover
02/2007 und 08/2007	Anstellungen als Werkstudent bei der VB Autobatterie GmbH & Co KGaA (VARTA / Johnson Controls), Hannover
03/2008 – 05/2008	Praxissemester und Diplomarbeit bei der ABB Automation GmbH, Minden, Bereich Feldbusentwicklung
12/2008 – 02/2010	Anstellung als wissenschaftliche Hilfskraft an der Fachhochschule Hannover Fakultät I - Fachgebiet Prozessinformatik und Automatisierungstechnik
03/2010 – 08/2010	Erstellung der Masterarbeit an der Fachhochschule Hannover

Berufstätigkeit

09/2010 – 06/2014	Anstellung als wissenschaftlicher Mitarbeiter an der Fachhochschule Hannover (heute: Hochschule Hannover) – Fachgebiet Prozessinformatik und Automatisierungstechnik
07/2014 bis heute	Anstellung bei der BASF SE in Ludwigshafen am Rhein

Gremientätigkeit

02/2009 bis heute	Mitarbeit im Arbeitskreis *„Installation Guides“* der PROFIBUS Nutzerorganisation e.V.
05/2011 bis heute	Mitarbeit im Arbeitskreis *„PROFINET Security“* der PROFIBUS Nutzerorganisation e.V.

Betreute Lehrveranstaltungen

03/2011 – 06/2014	„Labor für Speicherprogrammierbare Steuerungen“ an der Fachhochschule Hannover
04/2011 – 06/2011	Vorlesung „Prozessdatenverarbeitung und Feldbusse (PDV) – Teil Feldbusse“ an der Fachhochschule Hannover

Barsinghausen, den 07.07.2014