ABB Drives

Technischer Leitfaden
Cybersicherheit für ABB Frequenzumrichter

Power and productivity
for a better world™

Literaturverweis

Allgemeine Leitfäden		Code (Englisch)	Code (Deutsch)
[1]	*ABB 670 series IEC 2.0 Cyber Security Deployment Guideline*	*1MRK 511 309-UEN*	
[2]	*Cyber Security with ABB Ability™ System 800xA*		
[3]	*ESCoRTS Project (European network for the Security of Control and Real-Time Systems)*		
[4]	*NIST Special Publication 800-82, Revision 2, Guide to Industrial Control Systems (ICS) Security*		
[5]	*IEC 62443 series standards, Industrial communication networks – Network and system security*		
[6]	*Security Overview - Drive Remote Service Platform*	*9AKK106930A8297*	

Frequenzumrichter-Firmware-Handbücher			
[7]	*ACS880 primary control program firmware manual*	*3AUA0000085967*	3AUA0000111128
[8]	*ACS580 standard control program firmware manual*	*3AXD50000016097*	3AXD50000019770
[9]	*ACS380 machinery control program firmware manual*	*3AXD50000029275*	3AXD50000036601
[10]	*ACH580 HVAC control program firmware manual*	*3AXD50000027537*	3AXD50000027591

Handbücher und Anleitungen für Optionen		
[11]	*FENA-01/-11/-21 Ethernet adapter module user's manual*	*3AUA0000093568*
[12]	*NETA-21 remote monitoring tool user's manual*	*3AUA0000096939*
[13]	*Drive composer start-up and maintenance PC tool User's manual*	*3AUA0000094606*
[14]	*Ethernet tool network for ACS880 drives application guide*	*3AUA0000125635*

Im Internet finden Sie Handbücher und andere produktbezogene Dokumente im PDF-Format. Siehe Abschnitt *Dokumente-Bibliothek im Internet* auf der hinteren Einband-Innenseite. Wenn Handbücher nicht in der Dokumente-Bibliothek verfügbar sind, wenden Sie sich bitte an Ihre ABB-Vertretung.

Technischer Leitfaden

Cybersicherheit für ABB Frequenzumrichter

Inhaltsverzeichnis

3AXD10000620848 Rev B
DE
Übersetzung von Originaldokument
3AXD10000492137
GÜLTIG AB: 13.06.2017

Inhaltsverzeichnis

Literaturverweis 2

1. Einführung in den Leitfaden

Inhalt dieses Kapitels 7
Informationen über diese Anleitung 7
Haftungsausschluss 7
Glossar 8

2. Grundlagen der Cybersicherheit

Inhalt dieses Kapitels 13
Einleitung 13
Tiefenverteidigung 15
Allgemeine Risikominderungsverfahren und Cybersicherheitsrichtlinien 16
Automatisierungsnetzwerke 18
Cybersicherheit im Vergleich zur Sicherheit 19
Rollen und Verantwortlichkeiten 19
Allgemeine Cybersicherheitslösungen 20

3. Cybersicherheitsnormen

Inhalt dieses Kapitels 23
Cybersicherheitsnormen in der Automatisierung 23

4. Beispielfälle

Inhalt dieses Kapitels 27
Einleitung 27
Fall 1 – Industrielles Automatisierungsbeispiel (Fabrikumgebung) 28
Beschreibung 28
Cybersicherheits-Risikominderung und sichere Bereitstellung 30
Fall 2 – Externe Pumpstationen 33
Beschreibung 33
Cybersicherheits-Risikominderung und sichere Bereitstellung 34
Fall 3 – OEM-Maschinenausrüstung 35
Beschreibung 35
Cybersicherheits-Risikominderung und sichere Bereitstellung 36
Fall 1: OEM-Zugang über Netzwerk, Firewalls und Zugangspunkt des Kunden: . 36
Fall 2: Fall mit direktem Zugang für den OEM-Hersteller (nicht empfohlen) 36
Fall 4 – Gebäudeautomatisierung 37
Beschreibung 37
Cybersicherheits-Risikominderung und sichere Bereitstellung 38

5. Cybersicherheitsrichtlinien von ABB

Inhalt dieses Kapitels 41
Prinzip 41
Gerätesicherheitscenter (Device Security Assurance Center = DSAC) 42

Ergänzende Informationen

Anfragen zum Produkt und zum Service 43
Produktschulung 43
Feedback zu ABB Handbüchern 43
Dokumente-Bibliothek im Internet 43

1

Einführung in den Leitfaden

Inhalt dieses Kapitels

Dieses Kapitel enthält eine Inhaltsbeschreibung des Leitfadens sowie einen Haftungsausschluss und ein Glossar.

Informationen über diese Anleitung

Dieses Dokument ist ein informativer Leitfaden, der zu einem besseren Verständnis der Cybersicherheit, typischen Herausforderungen bei der Cybersicherheit und den erforderlichen Maßnahmen beitragen soll, die erforderlich sind, um Zuverlässigkeit, Integrität und Verfügbarkeit von drehzahlgeregelten Antriebssystemen vor unbefugtem Zugriff oder Cyberattacken zu schützen. Das Ziel des Dokuments besteht darin, die Cybersicherheits-richtlinien von ABB Drives vorzustellen und auf Fragen und Bedenken in Zusammenhang mit der Cybersicherheit einzugehen. Das Dokument kann auch als allgemeiner Leitfaden für die Anwendung von Cybersicherheit für Antriebe von ABB und zugehörige, vernetzte Produkte verwendet werden.

Haftungsausschluss

Dieses Dokument ist nicht als wortwörtliche Anleitung, sondern als informative Hilfe vorgesehen. Die Beispiele in diesem Leitfaden sind nur zur allgemeinen Verwendung vorgesehen und beinhalten nicht alle Einzelheiten, die für die Implementierung eines sicheren Systems erforderlich sind.

Es liegt allein in der Verantwortlichkeit des Kunden, eine sichere Verbindung zwischen dem Produkt und dem Netzwerk des Kunden oder einem anderen Netzwerk bereitzustellen und kontinuierlich zu sichern. Der Kunde muss ausreichende Sicherheitsmaßnahmen treffen und auf dem aktuellen Stand halten (einschließlich – jedoch nicht darauf beschränkt – die Installation von Firewalls, Anwendung von Authentifizierungsmaßnahmen, Verschlüsselung von Daten, Installation von Antivirus-Programmen usw.), um das Produkt, das Netzwerk,

dessen System und die Schnittstellen vor Sicherheitsverletzungen, unerlaubtem Zugriff, Eindringen, Sicherheitslücken und/oder Diebstahl von Daten oder Informationen zu schützen. ABB und ihre Konzerngesellschaften sind nicht haftbar für Schäden und/oder Verluste, die als Folge von Sicherheitsverletzungen, unerlaubtem Zugriff, Störungen, Eindringen, Sicherheitslücken und/oder Diebstahl von Daten und Informationen auftreten.

Glossar

In diesem Leitfaden verwendete Begriffe und Abkürzungen.

Begriff oder Abkürzung	Erläuterung
2G, 3G, 4G	Die zweite, dritte und vierte Generation der Mobilfunktechnologie.
Zugangskonto	Zugangskontrollfunktion, die es dem Benutzer erlaubt, auf eine bestimmte Gruppe von Daten oder Funktionen für bestimmte Geräte zuzugreifen.
Zugangskontrolle	Schutz von Systemressourcen vor unbefugtem Zugriff.
Verantwortlichkeit	Eigenschaft eines Systems (einschließlich all seiner Systemressourcen), die gewährleistet, dass die Maßnahmen einer Systementität eindeutig bis zu dieser Entität zurückverfolgt werden können, sodass sie für ihre Maßnahmen zur Rechenschaft gezogen werden kann.
ADFS	Active Directory Federation Services (Active Directory-Verbunddienste).
APN	Access Point Name ist der Name eines Gateways zwischen einem GSM-, GPRS-, 3G- oder 4G-Mobilfunknetz und anderen Netzen.
Authentifizieren	Prüfung der Identität eines Benutzers, Benutzergeräts oder einer anderen Entität oder der Integrität von gespeicherten, übertragenen oder auf andere Weise des Risikos einer unbefugten Modifikation ausgesetzten Daten in einem Informationssystem, oder zur Feststellung der Gültigkeit einer Datenübertragung.
Authentifizierung	Sicherheitsmaßnahme, um die Gültigkeit einer Übertragung, Meldung oder Quelle zu ermitteln, oder eine Maßnahme, um die Genehmigung einer Person zu prüfen, spezifische Arten von Informationen zu erhalten.
Autorisierung	Recht oder Genehmigung, die einer Entität gewährt wird, auf eine Systemressource zuzugreifen.
Verfügbarkeit	Fähigkeit eines Elements, in einem Zustand zu sein, um eine erforderliche Funktion unter bestimmten Bedingungen an einem bestimmten Zeitpunkt oder über einen bestimmten Zeitraum zu erfüllen, unter der Voraussetzung, dass die erforderlichen externen Ressourcen bereitgestellt werden.
BACnet BACnet/IP	BACnet ist ein Kommunikationsprotokoll für den Aufbau von Automatisierungs- und Steuerungs-/Regelungsnetzwerken. Definiert das MS/TP-Netzwerk (Master-Slave/Token-Passing). BACnet/IP ist entwickelt worden, damit das BACnet-Protokoll TCP/IP-Netzwerke nutzen kann.
BMS	Building Management System (Gebäudemanagementsystem).
CCTV	Closed-Circuit Television (Videoüberwachung).
Änderungs-management	Prozess der Kontrolle und Dokumentation jeder Änderung in einem System, um den einwandfreien Betrieb der Ausrüstung zu gewährleisten.
Gefährdung	Unbefugte Veröffentlichung, Modifikation, Ersatz oder Verwendung von Informationen.
Vertraulichkeit	Zusicherung, dass Informationen keinen unbefugten Personen, Prozessen oder Geräten zur Verfügung gestellt werden.

Begriff oder Abkürzung	**Erläuterung**
Cybersicher-heitsziel	Aspekt der Sicherheit, der dazu dient, bestimmte Maßnahmen zur Risikominderung anzuwenden, wie zum Beispiel Vertraulichkeit, Integrität, Verfügbarkeit, Benutzerauthentifizierung, Zugangsauthentifizierung, Verantwortlichkeit usw.
Denial of Service (DoS) (Verweigerung des Dienstes)	Verhinderung oder Unterbrechung von unbefugten Zugriff auf eine Systemressource oder die Verzögerung von Systemabläufen und-funktionen oder Unterbrechung des Betriebs
DMZ	Demilitarized Zone (Entmilitarisierte Zone). Ein physikalisches oder logisches Subnetzwerk, das die nach außen gerichteten Services einer Organisation enthält und einem größeren und nicht vertrauenswürdigen Netzwerk zeigt, normalerweise dem Internet
DNS	Domain Name System (Domain-Namenssystem)
FTP	File Transfer Protocol (Dateiübertragungsprotokoll)
FTP(S)	Das SSH-Datenübertragungsprotokoll oder sichere Datenübertragungsprotokoll ist ein Netzwerkprotokoll, das Dateizugriff, Dateiübertragung und Dateiverwaltung über jeden zuverlässigen Datenstrom ermöglicht
FW	Firewall. Ein Netzwerk-Sicherheitssystem, das auf Grundlage festgelegter Sicherheitsregeln den ein- und ausgehenden Netzwerk-Datenverkehr überwacht und steuert.
GPRS	General Packet Radio Service ist ein paketorientierter, mobiler Datenservice im Mobilfunksystem (GSM) der zweiten (2G) und dritten (3G) Generation
GSM	Globales Mobilfunksystem der zweiten Generation (2G)
Härten	Unter Härten versteht man den Prozess der Sicherung eines Systems durch die Reduzierung seiner verwundbaren Oberfläche
HMI	Human-Machine Interface (Mensch-Maschine-Schnittstelle)
HTTP	Das Hypertext-Übertragungsprotokoll ist ein Anwendungsprotokoll für dezentrale, kollaborative Hypermedia-Informationssysteme
HTTPS	Auch bekannt als HTTP over TLS, HTTP over SSL und HTTP Secure, ist ein Protokoll für die sichere Kommunikation über ein Computernetzwerk, das im Internet in großem Umfang verwendet wird
IACS	Industrial Automation and Control Systems (Industrielle Automatisierungs- und Steuerungssysteme)
ICS	Industrial Control System (Industrielles Steuerungssystem)
IDS	Intrusion Detection System (Eindringungs-Erkennungssystem). Ein Gerät oder eine Softwareanwendung, die Netzwerk- oder Systemaktivitäten auf schädliche Aktivitäten oder Regelverletzungen überwacht und Berichte an eine Managementstation erstellt
IEC	International Electrotechnical Commission (Internationale elektrotechnische Kommission)
IED	Intelligent Electronic Devices (Intelligente elektronische Geräte)
IEEE	Institute of Electrical and Electronics Engineers (Institut der Elektro- und Elektronikingenieure)
Vorfall	Ereignis, das nicht Teil des erwarteten Betriebs eines Systems oder Services ist und das eine Unterbrechung des vom System bereitgestellten Services oder eine Verringerung der Servicequalität verursacht oder verursachen kann

Begriff oder Abkürzung	Erläuterung
Integrität	Qualität eines Systems, die die logische Korrektheit und Zuverlässigkeit des Betriebssystems, die logische Vollständigkeit der den Schutzmechanismus implementierenden Hard- und Software sowie die Konsistenz der Datenstrukturen und das Vorhandensein der gespeicherten Daten widerspiegelt
ISA	International Society of Automation (Internationale Gesellschaft für Automatisierung)
ISMS	Information Security Management System (Managementsystem für Informationssicherheit). Ein Regelwerk für das Informationssicherheitsmanagement oder IT-Risiken
ISO	International Organization for Standardization (Internationale Organisation für Normung)
ISO 27K	Normen der Reihe ISO 27000
IT	Information Technology (Informationstechnologie). Computerbezogene, nicht greifbare Assets einer Organisation wie zum Beispiel Softwareanwendungen, Prozessprogramme und Personaldateien
LAN	Local Area Network (Lokales Netzwerk)
NERC	North American Electric Reliability Corporation (Nordamerikanische Organisation für die Zuverlässigkeit der Verbundnetze)
NIST	National Institute of Standards and Technology (Nationales Institut der Normen und Technologie)
NBT NS	NBT NS ist ein Hintergrundprogramm für die NetBIOS-Namenserkennung. Ermöglicht das Auffinden von Rechnern aus einem lokalen Netzwerk durch die Verwendung des NetBIOS-Hostnamens
NTP	Das Netzwerkzeitprotokoll ist ein Protokoll für die Synchronisierung von Rechneruhren über ein Netzwerk.
OEM	Der Begriff OEM (kurz für: Original Equipment Manufacturer = Erstausrüster) wird verwendet, wenn ein Unternehmen ein Teil oder ein Untersystem herstellt, das im Endprodukt eines anderen Unternehmens verwendet wird
Patchmanagement	Bereich des Systemmanagements, der die Beschaffung, Prüfung und Installation verschiedener Patches (Codeänderungen) bei einem verwalteten Computersystem umfasst
PBX	Private Branch Exchange (Nebenstellenanlage). Eine Telefonanlage oder Teilnehmervermittlungsanlage, die in einem Unternehmen eingesetzt wird und mehrere Endgeräte sowohl untereinander als auch mit einer oder mehreren Leitungen des öffentlichen Telefonnetzes verbindet
PKI	Die PKI (kurz für: Public Key Infrastructure = Öffentliche Schlüssel-Infrastruktur) dient zur Verwaltung und Verteilung von Schlüsseln und digitalen Zertifikaten in öffentlich zugänglichen Netzwerken, um eine sichere digitale Kommunikation zu gewährleisten.
SPS	Speicherprogrammierbare Steuerung. Programmierbares, mikroprozessorbasiertes Gerät, das in der Industrie verwendet wird, um Montagelinien und Anlagen zu steuern
PROFINET	Offener Kommunikationsstandard für industrielles Ethernet
RTU	Remote Terminal Unit (Fernbedienungsterminal)
SCADA	Supervisory Control and Data Acquisition (Überwachung, Steuerung und Datenerfassung)
SSH	SSH (kurz für: Secure Shell = Sichere Hülle) ist ein kryptografisches (verschlüsseltes) Protokoll, mit dem man auf einen entfernten Rechner mittels einer verschlüsselten Verbindung über ein unsicheres Netzwerk zugreifen kann
SSL	Secure Sockets Layer (Sichere Socket-Schicht). Siehe *TLS*.

Begriff oder Abkürzung	**Erläuterung**
TLS	TLS (kurz für: Transport Layer Security = Transportschichtsicherheit) und der Vorgänger SSL sind kryptografische Protokolle, die entwickelt wurden, um die Kommunikationssicherheit in einem Computernetzwerk zu gewährleisten (Datenschutz und Datenintegrität zwischen zwei kommunizierenden Computeranwendungen)
TR	Technischer Bericht der IEC
TS	Technische Spezifikation der IEC
USB	Universal Serial Bus (Universeller serieller Bus)
VLAN	Virtual Local Area Network (Virtuelles lokales Netzwerk). VLANs unterteilen ein bestehendes einzelnes physisches Netzwerk in mehrere logische Netzwerke. Jedes VLAN bildet dabei eine eigene Broadcast-Domain.

2

Grundlagen zur Cybersicherheit

Inhalt dieses Kapitels

In diesem Kapitel werden die Grundlagen zur Cybersicherheit beschrieben.

Einleitung

Ursprünglich wurden mit “Cybersicherheit” alle Maßnahmen beschrieben, die zum Ziel hatten, einen Computer oder ein Computersystem vor unbefugtem Zugriff oder einem Angriff zu schützen. Im Zusammenhang mit der Energie- und Automatisierungstechnologie hat der Begriff einen Bedeutungswandel erfahren und steht nun für die Maßnahmen, die ergriffen werden, um Zuverlässigkeit, Integrität und Verfügbarkeit von Energie- und Automatisierungstechnologien vor unbefugtem Zugriff oder einem Angriff zu schützen.

Cybersicherheit erstreckt sich auf alle Prozesse und Mechanismen, durch die digitale Ausrüstung, Daten und Services vor unbeabsichtigten oder unbefugten Zugriff, Veränderung oder Zerstörung gestützt werden; sie betrifft außerdem Sicherheitsmaßnahmen, um die Vertraulichkeit, Integrität und Verfügbarkeit von Daten sowohl bei der Übermittlung als auch im gespeicherten Zustand zu gewährleisten.

Cybersicherheit ist sowohl für ABB-Kunden als auch für ABB selbst mittlerweile von enormer Bedeutung. Dafür gibt es verschiedene Gründe, wie zum Beispiel die folgenden:

- Moderne Automatisierungs-, Schutz- und Steuerungssysteme sind oft hochspezialisierte IT-Systeme, die auf kommerziellen, serienmäßigen IT-Komponenten aufbauen und standardisierte, IP-basierte Kommunikationsprotokolle nutzen.
- Die Steuerungssysteme können auch dezentral und miteinander verbunden sein, was eine größere Angriffsfläche im Vergleich zu älteren und isolierten Systemen bedeutet.
- Die Steuerungssysteme basieren zunehmend auf Software.
- DoS-Angriffe (Denial-of-Service) und Malware (z.B. Würmer und Viren) sind mittlerweile weit verbreitet und haben sich bereits auf ICS (Industrielle Steuerungssysteme) ausgewirkt.
- Computersysteme umfassen heute eine Vielzahl intelligenter Geräte, einschließlich Smartphones, und zu den Netzwerken gehören nicht nur das Internet und private Datennetzwerke, sondern auch Bluetooth-, WLAN- und andere drahtlose Netzwerke.

Laut einer Definition beinhaltet die Cybersicherheit von industriellen Steuerungssystemen in der Regel drei Gefahrenkategorien:

- **Hacking**. Ein Angreifer hat es speziell auf ein industrielles Steuerungssystem abgesehen, um zum Beispiel den Anlagenbesitzer zu erpressen oder den Ruf eines Automatisierungsunternehmens zu schädigen. Dies kann erreicht werden, indem eine spezielle Malware entwickelt wird. Stuxnet ist ein Beispiel für diese Art eines zielgerichteten Angriffs.
- **Allgemeine Schadsoftware** Stellen Sie sich ein Szenario vor, bei dem ein Mitarbeiter einen Laptop mit dem Systemnetzwerk anschließt oder einen USB-Stick an einen Server anschließt. Auch wenn dahinter keine bösen Absichten stecken, besteht, wenn der Laptop oder der USB-Stick mit Malware infiziert ist, ein hohes Risiko, dass auch das Automatisierungssystem infiziert werden kann. Selbst wenn die Malware in diesen Fällen nicht ausgelegt ist, das Automatisierungssystem zu beschädigen, kann sie dennoch sehr schädlich sein.
- **Fehler von Mitarbeitern.** Ein Ingenieur will zum Beispiel die Steuerlogik in einem eingebetteten Gerät aktualisieren, schließt aber aus Versehen das Engineering-Tool an das falsche Gerät an; oder ein Ingenieur verbindet ein Netzwerkkabel mit dem falschen Anschluss eines Netzwerk-Switch.

Wenn es um Cybersicherheit geht, denken die meisten Menschen an Hacking. Diese Art von Angriffen macht tatsächlich nur einen kleinen Teil aller Vorfälle aus. Schadsoftware und Fehler von Mitarbeitern sind die Hauptursache von Vorfällen.

In den nächsten Abschnitten werden die grundsätzlichen Ansätze zum Datenschutz vorgestellt.

Konzept der Defense-in-Depth

Für die Bewältigung von Cybersicherheitsrisiken in einem industriellen Steuerungssystem existiert keine einzelne Lösung, genauso wenig gibt es ein vollständig sicheres System. Daher empfiehlt ABB, wie viele andere auch, das Konzept der "Defense-in-Depth"; darunter versteht man den koordinierten Einsatz mehrerer Abwehrmaßnahmen und die dafür notwendige Zuordnung von Menschen, Technologie und Abläufe in mehreren Schichten.

Defense-in-Depth ist ein Datenschutzkonzept, bei dem mehrere Schichten von Sicherheitskontrollen (Verteidigungslinien) in einem IT-System verteilt sind. Es ist auch als sogenannter “Burg-Ansatz” bekannt, da es mit einer mittelalterlichen Burg verglichen werden kann, die mehrere Verteidigungslinien (Mauern, nur ein einzelner Eingang, Burg in der Burg, Burggraben usw.) gegen bekannte Bedrohungen nutzt. Defense-in-Depth ist dazu vorgesehen, beim Ausfall einer Sicherheitskontrolle oder beim Auftreten einer Sicherheitslücke für Redundanz zu sorgen.

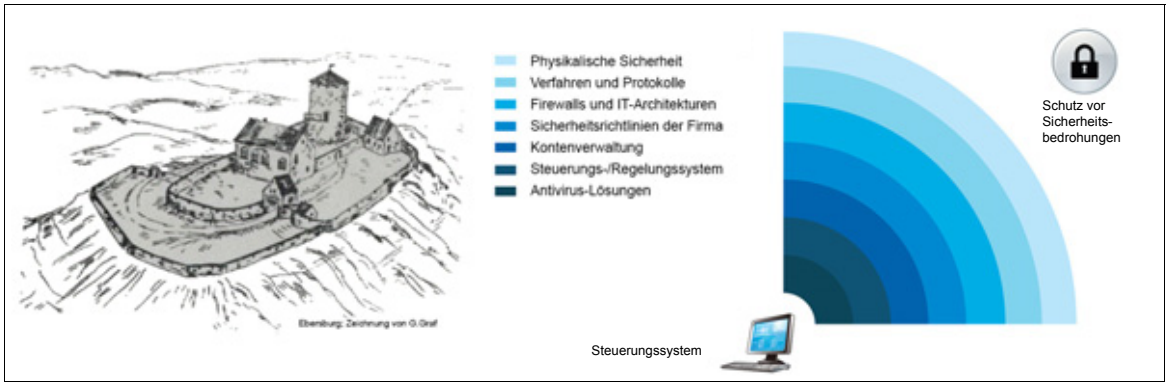

Abbildung 1. Eine mittelalterliche Burg als Beispiel für Defense-in-Depth und mehrschichtigen Schutz [2].

Der Grundgedanke hinter dem Tiefenverteidigungsansatz ist, ein System mithilfe verschiedener unabhängiger Methoden vor jedem Angriff zu schützen. Es handelt sich um eine auf Schichten basierende Taktik, die von der amerikanischen National Security Agency als ein umfassender Ansatz zur Datensicherheit entwickelt wurde.

Die Einrichtung von Schutzmechanismen, Verfahren und Richtlinien dient dazu, die Zuverlässigkeit eines IT-Systems zu erhöhen, während mehrere Verteidigungsschichten Spionage sowie direkte Angriffe auf kritische Systeme verhindern. In Hinblick auf die Verteidigung von Computernetzwerken müssen Maßnahmen zur Defense-in-Depth nicht nur Sicherheitslücken verhindern, sondern einer Organisation auch Zeit verschaffen, um einen Angriff zu erkennen und zu reagieren, und so die Konsequenzen einer Sicherheitslücke abzumildern.

In der IT-Welt gibt es keine einzelne Verteidigung, die unüberwindbar ist, und keine Datensicherheitsstrategie ist vollständig ohne eine Defense-in-Depth-Strategie. Für Unternehmen, die ihre Informationsbestände verteidigen, ist die Implementierung dieser Strategie nicht einfach. Während Burgen sich den Luxus leisten, nur einen einzelnen Eingang zu haben, besitzen die Netzwerke von Unternehmen mehrere Zugangspunkte (z.B. Supportverbindungen mit Zulieferern, Dienstleistern und Kunden), wodurch die Sicherheit zusätzlich beeinträchtigt wird. Darüber hinaus existieren heutzutage sehr viel mehr Bedrohungen als noch vor ein paar Jahren. In den frühen "1990er Jahren" war die Netzwerksicherheit im Prinzip eine Frage der Verteidigung gegen Angriffe auf Paketebene, und Firewalls die dafür nützlichen Router. Heute sind interne Ressourcen durch Pufferüberläufe, SQL-Einschleusung, bösartige Webseiten und aktive E-Mail-Inhalte, drahtlose Verbindungen, Phishing und vieles mehr gefährdet.

Es ist ausschlaggebend, sicherzustellen, dass Schutzmaßnahmen nicht nur breit gestaffelt sind, sondern auch in die Tiefe gehen. Die Sichtweise darf nicht auf den physikalischen Bereich begrenzt sein und muss über physikalische Netzwerk- und Systemgrenzen hinausgehen.

Um sicherzustellen, dass die Verteidigung wirklich tief gestaffelt ist, muss es möglich sein, eine bestimmte Bedrohung sowie ein bestimmtes Element auszuwählen, sodass im Ergebnis mehrere Mechanismen greifen, die dieses Element vor der ausgewählten Bedrohung schützen.

Das folgende Beispiel stammt aus *NIST Special Publication 800-82, Guide to Industrial Control Systems (ICS) Security* [4], in dem ein Modell einer Defense-in-Depth-Architektur in Unternehmen vorgestellt wird, die verschiedene industrielle Steuerungs- und Automatisierungssysteme auf der ganzen Welt unterhalten (siehe Abbildung unten).

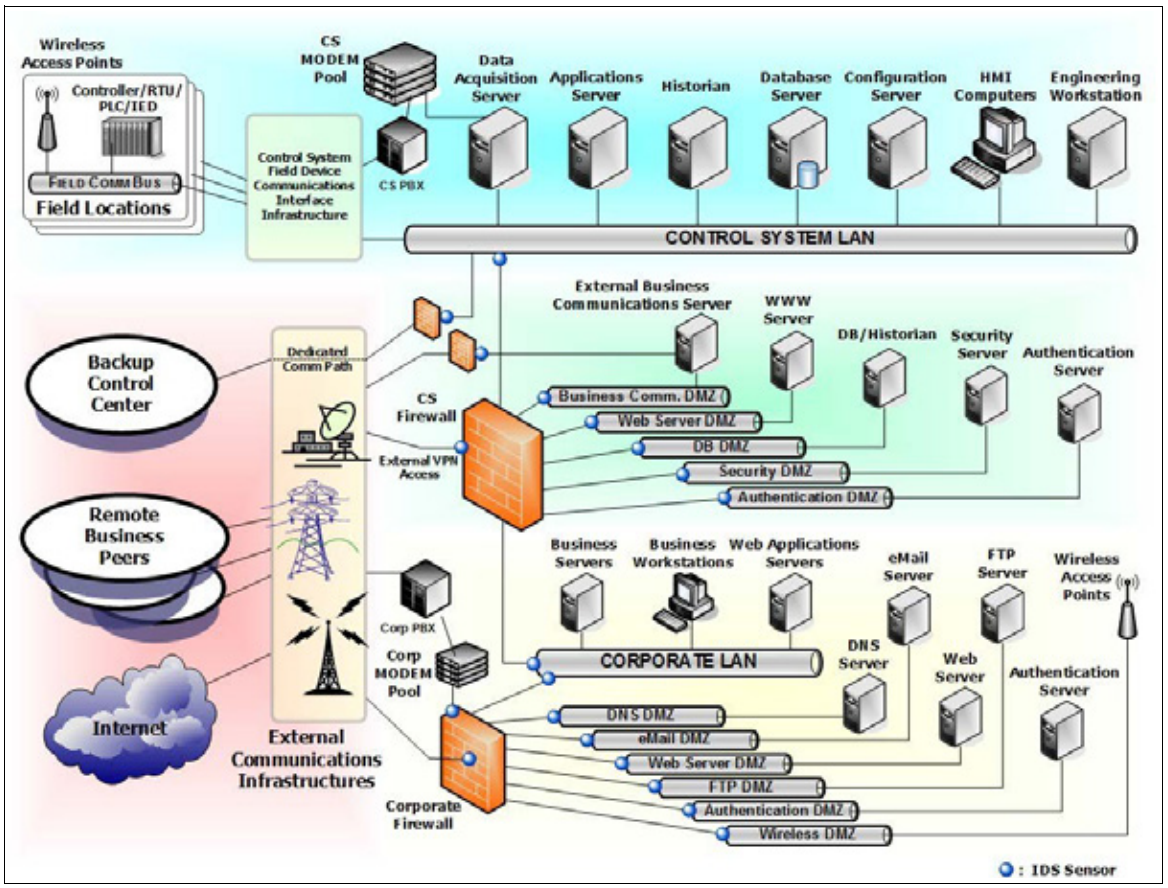

Abbildung 2. Defense-in-Depth-Architektur wie in [4] gezeigt.

Bei der Defense-in-Depth-Architektur ist das lokale Netzwerk (LAN) des Steuerungssystems durch Firewalls von anderen Firmennetzwerken klar abgegrenzt; außerdem gibt es separate entmilitarisierte Zonen (DMZ) für jede Funktion, wie zum Beispiel Archiv, Sicherheit und Authentifizierung. Die Aufteilung innerhalb dieses LAN ist nicht sichtbar, aber in Zukunft sind auch für diesen Teil immer mehr Kontrollmechanismen zur Wahrung der Cybersicherheit erforderlich. Anders ausgedrückt, ist es erforderlich, Zugangskontrollmechanismen auf Netzwerkebene hinzuzufügen, wie zum Beispiel Firewalls und Managed Switches, um den unbefugten Zugriff auf Automatisierungsnetzwerke, Geräte und Daten zu unterbinden.

Allgemeine Risikominderungsverfahren und Cybersicherheitsrichtlinien

Die Mehrzahl der Cybersicherheitsrisiken kann durch machbare Netzwerkarchitekturen, Zugangskontrolle und physikalische Sicherheitsmechanismen unter Kontrolle gehalten werden. Uneingeschränkte Sicherheit und Managementbedarf erfordern außerdem strenge Cybersicherheitsrichtlinien und einen Ansatz, der verschiedene Standpunkte und Maßnahmen umfasst, um das anvisierte Cybersicherheitsniveau in der Automatisierung aufrechtzuerhalten.

Die grundlegenden Risikominderungsverfahren und Cybersicherheitsrichtlinien sind im Folgenden aufgeführt:

- Physikalische Sicherheitsmechanismen
  - Feststellung von Manipulation zwecks unerlaubtem Zugriff (zum Beispiel Prüfung von Versiegelungen)
  - Manipulationssichere Ausrüstung (zum Beispiel die Aktivierung von Fehlersuchschnittstellen)
  - Abschließen von Einrichtungen und Räumen
  - Verriegelungsvorrichtungen für Schränke
  - Physikalischer Zugang auf Grundlage von Arbeitsgenehmigungen, Anlagensicherheit und Videoüberwachung
- Elektronische Zugangskontrolle
  - Externer Zugang mit Firewall, die jeden Zugang unbefugter Parteien verweigern muss
  - Kontobasierte, elektronische Zugangskontrolle
  - Verschlüsselung von Fernzugriffsdaten, die übermittelt werden
- Netzwerkarchitekturen und Protokolle
  - Unterteilte Netzwerkarchitekturlösung mit getrennten Automatisierungssegmenten
  - Aufteilung von Datennetzwerken in unabhängige Subnetzwerke, die die Problemausbreitung minimieren
  - Einrichtung sicherer Gateways und DMZ, die eine Kontrolle auf Anwendungsebene ermöglichen
  - Standort- und Automatisierungs-Firewalls werden verwendet und auf dem neuesten Stand gehalten
  - Virtual Private Network (VPN) Lösungen für Fernzugriff und strenge Zugangskontrolle
  - Kryptografische Protokolle und Algorithmen zur Sicherung der Datenkommunikation unter Verwendung von Authentifizierung, Integritäts- und Vertraulichkeitsschutz sowie Wiedergabeschutz
- Cybersicherheitsverfahren und -richtlinien
  - Zuverlässigkeitsprüfungen, Anleitung und Schulung von Personal und Unterauftragnehmern
  - Leitfaden darüber, welche Maßnahmen unter Verwendung welcher Tools von wem und wann zulässig sind
  - Protokollierung und Überwachungsmethoden der Cybersicherheit in Automatisierungssystemen und Netzwerken
- Computerrichtlinien
  - Backup und Aktualisierung werden verwendet und eine Wiederherstellung wurde geprüft
  - Endgeräteschutz wird verwendet und auf dem neuesten Stand gehalten
  - Zulässige Anwendungen sind spezifiziert und andere ausgeschlossen
  - Lösung für Medienverschlüsselung wird verwendet
- Kontenverwaltung
  - Authentifizierungsverfahren, bevor Geräte, Software oder Benutzer Zugriff auf das Netzwerk erhalten
  - Zugangskonto-Managementprozess wird verwendet und Rollen sind definiert
  - Entfernungsverfahren für Standardkonten und Passwörter
- Patchmanagement
  - Verwaltete Installation von Software und Sicherheitspatches, einschließlich Änderungsmanagement

Cybersicherheitslösungen erreichen fast alle Automatisierungsanwendungen. Das Konzept des “vertrauenswürdigen Netzwerks” bleibt sinnvoll und brauchbar. Aus Sicht der Cybersicherheit sollte das “vertrauenswürdige Netzwerk” als streng begrenzter und gut gehosteter Teil eines bestimmten Netzwerks oder Steuerungssystems betrachtet werden. Wenn also geplant (oder nur vermutet) wird, dass ein Teil einer Bereitstellung sich in einer unkontrollierten Umgebung ohne verantwortliches Domainmanagement und physikalische Zugangskontrolle befindet, dürfen das System und das Netzwerk nicht als vertrauenswürdig betrachtet werden. Hier sind machbare Cybersicherheitsverfahren und -Richtlinien immer erforderlich.

Der Cybersicherheitsansatz bei Automatisierungsanwendungen unterscheidet sich von demjenigen in Business-IT-Standardanwendungen. Oft ist es nicht möglich, bestimmte Steuerungssysteme zu aktualisieren, da der Betriebsprozess nicht lediglich für ein Software-Update unterbrochen werden kann. Darüber hinaus können Software-Updates oder Sicherheitspatches selten sein, da jede Änderung von den Herstellern in verschiedenen Konfigurationen getestet werden muss, bevor sie in der Praxis angewendet wird.

Es gibt erhebliche Risiken im Zusammenhang mit übermäßig komplexen Anforderungen oder Aktualisierungen für Cybersicherheitsprodukte und -funktionen, die den korrekten Betrieb unter allen Umständen eventuell nicht garantieren können. Daher können nicht alle komplexen IT-Sicherheitstools in der Automatisierung verwendet werden.

Automatisierungsnetzwerke

Heutzutage ist die Feldbuskonnektivität oft eine Anschlussbedingung, die Hersteller von Antrieben erfüllen müssen, um von Kunden in Betracht gezogen zu werden. Da industrielle Ethernet-Protokolle in Produktionsstätten mittlerweile weit verbreitet sind, steigt auch die Notwendigkeit, für Komponenten auf Feldebene, wie zum Beispiel drehzahlgeregelte Antriebe, Härtungsfunktionen zu implementieren.

Obwohl Feldbus-Technologien seit Modbus (von Modicon 1979 veröffentlicht) weiter entwickelt werden, unterstützt keiner der standardisierten industriellen Feldbusse die Authentifizierung oder andere grundlegende Cybersicherheitsverfahren. Dies war und ist der Hauptgrund, warum drehzahlgeregelte Antriebe normalerweise keine Möglichkeiten bieten, den Netzwerkdatenverkehr zu sichern. Dies ist auch die Begründung, weshalb Antriebe als verwundbar gegenüber einem bösartigen Systemzugriff, Datendiebstahl und der Manipulation durch feindliche Parteien angesehen werden.

Die für die industriellen Ethernet-Protokolle verantwortlichen Verbände haben damit begonnen, neue Ethernet-Standards zu migrieren, die einen höheren Cybersicherheitsschutz bieten, allerdings ist für diese Umstellung eine gewisse Zeit erforderlich.

Wie bereits erwähnt, ist es oft nicht einfach, bestimmte Steuerungssysteme zu aktualisieren; außerdem muss jede Aktualisierung sorgfältig geprüft werden, bevor sie vor Ort erfolgen kann. Auf der anderen Seite werden die Risiken teilweise gemindert, da für die Konnektivität an ein Automatisierungs- oder Steuerungsnetzwerk (SPS) auf oberer Ebene die Verkabelung, die Anschlüsse sowie die Inbetriebnahme der Kommunikationsschnittstelle, zum Beispiel die Feldbus-Schnittstelle eines Antriebs, separat erfolgen müssen. Dies hat zur Folge dass Antriebe in der Regel standardmäßig nicht über ein Netzwerk aktiviert werden oder über ein Netzwerk angeschlossen sind.

Cybersicherheit im Vergleich zur funktionalen Sicherheit

Cybersicherheit in der Automatisierung zielt auf die Wahrung eines kontinuierlichen Betriebs ab. Dies bedeutet, dass die Anforderungen an die funktionale Sicherheit und die Aufrechterhaltung des Betriebs an erster Stelle stehen und die Anforderungen an die Cybersicherheit diesen untergeordnet sind. Zum Beispiel darf es einer Antivirus-Software auf keinen Fall gestattet sein, den Betrieb eines Sicherheitssystems oder eines Prozesssteuerungssystems zu unterbrechen.

Die gleiche Priorität gilt für Fernzugrifflösungen. Keiner technischen Lösung darf es erlaubt sein, einen lokalen Bediener an der lokalen Steuerung eine Anlage zu hindern, selbst wenn der sichere Fernzugriff in den Störungszustand wechseln würde.

Das vorrangige Ziel bei der Automatisierung ist die Wahrung des sicheren Betriebs und der Daten auch in den folgenden Fällen:

- Fehlfunktion von Steuerung, Support und Backup-System
- Fehler durch Bediener
- Fernzugriffsituationen
- Wartungsmaßnahmen
- Online-Support

Die Ziele der Cybersicherheit sind den Anforderungen für den sicheren Betrieb untergeordnet. Die Ermittlung von Cyberattacken, Industriespionage sowie Schatzsoftware und unzulässiger Software sind wichtige untergeordnete Ziele.

Rollen und Verantwortlichkeiten

Normalerweise hat der Eigentümer eines Unternehmens die Hauptverantwortlichkeit für die Auswahl, Bereitstellung und Aufrechterhaltung der Cybersicherheit angewandter technischer Lösungen. Für eine Person ist es allerdings praktisch unmöglich, alle Aspekte der Cybersicherheit und der Produktionskontinuität zu kontrollieren. Die Zusammenarbeit mit vielen Partnern ist erforderlich, um ein sinnvoll umzusetzendes Maß an Cybersicherheit für den kontinuierlichen Betrieb zu entwickeln, aufzubauen und beizubehalten.

Dies sind Beispiele von Partnern und ihren Rollen, die eine gegenseitig unterstützende Zusammenarbeit in der Cybersicherheit gewährleisten:

- **Systemintegratoren.** Kompetenz und Erfahrung bei der Bewältigung von Integrationsproblemen sowie der Ermittlung möglicher Plattformschwächen und Cybersicherheit-Engpässen bei der Systemintegration.
- **Telekommunikations-Netzwerkbetreiber.** Einrichtung und Cybersicherheitsüberwachung von privaten Zugangspunkten und möglichen VPN- basierten Kommunikationswegen für Kunden.
- **Büro-Sicherheitsservices.** Physikalische Zugangskontrolle und Überwachung von Einrichtungen, Räumen, Archiven usw.
- **Automatisierungshersteller.** Validierung und Genehmigung aller Cybersicherheitslösungen, bevor sie vor Ort in Betrieb genommen werden. Beratung hinsichtlich sicherer Verwendung von Geräten und Anwendungen, Aktualisierungen, Patches, Wartungs- und Überwachungsservices usw.
- **Netzwerkgerätehersteller und LAN-Betreiberservices.** Einrichtung und Pflege einer sicheren Netzwerkarchitektur zusammen mit Managed Switches (VLANs), Routern (Netzwerke), Firewalls (Zugangskontrolle) und Überwachungsservices (Ermittlung von schädlichem Verhalten oder Schadsoftware).
- **Softwarehersteller.** Wartung von Betriebssystemsoftware, Antivirus-Software, Managementsoftware usw.

Allgemeine Cybersicherheitslösungen

Der Betrieb eines Automatisierungssystems kann vollständig ausfallen, weil nicht für Cybersicherheit gesorgt wurde und Schutzfunktionen nicht verwendet wurden.

Der sichere Betrieb muss in allen möglichen Fällen eines Automatisierungssystems geprüft werden. Eine Penetrationsprüfung kann im System verborgene Bedrohungen ans Licht bringen, deshalb sollte eine derartige Prüfung am Integrationsort durchgeführt werden, bevor das Automatisierungssystem in Betrieb genommen wird. Für die Penetrationsprüfung sind eventuell externe Fachleute erforderlich, die zum Beispiel mit Hacking-Tools und -methoden vertraut sind.

Cybersicherheitsniveaus und die entsprechenden Anforderungen machen leichter verständlich, ob in einem Projekt oder einem Automatisierungsservice ausreichend für Cybersicherheit gesorgt ist. Gute Beispiele für Anforderungen an die Cybersicherheit und Sicherheitsstufen finden sich in IEC 62443-3-3, *Systemanforderungen zur IT-Sicherheit und Security-Level* [5] (siehe Kapitel *Cybersicherheitsnormen*). Die Anforderungen müssen entsprechend den ermittelten Gefährdungen angewandt werden.

Es ist möglich, die anvisierte Cybersicherheitstufe beizubehalten, indem die neuen Schwachstellen in verwendeten Produkten konstant überwacht und die entsprechenden Softwarepatches soweit möglich angewandt werden. Netzwerke müssen im Hinblick auf unbefugten Zugriff und Spionagesoftware überwacht werden. Es ist nicht möglich, zu agieren, ohne zu wissen, welche Bedrohungen jeden Tag auftauchen können. Es ist wichtig, nachzuverfolgen, wer in einem Netzwerk anwesend ist und ob jemand versucht, auf dieses Netzwerk ohne Genehmigung zuzugreifen, zum Beispiel über eine Firewall-Schutzschicht. Es gibt darüber hinaus I'm Kontext der Cybersicherheit verwendete Überwachungservices für Netzwerke, die speziell verwendet und konfiguriert werden können, um Anomalien oder Angriffe zu melden, die sich während des Betriebs eines Automatisierungssystems ereignen.

Cybersicherheit muss in allen Phasen in Betracht gezogen werden. Andernfalls kann die Bedrohung unbemerkt ihr Ziel finden. Die nachfolgende Tabelle zeigt typische Überlegungen hinsichtlich der Cybersicherheit in verschiedenen Projektphasen.

Phase	**Maßnahmen zur Cybersicherheit**
Entwicklungs- und Pilotphasen	Firewalls und Fernzugriffslösungen (VPN) gemäß Unternehmensrichtlinien und Anforderungen der Cybersicherheit installieren.
	Fernzugriff nur befugtem Herstellerpersonal mit autorisierten Benutzerkonten gewähren.
	Zugang jedes Benutzerkontos von verschiedenen Herstellern auf Subnetzwerke oder Maschinen begrenzen, die zum Lieferumfang gehören.
	Vertrauenswürdige Softwarepakete nur von vertrauenswürdigen Quellen (zum Beispiel von der Website von ABB Drives mit HTTPS) installieren.
	Vom Hersteller genehmigte Patches installieren.
Inbetriebnahmephase	Härtung von Systemen. Prüfen und sicherstellen, dass gemäß Bereitstellungsrichtlinien eine spezifische Cybersicherheitskonfiguration in allen Netzwerken und Automatisierungsgeräten, Systemen und Software vorhanden ist. Unnötige Software und nicht benötigte Funktionen sollten aus dem Lieferumfang entfernt werden.
	Prüfen, ob alle Systeme und Cybersicherheitsmechanismen entsprechend den Spezifikationen arbeiten.
	Alle Benutzer über die eingerichtete Cybersicherheit sowie die Änderungsmanagementverfahren informieren und diesbezüglich schulen.
	Cybersicherheits-Überwachungssysteme für das Netzwerk einrichten und sicherstellen, dass diese auf keinen Fall den Systembetrieb negativ beeinflussen.
Wartung	Die Härtung durch strenge Zugangs- und Änderungskontrolle aufrechterhalten; nur geplante Änderungen und Patches an Systemen, einschließlich ABB-Produkten, Netzwerkgeräten und Betriebssystemen zulassen.
	Die Systemprotokolle auf unbefugten Zugriff oder anderes, verdächtiges Verhalten überwachen.
	Systemaktualisierungen und neue Funktionen planen und in Testeinrichtungen prüfen, bevor sie in Produktionssystemen in Betrieb genommen werden.

3

Cybersicherheitsnormen

Inhalt dieses Kapitels

In diesem Kapitel werden die Normen in Bezug auf die Cybersicherheit erläutert.

Cybersicherheitsnormen in der Automatisierung

ABB ist sich der Bedeutung von Cybersicherheitnormen bewusst und gehört als aktives Mitglied verschiedenen Industrieinitiativen an, einschließlich IEEE und IEC. Dieses Engagement stellt sicher, dass die Bedürfnisse unserer Kunden bei der Entwicklung neuer Normen berücksichtigt werden und dass ABB auf gleicher Höhe mit den neuesten Entwicklungen verbleibt. ABB als Unternehmen ist dadurch auch in der Lage, neue Normen in seine Produkte und Systeme einfließen zu lassen, sodass es für ABB-Kunden leichter ist, neue Bestimmungen einzuhalten.

Die wichtigsten Cybersicherheitsnormen für die Automatisierung sind:

- Reihe IEC 62443: *Industrielle Kommunikationsnetze – IT-Sicherheit für Netze und Systeme*
- NIST 800-53: *Security and Privacy Controls for U.S. Federal Information Systems and Organizations*
- NIST Cybersecurity Framework: Framework for Improving Critical Infrastructure Cybersecurity
- NERC CIP: Critical Infrastructure protection standards
- Reihe ISO 27000: Die Normenreihe ISO 27000 für alle Aspekte der IT-Sicherheit
- IEEE P 1686: *IEEE Draft Standard for Substation Intelligent Electronic Devices (IED) Cyber Security Capabilities*
- IEC 62351: Normen für den Datenaustausch für Energiesysteme und andere zugehörige Systeme einschließlich Energiemanagementsysteme, SCADA, dezentrale Automatisierung und Teleprotection.

Die verfügbaren Normen, Frameworks und Regelungen sind in *Abbildung 3* dargestellt. Sie sind entsprechend ihrer Relevanz für Betreiber und Hersteller geordnet sowie hinsichtlich der Frage, ob sie technische oder Management-/Prozess-/Richtlinienaspekte betreffen.

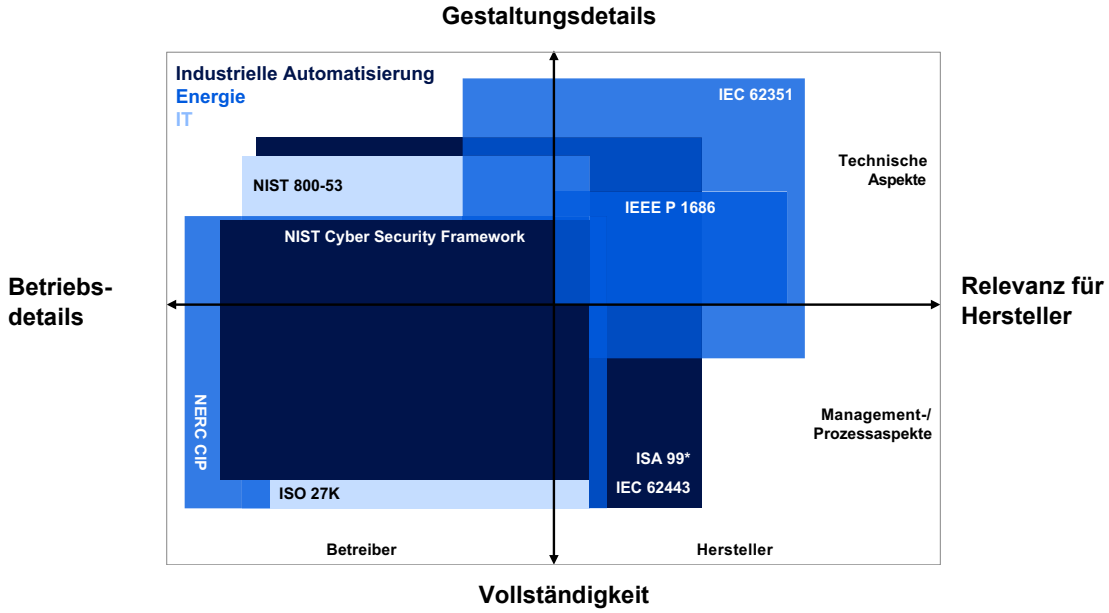

*Abbildung 3. Wichtige Cybersicherheitsnormen und ihre Geltungsbereiche. Erläuterung *) – Nach Abbruch des ESCoRTS-Projekts hat die ISA beschlossen, die Norm ISA 99 in ISA 62443 umzubenennen, um die Angleichung an die Reihe IEC 62443 deutlicher zu machen. [2], [3], [4], [5]*

Zwischen vielen Normen gibt es große Überlappungsbereiche, insbesondere bei denen, die für Betreiber oder Anlagenbesitzer nützlich sind.

Die Hauptreferenz für Anforderungen an die Cybersicherheit in der Automatisierung ist in der Norm IEC 62443 (auch als ISA 99 bekannt) dokumentiert, die den größten Geltungsbereich und die ausführlichsten Richtlinien enthält [5]. Das NIST Cybersecurity Framework, Version 1.0 wurde am 1. Februar 2014 veröffentlicht und enthält weniger Details. NERC CIP ist erwähnenswert, da Standorte, die an das öffentliche Stromnetz in den USA und Kanada angeschlossen sind, die Anforderungen der NERC CIP Norm erfüllen müssen.

Die International Electrotechnical Commission (IEC) ist eine weltweite Normungsorganisation, die alle Teile der Serie IEC 62443, die unter der allgemeinen Bezeichnung *Industrielle Kommunikationsnetze – IT-Sicherheit für Netze und Systeme veröffentlicht* wird, kontinuierlich entwickelt und pflegt. Diese Normen können über die IEC-Website bezogen werden. Die Normenreihe IEC 62443 mit Bezeichnungen ist in der Tabelle unten aufgeführt.

IEC-Referenz	Bezeichnung und Geltungsbereich
IEC/TS 62443-1-1	Terminologie, Konzepte und Modelle für die Sicherheit von industriellen Automatisierungs- und Steuerungssystemen (IACS)
IEC/TR 62443-1-2	Hauptglossar der Begriffe und Abkürzungen
IEC 62443-1-3	Definiert eine Reihe von Compliance-Metriken für die IACS-Sicherheit
IEC/TR 62443-1-4	IACS-Lebenszyklus und Anwendungsfälle
IEC 62443-2-1	Anforderungen an ein IACS-Sicherheitsmanagementsystem
IEC/TR 62443-2-2	Leitfaden für die Implementierung eines IACS-Sicherheitsmanagementsystems
IEC/TR 62443-2-3	Patchmanagement in IACS-Umgebungen

IEC-Referenz	Bezeichnung und Geltungsbereich
IEC 62443-2-4	Schwerpunkt auf der Zertifizierung von IACS-Zulieferer-Sicherheitsrichtlinien und Praktiken
IEC/TR 62443-3-1	Technischer Bericht über geeignete Technologien für IACS-bezogene Sicherheit
IEC 62443-3-2	Sicherheitsrisikobewertung und Systemauslegung
IEC 62443-3-3	Systemsicherheitsanforderungen und Sicherheitsstufen
IEC 62443-4-1	Anforderungen an die Produktentwicklung
IEC 62443-4-2	Detaillierte, technische Sicherheitsanforderungen für IACS-Komponenten

Die Ableitung von Cybersicherheitsanforderungen aus den oben genannten Normen für einen bestimmten Automatisierungsfall ist keine einfache Aufgabe. Auch hier haben die Anforderungen an Sicherheit und Betriebskontinuität Vorrang vor den Cybersicherheitsmaßnahmen. Vorausgesetzt, dass es möglich ist, die erforderlichen Anforderungen an Sicherheit und Betriebskontinuität zu erfüllen, können die Cybersicherheitsanforderungen anhand von Installationsumgebung, Anwendungsfällen und Bedrohungslandschaft als Basis für das Verständnis der Cybersicherheitsbedrohungen analysiert werden.

4

Beispielfälle

Inhalt dieses Kapitels

In den nächsten Abschnitten werden vier verschiedene Anwendungsumgebungen beschrieben, in denen drehzahlgeregelte Antriebe und Konnektivitätsprodukte von ABB in der Regel eingesetzt werden. Für jeden Fall stellen wir typische Anwendungsfälle, Herausforderungen im Hinblick auf die Cybersicherheit und sichere Verwendungspraktiken vor, d. h. die allgemeine Handhabung und Bewältigung von festgestellten Herausforderungen und Risiken im Zusammenhang mit der Cybersicherheit.

Einleitung

Das Ziel des Konzepts “Sicher ab Bereitstellung” besteht darin, zu gewährleisten, dass Produkte auf sichere Weise installiert, konfiguriert, betrieben und gewartet werden können. Dazu gehört, dass eingesetzte Software keine Schwachstellen oder Sicherheitslücken aufweist.

Wie in jedem Fall gezeigt, ermöglichen die Produkte von ABB Drives den netzwerkgestützten Fernbetrieb sowie die Fernüberwachung. Diese Netzwerk- und Konnektivitätsfunktionen steigern die Bedeutung, die der Verhinderung jeglichen unbefugten elektronischen Zugangs zu Automatisierungssystemen zukommt.

Fall 1 – Industrielles Automatisierungsbeispiel (Fabrikumgebung)

Beschreibung

In diesem Beispiel werden allgemeine Möglichkeiten des Schutzes der industriellen Automatisierungsumgebung gegen unbefugten Zugriff beschrieben.

In der Praxis gibt es zwischen industriellen Automatisierungssystemen erhebliche Unterschiede. Es gibt eine große Anzahl verschiedener Netzwerke und Automatisierungs-anwendungsarchitekturen, die innerhalb verschiedener Industriesektoren weltweit implementiert werden, wie zum Beispiel Fertigung, Prozessindustrie, Energieerzeugung und -verteilung. Deshalb ist dieses Beispiel nur zur allgemeinen Verwendung vorgesehen und beinhaltet nicht alle Einzelheiten, die für die Implementierung eines sicheren Systems erforderlich sind. Soweit es um Produkte von ABB Drives sowie entsprechende Konnektivitätsprodukte geht, sind alle Richtlinien und Anweisungen jedoch real und gültig.

Abbildung 4 stellt ein fiktives Werksnetzwerk mit Produkten von ABB Drives dar, das normalerweise sicher mit dem Firmennetzwerk des Kunden (in der Abbildung nicht sichtbar) über öffentliche oder private Netzwerke verbunden ist, aber auch mit anderen Automatisierungsnetzwerken innerhalb des Werkes.

In diesem Beispiel dienen ABB ACS880 Industrial Drives zur Darstellung drehzahlgeregelter Antriebe. Die anderen, abgebildeten Konnektivitäts- und Softwareprodukte von ABB Drives sind:

- AC500 / AC500-S Safety SPS (speicherprogrammierbare Steuerung).
- FENA-11/-21: Ethernet-Adaptermodul − ermöglicht die Ethernet-Kommunikation für Antriebe.
  - FENA-11 und -21 unterstützen industrielle Ethernet-Protokolle (Modbus/TCP, Ethernet/IP und PROFINET IO), die keine Cybersicherheitsfunktionen spezifizieren.
- NETA-21. Fernüberwachung für Antriebe.
  - Implementiert Sicherheitsfunktionen für die Kommunikation über nicht-vertrauenswürdige Netzwerke.
  - Umfasst Benutzerauthentifizierung, Benutzerkonten und sichere Kommunikation.
- Automation Builder mit Drive Manager-Plug-In. Integriertes Softwarepaket für Maschinenbauer und Systemintegratoren, um deren Maschinen und Systeme zu automatisieren.
  - Kombiniert die Tools, für die Konfiguration, Programmierung, Fehlerbeseitigung und Wartung von Automatisierungsprojekten über eine gemeinsame Schnittstelle erforderlich sind.
- Drive Composer. Software-Tool für die Inbetriebnahme und Wartung von ABB-Antrieben mit gemeinsamer Architektur.
  - Wird verwendet, um Antriebsparameter anzuzeigen und einzustellen und um die Prozessleistung zu überwachen und abzustimmen.

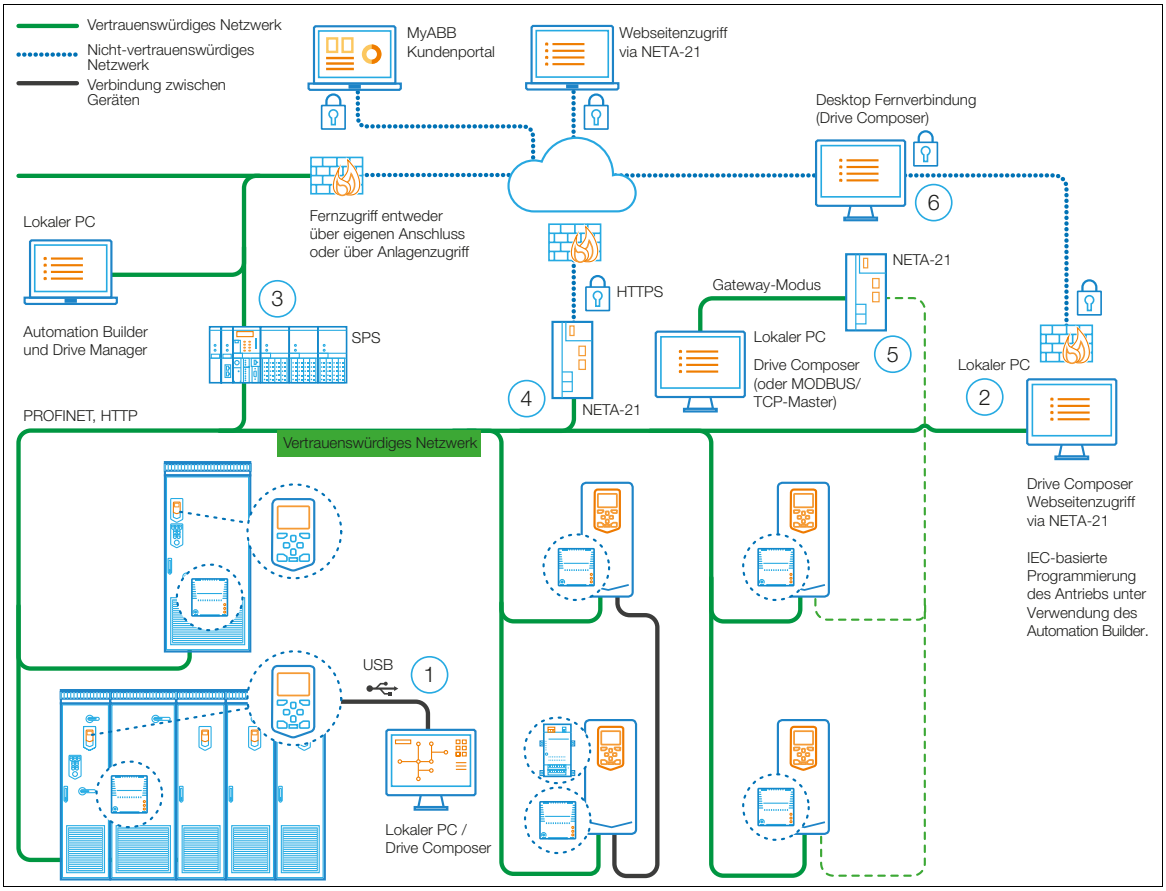

Abbildung 4. Industrielle Automatisierungsanlage. Verschiedene Netzwerkmöglichkeiten und ihre sichere Anwendung.

Abbildung 4 zeigt verschiedene Anwendungsfälle und Kommunikationsmöglichkeiten. Die darin angegebenen Punkte werden im Folgenden erläutert. Die gezeigten Anwendungsfälle sind:

- **Inbetriebnahme** der Antriebe und der Fertigungslinie unter Verwendung des Inbetriebnahme- und Wartungstools Drive Composer und/oder der Software-Suite Automation Builder über
  1. lokale Anschlüsse (serielle Punkt-zu-Punkt-Kommunikation, d.h. USB) oder
  2. ein gemeinsam verwendetes, übergeordnetes physikalisches Feldbus-Netzwerk (mit Steuerung) (z.B. PROFINET) unter Verwendung von Ethernet-Kommunikation und/oder
  3. auch Kommunikation über ein SPS-System unter Verwendung des Tools Drive Manager oder
  4. die Fernüberwachungstool-Webschnittstelle NETA-21 oder
  5. NETA-21 als Gateway dazwischen oder einen
  6. Desktop-Fernanschluss eines Drittherstellers.
- **Wartung und Störungssuche** mithilfe der oben genannten Tools und Kommunikationsnetzwerke
- **Fernsupport- und Fernzustands-Überwachungsservices**
- **On-Demand-Fernüberwachung** über ein nicht-vertrauenswürdiges Netzwerk (öffentliches Internet) unter Verwendung des Fernüberwachungtools NETA-21

Die dargestellte Architektur beinhaltet die folgenden Komponenten:

- In den öffentlichen Netzwerken gibt es Services, wie zum Beispiel:
  - Kundenportal (Cloud-basierter Service)
  - Fernüberwachung mittels Webseitenzugriff, zum Beispiel das Fernüberwachungstool NETA-21.
  - Desktop-Fernanschlüsse (Drive Composer)
- In einem vertrauenswürdigen Anlagennetzwerk gibt es:
  - Firewalls vor öffentlichen Netzwerken
  - SPS und lokale PCs (unterschiedliche Softwaretools installiert)
  - Antriebe, die an den Ethernet-Feldbus (z.B. PROFINET) über FENA-11/-21 angeschlossen sind
  - Antriebe, die über USB an einen lokalen PC angeschlossen sind
  - NETA-21, das über Firewall ebenfalls an öffentliche Netzwerke angeschlossen ist
  - NETA-21, das an die Antriebe mit EIA-485 und einen lokalen PC unter Verwendung des Gateway-Modus angeschlossen ist

Cybersicherheits-Risikominderung und sichere Anwendung

Die Idee ist, einen fundierten Schutz für jedes Netzwerk bereitzustellen, indem Firewall-Lösungen den internen, vertrauenswürdigen Netzwerken jedes Netzwerks zugewiesen werden.

- Filewalls, deren Konfigurationen und Zugriffsrichtlinien müssen sorgfältig verwaltet werden.

Anwendung von Ethernet-Feldbusadaptern FENA-11/-21

Der FENA-11/-21 muss in ein vertrauenswürdiges Netzwerk eingebettet werden (streng begrenzter und gut gehosteter Teil eines Netzwerks oder Steuerungssystems)

Auf der Servicekonfigurationsseite (Webseite) für den FENA-11/-21 können bestimmte Ethernet-Services deaktiviert werden. Standardmäßig sind alle Services aktiviert. Es wird empfohlen, nach der Inbetriebnahme die Services zu deaktivieren, die nicht verwendet werden:

- Kommunikation des PC-Tools oder Zugriff auf FENA-11/-21 Webseiten
- Änderung von IP-Einstellungen per Fernzugriff unter Verwendung des ABB IP-Konfigurationstools
- Fernzugriff auf Antriebe mit dem Drive Composer Tool über Ethernet
- Ping-Anfragen

Weitere Informationen siehe *FENA-11/-21 user manual* [11].

Anwendung von ACS880 Industrial Drives

Benutzerschloss. Für eine höhere Cybersicherheit kann ein Hauptpasswort festgelegt werden, um zum Beispiel zu verhindern, dass Parameterwerte verändert und/oder Firmware oder andere Dateien geladen werden. Mit der Benutzerschlossfunktion wird Folgendes verhindert:

- Firmware-Upgrades
- Konfiguration des Sicherheitsfunktionsmoduls (FSO-12/-21)
- Wiederherstellung von Parametern
- Laden von adaptiven Programmen oder Applikationsprogrammen
- Ändern der Startansicht des Bedienpanels
- Bearbeiten von FU-Texten
- Bearbeiten der Favoritenliste der Parameter auf dem Bedienpanel
- Konfigurationseinstellungen über das Bedienpanel, wie Zeit- und Datumsformate und das Ein-/Ausblenden der Uhranzeige.

Benutzerzugriffsebenen. Konfigurieren Sie für lokale Benutzerschnittstellen (Drive Composer und Bedienpanel) Parameter-Zugriffsrechte unter Verwendung der Parameterschlossfunktion.

Weitere Informationen siehe *ACS880 primary control program manual* [7].

Anwendung der Kommunikation von Drive Composer über Ethernet:

Drive Composer stellt die Ethernet-Kommunikation nur mit “erkannten Geräten” her, d. h. FENA-11/-21 Ethernet-Feldbusadaptern. Dies ist die Standardbetriebsart.

Weitere Informationen siehe *Ethernet tool network for ACS880 drives application guide* [14].

Anwendung von NETA-21

Konfigurieren Sie die Cybersicherheitsfunktionen von NETA-21 auf Grundlage des Prinzips, alles abzulehnen, was nicht benötigt oder verwendet wird.

- Ändern Sie das Standard-Administratorpasswort.
- Erstellen Sie nur solche Konten, die lokal oder extern genutzt werden, unter Verwendung von Rollen mit so wenig Zugriffsrechten wie möglich. Verwenden Sie starke Passwörter.
- Prüfen Sie, ob die neueste Firmwareversion des Tools NETA-21 verwendet wird, damit die neuesten Softwareversionen und Sicherheitspatches zur Verfügung stehen.
- Wenn Cloud-Services von ABB verwendet werden (zum Beispiel ABB Ability™ Condition Monitoring & Remote Assistance): Prüfen Sie regelmäßig die gewährten E-Mail-Zugriffe auf die myABB-Konten, um Missbrauch vorzubeugen, und melden Sie ABB unverzüglich falsche oder abgelaufene Konten.

Benutzen Sie für den sicheren Zugriff HTTPS, bei dem es sich um eine Kombination aus HTTP mit einer zusätzlichen Verschlüsselungsschicht aus SSL/TLS-Protokollen handelt, um einen sicheren Kanal über ein unsicheres Netzwerk zu erstellen.

Wenn der höchstmögliche Grad an Produktschutz benötigt wird, so ist es möglich, auch die folgenden Veränderungen durchzuführen:

- Tool-Einstellungen (werksseitige Tools): deaktivieren Sie den SSH-Service (Konto für werksseitigen Support), wenn die SSH-Konsole für Support und Diagnose nicht benötigt wird.
- Lokale Einstellungen: deaktivieren Sie NTP-Anfragen (Network Time Protocol), die NETA-21 an externe Server senden kann, oder ersetzen Sie diese durch lokale NTP-Zeit Server, sofern diese verfügbar sind.
- Geräteschnittstellen / Ethernet (Schnittstellen-Einstellungen): deaktivieren Sie den Hintergrund-Scan, der UDP-Suchanfragen über das lokale Netzwerk sendet, um über Ethernet angeschlossene ABB-Antriebe zu ermitteln.

Die folgenden Netzwerk-Services sollten deaktiviert werden, wenn sie nicht verwendet werden:

- NBT NS-Suche (NetBIOS-Namenssuchservice)
- FTPS-Service, auch wenn standardmäßig keine FTP(S)-Konten existieren
- Ethernet-Tool-Netzwerk, automatische Auffindbarkeit von NETA-21 innerhalb des lokalen Netzwerks.

Wenn NETA-21 und Drive Composer gleichzeitig über Ethernet verwendet werden, sollte der PC-Tool-freundliche Modus in NETA-21 benutzt werden.

Überwachen Sie aktiv das interne Netzwerk. Suchen Sie speziell nach nicht autorisierten Geräten.

Weitere Informationen siehe *NETA-21 remote monitoring tool user’s manual* [12] und *Ethernet tool network for ACS880 drives application guide* [14].

Sicherheitsaspekte in Bezug auf das Kundenportal und die Cloud werden in *Security Overview - Drive Remote Service Platform* [6] (verfügbar in der ABB Library) erläutert.

Cloud-Services benötigen lediglich eine ausgehende HTTPS-Verbindung (Port TCP:443) von NETA-21 zu Servern in Microsoft Azure. Cloud-Services nutzen eine zentrale Benutzer-Autorisierung und -verwaltung, wie zum Beispiel ADFS (Active Directory Federation Services).

Normale Härtungsanweisungen für NETA-21 gelten auch im Zusammenhang mit Cloud-Services. Es ist außerdem möglich, die gesamte Webschnittstelle von NETA-21 über die Cloud-Verbindung zu schließen (zum Beispiel, wenn NETA-21 an ein öffentliches Netzwerk angeschlossen ist).

Fall 2 – Fern gelegene Pumpstationen

Beschreibung

In diesem Beispiel werden allgemeine Möglichkeiten beschrieben, um fern gelegene Pumpstationen (Druckpumpenanwendung) in Echtzeit unter Verwendung permanenter drahtloser Verbindungen zu überwachen, zu betreiben und zu warten. Zusätzlich zu einem Beispiel für eine industrielle Automatisierungsanlage veranschaulicht es außerdem die Möglichkeit, dass Antriebe über eine Bluetooth-Schnittstelle (ACS-AP-W) mit der mobilen Drivetune-App verbunden werden können und diese als Gateway die Antriebe über mobile Netzwerke (3G/4G) an das Internet anschließen. In diesem Beispiel dienen ABB ACS580 General Purpose Drives zur Darstellung drehzahlgeregelter Antriebe.

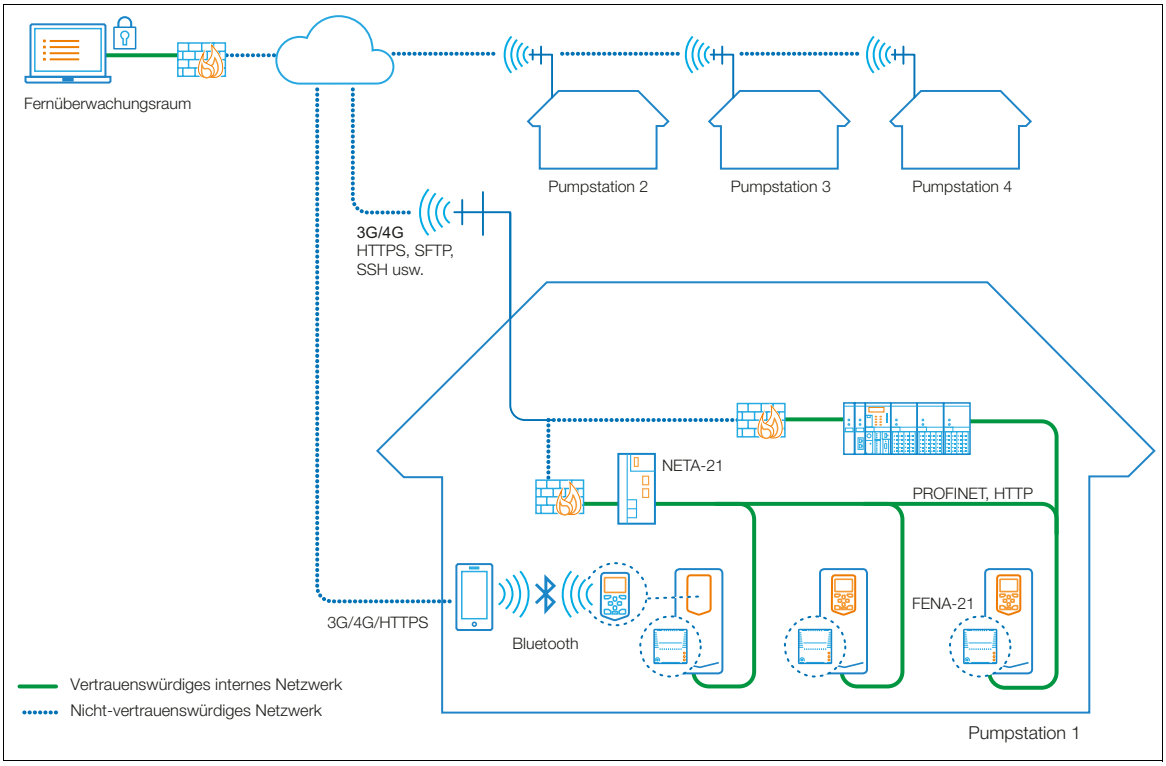

Abbildung 5. Wasserpumpstation mit permanenten drahtlosen Anschlüssen.

In diesem Beispiel können Frequenzumrichter eine oder mehrere Pumpen regeln und daher den Wasservolumenstrom auf Grundlage des Bedarfs steuern. Die neue Technologie und Steuerungsverfahren machen es möglich, erhebliche Energiemengen einzusparen, allerdings erhöht dieser Ansatz aus Sicht der Cybersicherheit die Anzahl der Feldautomatisierungsgeräte und damit die Risiken in Zusammenhang mit der Cybersicherheit. Externe Verbindungen sind in der Regel für lokale SPS- oder SCADA-Systeme implementiert worden.

Die Herausforderung besteht darin, eine Antwort auf die Frage zu finden, wie die Stationsnetzwerke und die Verbindungen gesichert werden können.

- Eine dezentrale Architektur erhöht die Notwendigkeit, den Zugriff auf andere lokale Stationen und Betreibersysteme einzuschränken.
- Eine lockere physikalische Zugangskontrolle hat zur Folge, dass das lokale Netzwerk nicht als vertrauenswürdig bezeichnet werden kann und bedeutet, dass ein tiefgreifender Schutz implementiert werden muss.

Cybersicherheits-Risikominderung und sichere Anwendung

Der Grundgedanke ist die Schaffung eines tiefgreifenden Schutzes für die Pumpstation, wie im Folgenden beschrieben:

- Stellen Sie einen eigenen Mobilfunk-Betreiberzugangspunkt (APN) für alle drahtlosen Verbindungen bei Pumpstationen bereit. Jeder bereitgestellte drahtlose Router darf nur über einen vertrauenswürdigen Mobilfunk-Betreiberzugangspunkt, der über mit dem Kunden vereinbarte Cybersicherheitsfunktionen verfügt, Verbindungen herstellen und zulassen (APN ist der Name eines Gateways zwischen einem GSM-, GPRS-, 3G- oder 4G-Mobilfunknetzwerk und anderen Netzwerken).
- Weisen Sie Firewall-Lösungen der Front der internen (vertrauenswürdigen) Netzwerke jeder Pumpstation zu: verwalten Sie sorgfältig alle Firewalls, deren Konfigurationen und Zugriffsrichtlinien.

Anwendung des ACS580 General Purpose Drives:

Anweisungen zur Anwendung des ACS580 siehe Abschnitt *Cybersicherheits-Risikominderung und sichere Anwendung* auf Seite *30*. Befolgen Sie die gleichen Verfahren. [8]

Anwendung von Ethernet-Feldbusadaptern FENA-11/-21:

Anweisungen zur Anwendung des FENA-11/-21 siehe Abschnitt *Cybersicherheits-Risikominderung und sichere Anwendung* auf Seite *30*. Befolgen Sie die gleichen Verfahren. [11]

Anwendung der Kommunikation von Drive Composer über Ethernet:

Anweisungen zur Anwendung des FENA-11/-21 siehe Abschnitt *Cybersicherheits-Risikominderung und sichere Anwendung* auf Seite *30*. Befolgen Sie die gleichen Verfahren. [14]

Anwendung von Drivetune, Komfort-Bedienpanel ACS-AP-W und Bluetooth-Verbindung:

- Deaktivieren Sie bei der Konfiguration der Bluetooth-Verbindung den Modus “Immer auffindbar”, falls nicht benötigt. Im Modus "Immer auffindbar" ist das Komfort-Bedienpanel ACS-AP-W von jedem Bluetooth-Gerät innerhalb des Funkbereichs auffindbar.
- Wenn der Modus "Immer auffindbar" benötigt wird, stellen Sie sicher, dass der für den Kopplungsprozess benötigte PIN-Code sich an einem sicheren Ort befindet oder nur befugte Personen Zugriff auf diesen haben.

Anwendung von NETA-21:

Konfigurieren Sie die Cybersicherheitsfunktionen von NETA-21 wie für den ersten Fall beschrieben. Ausführlichere Anweisungen zur Anwendung von NETA-21 siehe Abschnitt *Cybersicherheits-Risikominderung und sichere Anwendung* auf Seite *30*.

Fall 3 – OEM-Maschinenausrüstung

Beschreibung

Dieser Beispielfall entspricht demjenigen des industriellen Automatisierungsfalles; der Unterschied und die spezifische Erweiterung ist die Fernserviceverbindung des OEM-Herstellers. OEM-Hersteller bieten oft an, ihre Anlagen und auch die drehzahlgeregelten Antriebe von ABB in diesen Anlagen zu überwachen und Fernsupport zu leisten. Dieser Fernanschluss wird in der Regel über die VPN-Verbindung eines Drittanbieters (einschließlich Hard- und Software) implementiert. In diesem Beispiel dienen ACS380 und ACS880-M04 Machinery Drives von ABB zur Darstellung drehzahlgeregelter Antriebe.

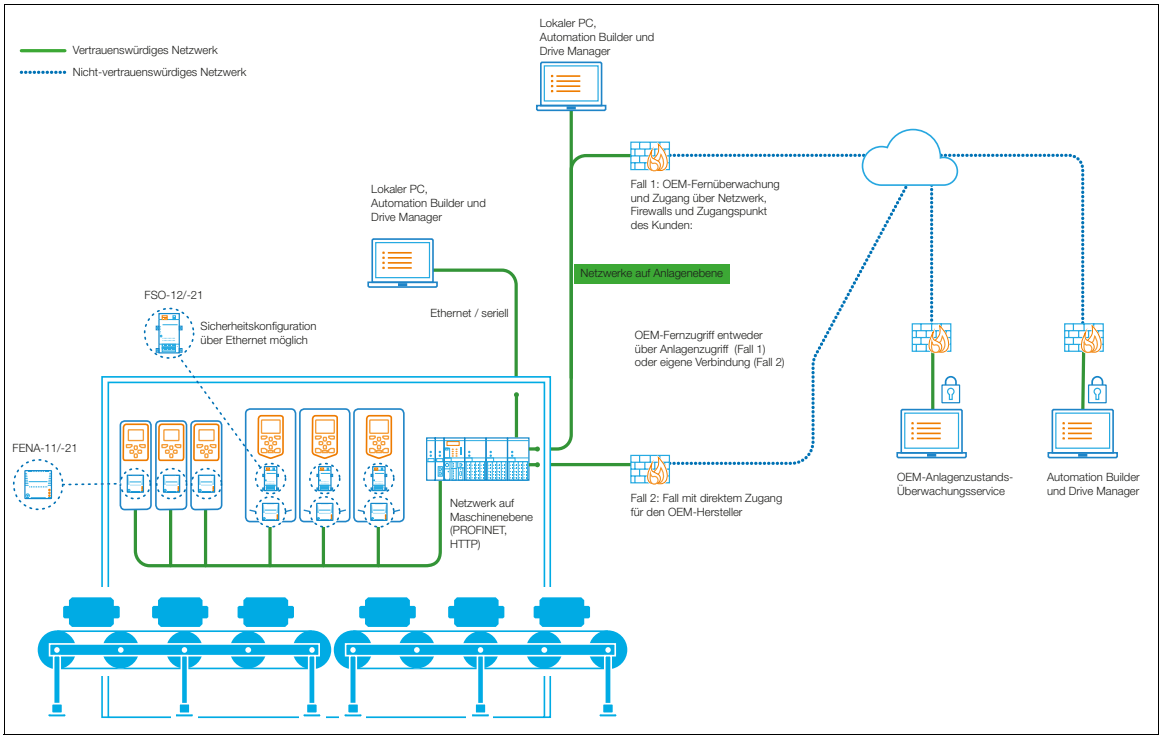

Abbildung 6. Beispielfall OEM-Anlage

In diesem Beispiel ist die OEM-Anlage (eine Flaschenabfüllanlage) eine separate Anlage oder Teil des Automatisierungsnetzes eines Werks einschließlich mehrerer drehzahlgeregelter Antriebe, SPS und anderer benötigter Zusatzausrüstung.

Der OEM hat zwei Alternativen für die Fernverbindung mit der Anlage im Werk des Endkunden:

- Über die Netzwerke, Firewalls und Zugangspunkte des Kunden
- Direkt von der OEM-Anlage über ein Modem, VPN-Router oder ähnlichem (nicht empfohlen)

Der OEM-Hersteller stellt einen Service bereit, um die Einsatzfähigkeit der Anlage zu gewährleisten, indem System, Software und Einstellungen der OEM-Anlage extern verwaltet und installiert werden. Zu den Services können Zustandsüberwachung, Optimierung, Fernsupport und Software-Updates gehören.

Der Endbenutzer sieht die OEM-Anlage als ein einzelnes System, auch wenn es SPS und interne Feldnetzwerk- und andere Steuerungseinheiten enthält. Endbenutzer steuern den gesamten Maschinenbetrieb mittels HMI oder einem Netzwerk auf Anlagenebene.

Cybersicherheits-Risikominderung und sichere Anwendung

Der Grundgedanke ist, einen externe Zugangspfgad für Services speziell von OEM-Herstellern zu sichern.

Fall 1: OEM-Zugang über Netzwerk, Firewalls und Zugangspunkt des Kunden:

- Installieren und verwalten Sie die Firewalls an vorderster Stelle im Netzwerk auf Anlagenebene.
- Verbinden Sie die Firewall des Unternehmens mit der Firewall des OEM-Herstellers unter Verwendung statischer, sicherer VPN-Gateway-to-Gateway-Verbindungen.
- Verweigern Sie standardmäßig alle Verbindungen von den Anlagennetzwerken zu anderen Netzwerken.
- Gestatten Sie nur authentifizierte und gesicherte Serviceverbindungen (HTTPS) zwischen OEM-Anlagen und externen OEM-Anlagentools.
- Stellen Sie die speziellen Managed Switch(es) für Netzwerke auf Anlagenebene bereit.
- Unterteilen Sie die verschiedenen Feldnetzwerke in unterschiedliche Segmente und verweigern Sie jegliche unnötige Datenkommunikation zwischen den Segmenten.
- Ermitteln und verwenden Sie die Cybersicherheitsfunktionen des Managed Switch, damit alle unnötigen Aktivitäten in den Subnetzwerken blockiert werden.
- Unterteilen Sie Managementsysteme und Verbindungen, um Netzwerksegmente mit allen erforderlichen Cybersicherheitfunktionen, die aktiviert sind, zu trennen.
- Verweigern Sie alle anderen Konnektivitätsmechanismen von Systemen auf Maschinenebene, um unbefugten Zugriff weitestgehend einzuschränken.
- Überwachen Sie Cybersicherheit, Topologie (Asset Management) und korrekten Betrieb der Anlagennetzwerke unter Verwendung der Cybersicherheits-Überwachungsmodule und Funktionen der Firewalls und Managed Switches.

Fall 2: Fall mit direktem Zugang für den OEM-Hersteller (nicht empfohlen)

- Stellen Sie einen eigenen Mobilfunk-Betreiberzugangspunkt (APN) für einen OEM-Maschinenhersteller bereit.
  - Der bereitgestellte drahtlose Router darf nur über einen vertrauenswürdigen Mobilfunk-Betreiberzugangspunkt, der über mit dem Kunden vereinbarte Cybersicherheitsfunktionen verfügt, Verbindungen herstellen und zulassen.
- Stellen Sie Firewall-Lösungen an der Netzwerkfront der OEM-Maschine bereit. Verwalten Sie sorgfältig die Filewall, deren Konfigurationen und Zugriffsrichtlinien.
- Deaktivieren Sie sorgfältig alle nicht benutzten Services aller Komponenten, um die Angriffsoberfläche zu verkleinern.
- Überwachen Sie aktiv die internen Netzwerkknoten und das Verhalten der Maschinen mittels Cybersicherheits-Überwachungsservices. Suchen Sie speziell nach falsch konfigurierten Geräten und möglichen Malware-Verhaltensmustern.

In beiden Fällen unterliegt die Anwendung von ABB Drive- und Konnektivitätsprodukten den Prinzipien, die anhand des Beispiels der Industrieanlage gezeigt wurden.

Anwendung von ACS380 und ACS880-M04 Machinery Drive:

Anweisungen zur Anwendung dieser Antriebe siehe Abschnitt *Cybersicherheits-Risikominderung und sichere Anwendung* auf Seite *30*. Befolgen Sie die gleichen Verfahren. [9]

Anwendung von Ethernet-Feldbusadaptern FENA-11/-21:

Anweisungen zur Anwendung des FENA-11/-21 siehe Abschnitt *Cybersicherheits-Risikominderung und sichere Anwendung* auf Seite *30*. Befolgen Sie die gleichen Verfahren. [11]

Anwendung der Kommunikation von Drive Composer über Ethernet:

Anweisungen zur Anwendung des FENA-11/-21 siehe Abschnitt *Cybersicherheits-Risikominderung und sichere Anwendung* auf Seite *30*. Befolgen Sie die gleichen Verfahren. [13], [14]

Fall 4 – Gebäudeautomatisierung

Beschreibung

In diesem Beispiel werden allgemeine Maßnahmen zur Fernüberwachung geographisch verteilter Gebäude beschrieben; es hat Ähnlichkeiten mit dem Beispiel der fern gelegenen Pumpstation. Der Hauptzweck besteht darin, verschiedene Gebäude und Gebäudesysteme von einem Kontrollraum aus zu überwachen, zu steuern und zu aktualisieren. In diesem Beispiel dienen Antriebe speziell aus dem HLK-Segment (Heizung, Lüftung und Klimaanlage), nämlich ACH550 und ACH580 von ABB, zur Darstellung drehzahlgeregelter Antriebe.

Die anderen zugehörigen Konnektivitätsprodukte von ABB Drives, die zusammen mit den ACH550 und ACH580 Antrieben gezeigt werden, sind:

- **FBIP-21**. Das FBIP-21-Adaptermodul für BACnet/IP ist ein optionales Gerät für ABB-Antriebe, zum Beispiel den ACH580, mit dem der Antrieb an ein BACnet/IP-Netzwerk angeschlossen wird.
- **RBIP-01**. Das BACnet/IP-Routermodul RBIP-01 ist ein BACnet-Router. Es passt als steckbares Modul in das Frequenzumrichtergehäuse und ist voll kompatibel mit allen ACH550 Standard Drive-Frequenzumrichtern für HLK.

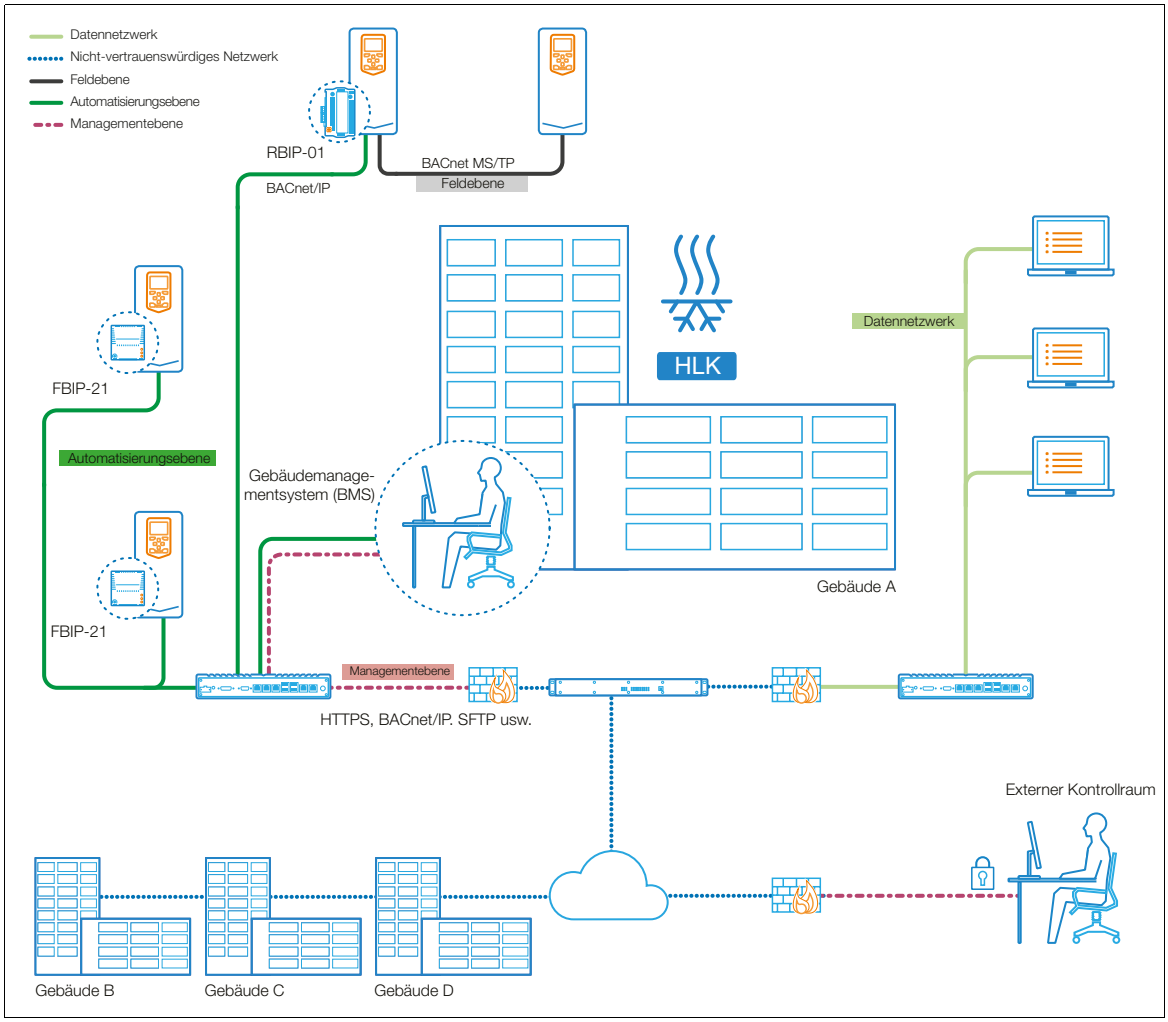

Abbildung 7. Fallbeispiel Gebäudeautomatisierung

In diesem Beispiel werden sichere Fernverbindungen mit verschiedenen Gebäuden in der Stadt benötigt (nur Campusbereiche und ähnliche Bereiche haben eventuell ihren eigenen lokalen Kontrollraum). Zu den über die Fernverbindungen übertragenen Daten gehören in der Regel:

- Alarme und andere Ereignisse
- Wöchentliche Planung (keine Überwachung für einzelne Geräte)
- Erfassung verschiedener Verbrauchsinformationen durch den zentralen Server

Normalerweise gibt es eine eigene Steuerung des Gebäudemanagementsystems, die planmäßige Timings und Steuerschleifen ausführt sowie Protokolle erstellt. Oft verwenden alle Geräte das gleiche physikalische und logische LAN für Betrieb und Management, auch zwischen Gebäuden

- Die komplette Automatisierung im selben Netzwerk (Automatisierungsebene)
- Separates LAN für die Daten von Benutzern in Gebäuden (Datennetzwerk)
- Die Trennung kann physikalisch oder virtuell unter Verwendung von Switches realisiert werden, allerdings werden eventuell dieselbe Internet-Konnektivität und dieselben Firewalls verwendet

Die Herausforderung besteht darin, eine Antwort auf die Frage zu finden, wie die Gebäudenetzwerke und die Verbindungen gesichert werden können.

- Aufwändige Verkabelung überall, außerdem sind drahtlose Geräte installiert
- Es ist schwierig, den physikalischen Zugriff auf die Verkabelung überall zu kontrollieren
- Gemeinsam genutztes IP-Netzwerk sowohl für Betriebs- als auch für Verwaltungszwecke

Cybersicherheits-Risikominderung und sichere Anwendung

Der Grundgedanke besteht darin, die verschiedenen lokalen Gebäudenetzwerke zu trennen und zu unterteilen.

- Installieren und verwalten Sie die Firewalls an vorderster Stelle in jedem Gebäudeautomatisierungsnetzwerk.
- Verbinden Sie jede Firewall der Gebäudeautomatisierung mit der Kontrollraum-Firewall unter Verwendung statischer, sicherer VPN-Gateway-to-Gateway-Verbindungen.
- Verweigern Sie alle Verbindungen von/zu den Gebäudeautomatisierungsnetzwerken und anderen Netzwerken.
- Gewähren Sie nur authentifizierte und gesicherte Managementverbindungen (HTTPS) zwischen Gebäudemanagementsystem und Kontrollraum.
- Aktivieren Sie zur Sicherung der Dateiübertragung das SFTP (SSH-Dateiübertragungsprotokoll).
- Stellen Sie spezielle Managed Switch(es) für Gebäudeautomatisierungsnetzwerke bereit.
- Unterteilen Sie die verschiedenen Gebäudeautomatisierungsnetzwerke in unterschiedliche Segmente und verweigern Sie jegliche unnötige Datenkommunikation zwischen den Segmenten.
- Ermitteln und verwenden Sie die Cybersicherheitsfunktionen des Managed Switch, damit alle unnötigen Aktivitäten in den Subnetzwerken blockiert werden.
- Unterteilen Sie Managementsysteme und Verbindungen, um Netzwerksegmente mit allen erforderlichen Cybersicherheitsfunktionen, die aktiviert sind, zu trennen.
- Verweigern Sie alle anderen Konnektivitätsmechanismen von Gebäudeautomatisierungssystemen, um unbefugten Zugriff weitestgehend einzuschränken.
- Überwachen Sie Cybersicherheit, Topologie (Asset Management) und korrekten Betrieb der Gebäudedatennetzwerke unter Verwendung der Cybersicherheits-Überwachungsmodule und Funktionen der Firewalls und Managed Switches.

In diesem Beispiel unterliegt die Anwendung von ABB Drive- und Konnektivitätsprodukten den Prinzipien, die anhand des Beispiels der Industrieanlage gezeigt wurden.

Anwendung des ACH580 HLK-Frequenzumrichters:

Anweisungen zur Anwendung des ACH580 siehe Abschnitt *Cybersicherheits-Risikominderung und sichere Anwendung* auf Seite *30*. Befolgen Sie die gleichen Verfahren. [10].

5

Cybersicherheitsrichtlinien von ABB

Inhalt dieses Kapitels

In diesem Kapitel werden die Richtlinien von ABB in Bezug auf die Cybersicherheit erläutert.

Grundsatz

ABB Drives nimmt alle Probleme im Zusammenhang mit der Cybersicherheit ernst und verfolgt konsequent Programme, die darauf abzielen, in enger Zusammenarbeit mit den Zulieferern und Kunden von ABB Produktfunktionen und Prozesse zu entwickeln und zu verbessern, um die Auswahl, Anwendung und Wahrung Cybersicherheit förderlicher, technischer Lösungen zu unterstützen, ohne substantielle Abstriche an Produktsicherheit, Leistung oder Produktivität in Kauf zu nehmen.

Lösungen von ABB Drives haben die Aufgabe, Geschäftsrisiken zu reduzieren, Benutzerfreundlichkeit und Zuverlässigkeit zu gewährleisten sowie die Einhaltung von Normen und gesetzlichen Vorschriften zu ermöglichen. ABB betont außerdem, dass Cybersicherheit kein statisches Ziel ist, sondern eine fortlaufende Entwicklung für bewährte Verfahren sein darstellt.

Device Security Assurance Center (DSAC)

ABB hat für alle ABB-Produkte Anforderungen hinsichtlich der Cybersicherheit festgelegt. Die Anforderungen gelten für jedes ABB-Produkt oder -system, das in Zusammenhang mit Software steht. ABB ist bestrebt, die Sicherheit und Robustheit seiner Produkte kontinuierlich zu verbessern, wobei die Prüfung der integrierten Sicherheit Teil des Entwicklungsprozesses ist. Ein eigenes, unabhängiges Sicherheitsprüfzentrum ist eingerichtet worden, in dem ABB-Produkte eingehenden Sicherheits- und Robustheitsprüfungen unterzogen werden.

Das Ziel des Device Security Assurance Center besteht darin, kontinuierliche Überprüfungen der von Protokollstapeln-Robustheit von Protokollstapeln und der Anfälligkeit eingebetteter Geräte bereitzustellen. Sie ermöglichen, dass:

- ABB Kunden mit Produkten beliefert, die strengsten Robustheitsnormen entsprechen.
- Produkte und Geräte von ABB vorhandenen und zukünftigen Bestimmungen entsprechen, die vom Gesetzgeber und der Industrie erlassen werden.
- ABB Vorreiter bei der Sicherheit von Automatisierungsgeräten ist.
- Ein zentraler Sicherheitsprüfprozess sowie die Anwendung modernster und strenger Verfahren einen gemeinsamen Ansatz garantiert, der auf Best-Practices beruht.

Für die Prüfungen werden zahlreiche hochmoderne Open-Source-Lösungen sowie kommerzielle Lösungen verwendet, einschließlich Geräte-Profiling, Prüfung auf bekannte Schwachstellen, Denial of Service und Protokoll-Fuzzing.

Ergänzende Informationen

Anfragen zum Produkt und zum Service

Um eine verdächtige Wahrnehmung zu melden oder die neuesten Informationen über Cybersicherheit abzurufen, besuchen Sie bitte das ABB Cybersecurity Portal oder senden Sie eine E-Mail an:

Web: http://www.abb.com/cybersecurity

E-Mail: cybersecurity@ch.abb.com

Gemeldete Cybersicherheitsvorfälle können der Webseite von ICS-CERT entnommen werden - https://ics-cert.us-cert.gov/alerts.

Informationen zu unternehmensweiten Cybersicherheitskonzepten, Prinzipien und sicherer Anwendung von ABB stehen unter anderem in *ABB 670 series 1.2 Cyber Security Deployment Guideline* [1] oder *Cyber Security with ABB Ability™ System 800xA* [2].

Produktschulung

Informationen zu Produktschulungen von ABB erhalten Sie auf der Internetseite new.abb.com/service/training.

Feedback zu ABB Handbüchern

Über Kommentare und Hinweise zu unseren Handbüchern freuen wir uns. Besuchen Sie hierzu bitte die Internetseite new.abb.com/drives/manuals-feedback-form.

Dokumente-Bibliothek im Internet

Im Internet finden Sie Handbücher und weitere produktbezogene Dokumente im PDF-Format auf www.abb.com/drives/documents.

Kontakt

www.abb.com/drives
www.abb.com/drivespartners

3AXD10000620848 Rev B (DE) 13.6.2017