SIEMENS
Ingenuity for life

Industrial Security

Cybersecurity für Telecontrol

Cybersecurity für die Wasser- und Abwasserwirtschaft

White Paper

Ausgabe 06/2020

siemens.de/telecontrol

Inhaltsverzeichnis

Einleitung

Das Rückgrat einer verlässlichen Wasserversorgung sind Anlagen und Systeme, die neben der eigentlichen Funktionalität auch bezüglich Cybersecurity von innen und außen geschützt sind. Mittlerweile existieren in vielen Ländern gesetzliche Anforderungen und Richtlinien, die Betreiber von sogenannten kritischen Infrastrukturen verpflichten, ihre Systeme entsprechend abzusichern und zu härten sowie entsprechende Nachweise darüber zu erbringen. Die Basis für eine ganzheitliche Betrachtung der Cybersecurity bietet der internationale Standard IEC 62443.

Cybersecurity für Telecontrol

1. Anforderungen im Bereich Wasser/ Abwasser

Die Voraussetzung einer funktionierenden Gesellschaft ist eine verlässliche und sichere öffentliche Infrastruktur, zum Beispiel für die Wasser- und Energieversorgung. Durch die voranschreitende Digitalisierung und die damit einhergehenden Trends zur Nutzung von Standard-IT-Diensten, Allverfügbarkeit von Mobilfunk und Internet und zur zunehmenden Vernetzung oder Verwendung von Cloud-Services nimmt die Gefahr weiter zu, dass die öffentliche Infrastruktur zur Zielscheibe von Cyberangriffen wird. Diese reichen von reiner Spionage über die Manipulation vertraulicher Daten bis hin zur Sabotage des kompletten Produktions- oder Prozessablaufes.

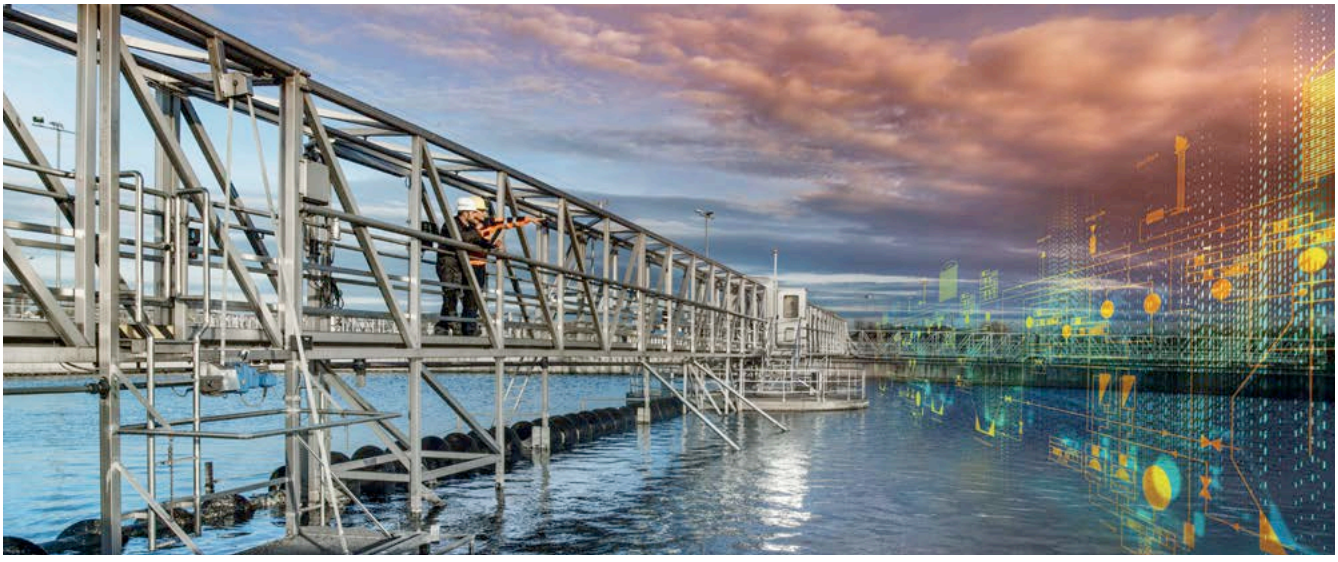
Aktivitäten in Deutschland

Vor diesem Hintergrund wurden zum Beispiel in Deutschland das IT-Sicherheitsgesetz erlassen und das Bundesamt für Sicherheit in der Informationstechnik als zentrale Anlaufstelle eingesetzt. Mit dem IT-Sicherheitsgesetz werden Betreiber sogenannter kritischer Infrastrukturen verpflichtet, IT-Systeme, Komponenten und Prozesse angemessen zu schützen und mindestens alle 2 Jahre einen Nachweis über die Erfüllung der Anforderungen gegenüber dem BSI zu erbringen.

https://www.bsi.bund.de

Gemäß den aktuellen Verordnungen gelten diejenigen Sektoren und Branchen als kritische Infrastrukturen, die von wesentlicher Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen, der Gesundheit, der Sicherheit und des wirtschaftlichen oder sozialen Wohlergehens der Bevölkerung sind. Dazu zählen die Bereiche Wasser, Energie, Ernährung, Transport und Verkehr, Gesundheit, IT und Telekommunikation, Finanz- und Versicherungswesen, Staat und Verwaltung sowie Medien und Kultur. Betroffen sind wiederum Anlagekategorien, die einen Schwellenwert von 500.000 versorgten Menschen überschreiten. Für den Sektor Wasser leitet sich hieraus zudem die Kenngröße von 22 Mio. m^3 Wasser (gefördert, verteilt, abgeführt oder aufbereitet) ab, ab welcher eine Anlage in den Bereich der kritischen Infrastruktur fällt.

https://www.kritis.bund.de



Schutz kritischer Infrastrukturen im Bereich Wasser/Abwasser

Cybersecurity für Telecontrol

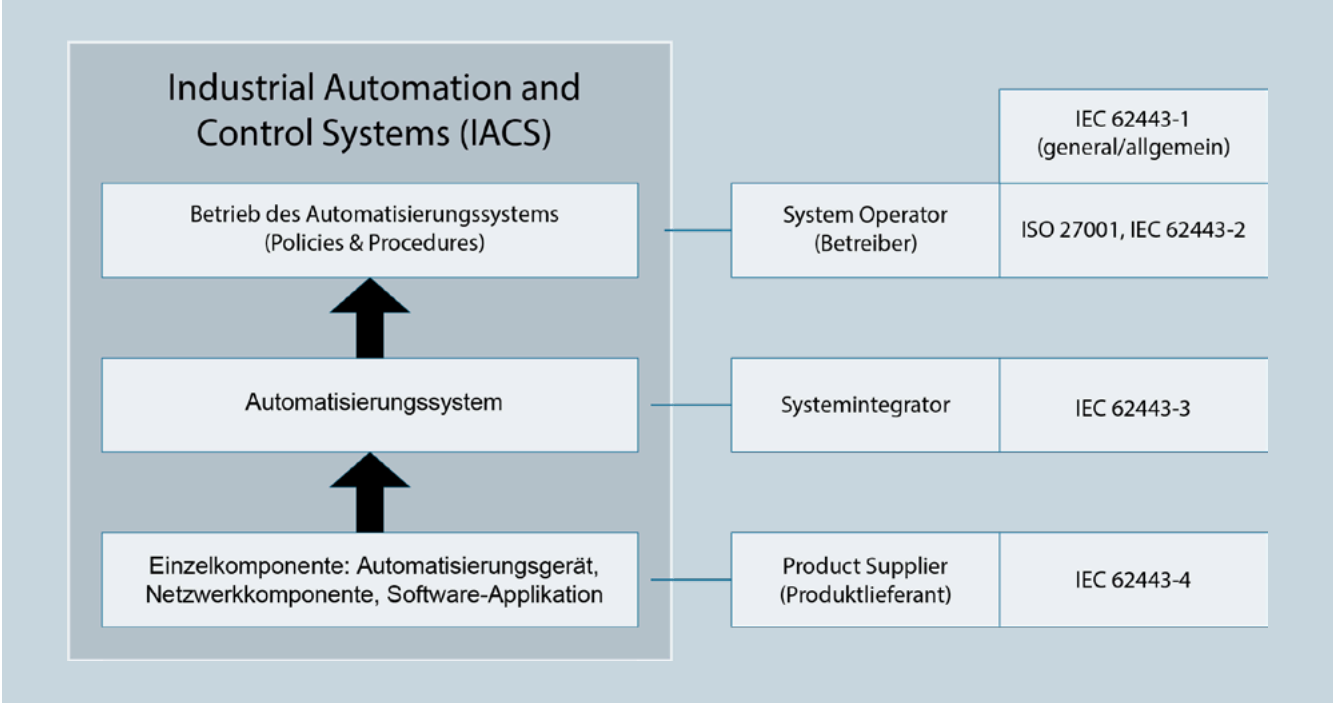
Um die Betreiber kritischer Infrastrukturen bei der Einhaltung der gesetzlichen Vorgaben zu unterstützen, haben Branchenverbände in Deutschland entsprechende Vorgaben und Anweisungen in branchenspezifischen Sicherheitsstandards festgelegt. Für den Sektor Wasser (Trinkwasserversorgung und Abwasserbeseitigung) werden Betreiber mit konkreten Anforderungen unterstützt, Maßnahmen zum Schutz des Anlagenbetriebs einzurichten [1, 2]. Unter Anderem betrifft das auch die Einrichtung und den Betrieb eines sogenannten „Information Security Management System" (ISMS), das die Einhaltung des aktuellen Stands der Technik in der Informationssicherheit ermöglichen soll, was wiederum durch entsprechende Nachweispflichten gefordert ist.
In Orientierungshilfen für die Branchenstandards wurde die Empfehlung ausgesprochen, ein ISMS auf Basis der ISO 27001 einzuführen. Darüber hinaus müssen Betreiber kritischer Infrastrukturen eine 24/7-Kontaktstelle einrichten, über die jederzeit mit den Behörden kommuniziert werden kann und über die auch alle aufgetretenen IT-Störungen den Behörden gemeldet werden müssen. Generell müssen entsprechende IT-Sicherheitsmaßnahmen ergriffen werden, um „die Verfügbarkeit der Systeme und Daten, Integrität der verarbeiteten Informationen und Systeme, Authentizität der Daten- und Informationsherkunft sowie Vertraulichkeit der Daten und Informationen" zu gewährleisten.

Während sich die oben genannte ISO-Normenreihe generell an Betreiber von IT-Systemen richtet, wird für die Betrachtung industrieller Systeme in Ergänzung der Standard IEC 62443 hinzugezogen, der sich in den letzten Jahren als richtungsweisende Normenreihe für Cybersecurity in der Industrie entwickelt hat und der zur ISO 27001 kompatibel ist.

Auch in weiteren Ländern der Europäischen Union sowie weltweit laufen Aktivitäten der Regierungen und Behörden, um die Rahmenbedingungen für entsprechende Schutzmaßnahmen wichtiger Bereiche zu definieren. Es werden Gesetze erlassen und Richtlinien geschaffen, um kritische Infrastrukturen und damit die Bevölkerung zu schützen und das gesellschaftliche Funktionieren sicherzustellen. Neben dem physischen Schutz geht es auch hier in erster Linie um die Absicherung gegenüber Cyberangriffen. Die Basis für eine ganzheitliche Betrachtung der Cybersecurity für Systeme und Anlagen bietet daher auch hier der internationale Standard IEC 62443.

2. IEC 62443: Gezielte Maßnahmen für Cybersecurity

Der aus mehreren Teilen bestehende Standard IEC 62443 befasst sich mit Cybersecurity von „Industrial Automation and Control Systems“ (IACS). Er wurde explizit für industrielle Umgebungen und deren spezifischen Anforderungen entwickelt und deckt alle Industriebereiche von diskreter Fertigung über Prozessindustrie bis zu verteilten Versorgungssystemen ab. In ihren verschiedenen Teilen adressiert die Normenreihe neben dem Anlagenbetreiber auch Systemintegratoren/ Anlagenbauer sowie die Produktlieferanten/Komponentenhersteller und Serviceanbieter. Auf diesem breiten Fundament hat Siemens eine umfassende Cybersecurity-Strategie etabliert, die dabei unterstützt, die Vorgaben des BSI sowie den Branchenstandard Wasser/Abwasser zu erfüllen und die gesamte Anlage bzw. das System effektiv vor Angriffen zu schützen.



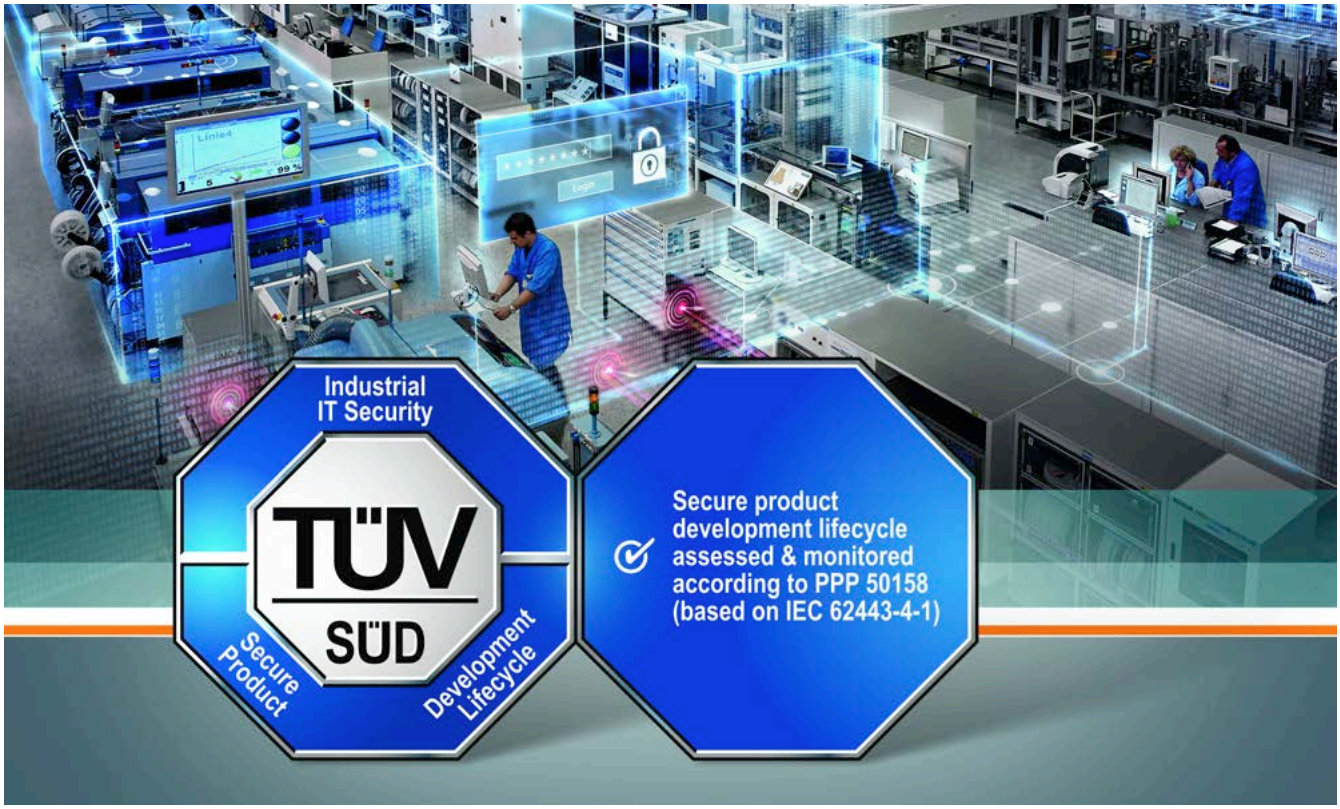
Überblick IEC 62443

Cybersecurity für Telecontrol

2.1 Zertifizierter Produktlebenszyklus gemäß IEC 62443-4-1

Der Teil 4-1 der IEC 62443 definiert die Art und Weise, wie die verwendeten Komponenten beim Produktlieferanten hergestellt werden. Dabei spielt es keine Rolle, ob es sich um eine Komponente mit dedizierten Security-Funktionen, wie zum Beispiel einer Firewall oder einem Switch, oder um eine komplexe Automatisierungskomponente handelt. Nur wenn der Verbund aller Komponenten, also das gesamte System, auf einem zuverlässigen und sicheren Fundament steht, kann ein wirkungsvolles Schutzkonzept darauf aufgebaut werden. So hat Siemens als erstes Unternehmen bereits im August 2016 eine auf IEC 62443-4-1 basierende Zertifizierung vom TÜV SÜD für den übergreifenden Entwicklungsprozess von Produkten der Automatisierungs- und Antriebstechnik, einschließlich der Industriesoftware, erhalten.

Dabei berücksichtigt der Standard unter anderem folgende Security-relevante Aspekte des Produktlebenszyklus: Fähigkeiten und Expertise, Prozess- und Qualitätssicherung, Security-Aspekte von Fremdkomponenten, sichere Architektur und sicheres Design, Handhabung von Security-Schwachstellen, Bereitstellung von Security-Updates sowie Patch- und Change-Management. Durch die Berücksichtigung dieser Aspekte wird bereits während der Entwicklungsphase eines Produktes darauf gezielt geachtet, Schwachstellen zu vermeiden und Sicherheitsrisiken durch die Wahl einer entsprechenden Systemarchitektur auszuschließen oder diese zu minimieren. Sollten sich dennoch Schwachstellen in einer Firm- oder Software ergeben, werden Anwender proaktiv darüber informiert und entsprechende Gegenmaßnahmen oder Security-Updates bereitgestellt.



TÜV SÜD IEC 62443-4-1 für Siemens

2.2 Produktanforderungen gemäß IEC 62443-4-2

Obwohl sich der Branchenstandard Wasser/Abwasser maßgeblich auf den Betrieb eines ISMS bezieht und somit maßgeblich die Einhaltung der Prozesse und Arbeitsanweisungen erfordert, müssen die eingesetzten Komponenten grundlegende technische Funktionen unterstützen, um den Betreibern kritischer Infrastrukturen die Möglichkeit zu geben, die Anforderungen der Branchenstandards zu erfüllen.

Das IRC-Portfolio (IRC: Industrial Remote Communication) im Bereich Fernwirktechnik/Telecontrol von Siemens unterstützt die notwendigen Security-Funktionen entweder direkt mit der jeweiligen Automatisierungskomponente oder in Kombination mit zusätzlichen Security-Komponenten von Siemens (gemäß Teil 3 der IEC 62443). Im Folgenden sind bespielhaft wichtige Funktionen aufgeführt, die dabei unterstützen, die Anlage oder das System sicher betreiben zu können und damit die notwendigen Security-Anforderungen zu erfüllen. Eine vollständige Analyse und eine Konzeption der Anlage bzw. des Systems sollte im Rahmen eines Security Assessments ermittelt werden, siehe Kapitel 4 „Security Assessment nach IEC 62443 / ISO 27001 von Siemens“ in diesem Dokument.

1. Signierte Firmware zum Schutz vor manipulierten Firmware-Updates

2. Sichere E-Mail-Übertragung über gesicherte Verbindungen

3. Sichere Ende-zu-Ende-Verschlüsselung mit OpenVPN/IPsec

4. Security Events zur Nachvollziehbarkeit sicherheitsrelevanter Systemereignisse

5. Reduzierte Angriffsoberfläche durch Deaktivieren ungenutzter Dienste

6. Schutz der Komponenten im Rahmen einer tiefengestaffelten Verteidigung (Defense in Depth)

Cybersecurity für Telecontrol

1. **Signierte Firmware zum Schutz vor manipulierten Firmware-Updates**
   Um Automatisierungskomponenten sowohl vor gefährlicher Schadsoftware als auch vor gefälschten oder manipulierten Firmware-Updates zu schützen, sind Updates digital signiert. Dank der automatisch initiierten Überprüfung dieser Signatur während eines Updatevorgangs wird sowohl die Authentizität als auch die Integrität der entsprechenden Dateien sichergestellt. Wird während dieses Prozesses eine Unregelmäßigkeit festgestellt, wird der Updateprozess automatisch abgebrochen, wodurch die Integrität der Komponente selbst gewährleistet wird. Manipulierte Firmware-Versionen, Schadprogramme oder andere nicht von Siemens signierter Datenpakete können folglich nicht auf der Komponente ausgeführt werden.
   Siemens unterstützt diese Funktionalität auch mit folgenden Telecontrol-Baugruppen: SIMATIC CP 1243-1, CP 1243-8 IRC, CP 1243-7 LTE, CP 1542SP-1 IRC, TIM 1531 IRC, RTU3000C.

2. **Sichere E-Mail-Übertragung über gesicherte Verbindungen**
   Um Informationen unter Wahrung der Vertraulichkeit von einer Automatisierungskomponente, z. B. einer Fernwirkbaugruppe SIMATIC RTU3000C, an einen definierten Empfänger zu übermitteln, bietet sich der E-Mail-Versand über eine verschlüsselte Verbindung an. Mit einem zuvor importierten digitalen Zertifikat besteht die Möglichkeit, E-Mails für den Versand per STARTTLS zu verschlüsseln. Auf diese Weise können neben kritischen Systemereignissen und Diagnosemeldungen auch Prozessdaten sicher an einen gewünschten Empfänger übermittelt werden. Ergänzend zur verschlüsselten Übermittlung können gezippte Anhänge durch ein vordefiniertes Passwort geschützt werden. So kann der Zugriff auf die übertragenen Daten je nach Anwendungsfall und Verantwortungsbereich zielgerichtet eingeschränkt werden.
   Siemens unterstützt diese Funktionalität auch mit folgenden Telecontrol-Baugruppen: SIMATIC CP 1243-1, CP 1243-8 IRC, CP 1243-7 LTE, CP 1542SP-1 IRC, TIM 1531 IRC, RTU3000C.

3. **Sichere Ende-zu-Ende-Verschlüsselung mit OpenVPN/IPsec**
   Um mit einer abgesetzten Komponente sicher kommunizieren zu können, bietet sich die Übertragung über Virtual Private Networks (VPNs) an. Dank der zertifikatsbasierten Authentifizierung der Teilnehmer und einer Ende-zu-Ende-Verschlüsselung lassen sich Informationen und Konfigurationen auch über öffentliche Netzwerke hinweg sicher übertragen. Durch die OpenVPN-Implementierung lassen sich gesicherte Tunnelverbindungen zwischen einer SIMATIC RTU3000C und einem beliebigen OpenVPN-Server einrichten, über den nicht nur Fernwirkprotokolle, sondern auch beliebige Konfigurationen, Firmware-Updates, Uhrzeitsynchronisationen oder Log-Informationen übertragen werden können. In Kombination mit der SINEMA Remote Connect Lösung von Siemens lässt sich mittels OpenVPN eine umfassende Fernzugriffslösung mit granularer Zugriffsberechtigung einrichten.
   Siemens unterstützt diese Funktionalität auch mit folgenden Telecontrol-Baugruppen: SIMATIC CP 1243-1, CP 1243-8 IRC, CP 1243-7 LTE, CP 1542SP-1 IRC, TIM 1531 IRC in Kombination mit Siemens Security-Komponenten, RTU3000C.

4. **Security Events zur Nachvollziehbarkeit sicherheitsrelevanter Systemereignisse**
   Um die Transparenz über Security-relevante Aktivitäten im gesamten Netzwerk und auf einzelnen Endgeräten aufrechtzuerhalten, unterstützen die Systemkomponenten, wie der CP 1243-8 IRC, eine Erfassung sogenannter Security Events. Dank diesen protokollierten Systemereignissen lassen sich beispielsweise unautorisierte Konfigurationsänderungen, Systemzugriffe oder Integritätsverletzungen nachvollziehen. Unter Berücksichtigung gängiger Datenschutzverordnungen lassen sich die erfassten Ereignisse mittels Syslog an übergeordnete Security-Applikationen, Analyse- und Archivierungssysteme schicken. In Verbindung mit einer sicheren Ende-zu-Ende-Verschlüsselung können die Ereignisse verschlüsselt an die gewünschten Empfänger übertragen werden.
   Siemens unterstützt diese Funktionalität auch mit folgenden Telecontrol-Baugruppen: SIMATIC CP 1243-1, CP 1243-8 IRC, CP 1243-7 LTE, CP 1542SP-1 IRC, TIM 1531 IRC in Kombination mit Siemens Security-Komponenten für die Zelle, RTU3000C.

Cybersecurity für Telecontrol

5. **Reduzierte Angriffsoberfläche durch Deaktivieren ungenutzter Dienste**
   Um die Angriffsoberfläche der Automatisierungsumgebung so gering wie möglich zu halten, können ungenutzte und nicht benötigte Netzwerkdienste über entsprechende Konfigurationsoberflächen dauerhaft deaktiviert werden. So lässt sich zum Beispiel der Zugriff auf das Web-Based-Management einer Komponente auf das sichere Protokoll HTTPS beschränken. Anfragen über die unsichere Variante HTTP werden an HTTPS weitergeleitet oder verworfen.
   Siemens verfolgt diesen Ansatz generell bei allen SIMATIC-Produkten für Telecontrol.

6. **Schutz der Komponenten im Rahmen einer tiefengestaffelten Verteidigung (Defense in Depth)**
   Um ein Automatisierungssystem umfassend und ganzheitlich vor Cyberangriffen zu schützen, sollte dieses gemäß den Empfehlungen der IEC 62443 und im Rahmen einer tiefengestaffelten Verteidigung eingerichtet werden. Für die hierfür wesentliche Netzwerksicherheit bietet Siemens ein umfangreiches Portfolio, mit dem die Systeme modular und bedarfsgerecht geschützt werden können. Mit SCALANCE S stehen zum Beispiel Industrial Security Appliances zur Verfügung, mit denen der Datenverkehr zu und von der geschützten Zelle kontrolliert und überwacht werden kann. Mit diesem Ansatz werden unterschiedliche Security-Maßnahmen kombiniert und wird der Schutz nicht nur in der Breite, sondern auch in der Tiefe ermöglicht.

   Weitere Informationen zum „Defense in Depth"-Schutzkonzept von Siemens finden Sie unter:
   www.siemens.de/industrialsecurity

Cybersecurity für Telecontrol

2.3 Systembetrachtung gemäß IEC 62443-3

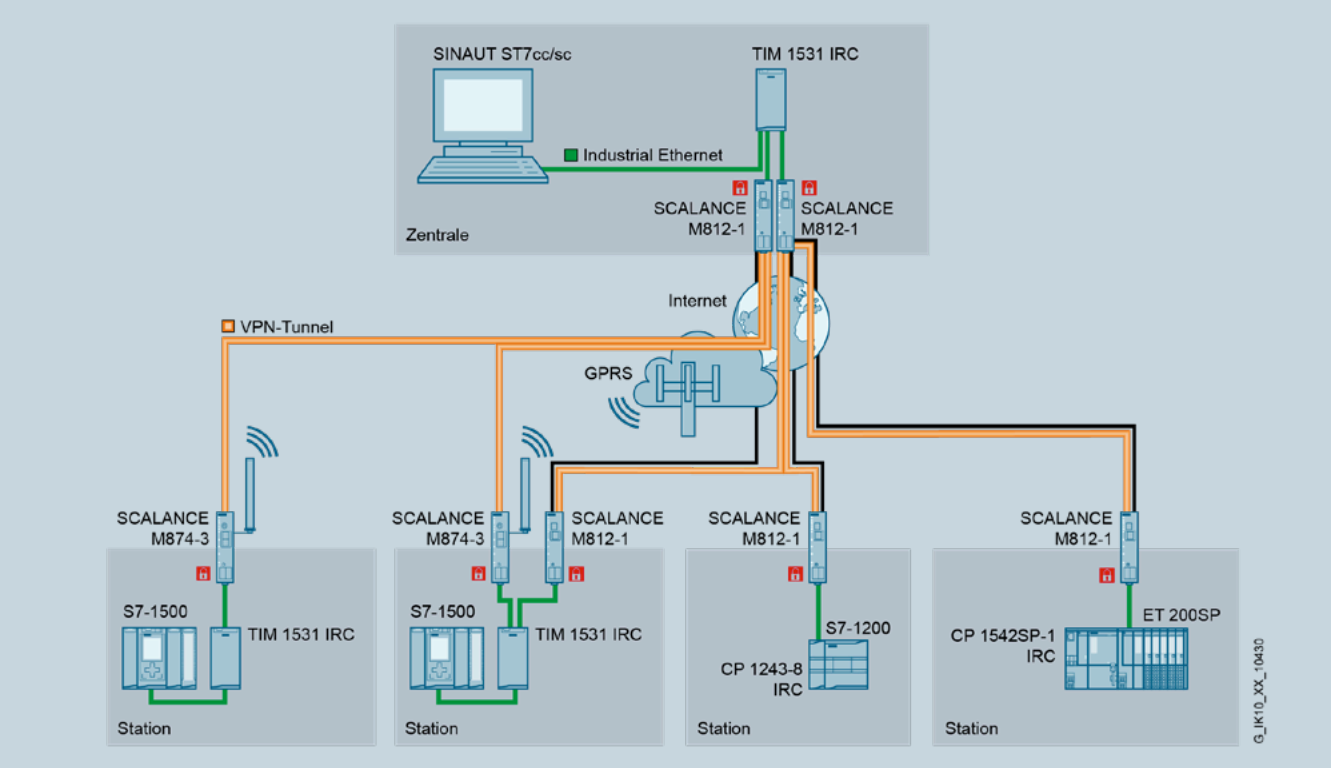
Basierend auf dem Konzept des modularen und bedarfsgerechten Cyberschutzes kann das Gesamtsystem bzw. die Anlagenlösung bestimmte fehlende technische Eigenschaften der Einzelkomponente kompensieren. Wenn beispielsweise eine Automatisierungskomponente keine Firewall-Funktionalität integriert hat, kann das durch vorgeschaltete Industrial Security Appliances erfolgen – z. B. Vorschalten eines SCALANCE S vor SIMATIC TIM 1531 IRC –, so dass die Kombination dieser Komponenten die geforderten Industrial-Security-Anforderungen erfüllt. Innerhalb eines Netzwerkverbundes eines Automatisierungssystems kommt es so zu einer Vielzahl an Gerätekombinationen und Möglichkeiten der Vernetzung.

Um bei Konzeption und Erstellung von sicheren Automatisierungslösungen zu unterstützen, stellt Siemens dokumentierte Musterkonfigurationen (Blueprints) zur Verfügung, die konform gemäß IEC 62443 ausgelegt sind und somit eine aus IT/OT-Sicht sichere Lösung darstellen.

Es werden Dokumentationen auf Basis der Siemens-SCADA-Systeme SIMATIC WinCC PROFESSIONAL/TIA, WinCC V7 und WinCC Open Architecture sowie auf Basis des Siemens-Leitsystems SIMATIC PCS 7 verfügbar sein.

Als Teil einer solchen Beispielkonfiguration zeigt die folgende Darstellung exemplarisch eine sichere Telecontrol-Konfiguration auf Basis des SIMATIC-Portfolios von Siemens. Die Fernwirkstationen (Remote Terminal Units: RTUs) sowie die Master-Station in der Zentrale bestehen aus Steuerungen der SIMATIC-Familie S7-1200 (Basic Controller), ET 200SP (Distributed Controller) sowie S7-1500 (Advanced Controller). Die Anbindung an die Leitstelle erfolgt über das öffentliche Netz mit SIMATIC Telecontrol-Baugruppen und SCALANCE Industrial Router (DSL und Mobilfunk). Die gesicherten Verbindungen von den Stationen zur Zentrale werden über VPN-Tunnel (OpenVPN) realisiert. Die Security-Funktionen werden entweder direkt von der Telecontrol-Baugruppe oder in Kombination mit den SCALANCE-Geräten erbracht.

https://www.siemens.de/telecontrol



Sichere Telecontrol-Lösung mit SIMATIC-Steuerungen von Siemens

Cybersecurity für Telecontrol

3. Always Active: Industrial Security Alerts und Updates

Das Thema Industrial Security bewegt sich in einem sehr dynamischen und komplexen Umfeld. Produkte, Systeme oder auch Technologien, die heute als sicher gelten, können morgen bereits überholt und unsicher sein. Daher bedarf es einer fortlaufenden Beobachtung und Anpassung der Sicherheitsmaßnahmen, so dass man sich immer auf dem neuesten Stand hinsichtlich der Security-Updates für die eingesetzten Produkte befindet. Damit das gelingt, untersucht „Siemens ProductCERT" alle entdeckten und gemeldeten Sicherheitsprobleme mit Bezug zu Siemens-Produkten, Lösungen und Services und veröffentlicht Security Advisories zu validierten Sicherheitsschwachstellen. Die Security Advisories enthalten Hinweise, wie mit der Schwachstelle umzugehen ist, und informieren über notwendige Schritte, die für einen geschützten Betrieb von Siemens-Produkten und Lösungen notwendig sind. Häufig wird ein Software- oder Firmware-Update angeboten oder bestimmte Aktionen werden empfohlen.
Über einen RSS-Feed können Security Advisories abonniert und angezeigt werden, so dass man mit den eingesetzten Siemens-Produkten immer auf dem neuesten Stand bleiben kann.

Weitere Informationen:
https://new.siemens.com/global/de/produkte/services/cert.html#Benachrichtigungen

4. Security Assessment nach IEC 62443/ ISO 27001 von Siemens

Um alle relevanten Punkte und Maßnahmen für den IT-Schutz und den sicheren Betrieb einer Anlage zu beachten und umzusetzen, empfiehlt sich eine ganzheitliche Security-Analyse. Mit den Security Assessments von Siemens werden alle Aspekte der Security von Produktionsstätten untersucht und analysiert. Die Assessments bieten Transparenz und ermitteln einen umfassenden Überblick über den Security-Ist-Zustand des Automatisierungssystems. Dies ist die Voraussetzung, um den Handlungsbedarf hinsichtlich Industrial Security zu erkennen und die richtigen Maßnahmen zum Schließen eventueller Sicherheitslücken zu ergreifen.

Hierbei orientieren sich die Assessments an den Normen IEC 62443 oder ISO 27001. Es werden Aspekte wie Netzwerkarchitektur der Anlage, Datenflüsse, Produktionssysteme und -prozesse sowie die Mitarbeiter selbst analysiert:

- Industrial Security Check:
  Das Ergebnis ist ein Bericht mit Empfehlungen von Maßnahmen zur Risikominderung
- Assessment IEC 62443/ISO 27001:
  Das Ergebnis ist ein Bericht mit Empfehlung zur Schließung der identifizierten Sicherheitslücken
- Risk & Vulnerability Assessment:
  In diesem Schritt werden Risiken identifiziert, analysiert, klassifiziert und bewertet. Das ist die Grundlage für eine risikobasierte, anlagenspezifische Security Roadmap, die auf den Kunden und die Kundenanlage zugeschnitten ist und ein umfassendes und einheitliches Sicherheitsniveau gewährleistet

Der Abschlussbericht enthält konkrete, genau auf die untersuchten Unternehmensbereiche zugeschnittene Vorschläge und Konzepte zur schrittweisen Verbesserung der Industrial Security. Die Assessments sind verfügbar für Siemens- und Drittanbieter-Systeme.

Kontakt:
www.siemens.de/industrial-security-services

5. Fazit

Für die IT-Security und den Schutz vor Angriffen auf Maschinen und Anlagen der öffentlichen Infrastruktur, insbesondere den Schutz von kritischen Infrastrukturen bspw. der Wasser- und Abwasserwirtschaft, ist eine ganzheitliche Systembetrachtung notwendig. Hier hat sich der Standard IEC 62443 als richtungsweisend entwickelt.

Neben den Security-relevanten Produkteigenschaften inklusive des zertifizieren Produktherstellungsprozesses sind hier vor allem Systemintegratoren sowie die Betreiber einer Anlage in der Pflicht, die vom BSI geforderten Sicherheitsanforderungen zu erfüllen. Siemens bietet ein komplettes Spektrum an Produkten, Blueprints und Services, um Schwachstellen zu erkennen, eine Anlage entsprechend zu härten und neben der eigentlichen Funktionalität auch zukünftig weiterhin alle Security-Anforderungen zu erfüllen.

www.siemens.de/industrial-security

6. Quellen

[1] DWA-Regelwerk: Merkblatt DWA-M 1060, IT-Sicherheit – Branchenstandard Wasser/Abwasser (Deutsche Vereinigung für Wasserwirtschaft, Abwasser und Abfall e. V: DWA), 08/2017. [https://www.dwa.de]

[2] DVGW-Regelwerk: Technischer Hinweis – Merkblatt, DVGW W 1060 (M), IT-Sicherheit – Branchenstandard Wasser/Abwasser (Deutscher Verein des Gas- und Wasserfaches e. V.), 08/2017. [https://www.dvgw-regelwerk.de]

Weitere Informationen

Herausgeber
Siemens AG

Digital Industries
Postfach 48 48
90026 Nürnberg
Deutschland

Artkelnummer DIFA-B10092-00

Security-Hinweise

Siemens bietet Produkte und Lösungen mit Industrial-Security-Funktionen an, die den sicheren Betrieb von Anlagen, Lösungen, Maschinen, Geräten und/oder Netzwerken unterstützen. Sie sind wichtige Komponenten in einem ganzheitlichen Industrial-Security-Konzept. Die Produkte und Lösungen von Siemens werden unter diesem Gesichtspunkt ständig weiterentwickelt. Siemens empfiehlt, sich unbedingt regelmäßig über Produkt-Updates zu informieren.

Für den sicheren Betrieb von Produkten und Lösungen von Siemens ist es erforderlich, geeignete Schutzmaßnahmen (z. B. Zellenschutzkonzept) zu ergreifen und jede Komponente in ein ganzheitliches Industrial-Security-Konzept zu integrieren, das dem aktuellen Stand der Technik entspricht. Dabei sind auch eingesetzte Produkte von anderen Herstellern zu berücksichtigen. Weitergehende Informationen über Industrial Security finden Sie unter

http://www.siemens.de/industrialsecurity

Um stets über Produkt-Updates informiert zu sein, melden Sie sich für unseren produktspezifischen Newsletter an. Weitere Informationen hierzu finden Sie unter

http://support.automation.siemens.com