Produktivität umfassend schützen

Industrial Security

siemens.de/industrial-security

Defense in Depth

Sicherheitsrisiken zwingen zum Handeln

Defense in Depth

Mit zunehmender Digitalisierung wird umfassende Sicherheit in der Automatisierung immer wichtiger. Deshalb ist Industrial Security ein Kernelement von Digital Enterprise, dem Lösungsansatz von Siemens auf dem Weg zu Industrie 4.0. Mit Defense in Depth bietet Siemens ein vielschichtiges Konzept, das Ihre Anlage sowohl rundum als auch in die Tiefe schützt. Das Konzept basiert auf Anlagensicherheit, Netzwerksicherheit und Systemintegrität nach den Empfehlungen der ISA 99/IEC 62443.

Anlagensicherheit

Anlagensicherheit sichert mit verschiedenen Methoden den physischen Zugang von Personen zu kritischen Komponenten. Dies beginnt mit dem klassischen Gebäudezutritt und reicht bis zur Sicherung sensibler Bereiche mittels Codekarten. Darüber hinaus umfasst die Anlagensicherheit die Integration von Prozessen und Richtlinien sowie die kontinuierliche Überwachung des Security-Status von Produktionsstätten für einen umfassenden Schutz.

Netzwerksicherheit

Produktionsnetze vor unberechtigten Zugriffen zu schützen ist heute insbesondere an den Verbindungsstellen zu anderen Netzen (z. B. Office oder Internet) unabdingbar. Zusätzliche Sicherheit bietet hier die Segmentierung einzelner Teilnetze wie das Zellenschutzkonzept mit SCALANCE S oder den Security-Kommunikationsprozessoren für SIMATIC. Die Datenübertragung kann zudem mit VPN geschützt werden, etwa für weltweite Fernzugriffe auf entlegene Anlagen über Internet oder Mobilfunknetze mit SCALANCE M.

Systemintegrität

Die dritte tragende Säule von Defense in Depth ist die Sicherung der Systemintegrität. Dies beinhaltet, Automatisierungssysteme und Steuerungen wie SIMATIC S7 Steuerungen sowie SCADA- und HMI-Systeme gegen unbefugte Zugriffe abzusichern oder darin enthaltenes Know-how zu schützen. Weiterhin geht es um die Authentifizierung von Benutzern und deren Zugriffsrechte sowie um die Systemhärtung gegenüber Angriffen.

Am Ball bleiben

Industrial Security ist eine sich ständig verändernde Herausforderung

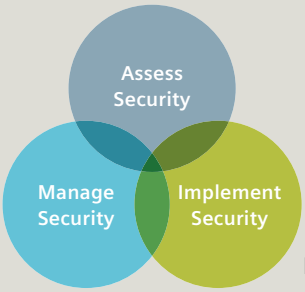
Wir wissen um die Bedeutung der industriellen Sicherheit und haben während der gesamten Entwicklung unserer Automatisierungsprodukte und -lösungen eine Reihe von entsprechenden Maßnahmen und Verfahren etabliert. Das beinhaltet unser Product Lifecycle Management (PLM), Supply Chain Management (SCM) und Customer Relationship Management (CRM).

Wir arbeiten eng mit unseren Zulieferern zusammen, um einen hohen Sicherheitsstandard in der gesamten Lieferkette zu gewährleisten. Hierzu gehören auch Softwarekomponenten von Drittherstellern, die wir auf mögliche Schwachstellen überprüfen.

Im Falle von Sicherheitsproblemen reagieren wir schnell, indem wir unsere Kunden informieren und ihnen schnellstmöglich Empfehlungen, Updates und Sicherheits-Patches zur Verfügung stellen. Damit erfüllen wir bereits heute zukünftige gesetzliche Anforderungen, wie es beispielsweise das deutsche IT-Sicherheitsgesetz vorgibt.

Außerdem stehen wir über FIRST (Forum of Incident Response and Security Teams) mit weltweit über 200 Security-Organisationen in Verbindung.

Siemens wird als Partner für die Industrie auch die neuen Anforderungen an IT-Security berücksichtigen.
Weitere Informationen zu Alerts, Updates und Patches finden Sie auf **www.siemens.de/industrial-security**



Plant Security Services

Mit Siemens Plant Security Services profitieren Industrieunternehmen vom umfassenden Know-how sowie der Fachkompetenz eines globalen Expertennetzwerks für Automatisierung und Cyber Security. Der ganzheitliche Ansatz des industriespezifischen Konzepts basiert auf modernsten Technologien sowie den geltenden Security-Normen und Standards. Bedrohungen oder Schadsoftware werden frühzeitig erkannt, die Schwachstellen im Detail analysiert und geeignete, umfassende Sicherheitsmaßnahmen eingeleitet. Kontinuierliche Überwachung gibt Anlagenbetreibern größtmögliche Transparenz über die Sicherheit ihrer Industrieanlage und somit jederzeit optimalen Investitionsschutz.

Anlagensicherheit

Anlagensicherheit – physischer Schutz und ganzheitliches Sicherheitsmanagement für Automatisierungsanlagen

Zugangskontrolle

Eine geregelte Zutrittskontrolle ist ein wesentlicher Faktor in der Absicherung kritischer Unternehmensbereiche. Siemens Building Technologies bietet ein umfangreiches Portfolio mit Angeboten, Lösungen und Services für den Schutz kritischer Infrastrukturen. Das Angebot reicht von Zutrittslösungen und Videoüberwachungssystemen bis hin zu Einsatzleitsystemen und Steuerungsplattformen.

Normen und Standards

Obwohl es Hunderte von IT-Sicherheitsstandards gibt, haben sich nur wenige als brauchbar für den industriellen Anlagenschutz erwiesen. Aufbauend auf unserer langjährigen Erfahrung beraten wir Sie bei der Auswahl und Implementierung der geeigneten Standards.

Vor allem der internationale Standard IEC 62443 / ISA99 hat sich im industriellen Umfeld der Automatisierung bewährt.

Definition von Richtlinien

Wir unterstützen Sie, die auf Ihre Anwendungssituation passenden Richtlinien zu definieren. Dabei berücksichtigen wir die einschlägigen Normen und Standards. Beispielsweise muss der Umgang mit Wechseldatenträgern eindeutig geregelt werden. Diese präzisen Richtlinien helfen, für alle Beteiligten ein hohes Sicherheitsniveau sicherzustellen, ohne die Produktivität einzuschränken. So wird industrielle Sicherheit eine der zentralen Aufgaben des Managements.

Security Monitoring

Wir erkennen und klassifizieren potenzielle Bedrohungen auf Basis einer kontinuierlichen Analyse und Korrelation der Protokolle sowie dem Abgleich mit Datenbanken. Im Falle einer Sicherheitsbedrohung benachrichtigen wir Sie umgehend und bieten auch sonst eine permanente Übersicht über den aktuellen Sicherheitsstatus der Anlage durch monatliche Statusberichte.

Netzwerksicherheit

Netzwerksicherheit zum Schutz von Produktionsnetzen

Schutz von Automatisierungsnetzen gegen unbefugte Zugriffe durch Netzzugangsschutz, Netzsegmentierung (beispielsweise DMZ) und verschlüsselte Kommunikation mit Security-Modulen.

Security-Module von Siemens sind speziell für den Einsatz in der Automatisierungstechnik optimiert und für die speziellen Anforderungen industrieller Netze ausgelegt.

Als erster Anbieter von Automatisierungstechnik erreichte Siemens die Achilles Level 2 Zertifizierung für Communication Robustness für mehrere Steuerungen, Security S7-Kommunikationsprozessoren und Security Appliances.

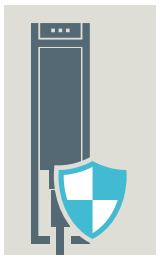
Diese Geräte können zusammen im TIA Portal konfiguriert werden – für eine durchgängige Security-Projektierung.

Sichere Fernwartung und Fernzugriffe mit geschützter Kommunikation

Siemens bietet ein umfangreiches Produktspektrum mit integrierten Sicherheitsfunktionen (Security Integrated) wie die Security-Module SCALANCE S, die Internet- und Mobilfunkrouter SCALANCE M sowie Security-Kommunikationsprozessoren für SIMATIC Steuerungen zum Schutz industrieller Netzwerke und gesicherter Fernzugriffe.
Diese Produkte unterstützen Stateful Inspection Firewall und gesicherte VPN-Kommunikation (Virtual Private Network) gegen unbefugte Zugriffe, Datenspionage und Manipulation.

Security Modules – SCALANCE S

Industrial Modems und Router – SCALANCE M



Security-Kommunikationsprozessoren

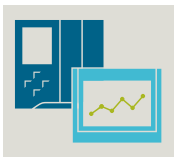
Systemintegrität

Systemintegrität – Sicherung von Automatisierungssystemen und Steuerungskomponenten

Schützen Sie Automatisierungskomponenten vor Cyber-Angriffen und unerlaubten Zugriffen und sichern Sie Ihr Know-how direkt im TIA Portal.

Ob Sie bestehendes Know-how schützen oder unautorisierten Zugriff auf Ihre Automatisierungsprozesse von vornherein ausschließen und damit Störungen in Ihren Produktionsprozessen verhindern wollen: Im Rahmen unseres durchgängigen Angebots für Industrial Security unterstützen wir Sie bei der gezielten Umsetzung von Maßnahmen gegen verschiedene Bedrohungsszenarien – und konzipieren Gesamtlösungen für maximalen Schutz.

Unsere integrierten Security-Funktionen schützen umfassend vor unbefugten Konfigurationsänderungen auf der Steuerungsebene sowie vor nicht autorisierten Netzwerkzugriffen. Sie verhindern das Vervielfältigen von Konfigurationsdaten und machen Manipulationsversuche an solchen Dateien einfacher erkennbar.



Controller und HMI-Systeme

Robuste Steuerungen und HMI-Systeme mit integrierten Sicherheitsfunktionen für mehrstufigen Zugangsschutz, Know-how- und Kopierschutz.

PC-basierte Systeme

Security-Funktionen für PC-basierte Automatisierungssysteme mit Whitelisting, Antivirus und Systemhärtung zur erhöhten Betriebssystemsicherheit.

Motion Control und Antriebe

Integrierte Security-Funktionen in SINUMERIK, SIMOTION und SINAMICS zum Schutz der getätigten Investition und Erhalt der Produktivität.

Prozessautomatisierung

Sichern der Produktivität in der Prozessindustrie mit dem Industrial Security-Konzept für SIMATIC PCS 7, basierend auf den Empfehlungen der IEC/ISA99.

Anlagensicherheit

- Physischer Zugangsschutz
- Prozesse und Richtlinien
- Umfassendes Security Monitoring

Netzwerksicherheit

- Zellenschutz und Perimeternetzwerk
- Firewalls und VPN

Systemintegrität

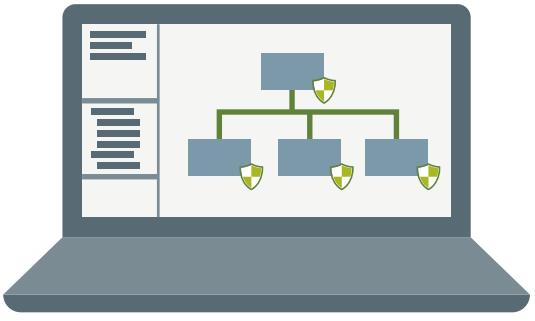
- Systemhärtung
- Patch Management
- Erkennung von Angriffen
- Authentifizierung und Zugriffsschutz

Industrial Security als Teil von Totally Integrated Automation

Mit industrietauglichen und im TIA Portal integrierten Security-Produkten für Netzwerksicherheit und Systemintegrität lässt sich Ihre Automatisierungslösung effizient absichern und das Defense-in-Depth-Konzept zum Schutz industrieller Anlagen und Automatisierungssysteme umsetzen. Die Integration in das TIA Portal ermöglicht die Projektierung von Standard- und Security-Funktionen in einem Projekt. So wird eine doppelte Eingabe der Daten vermieden, die Fehlerrate gesenkt und Engineeringzeit gespart.

Mit Industrial Security von Siemens gelingt es:

- die Anlagenverfügbarkeit zu steigern und zu erhalten
- Datenverlust zu vermeiden und vertrauliche Daten zu schützen
- die Wettbewerbsfähigkeit zu erhalten und zu verbessern
- gesetzliche Auflagen und Normen zu erfüllen
- Manipulation zu vermeiden und Werte abzusichern



Im TIA Portal integrierte Security-Funktionen

Erfahren Sie mehr:

siemens.de/industrial-security

Zuverlässige Industrial Security entdecken und erleben:

Lernen Sie das Defense-in-Depth-Konzept von Siemens im Detail kennen und informieren Sie sich ausführlich über alle Aspekte von Industrial Security.

Industrial Security – auf einen Blick!

Folgen Sie uns auf:
twitter.com/siemensindustry
youtube.com/siemens

Herausgeber
Siemens AG 2017

Digital Factory
Postfach 48 48
90026 Nürnberg
Deutschland

Artikel-Nr.: DFFA-B10076-01
Dispo 21507
170/74168
W-DFFA7-7P-21DE9
WS 03170.5
Gedruckt in Deutschland

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.**