SIEMENS

Übersichtsdokument • 03/2016

Security bei SIMATIC Controllern

SIMATIC S7-300/400/WinAC/1200/1500

https://support.industry.siemens.com/cs/ww/de/view/77431846

Gewährleistung und Haftung

Hinweis

Die Anwendungsbeispiele sind unverbindlich und erheben keinen Anspruch auf Vollständigkeit hinsichtlich Konfiguration und Ausstattung sowie jeglicher Eventualitäten. Die Anwendungsbeispiele stellen keine kundenspezifischen Lösungen dar, sondern sollen lediglich Hilfestellung bieten bei typischen Aufgabenstellungen. Sie sind für den sachgemäßen Betrieb der beschriebenen Produkte selbst verantwortlich. Diese Anwendungsbeispiele entheben Sie nicht der Verpflichtung zu sicherem Umgang bei Anwendung, Installation, Betrieb und Wartung. Durch Nutzung dieser Anwendungsbeispiele erkennen Sie an, dass wir über die beschriebene Haftungsregelung hinaus nicht für etwaige Schäden haftbar gemacht werden können. Wir behalten uns das Recht vor, Änderungen an diesen Anwendungsbeispiele jederzeit ohne Ankündigung durchzuführen. Bei Abweichungen zwischen den Vorschlägen in diesem Anwendungsbeispiel und anderen Siemens Publikationen, wie z. B. Katalogen, hat der Inhalt der anderen Dokumentation Vorrang.

Für die in diesem Dokument enthaltenen Informationen übernehmen wir keine Gewähr.
Unsere Haftung, gleich aus welchem Rechtsgrund, für durch die Verwendung der in diesem Anwendungsbeispiel beschriebenen Beispiele, Hinweise, Programme, Projektierungs- und Leistungsdaten usw. verursachte Schäden ist ausgeschlossen, soweit nicht z. B. nach dem Produkthaftungsgesetz in Fällen des Vorsatzes, der groben Fahrlässigkeit, wegen der Verletzung des Lebens, des Körpers oder der Gesundheit, wegen einer Übernahme der Garantie für die Beschaffenheit einer Sache, wegen des arglistigen Verschweigens eines Mangels oder wegen Verletzung wesentlicher Vertragspflichten zwingend gehaftet wird. Der Schadensersatz wegen Verletzung wesentlicher Vertragspflichten ist jedoch auf den vertragstypischen, vorhersehbaren Schaden begrenzt, soweit nicht Vorsatz oder grobe Fahrlässigkeit vorliegt oder wegen der Verletzung des Lebens, des Körpers oder der Gesundheit zwingend gehaftet wird. Eine Änderung der Beweislast zu Ihrem Nachteil ist hiermit nicht verbunden.
Weitergabe oder Vervielfältigung dieser Anwendungsbeispiele oder Auszüge daraus sind nicht gestattet, soweit nicht ausdrücklich von der Siemens AG zugestanden.

Security-hinweise

Siemens bietet Produkte und Lösungen mit Industrial Security-Funktionen an, die den sicheren Betrieb von Anlagen, Systemen, Maschinen und Netzwerken unterstützen.

Um Anlagen, Systeme, Maschinen und Netzwerke gegen Cyber-Bedrohungen zu sichern, ist es erforderlich, ein ganzheitliches Industrial Security-Konzept zu implementieren (und kontinuierlich aufrechtzuerhalten), das dem aktuellen Stand der Technik entspricht. Die Produkte und Lösungen von Siemens formen nur einen Bestandteil eines solchen Konzepts.

Der Kunde ist dafür verantwortlich, unbefugten Zugriff auf seine Anlagen, Systeme, Maschinen und Netzwerke zu verhindern. Systeme, Maschinen und Komponenten sollten nur mit dem Unternehmensnetzwerk oder dem Internet verbunden werden, wenn und soweit dies notwendig ist und entsprechende Schutzmaßnahmen (z.B. Nutzung von Firewalls und Netzwerksegmentierung) ergriffen wurden.

Zusätzlich sollten die Empfehlungen von Siemens zu entsprechenden Schutzmaßnahmen beachtet werden. Weiterführende Informationen über Industrial Security finden Sie unter http://www.siemens.com/industrialsecurity.

Die Produkte und Lösungen von Siemens werden ständig weiterentwickelt, um sie noch sicherer zu machen. Siemens empfiehlt ausdrücklich, Aktualisierungen durchzuführen, sobald die entsprechenden Updates zur Verfügung stehen und immer nur die aktuellen Produktversionen zu verwenden. Die Verwendung veralteter oder nicht mehr unterstützter Versionen kann das Risiko von Cyber-Bedrohungen erhöhen.

Um stets über Produkt-Updates informiert zu sein, abonnieren Sie den Siemens Industrial Security RSS Feed unter http://www.siemens.com/industrialsecurity.

Inhaltsverzeichnis

1 Risikominimierung durch Security

Die zunehmende Vernetzung und der Einsatz von bewährten Technologien der „Office-Welt“ in Automatisierungsanlagen führen zu einem erhöhten Bedarf an Sicherheit. Dabei reicht es nicht aus, nur einen oberflächlichen und limitierten Schutz anzubieten, da Angriffe von außen auf mehreren Ebenen erfolgen können. Für einen optimalen Schutz ist ein tiefes Sicherheitsbewusstsein notwendig

1.1 Sicherheitsstrategien

Motivation

Oberste Priorität in der Automatisierung hat die Aufrechterhaltung der Kontrolle über Produktion und Prozess. Auch Maßnahmen, die die Ausbreitung einer Sicherheitsbedrohung verhindern sollen, dürfen dies nicht beeinträchtigen. Der Einsatz eines adäquaten Schutzkonzepts soll sicherstellen, dass nur authentifizierte Benutzer über die ihnen zugewiesenen Bedienmöglichkeiten an authentifizierten Geräten autorisierte (erlaubte) Bedienungen durchführen können. Diese Bedienungen sollen ausschließlich über eindeutige und geplante Zugriffswege erfolgen, um während eines Auftrages eine sichere Produktion oder Koordination ohne Gefahren für Mensch, Umwelt, Produkt, zu koordinierende Güter und das Geschäft des Unternehmens zu gewährleisten.

Strategien

Basierend auf diesen Feststellungen umfasst ein Schutzkonzept generelle Verteidigungsstrategien, die die folgenden Angriffe abwehren sollen:

- Herabsetzung der Verfügbarkeit (z .B. "Denial of Service")
- Umgehung von einzelnen Sicherheitsmechanismen (z. B. "Man in the Middle")
- Absichtliche Fehlbedienung durch erlaubte Handlungen (z. B. nach Passwortdiebstahl)
- Fehlbedienungen durch nicht konfigurierte Benutzerrechte
- Ausspionieren von Daten (z. B. Rezepte und Betriebsgeheimnisse oder auch die Funktionsweise von Anlagen und ihren Sicherheitsmechanismen)
- Verändern von Daten (z. B. um Alarmmeldungen zu verharmlosen)
- Löschen von Daten (z. B. Logdateien zum Verschleiern von Angriffshandlungen)

Die Verteidigungsstrategie von Siemens verwendet Mechanismen einer Tiefgestaffelten Verteidigung (Defense in Depth).

Tiefgestaffelten Verteidigung

Das Konzept der Tiefenverteidigung beinhaltet eine gestaffelte bzw. geschichtete Struktur von Sicherheits- und Erkennungsmaßnahmen und -mechanismen auch auf Ebene der Einzelplatzsysteme. Es besitzt folgende Merkmale:

- Angreifer müssen damit rechnen, bei dem Versuch der Durchbrechung oder der Umgehung der einzelnen Schichten entdeckt zu werden.
- Eine Schwachstelle in einer Schicht dieser Architektur kann durch Abwehrmöglichkeiten in anderen Schichten aufgefangen werden.
- Die Systemsicherheit bildet eine eigene Schichtstruktur innerhalb der gesamten geschichteten Struktur der Netzwerksicherheit.

1.2 Umsetzung der Strategien zu Lösungen

1.2.1 Stärkung des Verantwortungsbewusstseins

Die erfolgreiche Umsetzung der Security-Strategien zu Security-Lösungen in den Automatisierungsanlagen, kann nur durch eine verantwortungsbewusste Zusammenarbeit aller Beteiligten erreicht werden. Dazu gehören insbesondere:

- Hersteller (Entwicklung, Systemtest, Security-Test)
- Projekteur und Integrator (Planung, Aufbau, Factory Acceptance Test)
- Betreiber (Bedienung und Administration)

Die Strategien und ihre Umsetzung müssen durch den ganzen Lebenszyklus einer Anlage hindurch (vom Beginn der Angebotserstellung, Planung und Design über die Migration bis zur Abrüstung der Anlage) beachtet und aktualisiert werden.

Die folgenden Aspekte ermöglichen, dass das Schutzkonzept in Automatisierungsanlagen seine Wirkung erreichen kann:

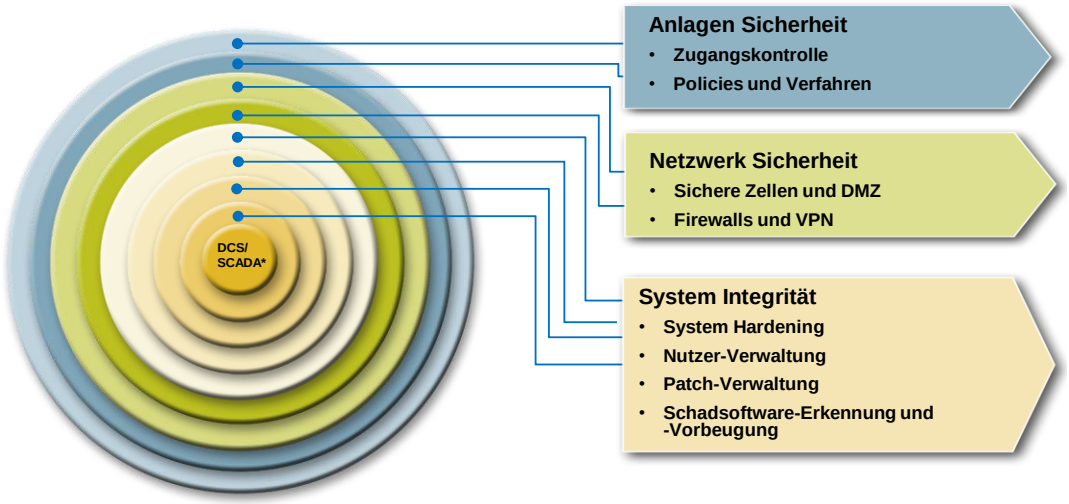
- den Einsatz stabiler, hochverfügbarer und systemgetesteter Produkte, die über eine Grundhärtung (IP-Hardening) und vordefinierte Security-Einstellungen verfügen und speziell für den industriellen Einsatz konzipiert wurden.
- eine moderne Projektierung, die aktuelle Techniken und Standards nutzt und ein an das Sicherheitsbedürfnis des Kunden angepasstes Anlagendesign ermöglicht
- den sorgfältigen und verantwortungsbewussten Betrieb der Anlagen und Komponenten gemäß ihrer vom Hersteller definierten Einsatzmöglichkeiten.

1.2.2 Das Schutzkonzept von Siemens: „Defense in Depth“

Zur Erreichung der geforderten Sicherheitsziele arbeitet Siemens nach der „Defense in Depth“-Strategie. Diese Strategie verfolgt den Ansatz eines mehrschichtigen Sicherheitsmodells bestehend aus folgenden Komponenten:

- Anlagensicherheit
- Netzwerksicherheit
- Systemintegrität

Abbildung 1-1



Der Vorteil dieser Strategie ist, dass ein Angreifer erst mehrere Sicherheitsmechanismen überwinden muss, um Schaden anrichten zu können. Die Sicherheitsanforderungen der einzelnen Schichten können individuell berücksichtigt werden.

Die Siemens-Lösung für die Anlagensicherheit

Die Basis für die Planung und Realisierung einer Industrial Security-Lösung ist die Implementierung eines zweckmäßigen, übergreifenden Sicherheitsmanagements.

Security-Management ist ein Prozess, der im Wesentlichen vier Schritte umfasst:

- Risikoanalyse mit Definition von Risikominderungsmaßnahmen: Diese Maßnahmen müssen in Abhängigkeit von den ermittelten Bedrohungen und Risiken für die Anlage definiert werden.
- Festlegung von Richtlinien und Koordination organisatorischer Maßnahmen.
- Abstimmung technischer Maßnahmen.
- Konsequenter Security-Management-Prozess mit regelmäßiger oder ereignisabhängiger Wiederholung der Risikoanalyse.

Die Siemens-Lösung für die Netzwerksicherheit

Befinden sich in einem Netzsegment Steuerungen oder andere intelligente Geräte, die über keinen oder nur einen minimalen Eigenschutz verfügen, bleibt nur die Möglichkeit, diesen Geräten eine abgesicherte Netzwerkumgebung zu schaffen. Am einfachsten ist dies mit speziellen Routern oder Gateways. Sie stellen die Sicherheit durch integrierte Firewalls in Industriequalität her und sind dadurch auch selbst geschützt. Zusätzliche Sicherheit bietet die Segmentierung einzelner Teilnetze z. B. mittels Zellenschutzkonzept oder über eine demilitarisierte Zone (DMZ).

Die von Siemens konzipierte Sicherheitslösung wurde speziell für die Anforderungen im Automatisierungsumfeld erarbeitet, um dem zunehmenden Bedarf an Netzwerksicherheit gerecht zu werden, die Störanfälligkeit der gesamten Produktionsanlage zu reduzieren und damit deren Verfügbarkeit zu erhöhen.

Hinweis Zu diesem Thema finden Sie im Siemens Industry Online Support ein Security Übersichtsdokument (Beitrags-ID: 27043887): http://support.automation.siemens.com/WW/view/de/27043887

Die Siemens-Lösung für die Systemintegrität

Zur Wahrung der Systemintegrität ist es wichtig, die Schwachstellen in PC-Systemen und in der Steuerungsebene zu minimieren. Siemens setzt diese Anforderung mit folgenden Lösungen um:

- Einsatz von Antivirus- und Whitelisting-Software
- Wartungs- und Updateprozesse
- Nutzer-Authentifizierung für Maschinen- oder Anlagenbetreiber
- Integrierte Zugriffsschutz-Mechanismen in Automatisierungskomponenten
- Schutz des Programmcodes durch Know-How-Schutz, Kopierschutz und der Vergabe von Passwörtern

1.3 Unterschiede zwischen Office und Industrial Security

Die in den PCs und Windows Betriebssystemen integrierten Security-Mechanismen bieten grundsätzlich ein hohes Maß an Sicherheit. Allerdings sind diese Maßnahmen typischerweise an die Anforderungen im Office Bereich ausgerichtet. Die zu schützenden Objekte sind im Industrial Security Bereich zwar durchaus ähnlich, jedoch unterscheiden sich deren Prioritäten teilweise deutlich voneinander. Während in der Office-IT typischerweise Vertraulichkeit und Integrität von Informationen höchste Priorität haben, stehen bei Industrial Security die Verfügbarkeit der Anlage bzw. deren Bedienbarkeit an erster Stelle. Bei der Auswahl geeigneter Security-Maßnahmen ist daher auch immer darauf zu achten, dass diese zwar den notwendigen Schutz bieten, jedoch den eigentlichen Betrieb nicht negativ beeinträchtigen.

1.4 Unterschiede zwischen Funktionaler Sicherheit und Industrial Security

Funktionale Sicherheit (Safety) adressiert den Schutz der Umgebung gegen Fehlfunktionen eines Systems. Auf der anderen Seite adressiert Industrial Security den Schutz des regulären Betriebes eines Systems gegen beabsichtigte oder unbeabsichtigte Störungen. Allerdings benötigen auch insbesondere Safety-Systeme Schutz gegen solche Störungen.

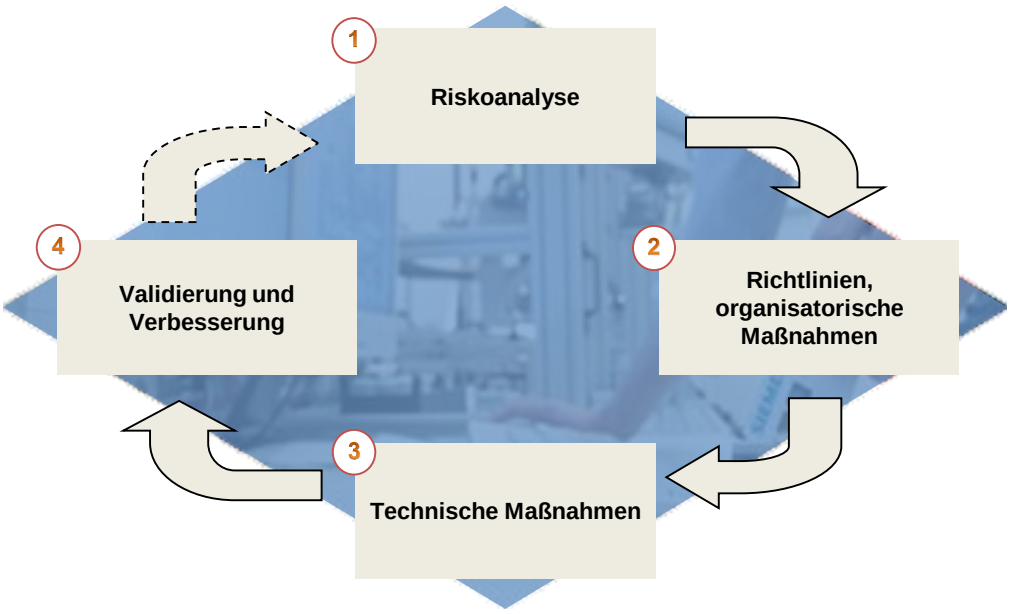
Es ist Aufgabe des Maschinenherstellers, entsprechende Safety-Mechanismen zu etablieren. Diese Mechanismen dürfen jedoch nicht primär in das „Defense in Depth“-Konzept integriert werden, auch wenn diese einen Beitrag dazu leisten können.

Während Safety-Bedrohungen prinzipiell gleich bleiben, können sich Security-Bedrohungen über die Lebensdauer einer Maschine / Anlage verändern. Daher ist eine regelmäßige Anpassung des Security-Schutzes erforderlich.

1.5 Security Management

Das Security Management bildet einen wesentlichen Bestandteil eines Industrial Security-Konzeptes zur Adressierung aller Security-relevanten Aspekte einer Automatisierungslösung – sei es einer einzelnen Maschine, einer Teil- oder einer Gesamtanlage. Da sich die Gefährdungslage einer Automatisierungslösung unabhängig von ihrer eigentlichen Funktion über ihren Lebenszyklus hinweg ändert, handelt es sich hierbei eher um einen Security Management Prozess. Dieser hat das Ziel, den notwendigen Security-Level einer Automatisierungslösung zu erreichen sowie dauerhaft beizubehalten. Mit dem Etablieren eines Security Management-Prozesses wird beispielsweise auch sichergestellt, dass durch die darin enthaltene Risikoanalyse nur geeignete Gegenmaßnahmen zur Reduktion der Risiken umgesetzt werden. Ein solcher Prozess könnte beispielsweise wie folgt aussehen:

Abbildung 1-2



2 Sicherheitsmechanismen der S7-CPU

Die folgenden Kapitel zeigen auf, welche integrierten Zugriffschutz-Mechanismen die SIMATIC S7-Controller anbieten.

2.1 Bausteinschutz

Übersicht

In STEP 7 V5.x und in STEP 7 (TIA Portal) stehen verschiedene Bausteinschutz-einrichtungen zur Verfügung, um das Know-How der Programme in den Bausteinen vor nicht autorisierten Personen zu bewahren.

- Know-How-Schutz
- S7-Block Privacy

Wird ein über diese Funktionen geschützter Baustein geöffnet, so kann nur die Bausteinschnittstelle (IN-, OUT- und IN/OUT-Parameter) und der Baustein-kommentar eingesehen werden. Der Programmcode, die temporären/statischen Variablen und die Netzwerkkommentare werden nicht angezeigt.
Eine Änderung des geschützten Bausteins ist nicht möglich

Nachstehende Tabelle gibt einen Überblick über die einzelnen Know-How-Schutzeinrichtungen:

Tabelle 2-1

Entwicklungs umgebung	Sprache	Bausteinschutz	Gültigkeit
STEP 7 V5.x	• KOP/ FUP/ AWL • SCL • S7-GRAPH • CFC	Know-How Schutz (nicht Passwortgeschützt)	S7-300/ 400 / WinAC
STEP 7 V5.5	• KOP/ FUP/ AWL • S7-SCL	S7-Block Privacy (Passwortgeschützt)	S7-300/ 400
STEP 7 (TIA Portal)	• KOP/ FUP/ AWL • S7-SCL • S7-GRAPH	Know-How Schutz (Passwortgeschützt)	S7-300/ 400
	• KOP/ FUP • S7-SCL		S7-1200 (V4)
	• KOP/ FUP/ AWL • S7-SCL		S7-1500

Bausteinübersicht

S7-Block-Privacy

Mit S7-Block Privacy können nur FBs und FCs geschützt werden.

Know-How-Schutz

Mit dem Attribut KNOW_HOW_PROTECT kann ein Know-How-Schutz für Bausteine vom Typ OB, FB und FC aktiviert werden.

Instanz-Datenbausteine können nicht manuell geschützt werden, da sie vom Know-How-Schutz des zugeordneten FB abhängig sind. Das heißt, dass der Instanzdatenbaustein eines Know-How-geschützten FBs auch einen Know-How-Schutz enthält. Dies ist unabhängig davon, ob der Instanz-Datenbaustein explizit angelegt oder durch einen Bausteinaufruf erzeugt wurde.

Im TIA Portal sind auch globale Datenbausteine zulässig. ARRAY-Datenbauseine können nicht mit einem Know-How-Schutz versehen werden.

Einschränkungen

Bausteine mit Bausteinschutz können in STEP 7 (ohne korrektes Passwort) nicht mehr weiter bearbeitet werden. Es sind auch keine Test- und Inbetriebnahme-Funktionen wie z. B. „Baustein beobachten" oder „Haltepunkte“ mehr möglich. Einzig die Schnittstellen des Bausteins bleiben sichtbar.

Folgende Aktionen sind mit einem geschützten Baustein durchführbar:

- Kopieren und Löschen
- Aufrufen in einem Programm
- Online/Offline-Vergleich
- Laden

S7-Block Privacy

S7-Block Privacy ist ein Erweiterungspaket von STEP 7 ab V5.5 zum Schutz von Funktionen und Funktionsbausteinen.

Bei der Verwendung von S7-Block Privacy ist folgendes zu beachten:

- S7-Block Privacy wird über Kontextmenüs bedient.
- Einmal geschützte Bausteine können nur mit dem richtigen Passwort und entsprechend mitgelieferter Rückübersetzungsinformation wieder entsperrt werden. Es ist daher empfehlenswert, das Passwort sicher aufzubewahren und/oder Kopien der ungeschützten Bausteine anzulegen.
- Geschützte Bausteine sind nur auf 400er-CPUs ab Version 6.0 ladbar, auf 300er-CPUs ab V3.2.
- Sind im Projekt Quellen enthalten, können die geschützten Bausteine mithilfe der Quellen durch Übersetzen wiederherstellt werden. Die Quellen können von S7-Block Privacy vollständig aus dem Projekt entfernt werden.

Hinweis Eine Anleitung zum Einrichten des Bausteinschutzes über S7-Block Privacy finden Sie im FAQ „Wie kann ab STEP 7 V5.5 der verbesserte Bausteinschutz für FBs und FCs eingerichtet werden?“ (BeitragsID: 45632073).
http://support.automation.siemens.com/WW/view/de/45632073

Know-How-Schutz (STEP 7 V5.x)

Bausteine in STEP7 V5.x können durch die Zugabe eines Bausteinattributs mit einem Schutz versehen werden. Das Schlüsselwort KNOW_HOW_PROTECT wird dabei bei der Programmierung des Bausteins in der Quelle angeben.

Der Bausteinschutz kann nur über die AWL-Quelle wieder aufgehoben werden. Stehen die AWL-Quellen dem Programm bzw. Projekt nicht mehr zur Verfügung, kann der Bausteinschutz für die Bausteine nicht mehr entfernt werden.

Es wird empfohlen, S7- Block Privacy als verbesserten Know-How-Schutzmechanismus zu verwenden.

Hinweis

Eine Anleitung zum Einrichten des Bausteinschutzes über das Schlüsselwort KNOW_HOW_PROTECT finden Sie im FAQ „Wie kann für selbst erstellte Bausteine ein Bausteinschutz eingerichtet werden?“ (BeitragsID: 10025431).

http://support.automation.siemens.com/WW/view/de/10025431

Know-How-Schutz (TIA-Portal)

Im TIA Portal erfolgt der Bausteinschutz über das Kontextmenü und der Angabe eines Passworts.

Folgende Punkte müssen dabei beachtet werden:

- Bei einem Vergleich zwischen der Offline- und der Online-Version von know-how-geschützten Bausteinen werden nur die nicht geschützten Daten verglichen.
- Von einem know-how-geschützten Baustein kann kein Typ in der Bibliothek erzeugt werden. Wird ein solcher Baustein in eine Bibliothek eingefügt, erhält auch die entstehende Kopiervorlage den Know-How-Schutz. Bei der Verwendung der Kopien wird daher das korrekte Passwort des Know-How-geschützen Bausteins benötigt.
  Soll ein Know-How-geschützter Baustein ohne Weitergabe des Passworts in einer Bibliothek verwendet werden, müssen bei der Programmierung dieser Bausteine folgende Punkte beachtet:
  - Zum Zeitpunkt der Übersetzung müssen alle aufgerufenen Code- und Datenbausteine bekannt sein. Es sind also keine indirekten Aufrufe zulässig.
  - Bei der Programmierung der Bausteine soll die Verwendung von PLC-Variablen und globalen Datenbausteinen vermieden werden.

Hinweis

Weitere Informationen finden Sie in der STEP 7 (TIA Portal) Onlinehilfe, unter:

- Know-How-Schutz für Bausteine einrichten
- Know-How-geschützte Bausteine öffnen
- Know-How-Schutz für Bausteine entfernen

Für S7-1200 (V4) und S7-1500-CPUs kann zusätzlich ein Kopierschutz eingerichtet werden, der die Ausführung an die CPU oder die Memory Card mit der festgelegten Seriennummer bindet.

2.2 Online Zugangs- und Funktionsbeschränkung

CPU-Schutzstufen

Die S7-CPU bietet drei (S7-300/ S7-400/ WinAC) bzw. vier (S7-1200(V4)/ S7-1500) Zugriffsstufen, um den Zugang zu bestimmten Funktionen einzuschränken. Mit dem Einrichten der Zugriffsstufe und der Passworte werden die Funktionen und Speicherbereiche limitiert, die ohne Eingabe eines Passworts zugänglich sind. Die einzelnen Zugriffsstufen sowie die Eingaben der dazugehörigen Passwörter werden in den Objekteigenschaften der CPU festgelegt.

Tabelle 2-2

Zugriffsstufen	Zugriffsbeschränkung
Stufe 1 (kein Schutz)	Die Hardware-Konfiguration und die Bausteine können von jedem gelesen und verändert werden.
Stufe 2 (Schreibschutz)	Mit dieser Zugriffsstufe ist ohne Angabe des Passworts nur lesender Zugriff erlaubt und somit folgende Funktionen ausführbar: • Lesen der Hardware-Konfiguration und der Bausteine • Lesen der Diagnosedaten • Laden der Hardware-Konfiguration und der Bausteine in das Programmiergerät. • Wechsel des Betriebszustands (RUN/STOP) (nicht bei S7-300 / S7-400 / WinAC) Ohne Eingabe des Passworts sind folgende Funktionen nicht ausführbar: • Laden der Bausteine und Hardware-Konfiguration in die CPU • schreibende Testfunktionen • Firmware-Update (online).
Stufe 3 (Schreib-/ Leseschutz)	Mit dieser Zugriffsstufe ist ohne Angabe des Passworts nur • der HMI-Zugang und • das Lesen der Diagnosedaten möglich. Ohne Eingabe des Passworts sind folgende Funktionen nicht ausführbar: • Laden der Bausteine und Hardware-Konfiguration in die bzw. von der CPU • schreibende Testfunktionen • Wechsel des Betriebszustands (RUN/STOP) (nicht bei S7-300 / S7-400 / WinAC) • Firmware-Update (online).
Stufe 4 (kompletter Schutz) S7-1200 (v4) S7-1500	Beim kompletten Schutz verbietet die CPU: • lesenden und schreibenden Zugriff auf die Hardware-Konfiguration und der Bausteine • HMI-Zugriff • Änderung bei der Server-Funktion für PUT/GET-Kommunikation • Lesenden und schreibenden Zugriff im Bereich "Erreichbare Teilnehmer" und im Projekt für Teilnehmer, die online geschaltet sind.

Betriebsverhalten bei aktivierter Schutzstufe

Eine passwort-geschütze CPU verhält sich im laufenden Betrieb wie folgt:

- Der Schutz der CPU ist wirksam, nachdem die Einstellungen in die CPU geladen wurden und eine neue Verbindung aufgebaut wurde.
- Vor der Ausführung einer Online-Funktion wird die Zulässigkeit geprüft und im Falle eines Passwortschutzes zur Passworteingabe aufgefordert.
- Die durch Passwort geschützten Funktionen können zu einem Zeitpunkt nur von einem PG/PC ausgeführt werden. Ein weiteres PG/PC kann sich nicht mit Passwort anmelden.
- Die Zugangsberechtigung zu den geschützten Daten gilt für die Dauer der Online-Verbindung oder bis die Zugangsberechtigung manuell über "Online > Zugriffsrechte löschen" wieder aufgehoben wird.

Hinweis Die Projektierung einer Zugriffsstufe ersetzt nicht den Know-How-Schutz. Sie verhindert unrechtmäßige Änderungen an der CPU durch Einschränkung der Downloadrechte. Die Bausteine auf der SIMATIC Memory Card sind jedoch nicht schreib- oder lesegeschützt. Zum Schutz des Programmcodes ist der Know-How-Schutz zu verwenden.

2.3 Kopierschutz (S7-1200 (V4) / S7-1500)

Der Kopierschutz ermöglicht es, dass das Programm oder die Bausteine mit einer bestimmten SIMATIC Memory Card oder CPU verknüpft werden. Durch die Verknüpfung mit der Seriennummer einer SIMATIC Memory Card bzw. einer CPU wird die Verwendung dieses Programms oder dieses Bausteins nur in Verbindung mit dieser definierten SIMATIC Memory Card oder CPU möglich.

Wird ein Baustein mit Kopierschutz in ein Gerät geladen, das mit der festgelegten Seriennummer nicht übereinstimmt, wird der gesamte Ladevorgang zurückgewiesen. Das bedeutet aber auch, dass selbst Bausteine ohne Kopierschutz nicht geladen werden.

Der Kopierschutz sowie die Eingaben der dazugehörigen Seriennummer erfolgt über die Bausteineigenschaften.

Hinweis Bei Einrichtung eines solchen Kopierschutzes für einen Baustein ist es wichtig, dass dieser Baustein auch einen Bausteinschutz erhält. Ohne Know-How-Schutz könnte jeder den Kopierschutz zurücksetzen

Allerdings muss zuerst der Kopierschutz eingerichtet werden, da die Einstellungen für den Kopierschutz schreibgeschützt sind, wenn der Baustein einen Know-How-Schutz besitzt.

2.4 Vor-Ort-Zugriffssperre (S7-1500)

Verriegelung der CPU

Die SIMATIC S7-1500 hat eine Frontklappe mit einem Display und Bedientasten. Zum Stecken bzw. Entnahme der SIMATIC Memory Card sowie für die manuelle Änderung des CPU-Betriebszustands muss diese geöffnet werden.

Zum Schutz der CPU vor unbefugtem Zugriff kann diese Frontklappe über die Verriegelungslasche ausreichend gesichert werden. Zur Wahl stehen z. B.:

- Frontklappe mit einem Schloss sichern
- Eine Plombe anbringen

Abbildung 2-1

Sperrung des Displays

Am Display können Sie den Zugriff auf eine passwortgeschützte CPU sperren (Vor-Ort-Sperre). Die Zugriffssperre wirkt nur, wenn der Betriebsartenschalter auf RUN steht. Die Zugriffssperre wirkt unabhängig vom Passwortschutz, d. h. wenn jemand über ein angeschlossenes Programmiergerät auf die CPU zugreift und das korrekte Passwort eingegeben hat, bleibt der Zugriff auf die CPU verwehrt. Die Zugriffssperre ist für jede Zugriffsstufe getrennt am Display einstellbar, d. h. dass z. B. der lesende Zugriff lokal erlaubt ist, der schreibende Zugriff lokal aber nicht erlaubt ist. Sie können ein Passwort für das Display in STEP 7 in den Eigenschaften der CPU parametrieren, so dass der lokale Zugriffsschutz über ein lokales Passwort geschützt ist.

2.5 Weitere Maßnahmen zum Schutz der CPU

Die folgenden Maßnahmen erhöhen zusätzlich den Schutz gegen unberechtigte Zugriffe auf Funktionen und Daten der S7-CPU von außen und über das Netzwerk:

- Deaktivieren bzw. Einschränkung des Webservers
- Deaktivieren der Uhrzeitsynchronisation über NTP-Server
- Deaktivieren der PUT/GET-Kommunikation (S7-1200(V4)/ S7-1500)

Hinweis In der Default-Projektierung der Baugruppen sind diese Funktionen standardmäßig deaktiviert.

Sicherheitsfunktionen für den Web-Server

Der Webserver bietet die Möglichkeit, die CPU über das firmeninterne Intranet fernzusteuern und zu beobachten. Auswertungen und Diagnose sind somit über große Entfernungen möglich.

Allerdings kann sich durch die Aktivierung des Webservers das Risiko von unberechtigten Zugriffen auf die CPU erhöhen.

Ist eine Aktivierung des Webservers erwünscht, sind folgende Maßnahmen zum Schutz der CPU ratsam:

- Zugriff über das sichere Übertragungsprotokoll „https“
- Projektierbare Nutzer- und Funktionsberechtigung über Benutzerliste
  - Benutzer anlegen
  - Ausführungsrechte festlegen
  - Passwörter vergeben

Mit der Benutzerverwaltung stehen Benutzern ausschließlich die Optionen zur Verfügung, die den Ausführungsrechten fest zugeordnet sind.
Ist ein Benutzer projektiert, kann dieser nach Anmeldung mit seinem Passwort entsprechend seiner Zugriffsrechte auf die Webseiten zugreifen. Voreingestellt ist ein Benutzer mit Namen "Jeder", welcher minimale Zugriffsrechte (Lesender Zugriff auf Intro- und Startseite) besitzt. Der Benutzer "Jeder" ist ohne Vergabe eines Passworts festgelegt und kann nicht verändert werden

Deaktivieren der PUT/GET-Kommunikation (S7-1200(V4)/ S7-1500)

Die CPU kann für eine Reihe von Kommunikationsdiensten Server sein. In diesem Modus ist es anderen Kommunikationsteilnehmer möglich, auf CPU-Daten zu zugreifen, ohne dass für die CPU explizit Verbindungen projektiert und programmiert wurden. Gleichsam entfällt für die lokale CPU die Möglichkeit, die Kommunikation zu den Clients kontrollieren.
Ob diese Art der Kommunikation im Betrieb für die lokale CPU zulässig ist oder nicht, wird in den Objekteigenschaften der CPU bestimmt.

In der Voreinstellung ist die Option "Zugriff über PUT/GET-Kommunikation durch entfernte Partner (...) erlauben" deaktiviert. In diesem Fall ist lesender und schreibender Zugriff auf CPU-Daten nur möglich bei Kommunikations-verbindungen, die eine Projektierung bzw. Programmierung sowohl für die lokale CPU als auch für den Kommunikationspartner voraussetzen. Zugriffe über BSEND/BRCV-Anweisungen sind z. B. möglich.
Verbindungen, für die die lokale CPU nur Server ist (d. h. für die lokale CPU ist keine Projektierung / Programmierung der Kommunikation zum Kommunikations-partner vorhanden), sind damit im Betrieb der CPU nicht möglich.
Dazu gehören z. B.

- PUT/GET-, FETCH/WRITE- oder FTP-Zugriffen über Kommunikationsmodule
- PUT/GET-Zugriffen von anderen S7-CPUs
- HMI-Zugriffen über PUT/GET-Kommunikation

3 Sicherheitsmechanismen der S7-CPs

Die folgenden Kapitel zeigen, welche Security-Mechanismen die SIMATIC S7-CPs (CP x43-1 Advanced V3 und CP 1x43-1) anbieten.

Hinweis Die Funktionen im CP 1543-1 sind ab STEP 7 Professional V12 inkl. Update 1 konfigurierbar.
Der CP 1243-1 benötigt mindestens STEP 7 Professional V13 Update 3.

Abbildung 3-1

CP 1543-1 CP 1243-1 CP 343-1 Advanced CP 443-1 Advanced

3.1 Stateful Inspection Firewall

Beschreibung

Die Filtereigenschaften eines Paketfilters lassen sich deutlich verbessern, wenn die IP-Pakete in ihrem Kontext überprüft werden. So ist es zum Beispiel wünschenswert, ein von einem externen Rechner kommendes UDP-Paket nur dann nach innen weiterzuleiten, wenn kurz zuvor von innen ein anderes UDP-Paket an denselben Rechner geschickt wurde (z. B. bei einer DNS-Anfrage eines Clients im Innennetz an einen externen DNS-Server). Um das zu ermöglichen, muss der Paketfilter zu allen aktuellen Verbindungen einen Status verwalten. Paketfilter, die das leisten, werden dementsprechend als **stateful** bezeichnet.

Eigenschaften

Stateful Inspection Firewalls haben folgende Eigenschaften:

- Bei TCP-Verbindungen. Nachahmung der Statusüberwachung eines vollständigen TCP/IP-Protokoll-Stacks
- Bei UDP-Verbindungen. Simulation virtueller Verbindungen
- Erzeugung und Löschen dynamischer Filterregeln

3.2 Datenverschlüsselung über VPN

Beschreibung

Ein VPN (virtuelles privates Netzwerk) bezeichnet ein privates Netzwerk, welches zur Übertragung privater Daten an ein privates Zielnetz ein öffentliches Netzwerk (z. B. Internet) als Transitnetzwerk benutzt. Die Netze müssen dabei untereinander nicht kompatibel sein.

VPN nutzt dafür zwar die Adressierungsmechanismen des Transitnetzwerks, verwendet aber eigene Netzwerkpakete, um den Transport privater Datenpakete von den anderen zu trennen. Diese Tatsache lässt die privaten Netzwerke wie ein gemeinsames, logisches (virtuelles) Netzwerk erscheinen.

IPSec

Ein wichtiger Bestandteil bei der Datenkommunikation über Netzwerkgrenzen hinweg ist IPSec (IP Security). Es ist eine standardisierte Protokollsuite und ermöglicht einen herstellerunabhängigen, sicheren und geschützten Datenaustausch über IP-Netze. Das wesentliche Ziel von IPSec ist der Schutz und die Absicherung der Daten während einer Übertragung über ein unsicheres Netzwerk. Alle bekannten Schwächen wie das Abhören und die Veränderung der Datenpakete können mit diesem Sicherheitsstandard unterbunden werden. Verschlüsselte Datenpakete, Authentifizierung und Authentisierung der Teilnehmer machen dies möglich.

3.3 NAT/NAPT (Adressumsetzung)

Beschreibung

Network Address Translation (NAT) bzw. Network Address Port Translation (NAPT) sind Verfahren zur Umsetzung von privaten IP-Adressen in öffentliche IP-Adressen.

Die Adressumsetzung mit NAT

NAT ist ein Protokoll zur Adressumsetzung zwischen zwei Adressräumen. Hauptaufgabe ist die Umsetzung von öffentlichen Adressen, d. h. IP-Adressen, die im Internet verwendet und auch geroutet werden, in private IP-Adressen und umgekehrt.

Durch diese Technik wird erreicht, dass die Adressen des internen Netzes nach außen im externen Netz nicht sichtbar sind. Die internen Teilnehmer sind im externen Netz nur über die in der Adressumsetzungsliste (NAT-Tabelle) festgelegten externen IP-Adressen sichtbar.

Das klassische NAT ist eine 1:1-Umsetzung, d. h. eine private IP-Adresse wird auf eine öffentliche umgesetzt.

Die Ansprechadresse für die internen Teilnehmer ist demnach eine externe IP-Adresse.

Die NAT-Tabelle enthält die Zuordnung von privaten und öffentlichen IP-Adressen und wird im Gateway oder Router konfiguriert und verwaltet.

Die Adressumsetzung mit NAPT

NAPT ist eine Variante von NAT und wird häufig mit diesem gleichgesetzt. Der Unterschied zu NAT liegt darin, dass bei diesem Protokoll auch Ports umgesetzt werden können.

Es gibt keine 1:1-Umsetzung der IP-Adresse mehr. Vielmehr existiert nur noch eine öffentliche IP-Adresse, die durch den Zusatz von Portnummern in eine Reihe von privaten IP-Adressen umgesetzt wird.

Die Ansprechadresse für die internen Teilnehmer ist eine externe IP-Adresse mit einer Portnummer.

Die NAPT-Tabelle enthält die Zuordnung von externen Ports auf die privaten IP-Adressen inklusive Portnummer und wird im Gateway oder Router konfiguriert und verwaltet.

3.4 Sichere IT-Funktionen

3.4.1 Das File Transfer Protocol (FTP)

Beschreibung

Das File Transfer Protocol ist ein spezifiziertes Netzwerkprotokoll zur Datenübertragung zwischen einem FTP-Server und FTP-Client bzw. clientgesteuert zwischen zwei FTP-Servern.

Mit FTP können Daten ausgetauscht, Verzeichnisse angelegt, umbenannt und auch gelöscht werden. Die Kommunikation zwischen FTP-Client und FTP-Server findet als Austausch von textbasierten Kommandos statt. Jeder vom FTP-Client gesendete Befehl führt zu einer Rückmeldung des FTP-Servers in Form eines Status-Codes und einer Meldung im Klartext.

Dafür legt FTP zwei logische Verbindungen an: einen Steuerkanal über Port 21 zur Übertragung von FTP-Kommandos und deren Antworten sowie einen Datenkanal über Port 20 zur Übertragung von Daten.

Bei passivem FTP werden beide Kanäle durch den FTP-Client, während bei aktivem FTP einer der Kanäle durch den FTP-Server initiiert wird.

Lösung für ein sicheres FTP

Zum Schutz der Daten während der Übertragung besteht auch bei FTP die Möglichkeit der Datenverschlüsselung und Authentifizierung.

Die einfachste Möglichkeit der Umsetzung einer gesicherten FTP-Verbindung ist das Secure Socket Layer Protocol (auch als Transport Layer Security bezeichnet). SSL (Secure Socket Layer) ist in der Darstellungsschicht des OSI-Schichtenmodells angesiedelt. Dabei wird der Datenstrom zu Beginn einer Verbindung unmittelbar auf unterster Bit-Ebene mit einem Schlüssel verschlüsselt.

Für die Identifikation und Authentifikation der Teilnehmer dient das SSL-Handshake Protokoll. Das Aushandeln eines Schlüssels für die Verschlüsselung erfolgt über das Public-Key Verfahren. Dazu sendet der FTP-Server ein Zertifikat mit seinem öffentlichen Schlüssel an den FTP-Client. Der öffentliche Schlüssel zu dem Zertifikat muss zuvor durch eine Zertifizierungsstelle und mit einer digitalen Signatur beglaubigt werden.

FTPS

Das explizite FTP für eine gesicherte Datenübertragung ist eine Kombination aus FTP und dem SSL-Protokoll und verwendet dieselben Ports wie im normalen FTP Modus (Port 20 / 21).

Als Schlüssel für SSL dient ein Zertifikat, das mit der Projektierung des Security-CPs generiert und geliefert wird.

Ein sicherer FTP-Datentransfer mit dem CP x43-1 Advanced V3 und CP 1x43-1 ist nur mit aktivierter Security-Funktion möglich und wird explizit in der Projektierung des CPs erlaubt.

3.4.2 Das Network Time Protocol (NTP)

Beschreibung

Das Network Time Protocol (NTP) ist ein standardisiertes Protokoll zur Synchronisation der Uhrzeit an mehreren Rechnern / Baugruppen über das Netzwerk. Die Genauigkeit liegt im Millisekundenbereich.

Die Uhrzeit wird dabei von einem NTP-Server den NTP-Clients zur Verfügung gestellt.

NTP (gesichert)

Gesichertes NTP ermöglicht eine sichere und authentifizierte Uhrzeitsynchronisation mithilfe von Authentifizierungsmethoden und einem gemeinsamen Verschlüsselungscode. Sowohl der NTP-Server, als auch die NTP-Clients müssen diese Funktion unterstützen.

Eine sichere Uhrzeitsynchronisation wird vom CP x43-1 Advanced V3 und CP 1x43-1 unterstützt, wenn die Security-Funktion aktiviert und die erweiterte NTP-Konfiguration explizit in der Projektierung des CPs in STEP 7 aktiviert ist.

3.4.3 Das Hypertext Transfer Protocol (HTTP)

Beschreibung

Das Hypertext Transfer Protocol (HTTP) gehört zur Familie der Internetprotokolle und ist ein standardisiertes Verfahren zur Übertragung von Daten in einem Netzwerk. HTTP wird bevorzugt für das Laden von Webseiten von einem Webserver auf einen Webbrowser verwendet.

HTTPS

Die Daten, die über HTTP transportiert werden, sind als Klartext lesbar und können von Dritten mitgehört werden.

Gerade jetzt – im Zeitalter des Onlinebanking, des Onlineeinkaufs und der sozialen Netzwerke – ist es wichtig, dass die Übermittlung vertraulicher und persönlicher Daten sicher und vor Unbefugten geschützt erfolgt.

Die einfachste Möglichkeit für eine abhörsichere Übertragung ist das Hypertext Transfer Protocol Secure (HTTPS).
HTTPS ist wie HTTP aufgebaut, nutzt aber zusätzlich für die Verschlüsselung das Secure Socket Layer Protocol.

3.4.4 Das Simple Network Management Protocol (SNMP)

Beschreibung

SNMP – Simple Network Management Protocol – ist ein UDP-basiertes Protokoll, das speziell zur Administration von Datennetzen spezifiziert wurde und sich mittlerweile auch als De-facto-Standard bei TCP/IP-Geräten etabliert hat.
Die einzelnen Knoten im Netz – Netzkomponenten oder auch Endgeräte – verfügen über einen sogenannten SNMP-Agenten, der Informationen in strukturierter Form bereitstellt. Diese Struktur wird als MIB (Management Information Base) bezeichnet. Der Agent ist im Netzknoten in der Regel als Firmwarefunktionalität realisiert.

Management Information Base – MIB

Eine MIB (Management Information Base) ist eine standardisierte Datenstruktur aus verschiedenen SNMP-Variablen, die in einer vom Zielsystem unabhängigen Sprache beschrieben werden. Durch die herstellerübergreifende Standardisierung der MIBs und der Zugriffsmechanismen lässt sich auch ein heterogenes Netzwerk mit Komponenten von unterschiedlichen Herstellern überwachen und steuern. Werden zur Netzüberwachung komponentenspezifische, nicht standardisierte Daten benötigt, so können diese in sogenannten „Private MIBs“ von den Herstellern beschrieben werden.

Das sichere SNMP (SNMPv3)

SNMP gibt es in verschiedenen Versionen: SNMPv1, SNMPv2 und SNMPv3. Die Urversion SNMPv1 und SNMPv2 sind teilweise immer noch im Einsatz. Auf den Einsatz von SNMPv1 und SNMPv2 sollte aber verzichtet werden, da in diesen Versionen keine bzw. nur eingeschränkte Sicherheitsmechanismen implementiert sind.

Ab der Version 3 bietet SNMP zusätzlich eine Benutzerverwaltung mit Authentifikation sowie die optionale Verschlüsselung der Datenpakete an. Durch diese Aspekte wurde die Sicherheit bei SNMP stark erhöht.
Das sichere SNMP wird vom CP x43-1 Advanced V3 und CP 1x43-1 unterstützt, wenn die Security-Funktion aktiviert und SNMPv3 explizit in der Projektierung des CPs in STEP 7 aktiviert ist.

4 Das Achilles Zertifizierungsprogramm

Motivation

Security in der industriellen Automatisierung kann nur durch die Zusammenarbeit von Herstellern, Anbietern, Anwendern und Betreibern erreicht werden. Ein wichtiger Bestandteil der Zusammenarbeit ist die Schaffung international einheitlich anwendbarer Standards, die eine Basis für zukunftsträchtige Security-Konzepte und -Lösungen bilden.

Schaffung einheitlicher Standards

Einen hohen öffentlichen Stellenwert in Bezug auf die Schaffung einheitlich anwendbarer Standards haben

- die Standards ISA 99 „Manufacturing and Control Systems Security“,
- die IEC 62443 „Security for Industrial Process Measurement and Control – Network and System Security“
- die deutsche Richtlinie VDI/VDE 2182 “Informationssicherheit in der industriellen Automatisierung”.

Während sich letzteres mit Vorgehensweisen und Mechanismen zur Absicherung von Automatisierungskomponenten und -systemen befasst, stellt sich das ISA Security Compliance Institut (ISCI) der Herausforderung, dafür einen einheitlichen Zertifizierungsrahmen zu schaffen.

Das Zertifizierungsprogramm Achilles

Das Zertifizierungsprogramm „Achilles" von Wurldtech gilt international als Standard für industrielle Cyber-Security.

Das Zertifikat bestätigt, dass Automatisierungssysteme über die nötige Funktionalität verfügen, um die Sicherheit und Stabilität von Industrieanlagen zu gewährleisten. Es dient als wichtiges Kriterium bei der Auswahl von IT-Lösungen. Die Robustheit gegen Netzwerkangriffe ist bei den Steuerungssystemen von Siemens durch das Achilles-Zertifizierungsprogramm bestätigt. Damit erfüllen die SIMATIC-CPUs höchste Sicherheitsanforderungen.
Gegliedert ist das Zertifizierungsprogramm in zwei Stufen:

- Achilles Communications Certification Level 1: Die erste Stufe des Zertifizierungsprogramms bestätigt über ein spezielles Testprogramm die Robustheit von Ethernet, IP, ARP, ICMP, TCP und UDP in den Baugruppen. Erfüllen diese alle Test-Anforderungen, erhalten die Baugruppen die Achilles Level 1 Zertifizierung.
- Achilles Level 2 Certification: Diese Folgestufe umfasst dieselben Protokolle wie Stufe 1. Allerdings wird jedes Protokoll ausführlicher getestet. Zusätzlich beinhaltet Stufe 2 mehr Test, Denial-of-Service (DoS)-Tests mit höherer Link-Rate und weitere Anforderungspunkte.
  Die getesteten Baugruppen von Siemens Industry besitzen alle die Achilles Level 2 Zertifizierung.

Hinweis

Eine Übersicht der zertifizierten Baugruppen finden Sie auf der Webseite von Wurldtech unter
http://devices.wurldtech.com/device_manufacturers/certifications/siemens_certified_products/

Informationen zu der Testumgebung und dem Testablauf finden Sie auf der Webseite von Wurldtech unter http://wurldtech.com/product_services/

5 Literaturhinweise

Literaturangaben

Diese Liste ist keinesfalls vollständig und spiegelt nur eine Auswahl an geeigneter Literatur wider.

Tabelle 5-1

	Themengebiet	Titel
/1/	STEP7 SIMATIC S7-300/400	Automatisieren mit STEP7 in AWL und SCL Autor: Hans Berger Publicis MCD Verlag ISBN: 978-3-89578-397-5
/2/	STEP7 SIMATIC S7-300/400	Automatisieren mit STEP 7 in KOP und FUP Autor: Hans Berger Publicis MCD Verlag ISBN: 978-3-89578-296-1
/3/	STEP7 SIMATIC S7-300	Automatisieren mit SIMATIC S7-300 im TIA-Portal Autor: Hans Berger Publicis MCD Verlag ISBN: 978-3-89578-357-9
/4/	STEP7 SIMATIC S7-400	Automatisieren mit SIMATIC S7-400 im TIA-Portal Autor: Hans Berger Publicis MCD Verlag ISBN: 978-3-89578-372-2
/5/	STEP7 SIMATIC S7-1200	Automatisieren mit SIMATIC S7-1200 Autor: Hans Berger Publicis MCD Verlag ISBN: 978-3-89578-355-5
/6/	STEP7 SIMATIC S7-1500	Automatisieren mit SIMATIC S7-1500 Autor: Hans Berger Publicis MCD Verlag ISBN: 978-3895784033
/7/	SIMATIC NET Security	SIMATIC NET Industrial Ethernet Security Grundlagen und Anwendung Projektierungshandbuch http://support.automation.siemens.com/WW/view/de/56577508
/8/	Handbuch S7-1500	SIMATIC S7-1500 Automatisierungssystem http://support.automation.siemens.com/WW/view/de/59191792
/9/	Handbuch S7-1200	SIMATIC S7-1200 Automatisierungssystem http://support.automation.siemens.com/WW/view/de/36932465
/10/	Handbuch S7-400	SIMATIC S7-400 Automatisierungssystem S7-400 CPU-Daten http://support.automation.siemens.com/WW/view/de/53385241
/11/	Handbuch S7-300	SIMATIC S7-300 CPU 31xC und CPU 31x: Technische Daten http://support.automation.siemens.com/WW/view/de/12996906
/12/	CP343-1 Advanced	Gerätehandbuch Teil B CP343-1 Advanced http://support.automation.siemens.com/WW/view/de/62046619
/13/	CP443-1 Advanced	Gerätehandbuch Teil B CP443-1 Advanced http://support.automation.siemens.com/WW/view/de/59187252
/14/	Handbuch CP1543-1	SIMATIC NET S7-1500 - Industrial Ethernet CP 1543-1 http://support.automation.siemens.com/WW/view/de/76476576

Internet-Link-Angaben

Tabelle 5-2

	Themengebiet	Titel
\1\	Siemens Industry Online Support	https://support.industry.siemens.com
\2\	Downloadseite des Beitrages	https://support.industry.siemens.com/cs/ww/de/view/77431846
\3\	Industrial Ethernet Security	http://support.automation.siemens.com/WW/view/de/18701555/130000
\4\	Getting Started S7-1500	http://support.automation.siemens.com/WW/view/de/71704272
\5\	Themenübersicht „Rundumschutz mit Industrial Ethernet“	https://support.industry.siemens.com/cs/de/de/view/50203404
\6\	Themenübersicht „Industrial Remote Communication“	https://support.industry.siemens.com/cs/de/de/view/64721753
\7\	Übersicht möglicher Konstellationen eines IP-basierten Remote Networks	https://support.industry.siemens.com/cs/de/de/view/26662448
\8\	SIMATIC NET Industrial Ethernet Security, Security in STEP 7 Professional einrichten	https://support.industry.siemens.com/cs/de/de/view/109477192
\9\	SIMATIC NET Industrial Ethernet Security - Security einrichten - Getting Started	https://support.industry.siemens.com/cs/de/de/view/109474411
\10\	SIMATIC NET - Industrial Ethernet Security - Security-Grundlagen und -Anwendung - Projektierungshandbuch	https://support.industry.siemens.com/cs/de/de/view/109474417

6 Historie

Tabelle 6-1

Version	Datum	Änderung
V1.0	09/2013	Erste Ausgabe
V2.0	03/2016	Ergänzung CP 1243-1, Einfügen weiterer Links