SIEMENS

SIMATIC

S7-1500 Security

Getting Started

Übersicht über die Schutzfunktionen der CPU 1

Zusätzlichen Zugriffsschutz über das Display einstellen 2

Know-how-Schutz 3

Kopierschutz 4

Schutz durch Verriegelung der CPU 5

Zugriffsschutz für die CPU projektieren 6

Schutz der HMI-Verbindung projektieren 7

03/2013

A5E03982395-01

Rechtliche Hinweise

Warnhinweiskonzept

Dieses Handbuch enthält Hinweise, die Sie zu Ihrer persönlichen Sicherheit sowie zur Vermeidung von Sachschäden beachten müssen. Die Hinweise zu Ihrer persönlichen Sicherheit sind durch ein Warndreieck hervorgehoben, Hinweise zu alleinigen Sachschäden stehen ohne Warndreieck. Je nach Gefährdungsstufe werden die Warnhinweise in abnehmender Reihenfolge wie folgt dargestellt.

⚠GEFAHR
bedeutet, dass Tod oder schwere Körperverletzung eintreten **wird**, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

⚠WARNUNG
bedeutet, dass Tod oder schwere Körperverletzung eintreten **kann**, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

⚠VORSICHT
bedeutet, dass eine leichte Körperverletzung eintreten kann, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

ACHTUNG
bedeutet, dass Sachschaden eintreten kann, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

Beim Auftreten mehrerer Gefährdungsstufen wird immer der Warnhinweis zur jeweils höchsten Stufe verwendet. Wenn in einem Warnhinweis mit dem Warndreieck vor Personenschäden gewarnt wird, dann kann im selben Warnhinweis zusätzlich eine Warnung vor Sachschäden angefügt sein.

Qualifiziertes Personal

Das zu dieser Dokumentation zugehörige Produkt/System darf nur von für die jeweilige Aufgabenstellung **qualifiziertem Personal** gehandhabt werden unter Beachtung der für die jeweilige Aufgabenstellung zugehörigen Dokumentation, insbesondere der darin enthaltenen Sicherheits- und Warnhinweise. Qualifiziertes Personal ist auf Grund seiner Ausbildung und Erfahrung befähigt, im Umgang mit diesen Produkten/Systemen Risiken zu erkennen und mögliche Gefährdungen zu vermeiden.

Bestimmungsgemäßer Gebrauch von Siemens-Produkten

Beachten Sie Folgendes:

⚠WARNUNG
Siemens-Produkte dürfen nur für die im Katalog und in der zugehörigen technischen Dokumentation vorgesehenen Einsatzfälle verwendet werden. Falls Fremdprodukte und -komponenten zum Einsatz kommen, müssen diese von Siemens empfohlen bzw. zugelassen sein. Der einwandfreie und sichere Betrieb der Produkte setzt sachgemäßen Transport, sachgemäße Lagerung, Aufstellung, Montage, Installation, Inbetriebnahme, Bedienung und Instandhaltung voraus. Die zulässigen Umgebungsbedingungen müssen eingehalten werden. Hinweise in den zugehörigen Dokumentationen müssen beachtet werden.

Marken

Alle mit dem Schutzrechtsvermerk ® gekennzeichneten Bezeichnungen sind eingetragene Marken der Siemens AG. Die übrigen Bezeichnungen in dieser Schrift können Marken sein, deren Benutzung durch Dritte für deren Zwecke die Rechte der Inhaber verletzen kann.

Haftungsausschluss

Wir haben den Inhalt der Druckschrift auf Übereinstimmung mit der beschriebenen Hard- und Software geprüft. Dennoch können Abweichungen nicht ausgeschlossen werden, so dass wir für die vollständige Übereinstimmung keine Gewähr übernehmen. Die Angaben in dieser Druckschrift werden regelmäßig überprüft, notwendige Korrekturen sind in den nachfolgenden Auflagen enthalten.

Siemens AG
Industry Sector
Postfach 48 48
90026 NÜRNBERG
DEUTSCHLAND

A5E03982395-01
℗ 03/2013 Änderungen vorbehalten

Inhaltsverzeichnis

1 Übersicht über die Schutzfunktionen der CPU 5
2 Zusätzlichen Zugriffsschutz über das Display einstellen 7
3 Know-how-Schutz 9
4 Kopierschutz 13
5 Schutz durch Verriegelung der CPU 15
6 Zugriffsschutz für die CPU projektieren 17
7 Schutz der HMI-Verbindung projektieren 21

Übersicht über die Schutzfunktionen der CPU

1

Einleitung

Dieses Kapitel beschreibt die folgenden Funktionen zum Schutz des Automatisierungssystems S7-1500 gegen unberechtigten Zugriff:

- Zugriffsschutz
- Know-how-Schutz
- Kopierschutz
- Schutz durch Verriegelung der CPU

Weitere Maßnahmen zum Schutz der CPU

Die folgenden Maßnahmen erhöhen zusätzlich den Schutz gegen unberechtigte Zugriffe auf Funktionen und Daten der S7-1500 CPU von außen und über das Netzwerk:

- Deaktivieren des Webservers
- Deaktivieren der Uhrzeitsynchronisation über NTP-Server
- Deaktivieren der PUT/GET-Kommunikation

Bei Verwendung des Webservers schützen Sie Ihr Automatisierungssystem S7-1500 vor unberechtigtem Zugriff, indem Sie in der Benutzerverwaltung passwortgesicherte Zugriffsrechte für bestimmte Benutzer einstellen.

Zusätzlichen Zugriffsschutz über das Display einstellen

2

Einleitung

Am Display einer S7-1500 CPU 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.

Vorgehen

Wenn in STEP 7 eine Zugriffsstufe mit Passwort konfiguriert ist, dann kann über das Display der Zugriff gesperrt werden.

Um den lokalen Zugriffsschutz für eine S7-1500 CPU am Display einzustellen, gehen Sie folgendermaßen vor:

1. Wählen Sie am Display das Menü Einstellungen > Schutz.
2. Bestätigen Sie die Wahl mit "OK" und stellen Sie für jede Zugriffsstufe ein, ob der Zugriff im Betriebsartenschalter Modus RUN erlaubt ist oder nicht:

   Erlauben: Zugriff auf die CPU ist möglich, in dem das entsprechende Passwort in STEP 7 eingegeben werden muss.

   Deaktivert im RUN: Wenn der Betriebsartenschalter auf RUN steht, kann sich kein Benutzer mehr mit den Rechten dieser Zugriffsstufe auf der CPU anmelden, obwohl ihm das Passwort dafür bekannt ist. Im STOP ist der Zugriff möglich mit Passworteingabe.

Zugriffsschutz für das Display

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.

Know-how-Schutz

3

Mit dem Know-how-Schutz können Sie einen oder mehrere Bausteine des Typs OB, FB, FC und globale Datenbausteine in Ihrem Programm vor unbefugtem Zugriff schützen. Sie können ein Passwort eingeben, um den Zugriff auf einen Baustein einzuschränken. Der Passwortschutz verhindert das unbefugte Lesen oder Ändern des Bausteins.

Ohne Passwort können nur die folgenden Informationen zum Baustein gelesen werden:

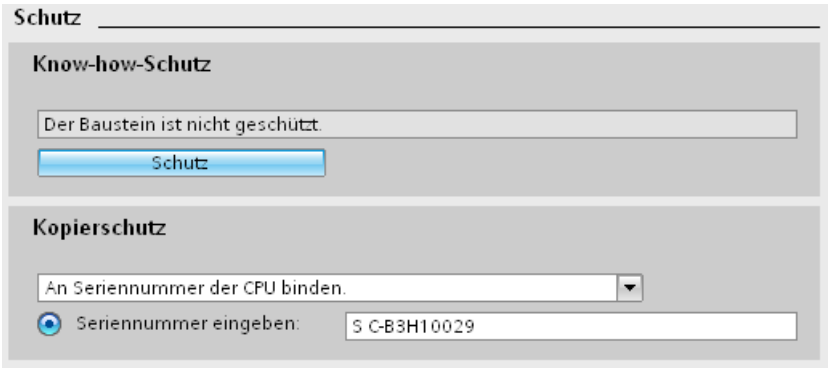
- Bausteintitel, Kommentar und Bausteineigenschaften
- Bausteinparameter (INPUT, OUTPUT, IN, OUT, RETURN)
- Aufrufstruktur des Programms
- Globale Variablen ohne Angaben der Verwendungsstelle

Weitere Aktionen, die mit einem know-how-geschützten Baustein durchführbar sind:

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

Know-how-Schutz für Bausteine einrichten

1. Öffnen Sie die Eigenschaften des jeweiligen Bausteins.
2. Wählen Sie unter "Allgemein" die Option "Schutz".



3. Klicken Sie auf die Schaltfläche "Schutz", um den Dialog "Know-how-Schutz" anzuzeigen.

4. Klicken Sie auf die Schaltfläche "Definieren", um den Dialog "Passwort definieren" zu öffnen.

5. Geben Sie das Passwort im Feld "Neues Passwort" ein. Wiederholen Sie das Passwort im Feld "Passwort bestätigen".
6. Bestätigen Sie die Eingabe mit "OK".
7. Schließen Sie den Dialog "Know-how-Schutz" mit "OK".

Ergebnis: Die ausgewählten Bausteine werden mit einem Know-how-Schutz versehen. In der Projektnavigation werden know-how-geschützte Bausteine mit einem Schloss markiert. Das eingegebene Passwort ist für alle ausgewählten Bausteine gültig.

Know-how-geschützte Bausteine öffnen

1. Doppelklicken Sie auf den Baustein um den Dialog "Zugriffsschutz" zu öffnen.
2. Geben Sie das Passwort für den know-how-geschützten Baustein ein.
3. Bestätigen Sie Ihre Eingabe mit "OK".

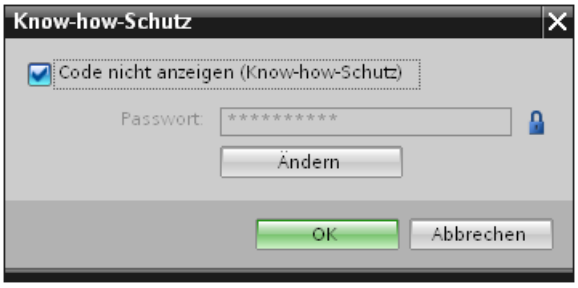
Ergebnis: Der know-how-geschützte Baustein wird geöffnet.

Nach dem Öffnen des Bausteins können Sie den Programmcode und die Bausteinschnittstelle des Bausteins so lange bearbeiten, bis Sie den Baustein oder das TIA-Portal schließen. Beim nächsten Öffnen des Bausteins muss das Passwort wieder eingegeben werden. Wenn Sie den Dialog "Zugriffsschutz" mit "Abbrechen" schließen, wird der Baustein zwar geöffnet, aber der Code des Bausteins wird nicht angezeigt und Sie können den Baustein nicht bearbeiten.

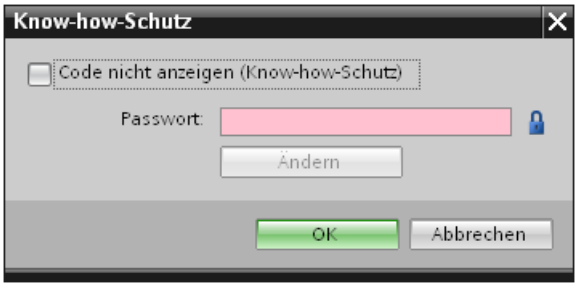
Der Know-how-Schutz des Bausteins wird nicht aufgehoben, wenn Sie den Baustein z. B. kopieren oder in eine Bibliothek einfügen. Dann sind auch die Kopien know-how-geschützt.

Know-how-Schutz für Bausteine entfernen

1. Wählen Sie den Baustein aus, bei dem Sie den Know-how-Schutz entfernen möchten. Der geschützte Baustein darf nicht im Programmeditor geöffnet sein.
2. Wählen Sie im Menü "Bearbeiten" den Befehl "Know-how-Schutz" um den Dialog "Know-how-Schutz" zu öffnen.
3. Deaktivieren Sie das Optionskästchen "Code nicht anzeigen (Know-how-Schutz)".



4. Geben Sie das Passwort ein.



5. Bestätigen Sie die Eingabe mit "OK".

Ergebnis: Der Know-how-Schutz wird für den ausgewählten Baustein aufgehoben.

Kopierschutz

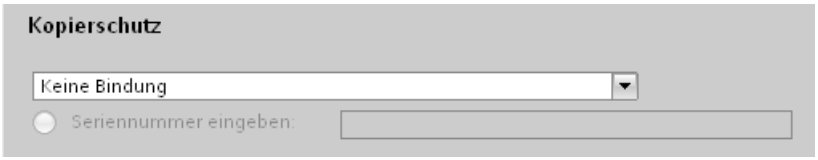
4

Der Kopierschutz ermöglicht Ihnen, das Programm oder die Bausteine mit einer bestimmten SIMATIC Memory Card oder CPU zu verknüpfen. 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 einer bestimmten SIMATIC Memory Card oder CPU möglich. Mit dieser Funktion kann ein Programm oder ein Baustein elektronisch (z. B. per E-Mail) oder durch Versenden eines Speichermoduls verschickt werden.

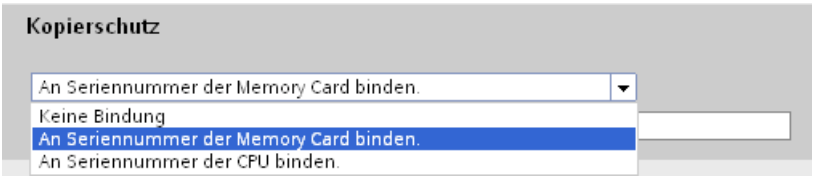
Wenn Sie einen solchen Kopierschutz für einen Baustein einrichten, versehen Sie diesen Baustein auch mit einem Know-how-Schutz. Ohne Know-how-Schutz kann jeder den Kopierschutz zurücksetzen. Allerdings müssen Sie den Kopierschutz zuerst einrichten, da die Einstellungen für den Kopierschutz schreibgeschützt sind, wenn der Baustein einen Know-how-Schutz besitzt.

Kopierschutz einrichten

1. Öffnen Sie die Eigenschaften des jeweiligen Bausteins.
2. Wählen Sie unter "Allgemein" die Option "Schutz".



3. Wählen Sie im Bereich "Kopierschutz" aus der Klappliste entweder den Eintrag "An Seriennummer der CPU binden" oder den Eintrag "An Seriennummer der Memory Card binden".



4. Geben Sie die Seriennummer der CPU oder der SIMATIC Memory Card ein.

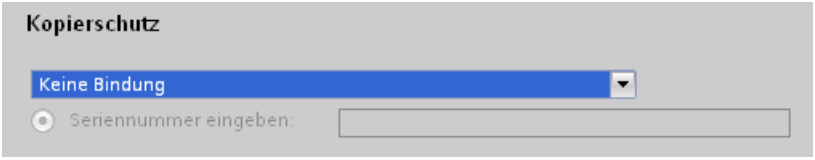
5. Im Bereich "Know-how-Schutz" können Sie nun den Know-how-Schutz für den Baustein einrichten.

Hinweis

Wenn Sie einen Baustein mit Kopierschutz in ein Gerät laden, das mit der festgelegten Seriennummer nicht übereinstimmt, wird der gesamte Ladevorgang zurückgewiesen. Das bedeutet, dass auch Bausteine ohne Kopierschutz nicht geladen werden.

Kopierschutz entfernen

1. Entfernen Sie einen eventuell vorhandenen Know-how-Schutz.
2. Öffnen Sie die Eigenschaften des jeweiligen Bausteins.
3. Wählen Sie unter "Allgemein" die Option "Schutz".
4. Wählen Sie im Bereich "Kopierschutz" aus der Klappliste den Eintrag "Keine Bindung".



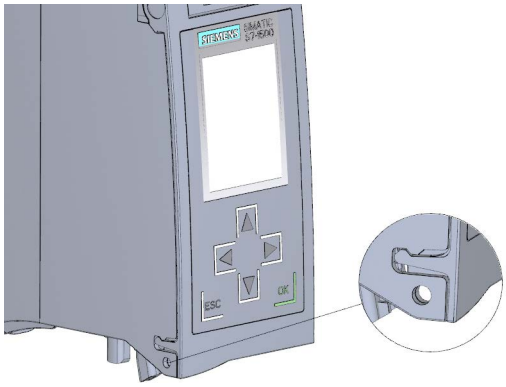
Schutz durch Verriegelung der CPU

5

Schützen Sie Ihre CPU vor unberechtigtem Zugriff durch eine ausreichend gesicherte Frontklappe.

Sie haben mit der Verriegelungslasche an der CPU z. B. folgende Möglichkeiten:

- Eine Plombe anbringen
- Frontklappe mit einem Schloss sichern (Bügeldurchmesser: 3 mm)



Zugriffsschutz für die CPU projektieren

6

Einleitung

Die CPU bietet vier Zugriffsstufen, um den Zugang zu bestimmten Funktionen einzuschränken.

Mit dem Einrichten der Zugriffsstufe und der Passworte für eine CPU schränken Sie die Funktionen und Speicherbereiche ein, die ohne Eingabe eines Passworts zugänglich sind. Die einzelnen Zugriffsstufen sowie die Eingaben der dazugehörigen Passwörter werden in den Objekteigenschaften der CPU festgelegt.

Zugriffsstufen der CPU

Zugriffsstufen	Zugangsbeschränkungen
Vollzugriff (kein Schutz)	Die Hardware-Konfiguration und die Bausteine können von jedem gelesen und verändert werden.
Lesezugriff	Mit dieser Zugriffsstufe ist ohne Angabe des Passworts nur lesender Zugriff auf die Hardware-Konfiguration und die Bausteine möglich, d. h. Sie können Hardware-Konfiguration und Bausteine ins Programmiergerät laden. Möglich ist außerdem der HMI-Zugang und Zugriff auf Diangosedaten. Sie können ohne Eingabe des Passworts keine Bausteine und keine Hardware-Konfiguration in die CPU laden. Außerdem ist ohne Passwort Folgendes **nicht** möglich: schreibende Testfunktionen, Wechsel des Betriebszustands (RUN/STOP) und Firmware-Update (online).
HMI-Zugriff	Mit dieser Zugriffsstufe ist ohne Angabe des Passworts nur der HMI-Zugang und der Zugriff auf Diagnosedaten möglich. Sie können ohne Angabe des Passworts weder Bausteine und die Hardware-Konfiguration in die CPU laden, noch von der CPU Bausteine und die Hardware-Konfiguration ins Programmiergerät laden. Außerdem ist ohne Passwort Folgendes **nicht** möglich: schreibende Testfunktionen, Wechsel des Betriebszustands (RUN/STOP) und Firmware-Update (online).
kein Zugriff (kompletter Schutz)	Wenn die CPU komplett geschützt ist, dann ist weder lesender noch schreibender Zugriff auf die Hardware-Konfiguration und die Bausteine möglich. Auch der HMI-Zugriff ist nicht möglich. Die Server-Funktion für PUT/GET-Kommunikation ist in dieser Zugriffsstufe deaktiviert (nicht änderbar). Durch die Legitimation mit dem Passwort erhalten Sie wieder Vollzugriff auf die CPU.

Jede Zugriffsstufe lässt auch ohne Eingabe eines Passworts den uneingeschränkten Zugriff auf bestimmte Funktionen zu, z. B. Identifikation über die Funktion "Erreichbare Teilnehmer".

Die Voreinstellung der CPU ist "ohne Einschränkung" und "ohne Passwortschutz". Um den Zugang zu einer CPU zu schützen, müssen Sie die Eigenschaften der CPU bearbeiten und ein Passwort einrichten.

Die Kommunikation zwischen den CPUs (über die Kommunikationsfunktionen in den Bausteinen) wird durch die Zugriffsstufe der CPU nicht eingeschränkt, es sei denn PUT/GET-Kommunikation ist deaktiviert.

Die Eingabe des richtigen Passworts gestattet den Zugriff auf alle Funktionen, die in der entsprechenden Stufe erlaubt sind.

Hinweis

Projektierung einer Zugriffsstufe ersetzt nicht den Know-how-Schutz

Die Parametrierung von Zugriffsstufen verhindert unrechtmäßige Änderungen an der CPU, indem die Rechte zum Download eingeschränkt werden. Bausteine auf der SIMATIC Memory Card sind jedoch nicht schreib- oder lesegeschützt. Um den Code von Bausteinen auf der SIMATIC Memory Card zu schützen, verwenden Sie den Know-how-Schutz.

Vorgehen Zugriffsstufen parametrieren

Um die Zugriffsstufen für eine S7-1500 CPU zu parametrieren, gehen Sie folgendermaßen vor:

1. Öffnen Sie die Eigenschaften der S7-1500 CPU im Inspektorfenster.
2. Öffnen Sie in der Bereichsnavigation den Eintrag "Schutz".

   Eine Tabelle mit den möglichen Zugriffsstufen wird im Inspektorfenster angezeigt.

3. Aktivieren Sie die gewünschte Zugriffsstufe in der ersten Spalte der Tabelle. Die grünen Haken in den Spalten rechts der jeweiligen Zugriffsstufe zeigen Ihnen, welche Operationen noch möglich sind, ohne das Passwort einzugeben.
4. Vergeben Sie in der Spalte "Passwort" in der ersten Zeile ein Passwort für die gewählte Zugriffsstufe. Wiederholen Sie zum Schutz vor Fehleingaben das gewählte Passwort in der Spalte "Bestätigung".

   Achten Sie darauf, dass das Passwort ausreichend sicher ist, d. h. dass es kein erkennbares Muster besitzt, das durch eine Maschine erkannt werden kann!

   Die Eingabe eines Passworts in der ersten Zeile (Zugriffsstufe "Vollzugriff ") ist obligatorisch und ermöglicht dem Passwort-Kenner uneingeschränkten Zugriff auf die CPU, unabhängig von der gewählten Schutzstufe.
5. Weisen Sie weiteren Zugriffsstufen nach Bedarf weitere Passwörter zu, falls die gewählte Zugriffsstufe das erlaubt.
6. Laden Sie die Hardware-Konfiguration, damit die Zugriffsstufe wirksam wird.

Verhalten einer passwortgeschützten CPU im Betrieb

Der Schutz der CPU ist wirksam, nachdem die Einstellungen in die CPU geladen wurden.

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 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.

Der Zugriff auf eine passwortgeschützte CPU im RUN kann lokal am Display eingeschränkt werden, so dass auch ein Zugriff mit Passwort nicht möglich ist.

Schutz der HMI-Verbindung projektieren

7

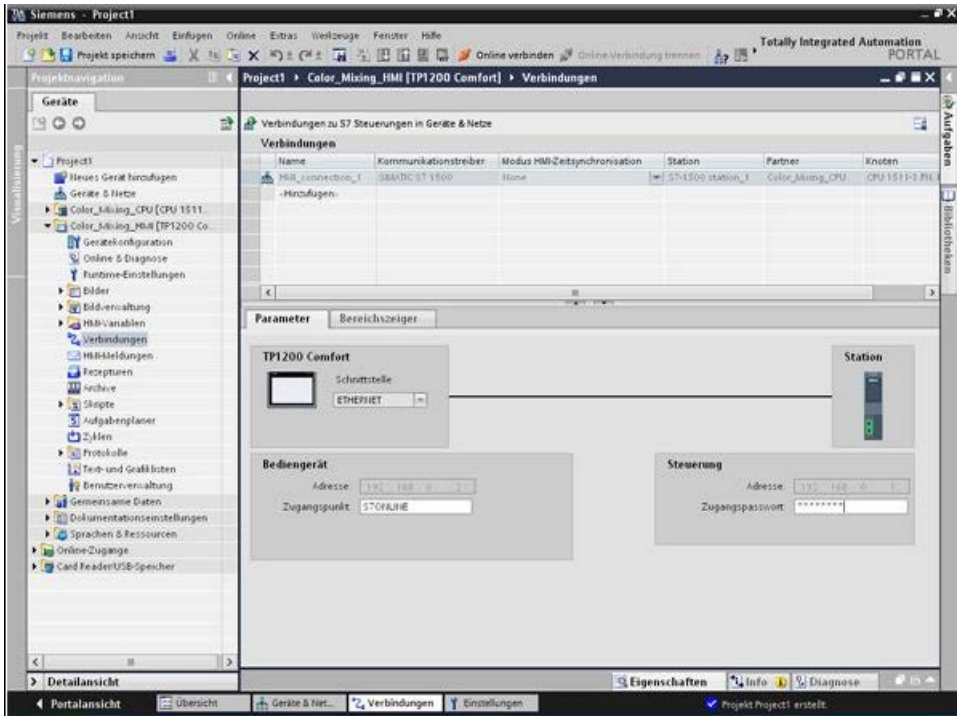
Einleitung

Wenn für die CPU die Schutzstufe "Kompletter Schutz" vergeben wurde, dann kann das Bediengerät nur mit dem dort hinterlegten Passwort auf die CPU zugreifen.

Diese Funktion steht Ihnen nur mit Bediengeräten von SIEMENS zur Verfügung.

Vorgehensweise

1. Öffnen Sie in der Projektnavigation den Editor "Verbindungen".
2. Wählen Sie die integrierte Verbindung aus.
3. Geben Sie das Passwort der CPU im Bereich "Passwort" ein.



Ergebnis

Das Bediengerät kann jetzt mit der CPU kommunizieren und Daten austauschen.