SIEMENS

SIMATIC
Industrie Software
Produktinformation zum Programmier- und Bedienhandbuch "SIMATIC Safety - Projektieren und Programmieren"

Produktinformation

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 (https://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 (https://www.siemens.com/industrialsecurity).

A5E44675171-AA, 04/2018

Inhalt

Diese Produktinformation enthält wichtige Informationen für die Erhaltung der Betriebssicherheit Ihrer Anlage. Die Produktinformation ist Bestandteil des gelieferten Produkts. Die darin enthaltenen Aussagen sind in Zweifelsfällen als aktueller anzusehen.

Korrektur im Kapitel "Konfigurationsdatei einspielen"

⚠ WARNUNG

Den erfolgreichen Import eines Sicherheitsprogramms über das Skript müssen Sie durch die Auswertung des entsprechenden Return-Werts (0x51A3) feststellen. Wenn der entsprechende Return-Wert nicht von dem Skriptbefehl PCSystem_Control zurückgegeben wird, ist der Import fehlgeschlagen und das alte Sicherheitsprogramm kann noch vorhanden sein.

Um Sicherzustellen, dass der Return-Wert nicht vom letzten Import stammt, müssen Sie vor dem Import den Return-Wert auf 0x3FF ("PCSystem_Control /ImportConfig“ ohne einen Dateinamen eingeben) zurücksetzen und anschließend prüfen, ob der Return-Wert auf 0x3FF zurückgesetzt wurde ("PCSystem_Control /GetStatus /ImportConfig" eingeben und anschließend "echo %errorlevel%" eingeben. Diese Anweisung muss den Return-Wert 0x3FF zurückliefern).

Wenn der Importvorgang von einem Server angestoßen wird, muss auch eine Rückmeldung über den positiven Return-Wert erfolgen.

Für die Nachvollziehbarkeit empfehlen wir Ihnen, den Importvorgang in einer Logdatei zu dokumentieren.

Wenn Sie den Import der Konfigurationsdatei händisch über die Windowskommandozeile (über Skriptbefehl) durchführen, müssen Sie entweder:

- Vor dem Import den Return-Wert auf 0x3FF rücksetzen und prüfen (siehe oben).
  - Den Import durchführen.
  - Den Return-Wert auswerteten ("PCSystem_Control /GetStatus /ImportConfig" eingeben und anschließend "echo %errorlevel%" eingeben. Diese Anweisung muss den Return-Wert 0x51A3 zurückliefern).
- Den Import durchführen.
  - Eine manuelle Programmidentifikation z. B. über das Panel der F-CPU durchführen. *(S083)*

Siemens AG
Division Digital Factory
Postfach 48 48
90026 NÜRNBERG
DEUTSCHLAND

Produktinformation zum Programmier- und Bedienhandbuch "SIMATIC Safety - Projektieren und Programmieren"
A5E44675171-AA, 04/2018

SIEMENS

SIMATIC
Industrial Software
Product Information for the programming and operating manual "SIMATIC Safety - Configuring and Programming"

Product Information

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial security measures that may be implemented, please visit (https://www.siemens.com/industrialsecurity).

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customers' exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under (https://www.siemens.com/industrialsecurity).

A5E44675171-AA, 04/2018

Content

This Product Information contains important details on maintaining the operational safety of your system. The Product Information is part of the product supplied. The statements provided in it should be considered more up-to-date than other documentation if uncertainties arise.

Correction in the "Importing the configuration file" section

⚠ WARNING

You determine the successful import of a security program via the script by evaluating the corresponding return value (0x51A3). If the corresponding return value is not returned by the script command PCSystem_Control, the import has failed and the old security program may still be present.

To ensure that the return value is not from the previous import, you need to reset the return value to 0x3FF ("PCSystem_Control /ImportConfig" without entering a data name) before the import and then check that the return value has been reset to 0x3FF (Enter "PCSystem_Control /GetStatus /ImportConfig" and then enter "echo %errorlevel%". This instruction must deliver the return value 0x3FF).

If the import operation is triggered by a server, feedback about the positive return value must be given.

For traceability, we recommend that you document the import operation in a log file.

If you import the configuration file manually from the Windows command line (via script command), you need to do one of the following:

- Reset the return value to 0x3FF and check it before the import (see above).
  - Perform the import.
  - Evaluate the return value (Enter "PCSystem_Control /GetStatus /ImportConfig" and then enter "echo %errorlevel%". This instruction must deliver the return value 0x51A3).
- Perform the import.
  - Perform manual program identification, e.g. via the panel of the F-CPU. *(S083)*

Siemens AG
Division Digital Factory
Postfach 48 48
90026 NÜRNBERG
GERMANY

Product Information for the programming and operating manual "SIMATIC Safety - Configuring and Programming"
A5E44675171-AA, 04/2018