SIEMENS

N 148/23

IP-Schnittstelle Secure

Applikationsprogrammbeschreibung

A6V11689762_de--_b

Smart Infrastructure

2019-07-05

Inhaltsverzeichnis

1 Informationen zur IP-Schnittstelle Secure und zum Applikationsprogramm

Produktfamilie: Systemgerät

Produkttyp: Schnittstelle

Hersteller: Siemens

Name: IP-Schnittstelle Secure N148/23

Bestell-Nr.: 5WG1 148-1AB23

Applikation: 0012 CO IP-Schnittstelle Secure 7204 02

Systemvoraussetzung:

- mind. ETS 5.7.3 oder höher

1.1 Haftungsausschluss Cyber-Sicherheit

Siemens offeriert ein Portfolio von Produkten, Lösungen, Systemen und Dienstleistungen mit Sicherheitsfunktionen, die den sicheren Betrieb von Anlagen, Systemen, Maschinen und Netzwerken unterstützen. Im Geschäftsfeld der Gebäudetechnik umfasst dies Systeme für Gebäudeautomation und -leittechnik, Brandschutz, Sicherheitsmanagement und physische Sicherheitssysteme.

Um Anlagen, Systeme, Maschinen und Netzwerke vor Online-Bedrohungen zu schützen, ist es erforderlich, ein ganzheitliches, dem neuesten Stand der Technik entsprechendes Sicherheitskonzept zu implementieren und stets auf dem aktuellen Stand zu halten. Das Portfolio von Siemens bildet nur einen Bestandteil eines solchen Konzeptes.

Sie sind dafür verantwortlich, unbefugten Zugang zu Ihren Anlagen, Systemen, Maschinen und Netzwerken zu verhindern. Diese sollten nur mit einem Netzwerk oder dem Internet verbunden werden, wenn und soweit die Verbindung erforderlich ist und angemessene Sicherheitsvorkehrungen (z. B. Firewalls bzw. Netzwerksegmentierung) vorhanden sind. Darüber hinaus sind die Sicherheitsempfehlungen von Siemens zu beachten. Für nähere Informationen kontaktieren Sie bitte Ihren Ansprechpartner bei Siemens oder besuchen Sie unsere Webseite https://www.siemens.com/global/de/home/unternehmen/themenfelder/zukunft-der-industrie/industrial-security.html.

Zur Verbesserung der Sicherheit wird das Portfolio von Siemens kontinuierlich weiterentwickelt. Siemens empfiehlt dringend, Updates zu verwenden, sobald diese zur Verfügung stehen, und stets die neusten Versionen zu verwenden. Werden Versionen verwendet, die nicht mehr unterstützt werden, oder werden neueste Updates nicht verwendet, kann sich Ihr Risiko bezüglich Online-Bedrohungen erhöhen. Siemens empfiehlt dringend, Sicherheitsempfehlungen zu den neuesten Sicherheitsgefährdungen, Patches und damit verbundenen Maßnahmen zu befolgen, die unter anderem unter https://www.siemens.com/cert/de/cert-security-advisories.htm veröffentlicht werden.

2 Funktion

2.1 Sicherheitsfunktionen der IP-Schnittstelle Secure

Die IP-Schnittstelle Secure unterstützt den Sicherheitsstandard „**KNX IP Secure**“ und bietet u. a. folgende Sicherheitsfunktionen:

- Gesicherter Zugriff nur von authentifizierten Geräten
- Sichere Inbetriebnahme über ETS

Bei der sicheren Inbetriebnahme über ETS wird das auf dem Gerät aufgedruckte Gerätezertifikat (FDSK = Factory Default Setup Key) eingelesen und genau für dieses Gerät im ETS-Projekt abgespeichert.

Weitere Informationen zu KNX IP Secure können in der Hilfe der ETS-Software sowie unter folgender Internetadresse nachgelesen werden:
https://support.knx.org

Alternativ ist auch die ungesicherte Inbetriebnahme ohne KNX IP Secure möglich. In diesem Fall ist das Gerät ungesichert und verhält sich wie andere KNX-Geräte ohne IP Secure.

2.2 Funktionen der IP-Schnittstelle Secure

Die IP-Schnittstelle Secure ist ein Reiheneinbaugerät zum Einbau in Verteilungen. Das Gerät nutzt den KNXnet/IP-Standard und dient als Schnittstelle zu KNX/EIB über Datennetzwerke unter Nutzung des Internetprotokolls (IP). Hierzu ermöglicht dieses Gerät den Buszugriff von einem PC oder anderen Datenverarbeitungsgeräten.

Anschlüsse und Spannungsversorgung

Die Verbindung zum KNX wird über eine Busanschlussklemme hergestellt (schwarz-rote Klemmen). Die Verbindung zum Datennetzwerk (IP über 10 oder 100BaseT (abhängig vom Switch)) erfolgt über eine RJ-45-Buchse.

Für den Betrieb benötigt die IP-Schnittstelle Secure zusätzlich eine Betriebsspannung. Die IP-Schnittstelle Secure kann diese Betriebsspannung über die Netzwerkleitung aus „Power over Ethernet“ gemäß IEEE 802.3af beziehen. Alternativ kann die Betriebsspannung über den zweiten Klemmenblock (weiß-gelbe Klemmen) aus einer Sicherheitskleinspannungs-Versorgung AC/DC 24 V oder aus einer Busspannungsversorgung (unverdrosselte Spannung, DC 29 V) bezogen werden. Sobald eine Sicherheitskleinspannungs-Versorgung am zweiten Klemmenblock angeschlossen ist, wird die Betriebsspannung aus dieser bezogen.

Fernzugriff

Auch wenn keine direkte Netzwerkverbindung zwischen einem PC und einer IP-Schnittstelle Secure besteht, kann durch Verwendung der geeigneten Netzinfrastruktur von Ferne sicher auf eine KNX-Installation zugegriffen werden.

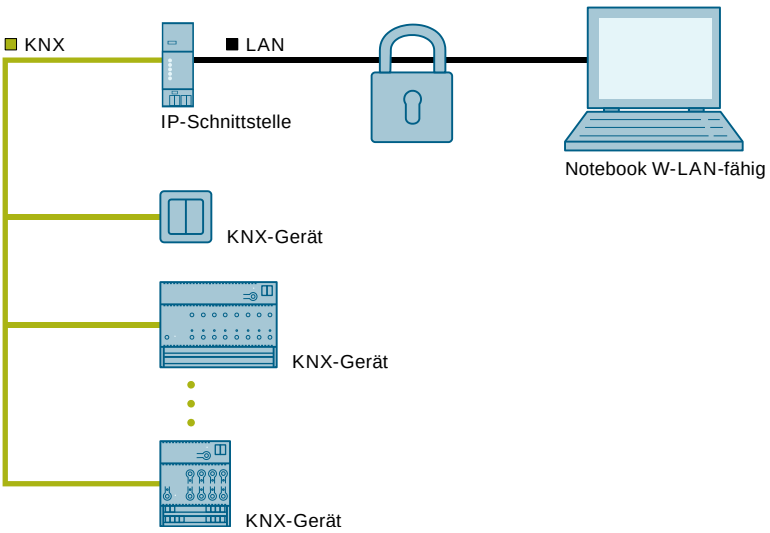

Abb. 1: Sicherer Fernzugriff

Weitere Funktionen

Die IP-Schnittstelle Secure hat folgende Merkmale:

- Einfache Anbindung an übergeordnete Systeme durch Nutzung des Internetprotokolls (IP)
- Direkter Zugriff von jedem Punkt im IP-Netzwerk auf die KNX-Installation (KNXnet/IP-Tunneling)
- Bis zu vier KNXnet/IP-Tunnelingverbindungen gleichzeitig möglich
- LED-Anzeigen für Betriebsbereitschaft, KNX-Kommunikation und IP-Kommunikation
- Einfache und sichere Konfiguration mit ETS
- Einfache Anbindung von Visualisierungssystemen und Facility-Management-Systemen
- Slot für SD-Karte (nicht in Verwendung)

3 Hinweise zur gesicherten Datenübertragung

- Gerät nur im gesicherten Modus betreiben.
- Gerät nur im gesicherten Modus direkt mit dem Internet verbinden.

  Das Gerät befindet sich im gesicherten Modus, wenn das Gerät über die sichere Inbetriebnahme in Betrieb genommen wurde, Secure Tunneling aktiviert ist und starke sowie unterschiedliche Passwörter verwendet werden.

Mögliche weitere Sicherheitsmaßnahmen sind unter anderem:

- Gerät im ungesicherten Modus nur in einer sicheren Netzwerkumgebung betreiben.
- Für die KNX-Kommunikation ein separates IP-Netzwerk mit eigener Hardware aufsetzen.
- Zugang zum (KNX-)IP-Netzwerk durch Nutzerkennungen und starke Passwörter auf einen berechtigten Personenkreis einschränken.
- Wenn das Gerät im ungesicherten Modus betrieben wird, Fernzugriffe auf das Gerät zusätzlich über eine VPN-Verbindung absichern.

  (Ein virtuelles privates Netzwerk (VPN) baut eine verschlüsselte und autorisierte Verbindung (VPN-Tunnel) von einem entfernten Ort in ein Netzwerk über das Internet auf. Diese VPN-Verbindung ermöglicht eine sichere und gegen Mithören geschützte Kommunikation zwischen einem entfernten Gerät und der KNX-Installation.)
- Wenn WLAN genutzt wird, voreingestellte SSID vom drahtlosen Access Point ändern. Das WLAN mit einem sicheren Verfahren (zurzeit z. B. WPA2) verschlüsseln.
- Netzwerkeinstellungen dokumentieren und dem Gebäudeeigentümer/-betreiber oder dem LAN-Administrator übergeben.
- Verwaltung von Zugangsrechten zu diesem KNXnet/IP-Gerät in einem IP-Netzwerk mit dem zuständigen IP-Netzwerkadministrator abstimmen.

Maßnahmen nach dem Austausch eines Geräts im Netzwerk

Wenn ein IP-Router Secure oder eine IP-Schnittstelle Secure im gesicherten Modus aus einem Netzwerk gestohlen oder aufgrund eines Defekts ausgetauscht wird, muss für alle anderen Geräte im Netzwerk die sichere Inbetriebnahme erneut durchgeführt werden. Hierzu in den Einstellungen des Projekts die Option "Sichere Inbetriebnahme" für jedes Gerät deaktivieren, wieder aktivieren und die neuen Daten erneut in die Geräte laden. (Das Laden der Daten in das Gerät zwischen der Deaktvierung und erneuten Aktivierung ist nicht erforderlich.)

Diese erneute sichere Inbetriebnahme ist erforderlich, da nicht ausgeschlossen werden kann, dass die Schlüssel, die sich in einem geschützten Bereich des Geräts befinden, ausgelesen werden können. Durch die erneute Inbetriebnahme werden neue Schlüssel generiert, die alten Schlüssel sind hiermit wertlos. Das entwendete Gerät funktioniert nun nicht mehr im Netzwerk.

Weitere Informationen zur KNX-Sicherheit

Weitere Informationen zu KNX-Sicherheit, wie z. B. eine Sicherheitscheckliste, können auf der Internetseite von KNX (http://www.knx.org) im Bereich „KNX Secure“ nachgelesen werden.

4 Gliederung der Einstellmöglichkeiten in ETS

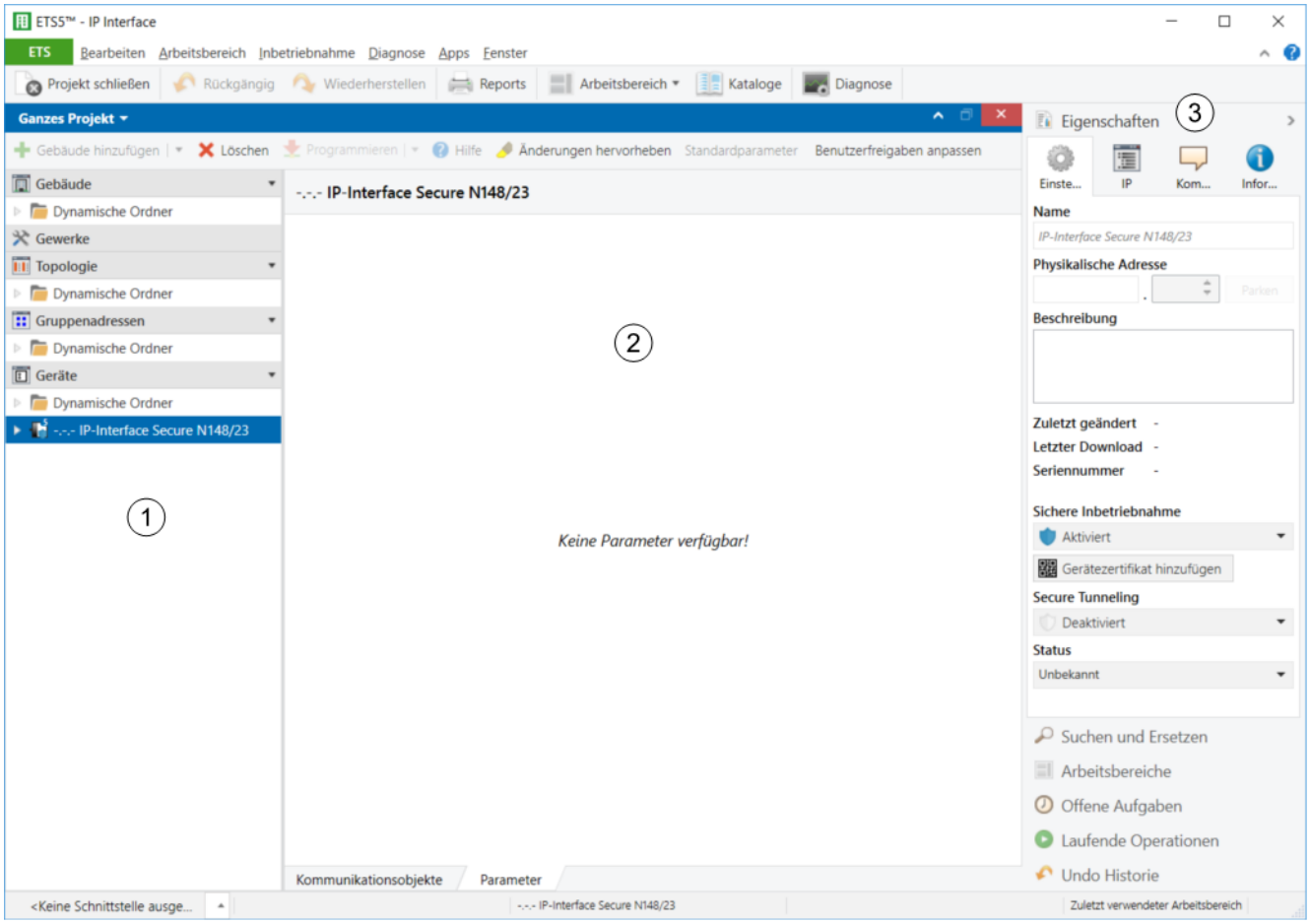

Abb. 2: Übersicht ETS

1 Baumansicht der verschiedenen Abschnitte (z. B. Geräte, Topologie, Gruppenadressen)

2 Parameterbereich

Falls für das in der Baumansicht ausgewählte Gerät Parameter vorhanden sind, können diese in diesem Bereich eingestellt, freigegeben oder gesperrt werden.

3 Bereich „Eigenschaften“ (z. B. Konfiguration von IP und Security, zusätzliche physikalische Adressen)

Parameter, die nicht der Standardeinstellung entsprechen, können mit der Schaltfläche ‚Änderungen hervorheben‘ gelb hinterlegt werden.

5 Inbetriebnahme

5.1 Funktion im Auslieferungszustand

Die Konfigurationsparameter sind im Auslieferungszustand wie folgt eingestellt:

- Physikalische Adresse der IP-Schnittstelle Secure: Einstellung: „15.15.255“ (=FFFF hex)
  - Namen und physikalische Adresse des Geräts festlegen [→ 9]
- IP-Adresszuweisung: Einstellung: „IP-Adresse automatisch beziehen“
  - IP-Adresse zuweisen [→ 9]

5.2 Lage QR-Code des Gerätezertifikats

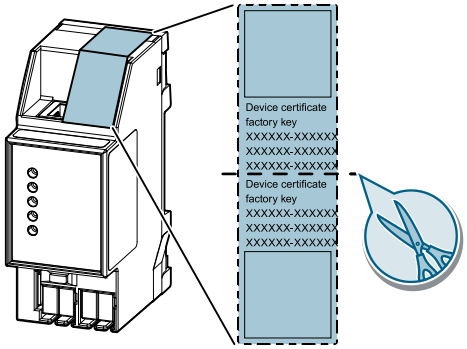

Abb. 3: Gerätezertifikat

Der QR-Code des Gerätezertifikats ist auf dem Gerät aufgeklebt. Der QR-Code ist doppelt vorhanden und kann daher zur einfacheren Inbetriebnahme abgetrennt werden.

5.3 Gerät in Betrieb nehmen

Gerät mit „KNX IP Secure“ in Betrieb nehmen

▷ Ein Projekt ist in ETS geöffnet.

1. Gerät zum Projekt hinzufügen.
   ⇨ Falls das Projekt noch nicht mit einem Passwort geschützt ist, wird das Fenster ‚Projektpasswort setzen‘ angezeigt.
2. Passwort in den Eingabefeldern ‚Neues Passwort‘ und ‚Passwort bestätigen‘ eingeben und mit ‚OK‘ bestätigen.
   ⇨ Das Fenster ‚Gerätezertifikat hinzufügen‘ wird angezeigt.
3. Falls eine Webcam vorhanden ist, Schaltfläche ‚…‘ drücken und den am Gerät aufgeklebten QR-Code einscannen.
4. Falls keine Webcam vorhanden ist oder der QR-Code nicht gelesen werden kann, auf dem Gerät aufgeklebten 6x6-stelligen Zertifikatsschlüssel eingeben.
   ⇨ Bei korrekt eingegebenem Zertifikatsschlüssel erscheint am Ende der Zeile ein grüner Haken. Zusätzlich werden die Seriennummer und der Fabrikschlüssel des Geräts angezeigt.

5. Angezeigte Seriennummer mit der auf dem Gerät aufgeklebten Seriennummer vergleichen.
   ⇨ Falls die Seriennummer nicht übereinstimmt, wurde der Zertifikatsschlüssel eines anderen Geräts eingegeben und die Übertragung von Daten wird später nicht funktionieren.
6. Eingaben mit ‚OK' bestätigen.
   ⇨ Das Gerät wurde zum Projekt hinzugefügt. Sicherheitsfunktionen von „KNX IP Secure" sind automatisch aktiviert.

Gerät ohne „KNX IP Secure" in Betrieb nehmen

Inbetriebnahme ohne „KNX IP Secure"

Alternativ kann das Gerät auch ohne KNX IP Secure in Betrieb genommen werden. In diesem Fall ist das Gerät ungesichert und verhält sich wie andere KNX-Geräte ohne die Funktion KNX IP Secure.

Zur Inbetriebnahme des Geräts ohne KNX IP Secure Gerät im Abschnitt ‚Topologie' oder ‚Geräte' markieren und im Bereich ‚Eigenschaften' in der Registerkarte ‚Einstellungen' die Option ‚Sichere Inbetriebnahme' auf ‚Deaktiviert' setzen.

5.4 Namen und physikalische Adresse des Geräts festlegen

Ein eindeutiger Name des Geräts hilft dabei, das Gerät in einer KNXnet/IP-Visualisierung oder innerhalb eines Projekts in ETS eindeutig wiederzuerkennen und zu finden.

▷ Das Gerät wurde zum Projekt hinzugefügt.

1. Gerät im Abschnitt ‚Topologie' oder ‚Geräte' auswählen.
2. Im Bereich ‚Eigenschaften' in die Registerkarte ‚Einstellungen' wechseln.
3. Im Eingabefeld ‚Name' einen eindeutigen Namen mit maximal 30 Zeichen für das ausgewählte Gerät eingeben.
4. Im Eingabefeld ‚Physikalische Adresse' die physikalische Adresse des Geräts eingeben. Die Adresse darf noch nicht vergeben sein.
   ⇨ Die Einstellungen werden automatisch gespeichert.

5.5 IP-Adresse zuweisen

Für Details zur IP-Adresse und zu weiteren Netzwerkeinstellungen lokalen Netzwerkadministrator kontaktieren.

▷ Das Gerät wurde zum Projekt hinzugefügt.

1. Gerät im Abschnitt ‚Topologie' oder ‚Geräte' auswählen.
2. Im Bereich ‚Eigenschaften' in die Registerkarte ‚IP' wechseln.
3. Einstellungen zur IP-Adresse wie gewünscht vornehmen.

   ⇨ Die Einstellungen werden automatisch gespeichert.

Folgende Einstellungen sind möglich:

- **IP-Adresse automatisch beziehen**
  Bei Auswahl dieser Option wird dem Gerät automatisch eine IP-Adresse zugewiesen. Dies geschieht entweder über einen DHCP-Dienst im Netzwerk oder, falls kein DHCP-Dienst konfiguriert wurde, über das Gerät selbst (AutoIP). Die zur Konfiguration des DHCP-Diensts benötigte MAC-Adresse des Geräts kann unterhalb dieser Einstellmöglichkeit oder direkt am Gerät von einem Aufkleber abgelesen werden.
- **Feste IP-Adresse verwenden**
  Bei Auswahl dieser Option werden weitere Eingabefelder eingeblendet, in denen die gewünschte IP-Adresse für das Gerät sowie die Subnetzmaske und der Standardgateway eingegeben werden können.

5.6 Zusätzliche physikalische Adressen einrichten

Für eine stabile Kommunikation des Geräts über KNXnet/IP-Tunneling muss das Gerät für jede Verbindung eine eigene physikalische Adresse verwenden.

Diese zusätzlichen Adressen dürfen nicht mit der physikalischen Adresse des Geräts identisch sein und dürfen auch von keinem anderen Busgerät verwendet werden.

Beim Einfügen des Geräts in ein Projekt in ETS werden automatisch zusätzliche physikalische Adressen für das Gerät angelegt, die bei Bedarf geändert werden können.

Weitere Informationen zur Vergabe und zur Änderung von physikalischen Adressen können in der Hilfe der ETS-Software nachgelesen werden.

Das Zurücksetzen der physikalischen Adressen erfolgt bei der Zurücksetzung des gesamten Geräts in den Auslieferungszustand: Gerät in den Auslieferungszustand zurücksetzen [➞ 12]

6 Hilfe bei Fehlern und Problemen

6.1 Häufige Fragen

Häufige Fragen

Für häufige Fragen zum Produkt und deren Lösung siehe:
https://support.industry.siemens.com/cs/ww/en/ps/faq

FAQ

6.2 Mögliche Fehler

Fehler	Abhilfe
Gerätezertifikate sind fehlerhaft	Gerätezertifikate überprüfen [→ 11]
Physikalische Adressen wurden mehrfach verwendet	Physikalische Adressen prüfen und/oder zurücksetzen und neu vergeben Zusätzliche physikalische Adressen einrichten [→ 10] Fehleranalyse mit Hilfe von ETS [→ 11]

Tab. 1: Mögliche Fehler

6.3 Fehleranalyse mit Hilfe von ETS

Zur Fehleranalyse in ETS gibt es u. a. folgende Möglichkeiten:

Bereich ‚Diagnose'

In diesem Bereich können u. a. physikalische Adressen, der Gruppenmonitor und der Busmonitor überprüft werden.

Bereich ‚Reports':

In diesem Bereich können Details zu verschiedenen Bereichen des Projekts als Datei exportiert oder direkt gedruckt werden.

Für weitere Informationen zu ETS siehe Online-Hilfe der ETS-Software.

6.4 Gerätezertifikate überprüfen

1. Schaltfläche ‚ETS' in der Menüleiste drücken.
2. Projekt aus der Liste auswählen.
   ⇨ Auf der rechten Seite werden Details zum Projekt angezeigt.
3. Registerkarte ‚Sicherheit' auswählen.
   ⇨ Eine Liste der zum Projekt gehörenden Gerätezertifikate wird angezeigt.

7 Gerät in den Auslieferungszustand zurücksetzen

!	*HINWEIS*
	Datenverlust durch Zurücksetzen des Geräts! Beim Zurücksetzen des Geräts werden alle eingegebenen Parameter und vorgenommenen Einstellungen gelöscht. • Sicherstellen, dass das Gerät wirklich zurückgesetzt werden soll.

Gerät in den Auslieferungszustand zurücksetzen

- Lerntaste drücken (mindestens 20 Sekunden), bis die Programmier-LED anfängt, schnell zu blinken.

⇨ Die Programmier-LED blinkt für 8 Sekunden.

⇨ Das Gerät wurde in den Auslieferungszustand zurückgesetzt. Alle Parametereinstellungen wurden gelöscht.

Stichwortverzeichnis

Herausgegeben von
Siemens Schweiz AG
Smart Infrastructure
Global Headquarters
Theilerstrasse 1a
CH-6300 Zug
+41 58 724 2424
www.siemens.com/buildingtechnologies