isH4Cube

HANDBUCH

THORSIS TECHNOLOGIES

EG-KONFORMITÄTSERKLÄRUNG

Hiermit erklären wir, dass das nachstehend bezeichnete Gerät in seiner Konzeption und Bauart sowie in der von uns in Verkehr gebrachten Ausführung den grundlegenden Sicherheits- und Gesundheitsanforderungen der EG-Richtlinie 2014/30/EU entspricht. Die Produkte enthalten keine der durch EU-Richtlinie 2002/95/EG (RoHS) und 2011/65/EU (RoHS II) verbotenen Stoffe, sowie keine Stoffe der REACH-Kandidatenliste in Konzentrationen > 0,1%.
(Stoffe siehe https://echa.europa.eu/candidate-list-table)
Alle angewendeten RoHS-Ausnahmen gemäß Annex III von 2011/65/EU (RoHS II) sind auf Seite 22 dieses Handbuchs eingetragen.

⚠ **BEI EINER MIT DER THORSIS TECHNOLOGIES GMBH NICHT ABGESTIMMTEN ÄNDERUNG DER GERÄTE VERLIERT DIESE ERKLÄRUNG IHRE GÜLTIGKEIT!**

Produktname	Bestellnummer
isH4Cube	14400-0201

ANGEWANDTE NORM: DIN EN IEC 61326-1:2022-11

Hersteller
Thorsis Technologies GmbH
Oststr. 18
39114 Magdeburg

Magdeburg, 01.04.2026

Dipl.-Inf. Michael Huschke,
Geschäftsführer

BRITISCHE KONFORMITÄTSERKLÄRUNG

Die Thorsis Technologies GmbH erklärt als Hersteller in alleiniger Verantwortung, dass die in der Liste aufgeführten Produkte mit den Anforderungen der folgenden britischen Gesetzgebung übereinstimmen:

- S.I. 2019/1246 The Product Safety, Metrology and Mutual Recognition Agreement (Amendment)(EU Exit) regulations 2019
- S.I. 2020/852 The Product Safety and Metrology (Amendment)(EU Exit) regulations 2020
- S.I. 2016/1091The Electromagnetic Compatibility Regulations 2016
- S.I. 2012/3032 The Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment Regulations 2012

Produktname	Bestellnummer
isH4Cube	14400-0201

BEI EINER MIT DER THORSIS TECHNOLOGIES GMBH NICHT ABGESTIMMTEN ÄNDERUNG DER GERÄTE VERLIERT DIESE ERKLÄRUNG IHRE GÜLTIGKEIT!

ANGEWANDTE NORM: DIN EN IEC 61326-1:2022-11
ZERTIFIZIERUNG: KEINE

Hersteller
Thorsis Technologies GmbH
Oststr. 18
39114 Magdeburg
Deutschland

Magdeburg, 01.03.2026

Dipl.-Inf. Michael Huschke,
Geschäftsführer

UK CA

Inhaltsverzeichnis

1. EINLEITUNG 5
1.1 **Technische Details** 5
1.2 **Abmessungen** 6
1.3 **Anschlussbelegung** 7
1.4 **Schematische Darstellung der Eingangsschaltung** 7
1.5 **LEDs** 8
1.6 **Auf Werkseinstellungen zurücksetzen** 9

2. HARDWARE INSTALLATION 10
2.1 **Sicherheitshinweise** 10
2.2 **Besondere Nutzungsbedingungen** 11
2.3 **Elektrische Installation** 11
2.4 **isH4Cube Funktionsprinzip** 12
2.4 **Anschlussbeispiele von HART-Geräten an den isH4Cube** . . 13

3. WEB OBERFLÄCHE 14
3.1 **Konfiguration der IP-Adresse** 14
3.2 **Aktualisierung der Firmware** 15
3.3 **Systemneustart** 15
3.4 **Passwortschutz** 16
3.5 **Aktivierung der MODBUS Funktion** 17
3.6 **Protokolle** 18
3.6.1 Modbus Status 18
3.6.2 HART over IP 19
3.6.3 FDI Server 20
3.7 **Geräteliste** 21
3.8 **HART Protokollmonitor** 21

4. INTEGRATION IN ABB FIM 22
4.1 **Hinzufügen des Kommunikationsservers** 22
4.2 **Zertifikate austauschen** 25
4.3 **Kommunikationsserver in FIM hinzufügen** 28
4.4 **Geräte erkennen** 29

5. ERKLÄRUNG ZUR ROHS-KONFORMITÄT 22

6. HANDBUCH AKTUALISIERUNG 23

1. Einleitung

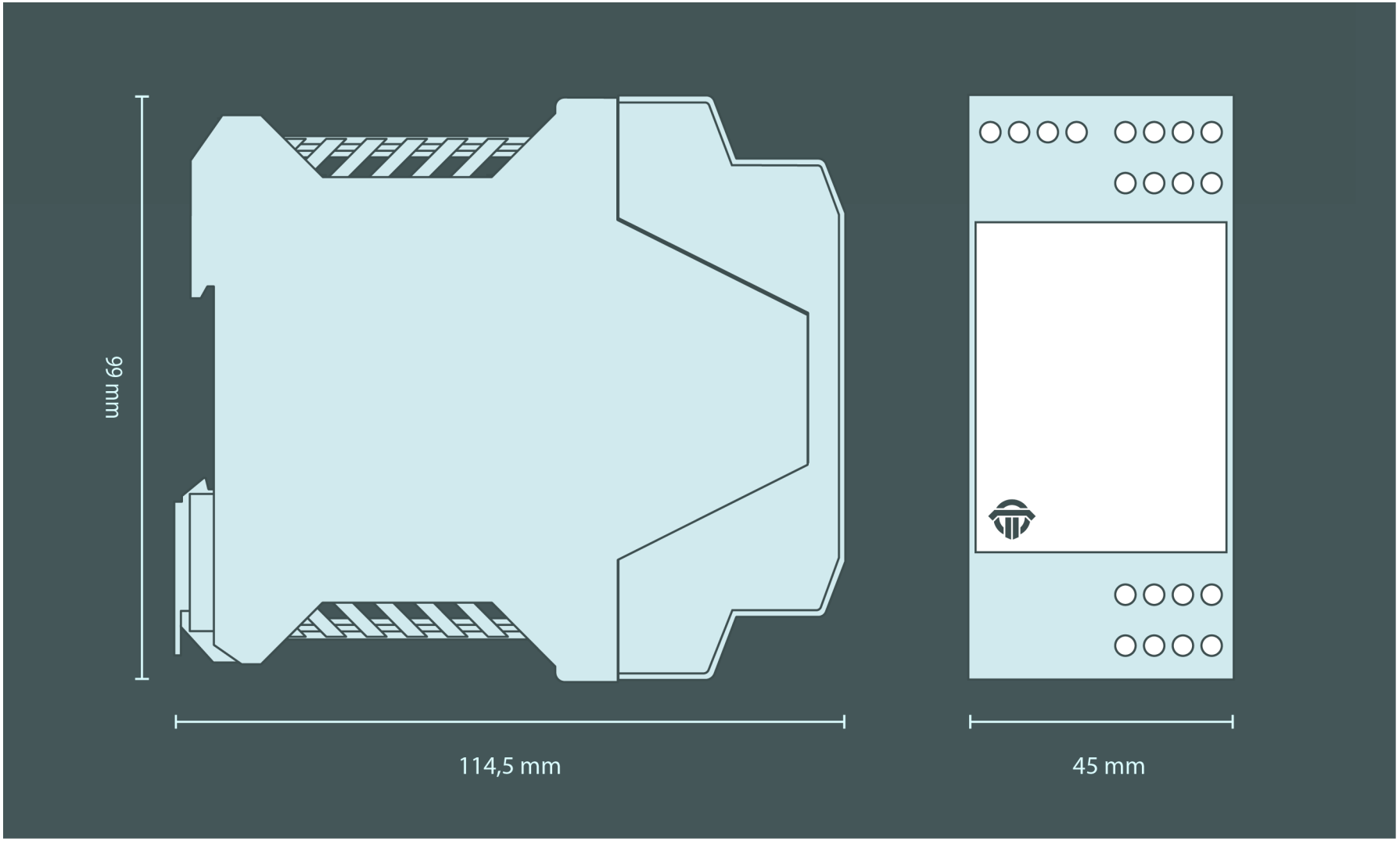
Das isH4Cube ist ein Gateway für den Anschluss von HART Feldgeräten an ein Ethernet-Netzwerk. Es konvertiert das HART Protokoll in eine Reihe von unterschiedlicher Ethernetprotokolle wie z.B. HART-IP, Modbus-TCP oder Profinet.

Das Gateway verfügt über 4 HART-Anschlüsse, die jeweils mit einem separaten HART-Modem ausgestattet sind. Dadurch können die 4 Kanäle unabhängig voneinander betrieben werden. Durch die parallele Verarbeitung von HART-Anfragen auf verschiedenen Kanälen wird die Systemleistung deutlich gesteigert.
Alle 4 Kanäle sind galvanisch getrennt und bieten einen optional nutzbaren 240-Ohm-Schleifenwiderstand.

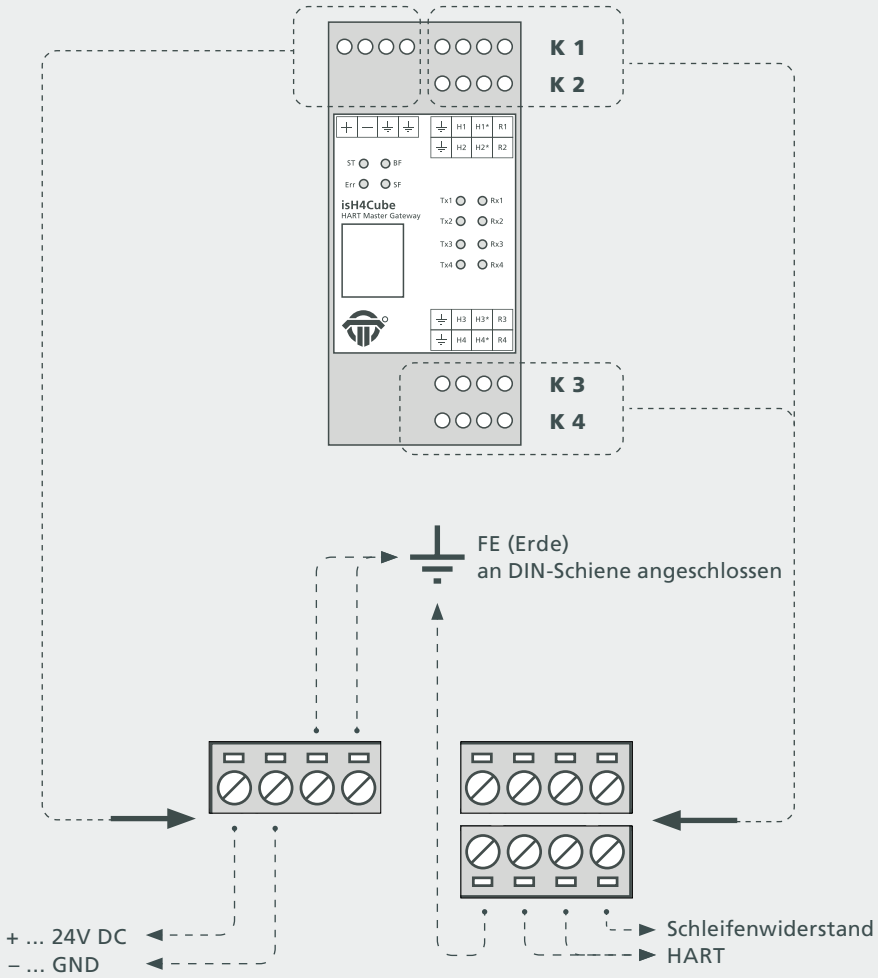
1.1 Technische Details

isH4Cube	
Bestellnummer	**14400-0201**
Prozessor	ATSAM9X60D
RAM	64 MByte
Flash	256 MByte
Übertragungsrate	Ethernet: 10 Mbit/s – 100 Mbit/s HART: 1200 Bit/s
Stromversorgung	19,2V .. 30V DC
Leistungsaufnahme	60mA (typ. bei 24V DC)
galvanische Trennung	ja
Schutzart	IP20
Gehäusematerial	Polyamide
Abmessungen (L x W x H)	114,5mm x 45mm x 99mm
Gewicht	ca. 200g
Betriebstemperatur	- 20° C <= T_{amb} <= 70° C / -4° F <= T_{amb} <= 158° F
Lagertemperatur	- 40° C <= T_{amb} <= 85° C / - 40° F <= T_{amb} <= 185° F

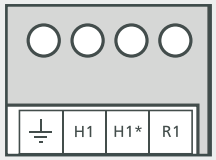
1.2 Abmessungen

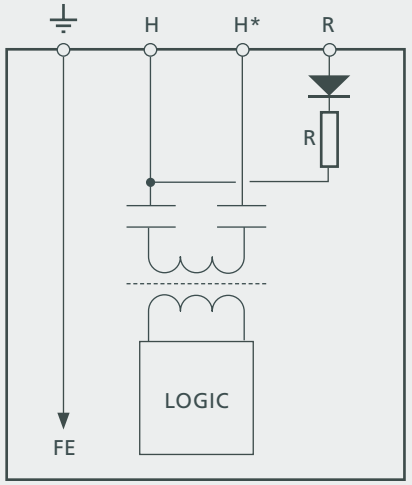


1.3 Anschlussbelegung



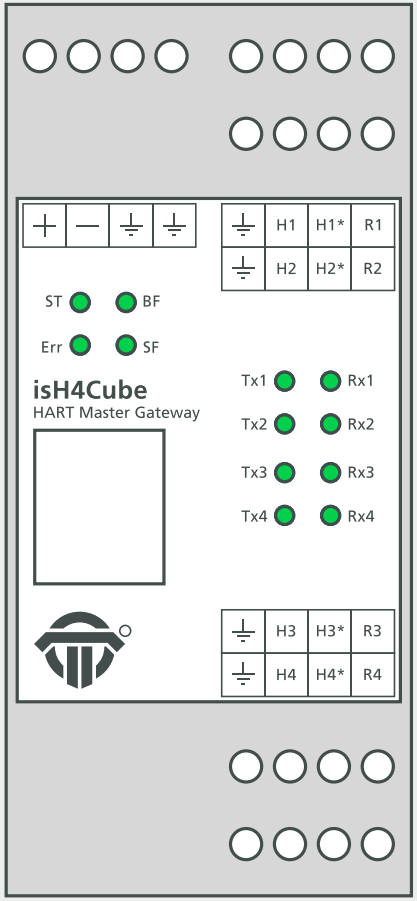
1.4 Schematische Darstellung der Eingangsschaltung





R.. Schleifenwiderstand (240 Ohm)

1.5 LEDs



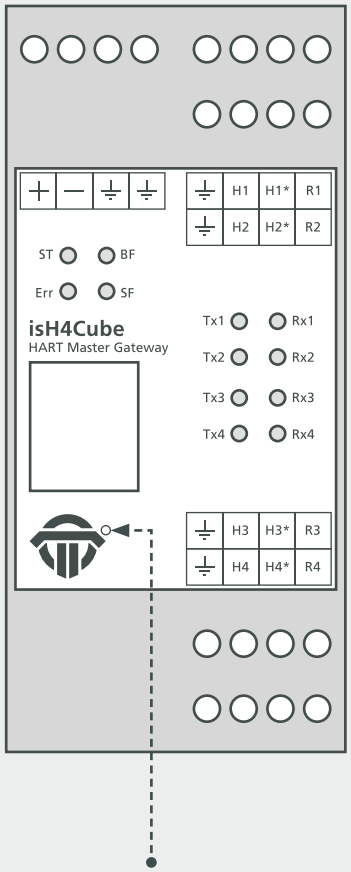
Der isH4Cube verfügt über 12 LEDs. Vier davon zeigen den Status des Gateways an, die übrigen acht LEDs den Status der einzelnen Kanäle (jeweils zwei LEDs pro Kanal).

- **ST:** Status LED, leuchtet nach dem Einschalten rot, wechselt dann im Betrieb auf Grün.
- **Err:** Error LED, leuchtet rot bei einem Anwendungsfehler
- **BF:** Busfehler (Profinet)
- **SF:** Systemfehler (Profinet)

Nach dem Einschalten leuchten alle vier LEDs etwa eine Sekunde lang rot und wechseln dann auf Grün. Während des Bootvorgangs erlischt eine LED nach der anderen, bis nur noch die ST-LED grün leuchtet. Damit ist der Bootvorgang abgeschlossen.

- **TX1-TX4:** Grün - Das Gateway sendet eine HART-Nachricht.
- **RX1-RX4:** Grün - Das Gateway empfängt eine HART-Nachricht.

1.6 Auf Werkseinstellung zurücksetzen



Für den Fall, dass ein Benutzer alle Einstellungen des Gerätes auf den Auslieferungszustand zurücksetzen muss, befindet sich auf dem Gerät eine Reset-Taste. Diese Taste befindet sich hinter einer kleinen Öffnung unterhalb des RJ45-Anschlusses.
Das Zurücksetzen auf Werkeinstellung kann z.B. notwendig sein, falls ein Benutzer die IP-Adresse oder das Passwort geändert hat und sich dann nicht mehr daran erinnern kann. Ein anderes Beispiel, bei dem das Zurücksetzen auf Werkseinstellung hilfreich sein kann ist, wenn die IP-Adresse auf DHCP eingestellt wurde, aber gar kein DHCP-Server im Netz verfügbar ist. In einem solchen Fall hilft ein Rücksetzen auf Werkseinstellungen, um wieder auf die Weboberfläche das Gateways zugreifen zu können.

Auf Werkseinstellungen zurücksetzen

Möchte man nur die Einstellungen zurücksetzen, so muss man die Reset-Taste im laufenden Betrieb für mindestens 5 Sekunden drücken. Anschließend startet das Gerät neu und alle Einstellungen werden gelöscht. Die IP-Adresse hat dann wieder den Standardwert 192.168.0.10 und alle Einstellungen befinden sich wieder im Auslieferungszustand.

Firmware-Wiederherstellung

Sollte nach (z.B.) einem fehlgeschlagenen Firmwareupdate das Gateway überhaupt nicht mehr starten, so kann man mit der Reset-Taste auch den alten Stand der Firmware wiederherstellen.
Um die Firmware vollständig zurückzusetzen, gehen Sie wie folgt vor:

- Schalten Sie das Gerät aus.
- Drücken Sie die Taste (z. B. mit einer Büroklammer) und halten Sie sie gedrückt.
- Schalten Sie das Gerät wieder ein, während Sie die Reset-Taste weiterhin gedrückt halten.
- Warten Sie mindestens 5 Sekunden, bevor Sie die Reset-Taste loslassen.

Nach dem Loslassen der Reset-Taste benötigt die Firmware einige Zeit, um auf die Werkseinstellungen zurückgesetzt zu werden. Trennen Sie das Gerät nicht vom Stromnetz. Nach der Firmware-Wiederherstellung befinden sich alle Einstellungen und die Firmware-Version wieder im Auslieferungszustand. Das bedeutet, dass alle Firmware-Updates rückgängig gemacht wurden und erneut installiert werden müssen.

2. Hardware Installation

2.1 Sicherheitshinweise

Installationshinweise

Installation, Betrieb und Wartung dürfen nur von qualifiziertem Personal und in Übereinstimmung mit Ihren örtlichen und nationalen technischen Vorschriften und Sicherheitsrichtlinien durchgeführt werden.

Reparieren Sie das Gerät nicht selbst, sondern ersetzen Sie es durch ein gleichwertiges Gerät.
Reparaturen dürfen nur vom Hersteller durchgeführt werden.

Der Hersteller haftet nicht für Schäden, die durch Nichtbeachtung entstehen.

2.2 Besondere Nutzungsbedingungen

Das Gerät muss in einem Gehäuse installiert werden, das einen Schutzgrad von mindestens IP 54 gemäß IEC/EN 60079-15 bietet und das im normalen Betrieb ohne Verwendung eines Werkzeugs als nicht zugänglich angesehen wird.

Es ist ein Überspannungsschutz vorzusehen, der auf höchstens 140 % des Spitzenwerts der Nennspannung an den Versorgungsanschlüssen des Geräts eingestellt ist.

Der isH4Cube muss senkrecht auf einer 35 mm DIN-Schiene montiert werden.

Der isH4Cube ist ein offenes System und gemäß UL/CSA-Zulassung ein „offener Typ“. Die Module müssen in einem Schaltschrank, einem geeigneten Gehäuse oder einem geschlossenen elektrischen Betriebsraum installiert werden, der nur autorisiertem Wartungspersonal zugänglich ist.

2.3 Elektrische Installation

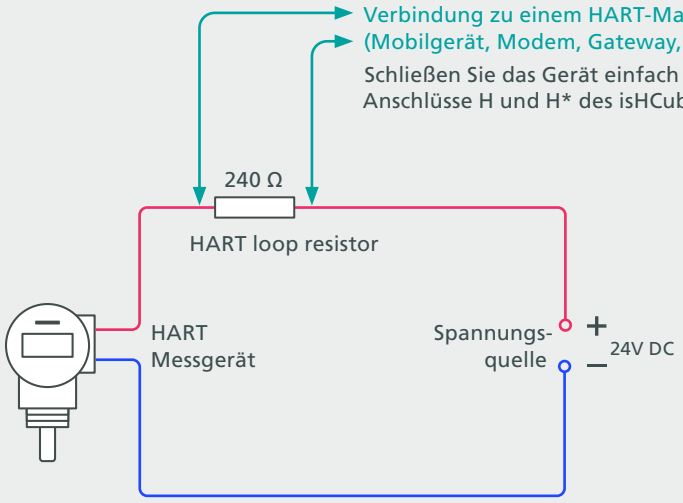
Stellen Sie vor der Installation der Module und der Verkabelung sicher, dass das System stromlos ist.

Zur Versorgung der Module dürfen nur Stromversorgungen mit einer sicheren, galvanisch getrennten Kleinspannung (SELV) verwendet werden.

Kabeleinführungen und Feldverdrahtung müssen für eine Betriebstemperatur von mindestens +20° C über der Umgebungstemperatur geeignet sein.

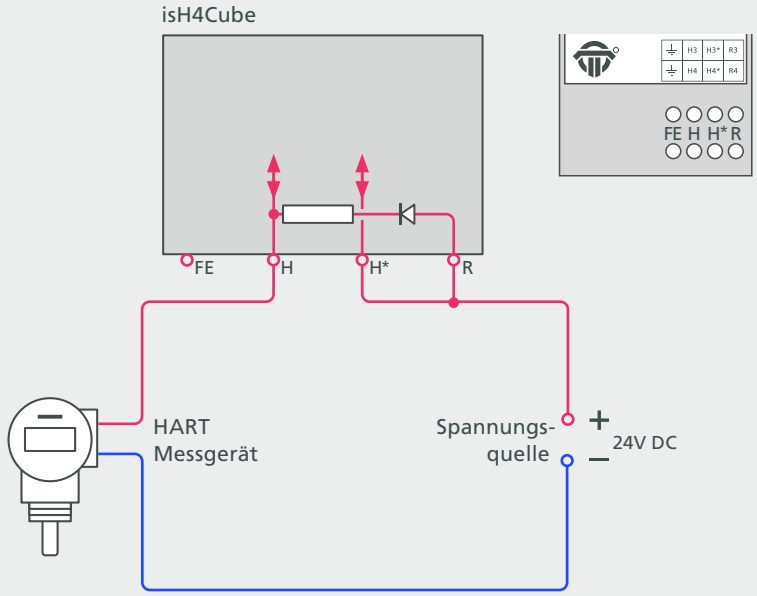
2.4 isH4Cube Funktionsprinzip

Die Illustration zeigt einen schematischen Aufbau einer einfachen HART-Schleife.



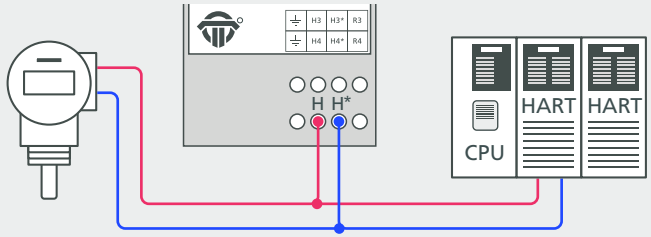
Jede HART-Schleife besteht (mindestens) aus einer Spannungsquelle, einem HART-Schleifenwiderstand und einem HART-Messgerät, die in Reihe geschaltet sind.

Die Illustration zeigt eine mögliche Einbindung des isH4Cube in eine HART-Schleife.

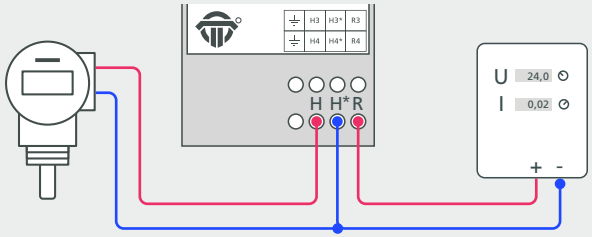


Bei Verwendung des isH4Cube kann die HART-Schleife den internen Widerstand nutzen, der über den R-Anschluss des isH4Cube's bereitgestellt wird.

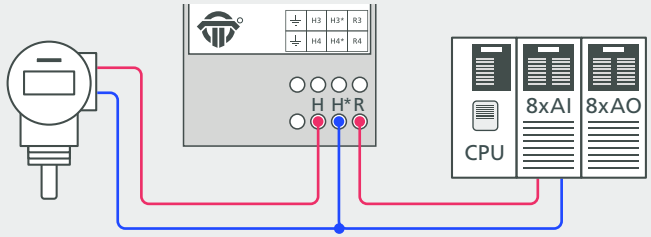
2.5 Anschlussbeispiele von HART-Geräten an den isH4Cube



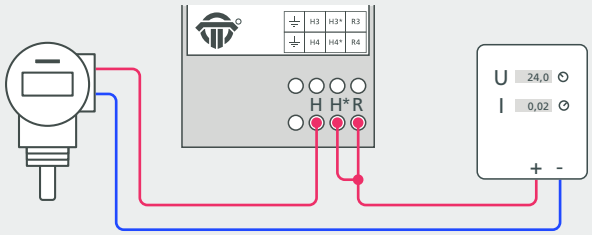
SPS mit integriertem
HART-Schleifenwiderstand



Spannungsquelle



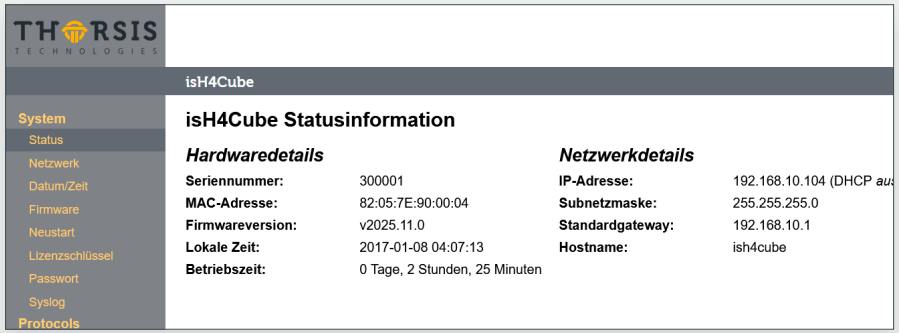
SPS ohne integriertem
HART-Schleifenwiderstand



Spannungsquelle

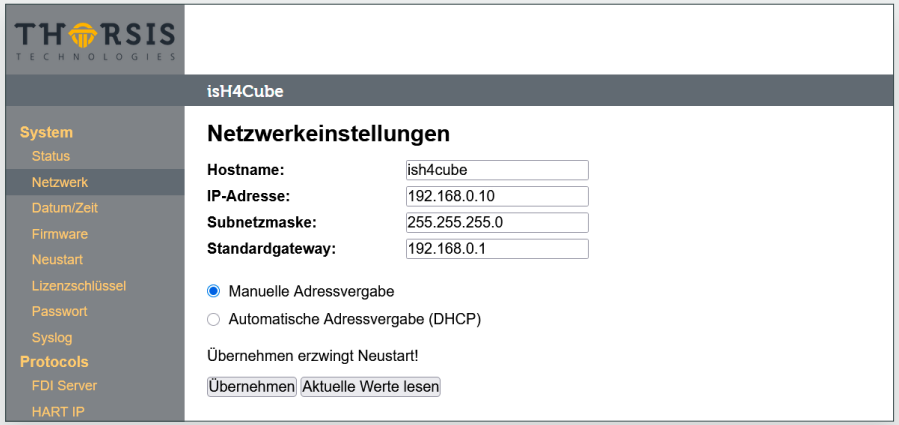
3. Web Oberfläche

3.1 Konfiguration der IP-Adresse



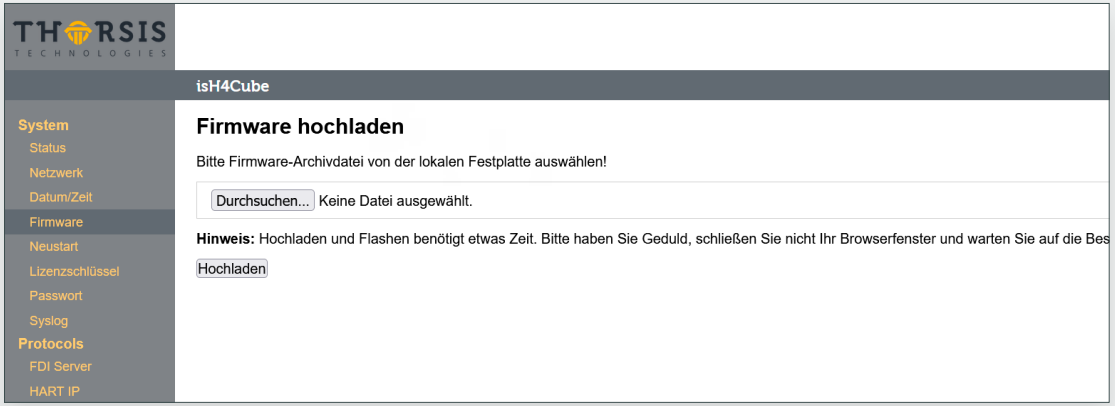
Die IP-Adresse des Gateways im Auslieferungszustand lautet: 192.168.0.10 Subnetzmaske 255.255.255.0
Geben Sie in einem beliebigen Browser die IP-Adresse des isH4Cubes ein. Sie sollten nun diese Website sehen.
Dies ist eine Übersicht über den aktuellen Status.

Klicken Sie auf „Netzwerk“ und Sie gelangen zur Konfigurationsmaske.



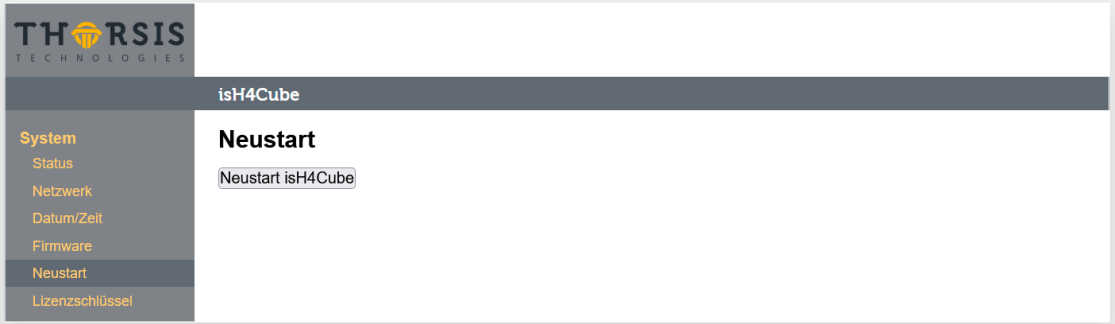
Hier können Sie den Hostnamen, die IP-Adresse, die Subnetzmaske und das Standard-Gateway ändern. Sie können die IP-Adresse manuell festlegen oder durch einen DHCP-Server zuweisen lassen. Durch Drücken der Schaltfläche “Übernehmen” werden die Änderungen übernommen.

3.2 Update der Firmware



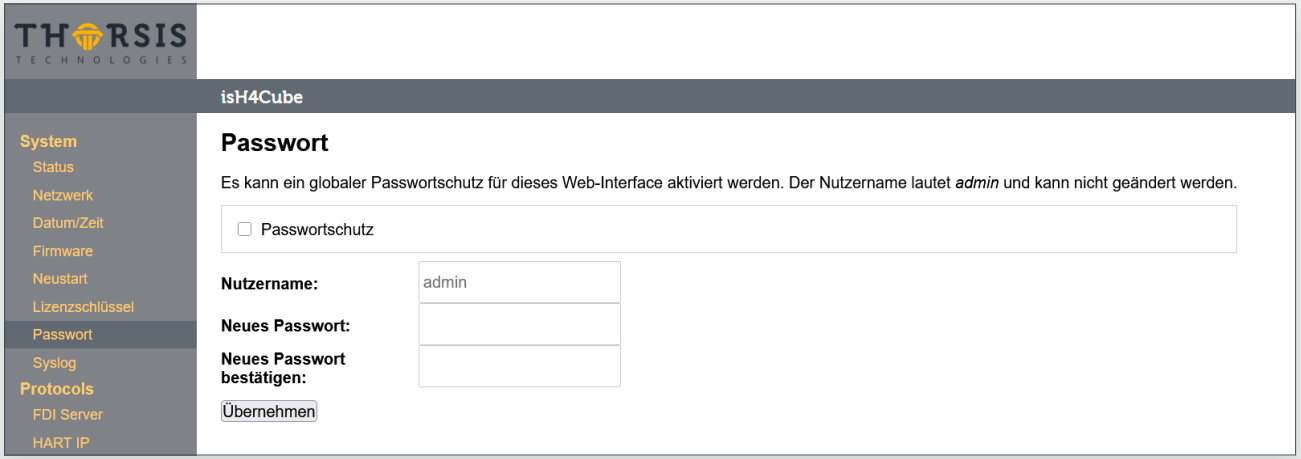
Wenn für Ihr Gerät eine neue Firmware verfügbar ist, können Sie diese über die Weboberfläche flashen. Gehen Sie zum Menü Firmware und wählen Sie die Datei aus, die Sie flashen möchten. Klicken Sie auf die Schaltfläche Hochladen und warten Sie, bis eine Bestätigung angezeigt wird, dass der Upload erfolgreich war. Nach dem erfolgreichen Update muss der isH4Cube über die Restart-Funktion in der Weboberfläche neu gestartet werden.

3.3 Systemneustart



Um das Gateway neu zu starten, rufen Sie das Restart-Menü auf und klicken Sie auf die Schaltfläche „Neustart isH4Cube“.

3.4 Passwortschutz



Um einen globalen Kennwortschutz für die Weboberfläche zu aktivieren, klicken Sie links auf das Menü Kennwort.

Aktivieren Sie den Passwortschutz, indem Sie in das Kontrollkästchen klicken. Geben Sie Ihr Passwort ein und wiederholen Sie es im Feld darunter.

Klicken Sie auf die Schaltfläche „Übernehmen“, um Ihre Einstellungen zu bestätigen.

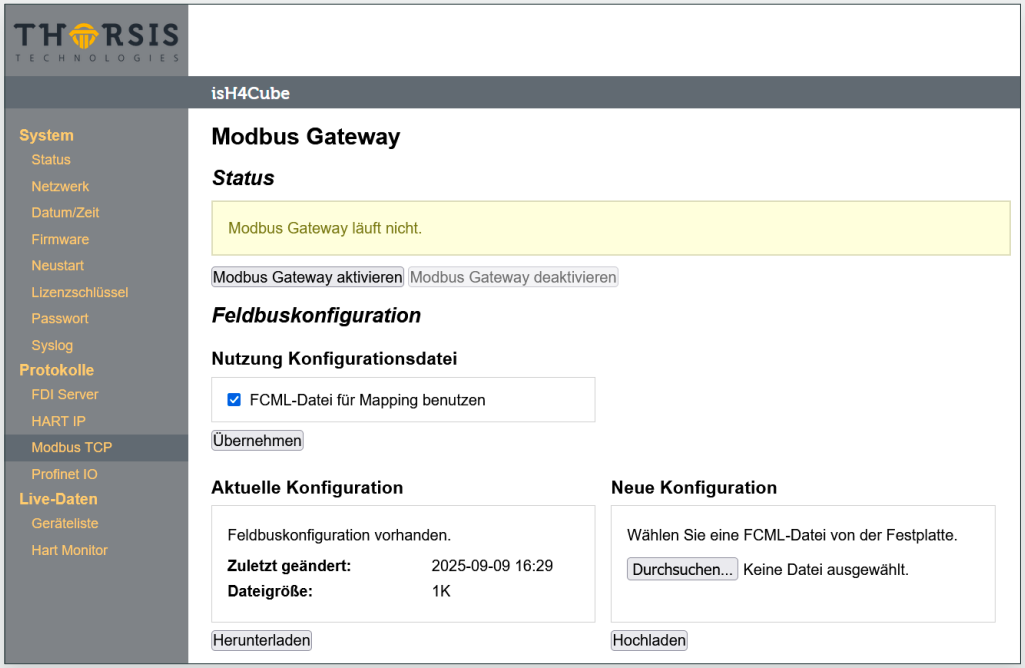
Bitte beachten Sie, dass der Benutzername immer *admin* ist und nicht geändert werden kann.

3.5 Aktivierung der MODBUS Funktion

Um die MODBUS-Funktionalität freizuschalten, müssen Sie einen gültigen Lizenzcode eingeben. Gehen Sie zur Seite Lizenzschlüssel und geben Sie den Schlüssel ein. Nachdem Sie auf Übernehmen geklickt haben, wird die MODBUS-Funktion aktiviert.
Aktivieren Sie das MODUBS-Gateway, indem Sie zum Menüpunkt „Modbus TCP“ wechseln.

3.6 Protokolle

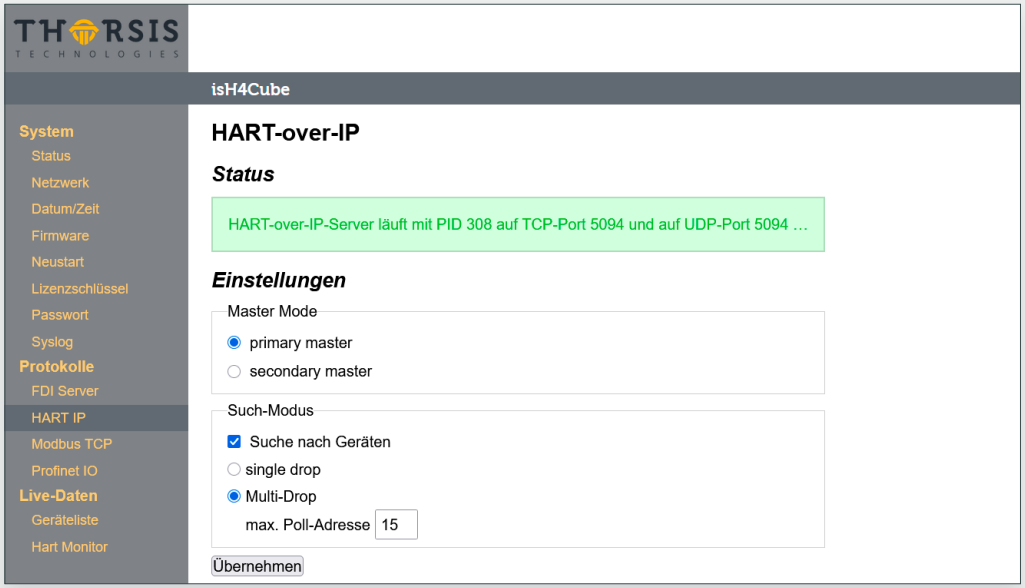
3.6.1 Modbus Status



Das Menü MODBUS Gate zeigt eine Übersicht über den MODBUS-Status. Hier können Sie eine FCML-Konfigurationsdatei hochladen, und Sie können den Modbus-Server starten oder stoppen.

Bitte beachten Sie, dass der Modbus-Server nicht zeitgleich mit dem FDI Communication Server oder der Profinet Funktion laufen kann. Vor dem Starten des Modbus Servers beenden Sie ggf. erst diese anderen Dienste.

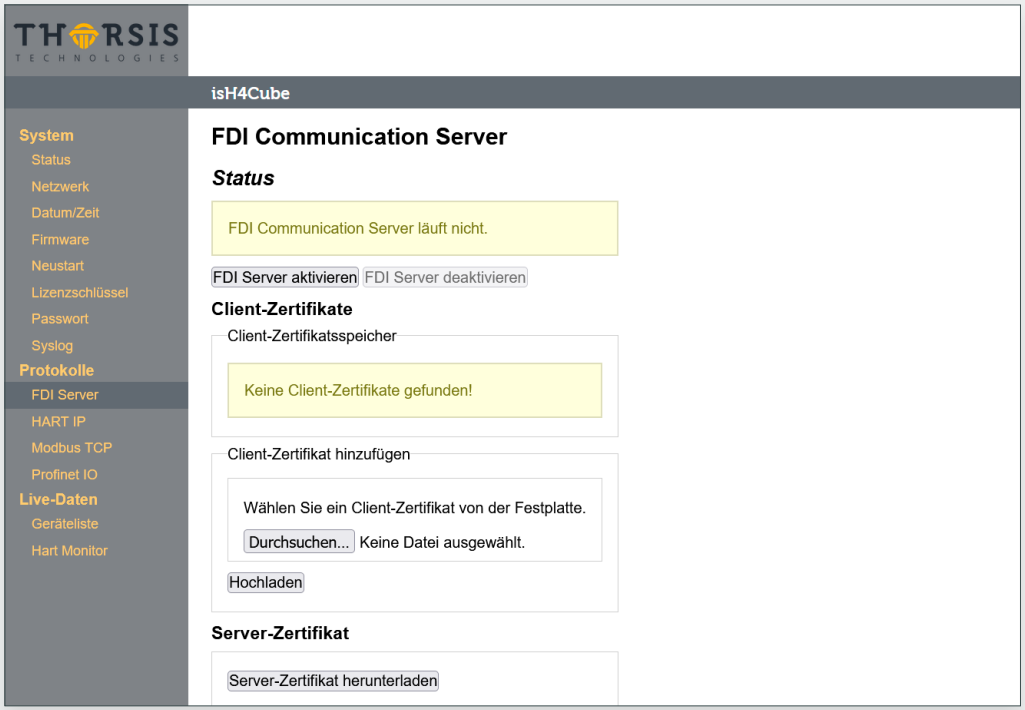
3.6.2 HART over IP



Aktivieren oder deaktivieren Sie HART-over-IP auf dieser Seite. Sie können ausserdem den Mastertyp auf den 4 Kanälen als Primary Master oder als Secondary Master einstellen.

Wenn die Checkbox „Suche nach Geräten" aktiviert wird, dann sucht das Gateway permanent auf den 4 HART-Kanälen nach angeschlossenen HART-Geräten. Stellen Sie dazu auch den Bereich der Polladressen ein, der in diese Suche einbezogen werden soll.

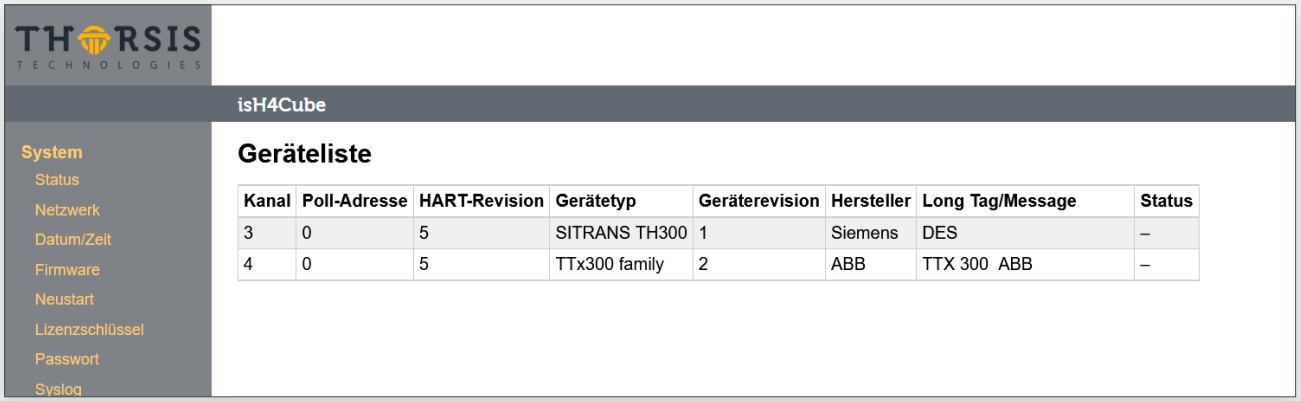
3.6.3 FDI Server



Unter dem Menüpunkt “FDI Server” können Sie Einstellungen vornehmen, um über den neuen FDI Standard auf Feldgeräte zuzugreifen. Dazu gehört der Austausch der Zertifikate.
Ausserdem können Sie auf dieser Seite den FDI Server starten oder stoppen.

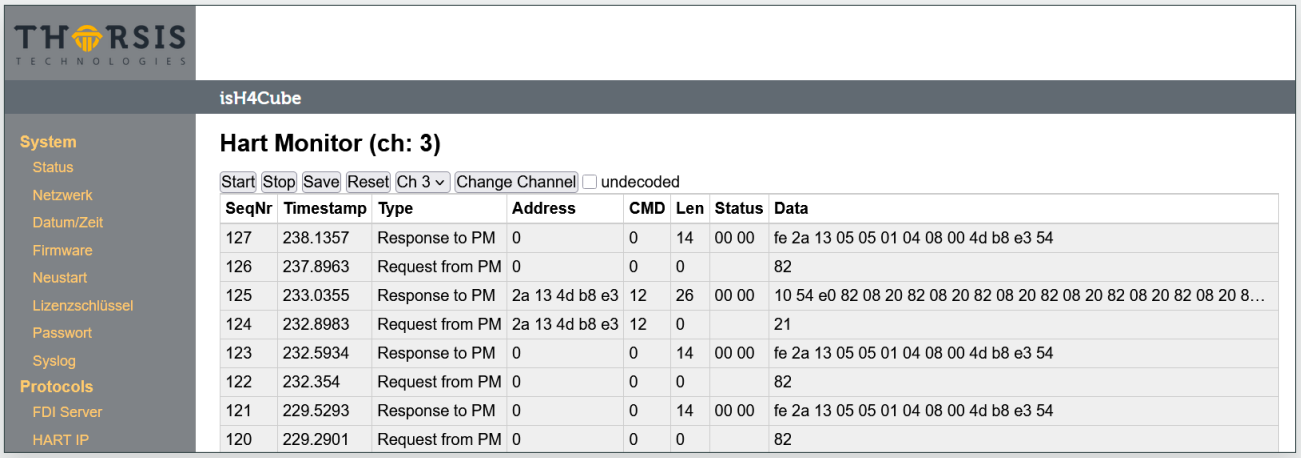
Beachten Sie bitte, dass der FDI Server nicht gleichzeitig mit aktivierter Modbus- oder Profinet-Funktion laufen kann. Beenden Sie ggf. diese Dienste vor dem Start des FDI Servers.

3.7 Geräte Liste



Der isH4Cube überwacht alle Kanäle auf angeschlossene HART Geräte. Alle an einem der 4 Kanäle gefundenen HART-Geräte werden auf dieser Seite angezeigt.

3.8 HART Protokollmonitor



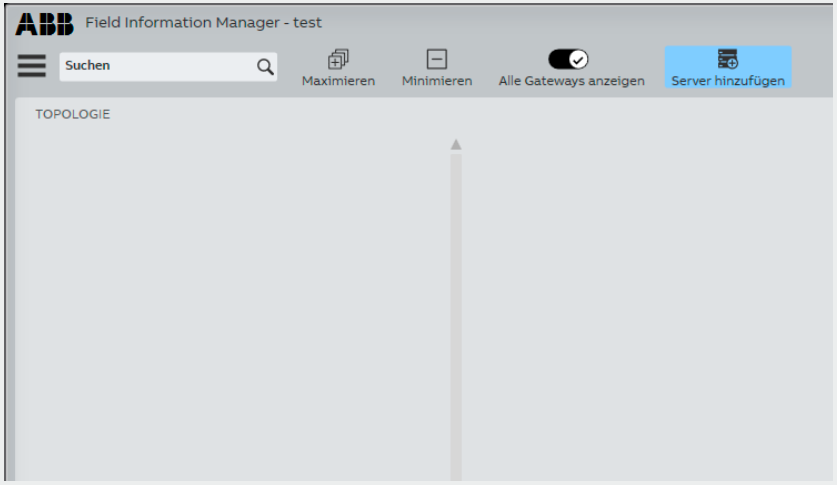
Zur Diagnose oder zur Ursachensuche bei Kommunikationsproblemen hat des isH4Cube einen eingebauten Protokollmonitor. Dieser Protokollmonitor zeigt alle HART Nachrichten von einem der 4 Kanäle auf dieser Seite an. Sie Können den Kanal auswählen, der überwacht werden soll. Es kann immer nur 1 Kanal überwacht werden.

4. Integration in ABB FIM

4.1 Hinzufügen des Kommunikationsservers

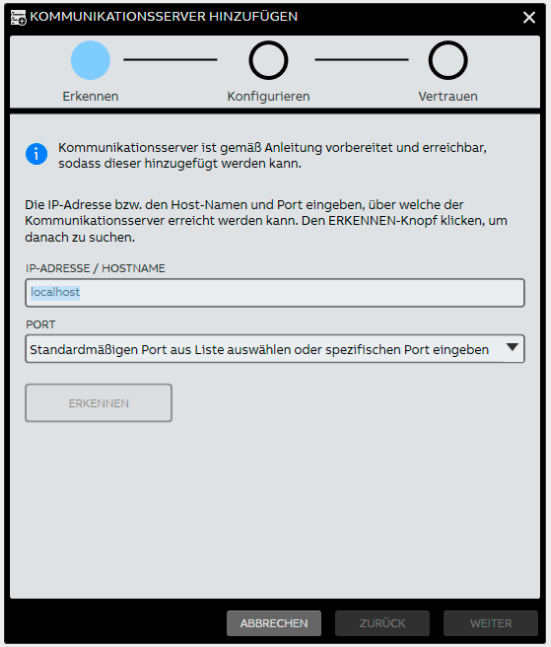
Schritt 1 – Kommunikationsserver hinzufügen

Öffnen Sie im ABB Field Information Manager die Ansicht Topology. Klicken Sie anschließend in der Symbolleiste auf Server hinzufügen, um einen neuen Kommunikationsserver zum Projekt hinzuzufügen.



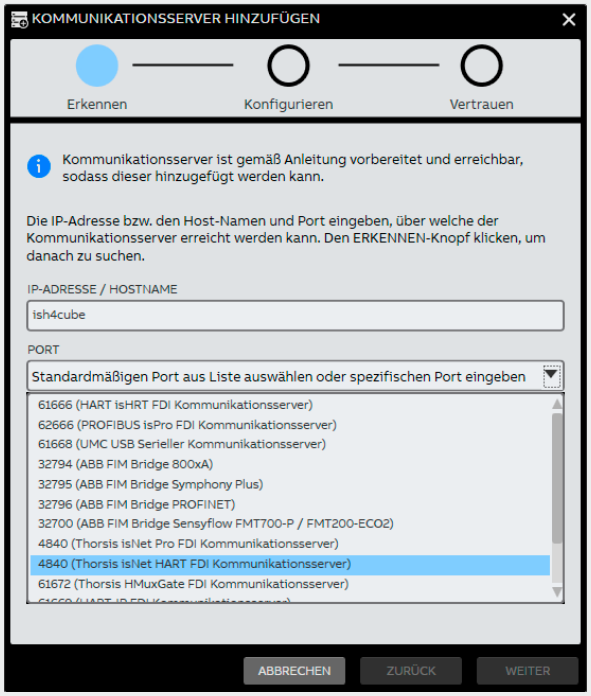
Schritt 2 – Verbindung vorbereiten

Das Dialogfenster KOMMUNIKATIONSSERVER HINZUFÜGEN wird geöffnet. Geben Sie im Feld IP ADRESSE / HOSTNAME den Hostnamen oder die IP-Adresse des isH4Cube ein. Wählen Sie anschließend den gewünschten Port aus.



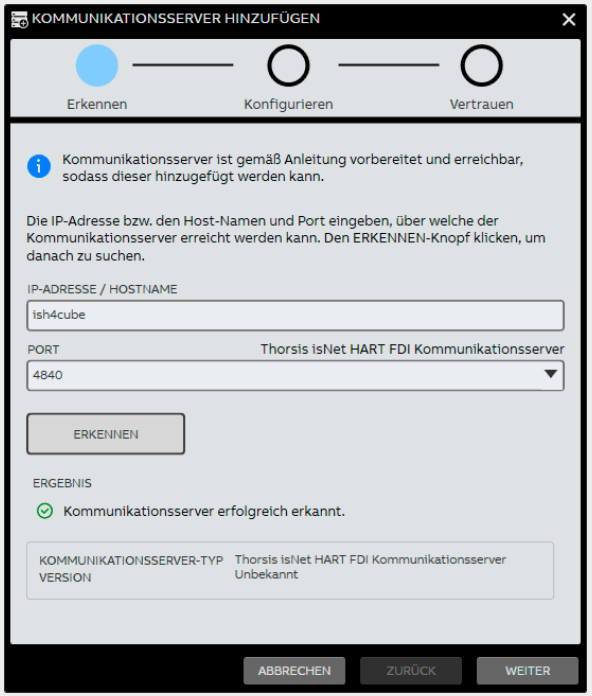
Schritt 3 – Kommunikationsserver auswählen

Wählen Sie den Eintrag Thorsis isNet HART FDI Kommunikationsserver aus der Liste der Server aus.



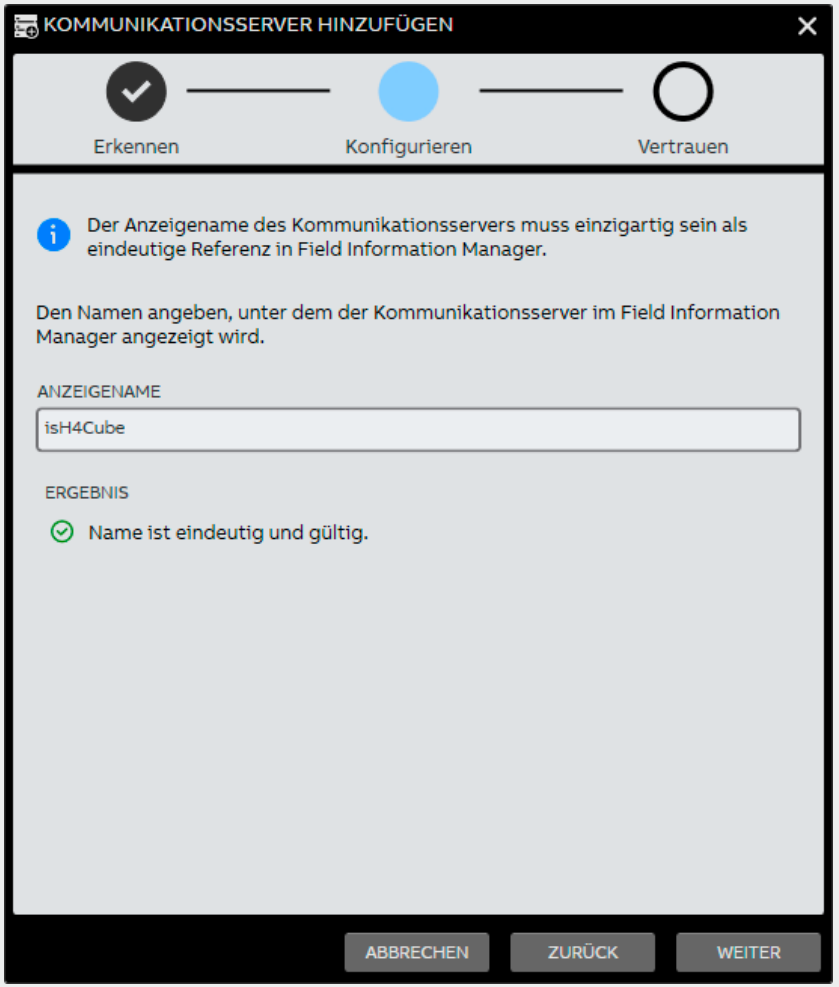
Schritt 4 – Kommunikationsserver erkennen

Nach erfolgreicher Verbindung wird der Kommunikationsserver erkannt und im Dialog angezeigt. Überprüfen Sie die angezeigten Informationen und klicken Sie anschließend auf WEITER.



Schritt 5– Namen vergeben

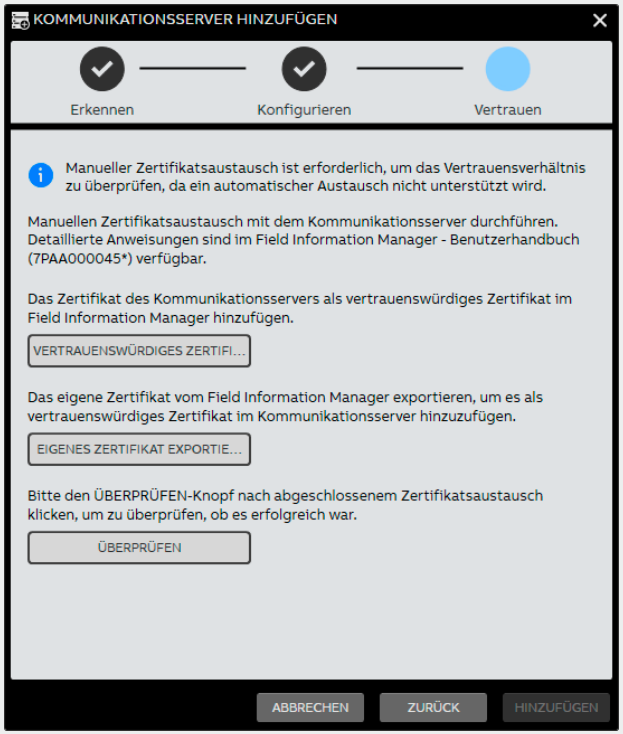
Geben Sie einen eindeutigen Namen für den Kommunikationsserver innerhalb Ihres FIM-Projektes ein. Dieser Name dient ausschließlich der Identifikation im Projekt und kann frei gewählt werden.



4.2 Zertifikate austauschen

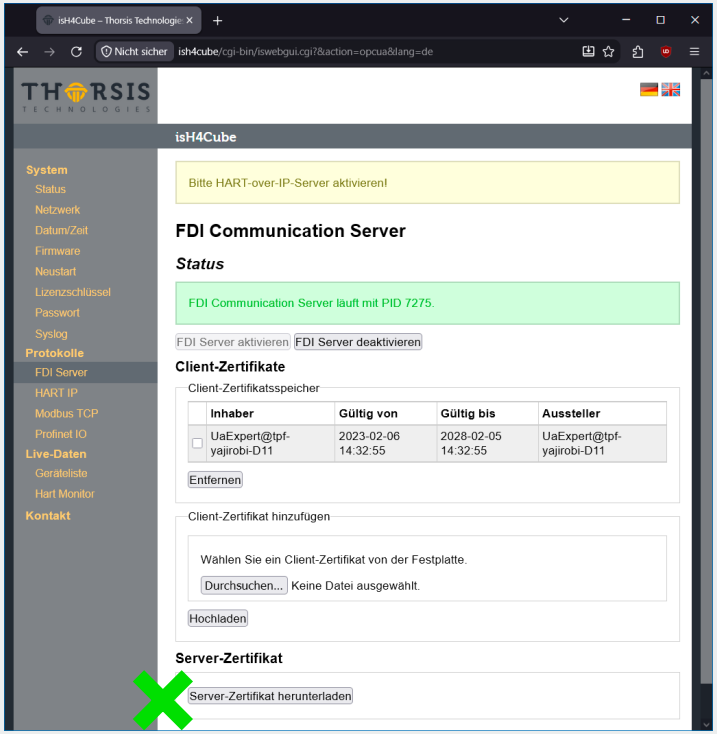
Schritt 6 – Zertifikatsverwaltung öffnen

Im nächsten Schritt wird die gegenseitige Vertrauensstellung zwischen ABB Field Information Manager und dem isH4Cube eingerichtet. Öffnen Sie hierzu die Zertifikatsverwaltung des Assistenten.



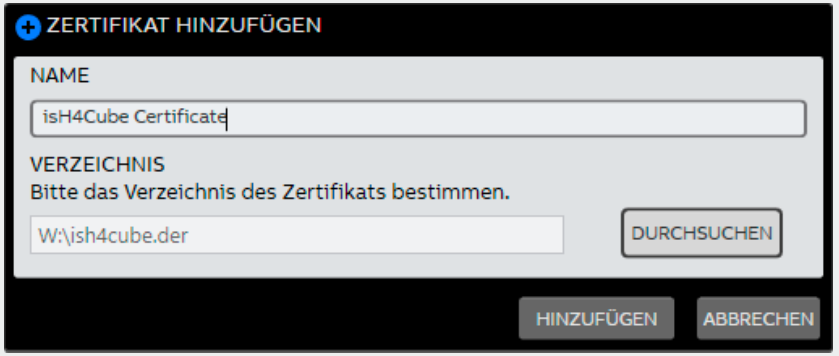
Schritt 7 – Serverzertifikat herunterladen

Öffnen Sie die Weboberfläche des isH4Cube und wechseln Sie zum Menü FDI Communication Server um das Serverzertifikat über Server-Zertifikat herunterladen auf Ihren Computer herunterzuladen.



Schritt 8 – Serverzertifikat im FIM hinzufügen

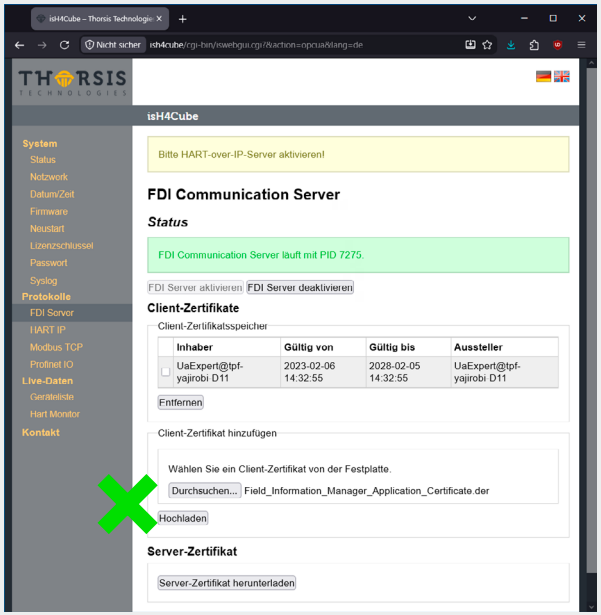
Wechseln Sie zurück zum ABB Field Information Manager und klicken Sie auf ZERTIFIKAT HINZUFÜGEN. Wählen Sie das zuvor heruntergeladene Serverzertifikat aus und bestätigen Sie den Dialog mit HINZUFÜGEN. Dadurch wird das Zertifikat als vertrauenswürdig gespeichert.



Schritt 9 – FIM-Zertifikat zum isH4Cube übertragen

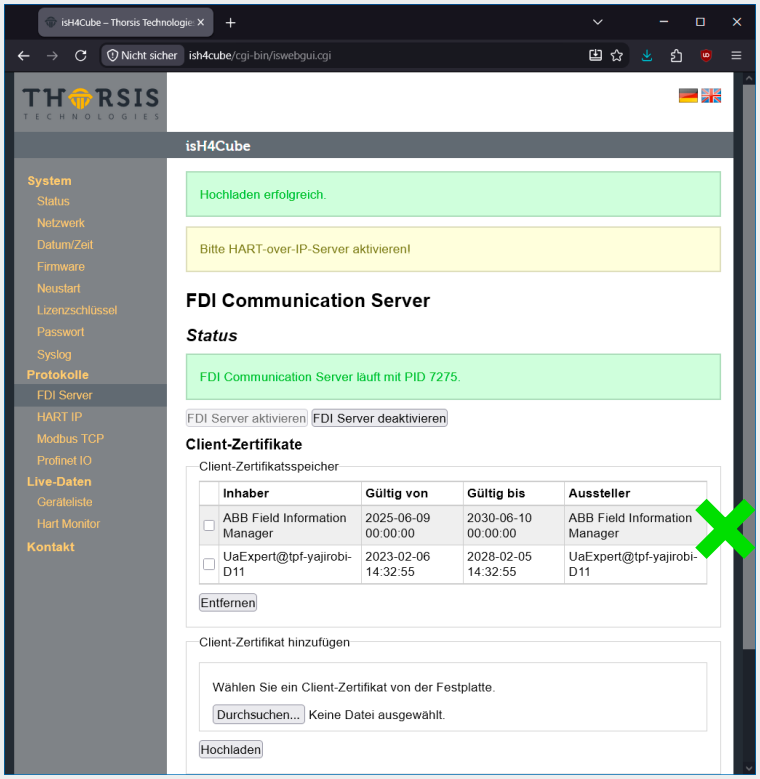
Exportieren Sie anschließend das Anwendungszertifikat des ABB Field Information Managers und laden Sie dieses über den Bereich Client-Zertifikat hinzufügen auf der Weboberfläche des isH4Cube hoch.

HINWEIS: Das Anwendungszertifikat des ABB Field Information Managers erhält man über den Button [EIGENES ZERTIFIKAT EXPORTIEREN] *siehe Schritt 6*.



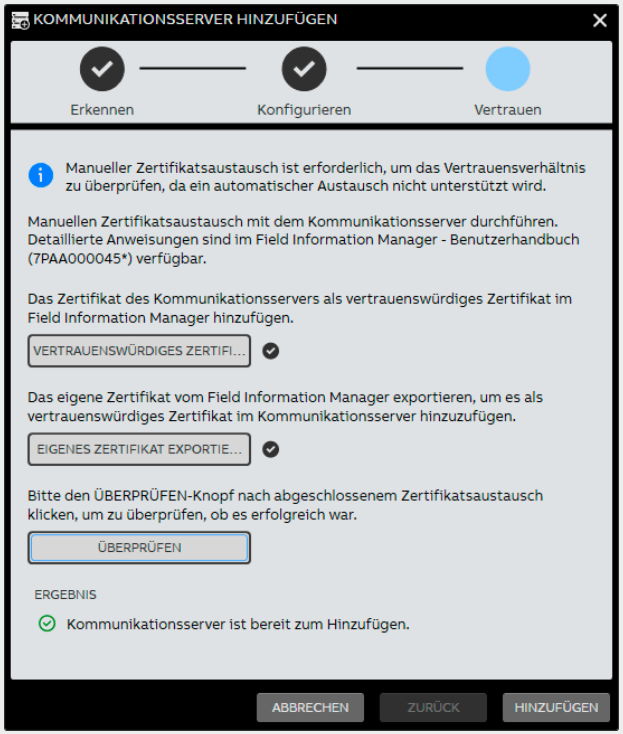
Schritt 10 – Zertifikat erfolgreich installiert

Nach dem Hochladen erscheint das Zertifikat in der Liste der Client-Zertifikate. Damit wurde das FIM-Zertifikat erfolgreich auf dem isH4Cube installiert.



Schritt 11 – Zertifikate überprüfen

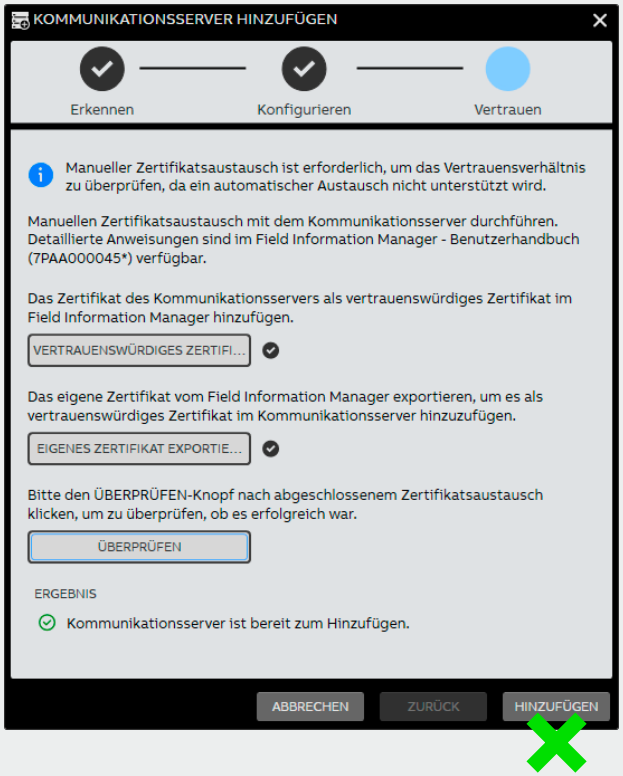
Kehren Sie zum ABB Field Information Manager zurück und klicken Sie auf ÜBERPRÜFEN. Nach erfolgreicher Prüfung bestätigt der Assistent, dass die gegenseitige Vertrauensstellung hergestellt wurde und der Kommunikationsserver hinzugefügt werden kann.

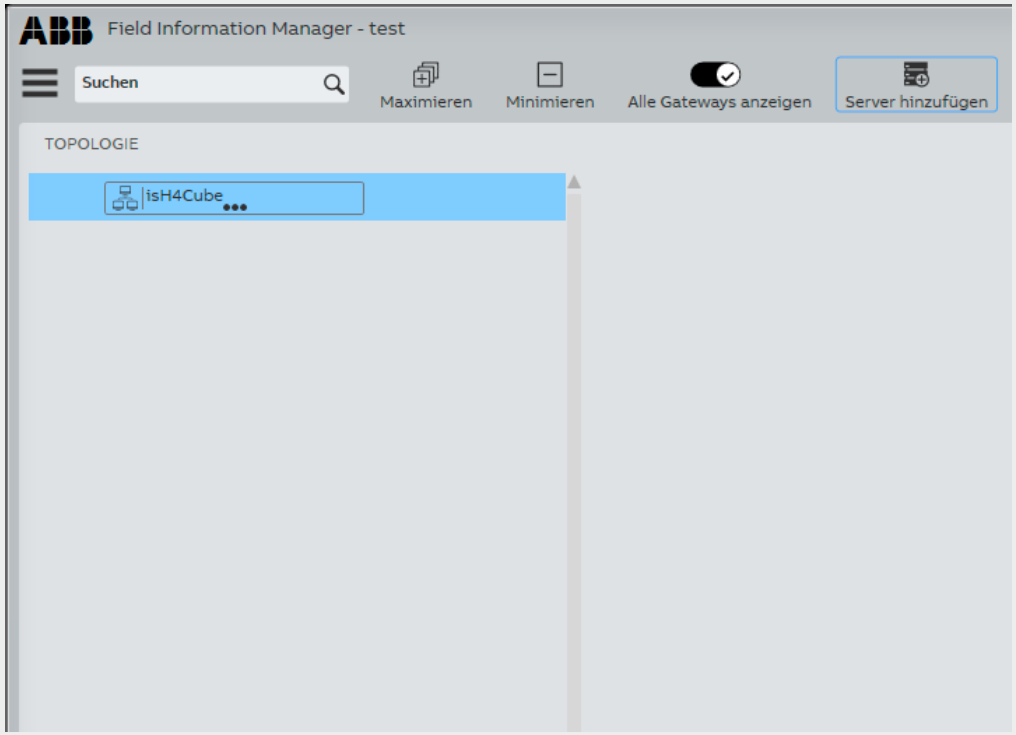


4.3 Kommunikationsserver in FIM hinzufügen

Schritt 12 – Server zum Projekt hinzufügen

Klicken Sie auf HINZUFÜGEN, um den Kommunikationsserver dauerhaft in das aktuelle FIM-Projekt zu übernehmen. Anschließend erscheint der Kommunikationsserver in der Topologie des ABB Field Information Managers.

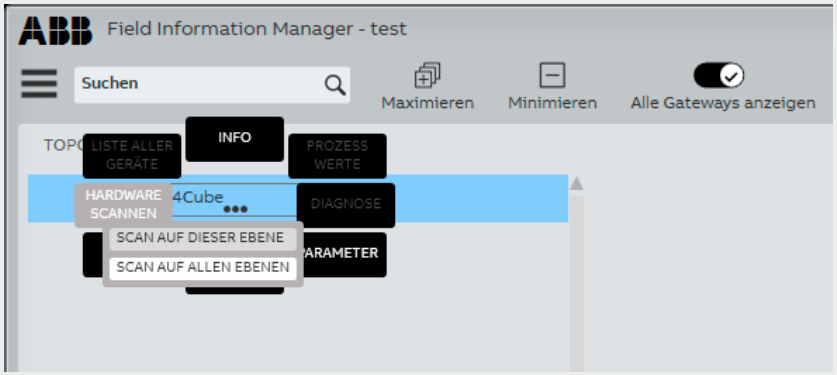




4.4 Geräte erkennen

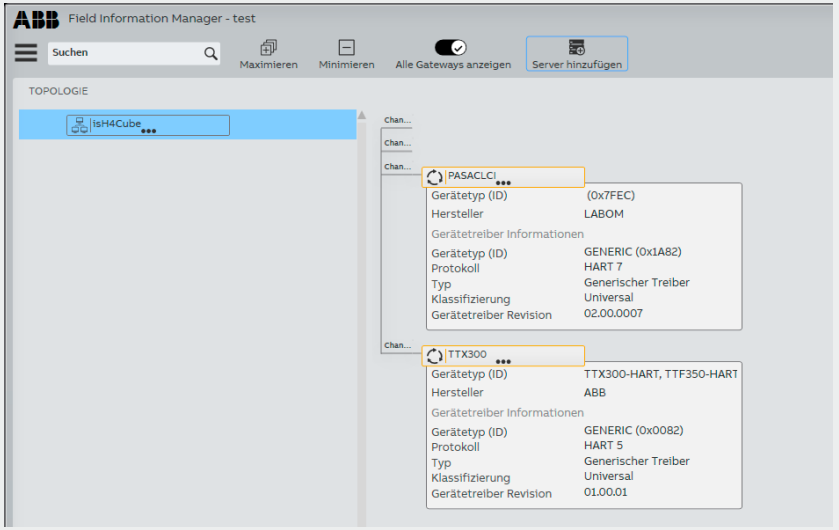
Schritt 13 – Gerätesuche starten

Markieren Sie den neu hinzugefügten Kommunikationsserver und starten Sie einen Hardware-Scan. Während des Scans werden alle angeschlossenen Feldgeräte automatisch gesucht.



Schritt 14 – Feldgeräte verwenden

Nach Abschluss des Hardware-Scans werden die gefundenen Feldgeräte in der Topologie angezeigt. Die Geräte stehen nun für Diagnose, Parametrierung und weitere FDI-Funktionen im ABB Field Information Manager zur Verfügung.



5. Erklärung zur RoHS-Konformität

Als Ergebnis unserer Produktprüfung und aufgrund der gesetzlichen Bestimmungen (Stand: 12. Dezember 2019) bestätigt die Thorsis Technologies GmbH, dass die nachstehenden Informationen genau den Beschränkungen für Stoffe nach Richtlinie 2011/65/EU (RoHS2), einschließlich Phthalaten (DEHP, BBP, DBP, DIBP), nach Richtlinie 2015/863/EU und nach Verordnung (EG) Nr. 1907/2006 (REACH-Verordnung) entsprechen. Hinsichtlich der in diesem Bericht enthaltenen Informationen stützt sich die Thorsis Technologies GmbH auf die Aussagen und Angaben seiner Lieferanten und Dienstleister.
In Übereinstimmung mit DIN EN 50581 umfassen die im Bericht enthaltenen Informationen eine Lieferantenerklärung zu Ausnahmeregelungen und können als Nachweis für die Erstellung einer technischen Dokumentation herangezogen werden. Diese Informationen beruhen auf unserem gegenwärtigen Wissensstand und den durch unsere Lieferanten zur Verfügung gestellten Informationen und können sich ändern.

Gegenwärtige und zukünftige Produkte, die mit den Anforderungen der Richtlinie 2011/65/EU (RoHS 2) übereinstimmen, werden entsprechend auf unserer Website und unseren Verpackungen gekennzeichnet.

Die Thorsis Technologies GmbH verwendet in seinen Produkten keine der in Anhang XVII der REACH-Verordnung aufgeführten Stoffe in Konzentrationen, die die in den Anwendungsbereich der Verordnung fallenden Grenzwerte überschreiten. Um unseren Kunden gegenüber eine hohe Produktsicherheit sicherzustellen, und zur Einhaltung der gesetzlichen Bestimmungen haben wir die Umsetzung der REACH-Verordnung in Übereinstimmung mit der am 17.01.2023 aktualisierten Kandidatenliste überprüft. Gemäß Artikel 33 der REACH-Verordnung ist die Thorsis Technologies GmbH verpflichtet, Kandidatenstoffe, die mit einem Massenanteil von mehr als 0,1% in seinen Produkten enthalten sind, zu melden.

6. Handbuch Aktualisierung

Version	Datum	Beschreibung
1.0	07.04.2026	initiale Version
1.1	04.08.2026	Inhaltserweiterung

© Letzte Änderung 4. August 2026

THORSIS TECHNOLOGIES

Thorsis Technologies GmbH
Oststr. 18
39114 Magdeburg
Germany

Tel +49 391 544 563-1000
info@thorsis.com
www.thorsis.com