SIEMENS

SIMATIC Ident

RFID-Systeme SIMATIC RF360R

Projektierungshandbuch

01/2023

C79000-G8900-C629-03

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
Digital Industries
Postfach 48 48
90026 NÜRNBERG
DEUTSCHLAND

C79000-G8900-C629-03
Ⓟ 01/2023 Änderungen vorbehalten

Inhaltsverzeichnis

Einleitung

1

Zweck dieser Betriebsanleitung

Dieses Handbuch enthält alle Informationen, die für das Inbetriebnehmen und Parametrieren des Readers SIMATIC RF360R notwendig sind.

Das Handbuch richtet sich an:

- Inbetriebnehmer
- Projektierer
- Servicetechniker

Erforderliche Grundkenntnisse

Zum Verständnis der Betriebsanleitung sind allgemeine Kenntnisse auf dem Gebiet der Automatisierungstechnik und Identifikationssysteme erforderlich.

Gültigkeitsbereich dieser Dokumentation

Diese Dokumentation ist gültig für für alle Liefervarianten des Reader SIMATIC RF360R ab dem Ausgabestand "01" und Lieferstand ab 01/2023, sowie den Firmware-Stand V2.1.

Marken

Folgende und eventuell weitere nicht mit dem Schutzrechtsvermerk ® gekennzeichnete Bezeichnungen sind eingetragene Marken der Siemens AG:

SIMATIC ®, SIMATIC RF ® und MOBY ®

Einordnung in die Dokumentationslandschaft

Informationen zu den Eigenschaften, technischen Daten und Einsatzoptionen des Readers SIMATIC RF360R finden Sie im Systemhandbuch "SIMATIC RF300".

Zusätzlich zu dieser Betriebsanleitung benötigen Sie die Betriebsanleitung zu der eingesetzten Steuerung S7-300, S7-400, S7-1200 oder S7-1500. Bei Verwendung einer S7-Steuerung finden Sie Informationen zur Programmierung der Baugruppe sowie eine vollständige Fehlerbeschreibung in der Beschreibung der Funktionsbausteine "Ident-Profil und Ident Bausteine", des RFID-Normprofils, sowie des FB 45.

Alle relevanten Informationen zur XML-Projektierung und -Programmierung finden Sie in dem Handbuch "XML-Programmierung für SIMATIC Ident". Ausführliche Informationen zu Projektierung und -Programmierung über OPC UA finden Sie in dem Handbuch "OPC UA für SIMATIC Ident". Informationen zu Projektierung und -Programmierung über EtherNet/IP finden Sie in dem Handbuch "Ident-Profil, Add-On Instruction für Rockwell-Systeme".

Die aktuellen Versionen der verschiedenen Handbücher finden Sie auf den Seiten des Siemens Industry Online Support (https://support.industry.siemens.com/cs/ww/de/ps/14970/man).

Abkürzungen und Namenskonventionen

Innerhalb dieser Dokumentation werden folgende Begriffe/Abkürzungen synonym verwendet:

Transponder, Tag	Datenträger, Mobiler Datenspeicher (MDS)
Kommunikationsmodul (CM)	Anschaltmodul (ASM)

Security-Empfehlungen

2

Um nicht autorisierten Zugriff zu unterbinden, beachten Sie folgende Security-Empfehlungen, im Umgang mit dem Reader und WBM (Web Based Management).

Allgemein

- Stellen Sie regelmäßig sicher, dass das Gerät diese Empfehlungen und/oder andere interne Security-Richtlinien erfüllt.
- Bewerten Sie Ihre Anlage ganzheitlich im Hinblick auf Sicherheit. Nutzen Sie ein Zellenschutzkonzept mit entsprechenden Produkten.
- Halten Sie die Software aktuell. Verwenden Sie die jeweils aktuelle Firm-/Software-Version des Geräts. Informieren Sie sich regelmäßig über Sicherheits-Updates der Produkte und wenden Sie diese an. Ab der Veröffentlichung einer neuen Version werden Vorgängerversionen nicht mehr unterstützt und nicht gewartet.

  Hinweise auf Produktneuigkeiten und neue Software-Versionen finden Sie unter folgender Adresse:
  Link: (https://support.industry.siemens.com/cs/ww/de/ps/26319)
- Verbinden Sie das Gerät nicht direkt mit dem Internet. Betreiben Sie das Gerät innerhalb eines geschützten Netzwerkbereichs. Setzen Sie zur Anbindung des internen geschützten Netzwerks an externe Netzwerke eine Firewall ein. Konfigurieren Sie diese mit restriktiven Regeln.
- Nutzen Sie für die Datenübertragung über ein unsicheres Netzwerk zusätzliche Security-Komponenten die einen verschlüsselten VPN-Tunnel (IPsec, OpenVPN) bereitstellen.
- Trennen Sie Verbindungen ordnungsgemäß (z. B. Abmeldung im WBM).

Physischer Zugang

- Beschränken Sie den physischen Zugang zu dem Gerät auf qualifiziertes und berechtigtes Personal.
- Die Geräte besitzen einen "Low-Level-Service-Zugang" der nur mittels zusätzlicher Hardware-Verschaltung aktiviert werden kann. Der Zugang dient dazu im Service-Fall dem Siemens-Personal weitergehende Untersuchungen zu ermöglichen. Der Zugang darf nur von qualifizierten Service-Personal benutzt werden, andernfalls führt dessen Nutzung zum Verlust der Gewährleistung.

Security-Funktionen

- Aktivieren Sie nur Protokolle, die Sie wirklich für den Einsatz des Gerätes benötigen. Beachten Sie, dass ab Werk alle Protokolle nutzbar sind. Während das Gerät jedoch eine Verbindung über ein Protokoll aufgebaut hat, sind währenddessen alle anderen Protokolle deaktiviert.
- Deaktivieren Sie EtherNet/IP, falls sie dies nicht benötigen. Aktiveren sie EtherNet/IP nur dann, wenn Sie eine Verbindung mit EtherNet/IP benötigen.
- Die XML-Protokolle werden unverschlüsselt gesendet. Stellen Sie durch geeignete Maßnahmen sicher, dass die XML-Kommunikation abhörsicher ist.
- Für optimale Sicherheit verwenden Sie die Authentifizierungs- und Verschlüsselungsmechanismen von SNMPv3. SNMPv1 ist als unsicher eingestuft und sollten nur bei absoluter Notwendigkeit verwendet werden.
- Verwenden Sie die neueste mit dem Produkt kompatible Webbrowser-Version, um sicherzustellen, dass die sichersten verfügbaren Verschlüsselungsverfahren eingesetzt werden.
- Beschränken Sie den Zugriff auf das Gerät durch ein externes Gerät mittels einer Firewall oder Regeln in einer Zugriffsliste (ACL – Access Control List). Die Konfiguration der Firewall und Zugriffsliste kann ausschließlich über ein externes Gerät erfolgen.
- Das Gerät verfügt über einen Schutz gegen Brute-Force-Angriffe, um das Systems gegen Ausprobieren verschiedener Passwörter zu sichern. Beschränken Sie die maximal zugelassenen, fehlgeschlagenen Anmeldeversuche.
- Das Gerät verfügt über eine automatische Trennfunktion ("Session Timeout"). Legen Sie die Zeitspanne fest, nach der die Verbindung zu dem Gerät automatisch getrennt wird.
- Sperren Sie ungenutzte physische Ports auf dem Gerät. Ungenutzte Ports können verwendet werden, um unerlaubt auf die Anlage zuzugreifen.
- Konfigurationsdateien können vom Gerät heruntergeladen werden. Stellen Sie sicher, dass die Konfigurationsdateien angemessen geschützt sind. Sie können die Dateien z. B. digital signieren und verschlüsseln, sie an einem sicheren Ort speichern oder Konfigurationsdateien ausschließlich über sichere Kommunikationskanäle übertragen.
- Das Gerät bietet Möglichkeiten, die Konfiguration zu sichern und wiederherzustellen. Aus sicherheitstechnischen Gründen wird weder die IP-Adresse der Netzwerkschnittstelle, noch Daten der lokalen Benutzerverwaltung gesichert. Für die Verwaltung diese Daten empfehlen wir die Verwendung des Netzwerkmanagementsystems "SINEC NMS".

Authentifizierung

Hinweis

Zugänglichkeitsrisiko - Gefahr des Datenverlusts

Verlieren Sie die Passwörter für das Gerät nicht. Der Zugriff auf das Gerät kann nur durch Zurücksetzen des Geräts auf die Werkseinstellungen wiederhergestellt werden, wodurch sämtliche Konfigurationsdaten entfernt werden.

- Verwenden Sie stets die Benutzerverwaltung und legen Sie neue Benutzer-Profile an.
- Ersetzen Sie die Standardpasswörter für alle Benutzerkonten, Zugriffsmodi und Anwendungen (sofern zutreffend), bevor Sie das Gerät einsetzen.
- Definieren Sie Regeln für die Nutzung der Geräte und die Vergabe von Passwörtern.
- Legen Sie Passwortrichtlinien fest.
- Verwenden Sie Passwörter mit hoher Passwortstärke. Vermeiden Sie schwache Passwörter (wie "Passwort1", "123456789", "abcdefgh") oder sich wiederholende Zeichen (wie "abcabc"). Diese Empfehlung gilt auch für auf dem Gerät konfigurierte symmetrische Passwörter/Schlüssel.
- Stellen Sie sicher, dass alle Passwörter geschützt und unzugänglich für unbefugtes Personal sind.
- Verwenden Sie ein Passwort nicht für verschiedene Benutzer und Systeme.
- Bewahren Sie Passwörter an einem sicheren Ort (nicht online) auf, damit Sie sie bei Verlust zur Hand haben.
- Ändern Sie regelmäßig Passwörter und Schlüssel, um die Sicherheit zu erhöhen.
- Ein Passwort muss geändert werden, wenn es unbefugten Personen bekannt geworden ist oder der Verdacht dazu besteht.

Zertifikate und Schlüssel

- Im Gerät ist ein voreingestelltes SSL/TLS-Zertifikat für den Zugriff auf das WBM vorhanden. Ersetzen Sie dieses Zertifikat durch ein selbst erstelltes höherwertiges Zertifikat mit Schlüssel.
  Verwenden Sie ein Zertifikat, das entweder durch eine zuverlässige externe oder interne Zertifizierungsstelle signiert ist.
- Nutzen Sie eine Zertifizierungsstelle inklusive Schlüsselwiderruf und -verwaltung, um die Zertifikate zu signieren.
- Verwenden Sie Zertifikate im Format "PKCS #12".
- Verwenden Sie Zertifikate mit einer Schlüssellänge von 4096 Bit.
- Stellen Sie sicher, dass benutzerdefinierte private Schlüssel geschützt und unzugänglich für unbefugte Personen sind.
- Ändern Sie bei Verdacht auf eine Sicherheitsverletzung sofort alle Zertifikate und Schlüssel.

- Verifizieren Sie Zertifikate anhand des Fingerprints auf Server- und Clientseite, um "Man-in-the-middle"-Angriffe zu verhindern. Verwenden Sie hierzu einen zweiten, sicheren Übertragungsweg.
- Bevor Sie das Gerät zur Reparatur an Siemens zurückschicken, ersetzen Sie die aktuellen Zertifikate und Schlüssel durch temporäre Wegwerfzertifikate und -schlüssel, die bei der Rückkehr des Geräts zerstört werden können.
- Wenn Protokolle Zertifikate und Schlüssel unterstützen, bevorzugen Sie Zertifikate.
- Verwenden Sie bei dem Betrieb über OPC UA immer das Security-Verfahren "Signieren und verschlüsseln".
- Folgende Verschlüsselungsalgorithmen werden unterstützt:

Protokoll	**Unterstütze Verschlüsselungsalgorithmen**	**Unterstützer Schlüssel und Größe**
Webbrowser	SHA1 SHA256 mit RSA SHA384 mit RSA SHA512 mit RSA	RSA 2048 bit RSA 4096 bit
OPC UA	SHA256 mit RSA SHA384 mit RSA SHA512 mit RSA	RSA 2048 bit RSA 4096 bit

- Informationen zu den von den verschiedenen Zertifikat-Typen unterstützten Dateiformaten finden Sie im Kapitel "Der Menüpunkt "Zertifikate" (Seite 80)".
- Informationen zu den von dem Gerät unterstützten Verschlüsselungsverfahren finden Sie im Kapitel "Verschlüsselungsmethoden (Ciphers) (Seite 119)".

Firmware

Die Firmware selbst ist signiert und verschlüsselt. Damit ist sichergestellt, dass nur von Siemens erstellte Firmware in das Gerät geladen werden kann.

Außerbetriebnahme

Nehmen Sie das Gerät ordnungsgemäß außer Betrieb, um zu verhindern, dass unbefugte Personen an vertrauliche Daten im Gerätespeicher gelangen.
Setzen Sie das Gerät hierzu auf Werkseinstellungen zurück.

2.1 Protokolle

Sichere/Unsichere Protokolle

- Verwenden Sie möglichst ausschließlich sichere Protokolle. Vermeiden oder deaktivieren Sie unsichere Protokolle und Dienste. Wenn Sie unsichere Protokolle und Dienste benötigen, stellen Sie sicher, dass das Gerät in einem geschützten Netzwerkbereich betrieben wird.

  Die folgenden Protokolle bieten sichere Alternativen:

  - HTTP → HTTPS

    HTTPS ist ab Werk aktiviert. HTTP ist als unsicher eingestuft, kann bei Bedarf jedoch zu einem späteren Zeitpunkt jedoch wieder aktiviert werden.

  - SNMPv1 → SNMPv3

    SNMPv1 ist ab Werk aktiviert, um den Betrieb des Geräts in einem PROFINET-Umfeld zu erleichtern. Prüfen Sie die Notwendigkeit der Nutzung von SNMPv1. SNMPv1 ist als unsicher eingestuft. Nutzen Sie die Möglichkeit den Schreibzugriff zu unterbinden. Das Produkt bietet entsprechende Einstellmöglichkeiten.
    Wenn SNMP aktiviert ist, ändern Sie die Community-Namen. Falls kein uneingeschränkter Zugriff erforderlich ist, beschränken Sie den Zugriff über SNMP.
- Aktivieren Sie nur Dienste/Protokolle, die Sie für den Einsatz des Systems benötigen, so auch die eingebauten Schnittstellen/Ports. Nicht verwendete Ports können potenziell für den Zugriff auf das Netzwerk hinter dem Gerät genutzt werden.
- Beschränken Sie die nach außen angebotenen Dienste und Protokolle auf das erforderliche Mindestmaß.
- DCP ist als unsicher eingestuft. Prüfen Sie die Notwendigkeit der Nutzung von DCP. Wenn DCP benötigt wird, aktivieren Sie für die DCP-Funktion nach der Inbetriebnahme den Modus "Schreibgeschützt".
- Verwenden Sie bei der Nutzung von OPC UA ausschließlich Profile mit sicheren Verschlüsselungen und Authentifizierungen.

Liste verfügbarer Protokolle

Nachfolgend werden alle verfügbaren Protokolle und deren Ports aufgelistet, welche bei SIMATIC RF360R verwendet werden.

Tabelle 2- 1 Liste verfügbarer Protokolle

Dienst/ Protokoll	Protokoll/ Portnummer	Voreingestellter Portstatus	Port konfigurierbar	Port-Nummer konfigurierbar	Authentifizierung	Verschlüsselung [1]
DHCP	UDP/68	Offen	✓	--	--	--
PROFINET	UDP/34964 UDP/49152-65535	Offen	✓	--	--	--
HTTP	TCP/80	Geschlossen	✓	--	--	--
HTTPS	TCP/443	Offen	✓	--	✓	✓
NTP	UDP/123	Geschlossen	✓	--	--	--
SNMP	UDP/161	Offen	✓	--	✓ (wenn konfiguriert)	✓ (wenn konfiguriert)
EtherNet/IP	TCP/44818 UDP/44818 UDP/2222	Offen	✓	--	--	--
OPC UA	TCP/4840	Offen	✓	✓	✓ (wenn konfiguriert)	✓ (wenn konfiguriert)
XML	TCP/10001	Offen [2]	✓	✓	--	--
Syslog	UDP/49152-65535	Geschlossen	✓ [3]	--	--	--

[1] Weitere Informationen zu den verwendeten Verschlüsselungsverfahren finden Sie im Anhang.

[2] Gilt für die Protokollnummer 10001, alle anderen sind geschlossen.

[3] Nur ausgehend, wenn konfiguriert.

Erläuterung zu der Tabelle:

- Authentifizierung

  Gibt an, ob eine Authentifizierung des Kommunikationspartners stattfindet.

- Verschlüsselung

  Gibt an, ob die Übertragung verschlüsselt wird.

2.2 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 einen Bestandteil eines solchen Konzepts.

Die Kunden sind dafür verantwortlich, unbefugten Zugriff auf ihre Anlagen, Systeme, Maschinen und Netzwerke zu verhindern. Diese Systeme, Maschinen und Komponenten sollten nur mit dem Unternehmensnetzwerk oder dem Internet verbunden werden, wenn und soweit dies notwendig ist und nur wenn entsprechende Schutzmaßnahmen (z.B. Firewalls und/oder Netzwerksegmentierung) ergriffen wurden.

Weiterführende Informationen zu möglichen Schutzmaßnahmen im Bereich 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, Produkt-Updates anzuwenden, sobald sie 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/cert

Hinweis zum Firmware-/Software-Support

Informieren Sie sich regelmäßig über neue Firmware-/Software-Versionen oder Sicherheits-Updates und wenden Sie diese an. Ab der Veröffentlichung einer neuen Version werden Vorgängerversionen nicht mehr unterstützt und nicht gewartet.

Beschreibung

3

3.1 Eigenschaften der Reader

Anwendungsbereich

Der Reader SIMATIC RF360R wurde speziell für den Einsatz in der industriellen Produktion zur Steuerung und Optimierung des Materialflusses, innerhalb eines zugangsgesicherten Bereichs konzipiert. Dabei zeichnet sich der Reader durch eine hohe Datenübertragungsgeschwindigkeit aus. Der Reader kann ISO 15693- und RF300-Transponder (proprietär) bearbeiten.

Gegenüber anderen Readern der SIMATIC RF300-Produktfamilie - welche üblicherweise eine RS422-Schnittstelle zur Kommunikation mit höher gelagerten Kommunikationsmodulen aufweisen - verfügt der RF360R über zwei PROFINET IO-Schnittstellen. Aufgrund dieser Besonderheit kann der Reader sowohl in der Feldebene über einen Direktanschluss an eine S7-Steuerung als auch über einen PC oder in der IT-Ebene betrieben werden. Dies ermöglicht es, dass parallel zum regulären Betrieb Diagnosedaten, wie z. B. die verarbeiteten Transponder-Daten oder die Logbuch-Einträge, an höher gelagerte Systeme über OPC UA oder XML übertragen werden können. Zusätzlich dazu kann PROFINET IO an eine weitere Baugruppe weitergeschleift werden.

Bild 3-1 Reader SIMATIC RF360R

Neben den bekannten Konfigurierungsarten über TIA Portal und GSDML ist bei diesem Reader zusätzlich ein Web Based Management (WBM) integriert, mit welchem über einen Standard-Browser die Geräte eingestellt werden können. Das WBM unterstützt Sie bei Inbetriebnahme,

Diagnose und Wartung. Außerdem ermöglicht es das Lesen/Schreiben von Transponder-Daten.

Aus Sicherheitsgründen sollten Sie das Gerät ausschließlich innerhalb eines geschützten Netzwerkbereichs betreiben und nicht direkt mit dem Internet verbinden.

Weitere Informationen zu den verschiedenen RFID-Geräten und optischen Lesegeräten finden Sie im Internet, auf der Seite des "Siemens Industry Online Support (https://support.industry.siemens.com/cs/ww/de/ps/14970/man)".

Merkmale

Folgende Merkmale kennzeichnen die Reader RF360R aus:

Tabelle 3- 1 Merkmale des Readers

Merkmale	RF360R
Ethernet-Schnittstellen	2x M12, Switch integriert Übertragungsgeschwindigkeit: 100 MBit/s
Schutzart	IP67
Konfigurations-/ Diagnosemöglichkeiten	STEP 7 (TIA Portal), GSDML, WBM (Webbrowser)
Applikationsprotokolle	PROFINET IO, EtherNet/IP, OPC UA, XML
Funktionsbausteine	Ident-Profil, Faceplate für PCS 7
Unterstützte SIMATIC-Steuerungen	S7-300, S7-400, S7-1200, S7-1500
Unterstützte Fremdsteuerungen	Source Code des Ident-Profil verfügbar. Alle Steuerungen mit PROFINET- und IEC 61131-Programmierung werden unterstützt.
Lesbare Transponder-Standards	ISO 15693 RF300 (proprietär)

ACHTUNG
IRT wird nicht unterstützt Beachten Sie, dass der Reader kein IRT (Isochronous Real Time) unterstützt. Der Reader kann auch nicht als IRT-Durchleiter fungieren (z. B. in einer Linienstruktur). Der Reader kann in MRP-Ringen als Client projektiert werden. Eine Netzwerkdiagnose über SNMP wird von dem Reader unterstützt.

ACHTUNG
Betrieb in VLAN Beachten Sie, dass der Reader nicht in VLANs betrieben werden kann, deren ID ≠ 0 ist.

3.2 Anwenderspezifische Vorgehensweise

Der Reader der SIMATIC RF360R ist ab Werk vorkonfiguriert und kann direkt in Betrieb genommen werden. Werkseitig bezieht der Reader seine IP-Adresse über einen DHCP-Server.

Wie beschrieben, ist der Reader für verschiedene Umgebungen und Anforderungen konzipiert.

Wenn Sie den Reader in einer Automatisierungsumgebung betreiben, erfolgt die Konfiguration, Projektierung und Programmierung aus Sicht eines S7-Anwenders. Eine Integration in Fremdsteuerungen (z. B. Rockwell-Steuerungen) ist selbstverständlich auch möglich. In diesem Fall erfolgt die Konfiguration, Projektierung und Programmierung aus Sicht eines Rockwell-Anwenders. Wenn Sie den Reader in einer XML-Umgebung betreiben, erfolgt die Konfiguration und Programmierung aus Sicht eines XML-Anwenders. Wenn Sie den Reader in einer OPC UA-Umgebung betreiben, erfolgt die Konfiguration und Programmierung aus Sicht eines OPC UA-Anwenders.

Wollen Sie den Reader an Ihre Bedürfnisse anpassen, empfehlen wir Ihnen folgende anwenderspezifische Vorgehensweise:

Vorgehensweise als S7-Anwender

1. Hardware anschließen

   Informationen dazu finden Sie im Kapitel "Hardware anschließen (Seite 20)".

2. IP-Adresse / Gerätename vergeben

   Informationen dazu finden Sie im Kapitel "IP-Adresse / Gerätename über SINEC PNI vergeben (Seite 28)" oder "IP-Adresse / Gerätename über STEP 7 vergeben (Seite 26)".

3. Reader und ggf. Kommunikationsmodul konfigurieren

   Informationen dazu finden Sie im Kapitel "Projektierung über PROFINET IO (STEP 7) (Seite 31)" oder "Konfigurieren über das WBM (Seite 37)".

4. Reader-Befehle projektieren/programmieren

   Informationen dazu finden Sie im Kapitel "Programmieren über SIMATIC-Steuerung (Seite 87)".

Vorgehensweise als XML-Anwender

1. Hardware anschließen

   Informationen dazu finden Sie im Kapitel "Hardware anschließen (Seite 20)".

2. IP-Adresse / Gerätename vergeben

   Informationen dazu finden Sie im Kapitel "IP-Adresse / Gerätename über SINEC PNI vergeben (Seite 28)".

3. Reader konfigurieren

   Informationen dazu finden Sie im Kapitel "Projektierung über XML (Seite 35)" oder "Konfigurieren über das WBM (Seite 37)".

4. Reader-Befehle programmieren

   Informationen dazu finden Sie im Kapitel "Programmieren über XML (Seite 87)".

Vorgehensweise als OPC UA-Anwender

1. Hardware anschließen

   Informationen dazu finden Sie im Kapitel "Hardware anschließen (Seite 20)".

2. IP-Adresse / Gerätename vergeben

   Informationen dazu finden Sie im Kapitel "IP-Adresse / Gerätename über SINEC PNI vergeben (Seite 28)".

3. Reader konfigurieren

   Informationen dazu finden Sie im Kapitel "Projektierung über OPC UA (Seite 35)" oder "Konfigurieren über das WBM (Seite 37)".

4. Reader-Befehle programmieren

   Informationen dazu finden Sie im Kapitel "Programmieren über OPC UA (Seite 88)".

Vorgehensweise als Rockwell-Anwender

1. Hardware anschließen

   Informationen dazu finden Sie im Kapitel "Hardware anschließen (Seite 20)".

2. IP-Adresse / Gerätename vergeben

   Informationen dazu finden Sie im Kapitel IP-Adresse / Gerätename über SINEC PNI vergeben (Seite 28)" oder "IP-Adresse über DHCP vergeben (Seite 30)".

3. Reader konfigurieren

   Informationen dazu finden Sie im Kapitel "Projektieren über Studio 5000 Logix Designer (Seite 35)" und "Konfigurieren über das WBM (Seite 37)".

4. Reader-Befehle projektieren/programmieren

   Informationen dazu finden Sie im Kapitel "Programmieren über Rockwell-Steuerung (Seite 88)".

Orientierung im Dokument

Im weiteren Verlauf des Dokuments werden Ihnen diese Symbole dabei helfen, sich schnell zu orientieren und herauszufinden, ob das jeweilige Kapitel für Sie von Interesse ist oder nicht. Ausschließlich jene Kapitel mit anwenderspezifischen Inhalten, also Inhalten, die schnittstellengebunden sind, enthalten diese Symbole. Kapitel ohne diese Symbole sind allgemeingültig und für alle Anwendungsbereiche relevant.

Inbetriebnahme

4

4.1 Wichtige Hinweise zum Geräteeinsatz

Sicherheitshinweise für den Geräteeinsatz

Die folgenden Sicherheitshinweise sind für Aufstellung und Betrieb des Gerätes und alle damit zusammenhängenden Arbeiten wie Montage, Anschließen, Geräteaustausch oder Öffnen des Gerätes zu beachten.

Allgemeine Hinweise

⚠WARNUNG

Sicherheitskleinspannung

Das Gerät ist für den Betrieb mit einer direkt anschließbaren Sicherheitskleinspannung (Safety Extra Low Voltage, SELV) durch eine Spannungsversorgung mit begrenzter Leistung (Limited Power Source, LPS) ausgelegt (Dies gilt nicht für 100 V...240 V-Geräte).

Deshalb dürfen nur Sicherheitskleinspannungen (SELV) mit begrenzter Leistung (Limited Power Source, LPS) nach IEC 60950-1 / EN 60950-1 / VDE 0805-1 mit den Versorgungsanschlüssen verbunden werden oder das Netzteil für die Versorgung des Geräts muss NEC Class 2 gemäß National Electrical Code (r) (ANSI / NFPA 70) entsprechen.

Zusätzlich bei Geräten mit redundanter Spannungsversorgung:

Wenn das Gerät an eine redundante Spannungsversorgung angeschlossen wird (zwei getrennte Spannungsversorgungen), müssen beide die genannten Anforderungen erfüllen.

ACHTUNG

Veränderungen nicht zulässig

Veränderungen an den Geräten sind nicht zulässig. Bei Nichteinhaltung erlöschen die funktechnischen Zulassungen, die entsprechenden Länderzulassungen (z. B. CE oder FCC), sowie die Herstellergarantie.

Überspannungsschutz

ACHTUNG
Schutz der externen Spannungsversorgung DC 24 V Wenn die Baugruppe über ausgedehnte 24 V-Versorgungsleitungen oder Netze gespeist wird, dann sind Einkopplungen starker elektromagnetischer Pulse auf die Versorgungsleitungen möglich, die z. B. durch Blitzschlag oder das Schalten großer Lasten entstehen können. Der Anschluss der externen Spannungsversorgung DC 24 V ist nicht gegen starke elektromagnetische Pulse geschützt. Versehen Sie blitzschlaggefährdete Leitungen mit einem geeigneten Überspannungsschutz.

Reparaturen

⚠ **WARNUNG**
Reparaturen ausschließlich durch autorisiertes Fachpersonal Reparaturen dürfen nur von autorisiertem Fachpersonal durchgeführt werden. Durch unbefugtes Öffnen und unsachgemäße Reparaturen können erhebliche Sachschäden oder Gefahren für den Benutzer entstehen.

4.2 Hardware anschließen

Vor der Montage und Inbetriebnahme

ACHTUNG
Lesen zugehöriger Handbücher Lesen Sie vor der Montage, dem Anschließen und der Inbetriebnahme die entsprechenden Abschnitte in dem Handbuch der verwendeten Steuerung, sowie die entsprechenden Abschnitte im Systemhandbuchs "SIMATIC RF300". Gehen Sie bei der Montage und dem Anschließen entsprechend den darin enthaltenen Beschreibungen vor.

ACHTUNG
Montage/Demontage im spannungslosen Zustand Verdrahten Sie den PC bzw. die Steuerung und die anzuschaltenden Module und Reader nur im spannungslosen Zustand. Stellen Sie sicher, dass während der Montage/Demontage der Geräte die Spannungsversorgung ausgeschaltet ist.

Schnittstellen

① Status-LEDs
(Statusanzeige des Readers und der PROFINET-Verbindung)

② Reader-LEDs
(Betriebszustände des Readers)

③ Schnittstelle für die Spannungsversorgung
X80 (M12, 4-polig, L-codiert)

④ Schnittstelle für PROFINET IO
X1 P1R (M12, 4-polig, D-codiert)

⑤ Schnittstelle für PROFINET IO
X1 P2R (M12, 4-polig, D-codiert) [1)]

Bild 4-1 Schnittstellen des Readers SIMATIC RF360R

[1)] Über die M12-Rundbuchse ⑤ können Sie PROFINET IO weiterschleifen.

Voraussetzung

- Der Reader wurde montiert.
- Verdrahten Sie den Reader ausschließlich bei ausgeschalteter Versorgungsspannung.

ACHTUNG
Verwendung von vorkonfektionierten Kabeln nur in Verbindung mit hochohmigen Verbrauchern Achten Sie bei der Verwendung von vorkonfektionierten Kabeln darauf, dass die Ader (L2) die mit Pin 4 des RF360R verbunden ist bzw. wird, nur mit hochohmigen Verbrauchern (> 22 kOhm) verbunden ist. Kann dies nicht gewährleistet werden, dann darf die Ader nicht mit dem Pin 4 der RF360R-Buchse verbunden werden.

Vorgehensweise

Gehen Sie folgendermaßen vor, um den Reader anzuschließen:

1. Schließen Sie den Reader mit Hilfe eines Ethernet-Kabels an einen PC oder ein Switch bzw. an eine Steuerung an ④.

   Verwenden Sie ein Anschlusskabel mit M12-Stecker (4-polig).

2. Verbinden Sie den Reader ggf. mit einem weiteren Reader SIMATIC RF360R ⑤.

   Verwenden Sie zum Weiterschleifen von PROFINET IO ein Anschlusskabel mit M12-Stecker (4-polig).

3. Schließen Sie den Reader mit Hilfe des Anschlusskabels an der Spannungsversorgung an ③.

Der Reader ist betriebsbereit, wenn die "R/S"-LED grün leuchtet/blinkt. Blinkt die "R/S"-LED, wartet der Reader auf eine Verbindung. Leuchtet die "R/S"-LED statisch, ist der Reader mit der Steuerung verbunden.

Ausführliche Informationen zur Montage sowie Bestelldaten (Reader, Anschlusskabel, Weitbereichsnetzteil, ...) finden Sie im Systemhandbuch "SIMATIC RF300".

4.3 Netztopologie

Der Aufbau des Kommunikationsnetzes kann als Linien-/Reihen-, Stern- oder Ring-Topologie erfolgen.

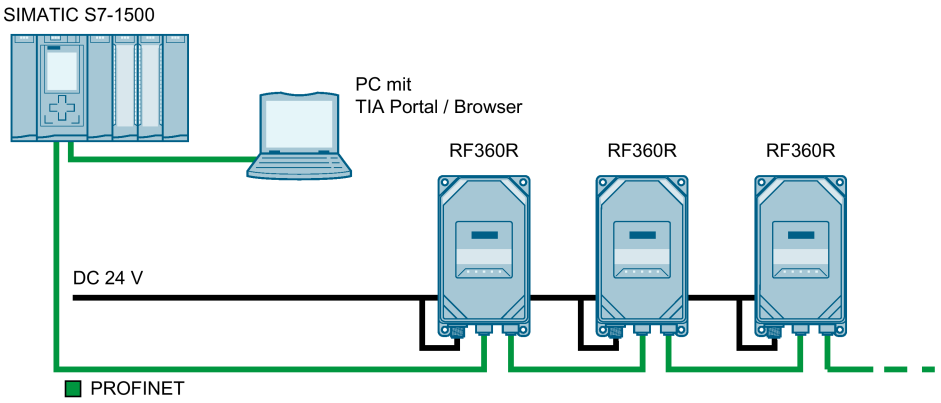


Bild 4-2 Konfigurationsgrafik einer Linien-/Reihen-Topologie

Beachten Sie bei der Linien-/Reihen-Topologie, dass, wenn die Kommunikationsverbindung eines Readers zur Steuerung unterbrochen wird, die Kommunikationsverbindung zu allen nachfolgenden Readern ebenfalls unterbrochen wird.

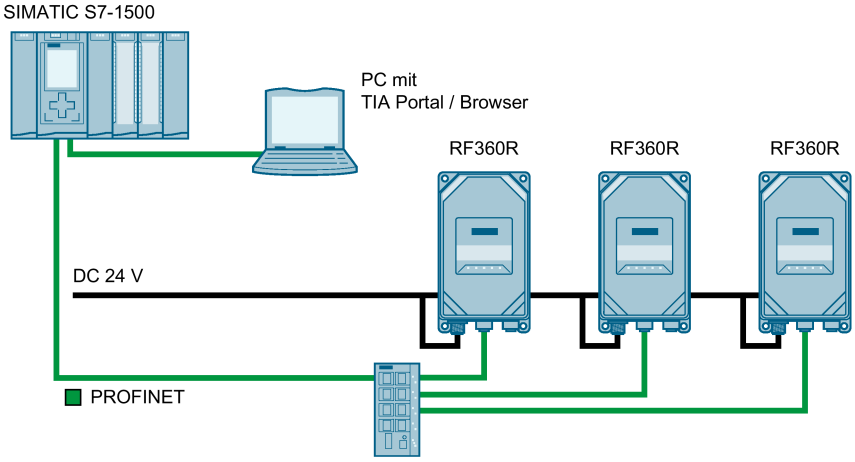


Bild 4-3 Konfigurationsgrafik einer Stern-Topologie

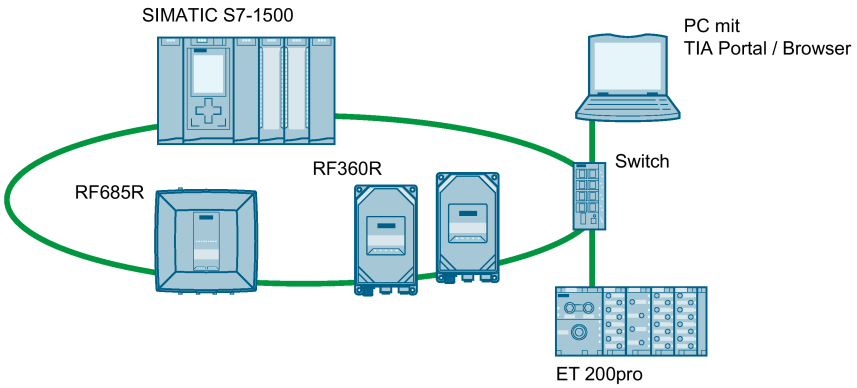


Bild 4-4 Konfigurationsgrafik einer Ring-Topologie

Medienredundanz

Medienredundanz ist eine Funktion zur Sicherstellung der Netz- und Anlagenverfügbarkeit. Redundante Übertragungsstrecken bei der MRP-Ring-Topologie sorgen dafür, dass bei Ausfall einer Übertragungsstrecke ein alternativer Kommunikationsweg zur Verfügung gestellt wird. Um dies zu ermöglichen, müssen Sie die Reader als Client des Medienredundanz-Protokolls (MRP) in STEP 7 (Basic / Professional) projektieren.

MRP ist Bestandteil der PROFINET-Standardisierung nach IEC 61158.

Aufbau einer MRP-Ring-Topologie

Zum Aufbau einer MRP-Ring-Topologie mit Medienredundanz müssen Sie die beiden freien Enden einer Reihen-Topologie in einem Gerät zusammenführen. Der Zusammenschluss der Reihen-Topologie zu einem Ring erfolgt über zwei Netzwerkports eines der Geräte (Ringports). Die Reader können über die Netzwerkports "X1P1R" und "X1P2R" als Clients in eine MRP-Ring-Topologie integriert werden.

Weitere Informationen zum Aufbau einer MRP-Ring-Topologie und deren Projektierung finden Sie in der Online-Hilfe von STEP 7 sowie in der "SIMATIC PROFINET Systembeschreibung (https://support.industry.siemens.com/cs/ww/de/view/19292127)".

Adressieren und Projektieren

5

Geräte-Uhrzeit synchronisieren

Beachten Sie, dass die Uhrzeit der Geräte-Uhr der UTC-Zeit entspricht und nicht an Zeitzonen angepasst werden kann. Es wird empfohlen die Uhrzeit mit einem NTP-Server zu synchronisieren, um eindeutige Zeitangaben zu erhalten. Bei einem Neustart des Geräts wird die Uhrzeit zurückgesetzt und muss synchronisiert werden.

5.1 IP-Adresse / Gerätename vergeben

Um eine einwandfrei funktionierende Kommunikation zwischen PC und Reader bzw. Steuerung und Reader sicherzustellen, müssen Sie den einzelnen Readern eindeutige IP-Adressen bzw. Gerätenamen zuweisen. Abhängig davon in welcher Infrastruktur Sie den Reader betreiben wollen, gibt es folgende unterschiedliche Vorgehensweisen:

- Reader als S7-Anwender in einer Automatisierungsumgebung betreiben.

  Die eindeutige Zuordnung erfolgt über den Gerätenamen und wird mit Hilfe des TIA Portal (STEP 7 Basic / Professional) vergeben.

- Reader als als XML- oder OPC UA-Anwender in einer IT-Umgebung betreiben.

  Die eindeutige Zuordnung erfolgt über DHCP oder die IP-Adresse und kann mit Hilfe von SINEC PNI vergeben werden.

- Reader als Rockwell-Anwender (EtherNet/IP) in einer Automatisierungsumgebung betreiben

  Die eindeutige Zuordnung erfolgt über die IP-Adresse mit Hilfe eines DHCP-Servers.

Die IP-Adressen der Reader werden werkseitig über DHCP zugewiesen. Nachdem dem Reader eine IP-Adresse zugewiesen wurde, können Sie diese später auch mit Hilfe des WBM ändern.

Hinweis

Unterstützung der Option "12"

Bei der Adressenvergabe über DHCP wird auch die Option "12" (hostname) unterstützt. Der hostname kann aus der SNMP-Variablen "sysName" entnommen werden.

Die Variable kann über SNMP-Tools beschrieben werden.

Im Folgenden werden diese alternativen Vorgehensweisen beschrieben.

5.1.1 IP-Adresse / Gerätename über STEP 7 vergeben

Voraussetzungen

STEP 7 Basic / Professional ist installiert, der Reader ist angeschlossen und hochgelaufen.

Vorgehensweise

Gehen Sie folgendermaßen vor, um dem Reader einen eindeutigen Gerätenamen zuzuweisen:

1. Rufen Sie das TIA Portal über "Start > Alle Programme > Siemens Automation > TIA Portal Vxx" auf.
2. Legen Sie ein neues Projekt an.
3. Wechseln Sie in die Projektansicht.
4. Fügen Sie über die Projektnavigation über den Menübefehl "Neues Gerät hinzufügen" eine SIMATIC-Steuerung in das Projekt ein.

   Reaktion: Die Gerätesicht wird geöffnet und die Steuerung wird angezeigt.
5. Wechseln Sie in die Netzsicht und ziehen Sie den Reader aus dem Hardware-Katalog in das Projekt.
6. Weisen Sie den Reader der Steuerung zu.
7. Klicken Sie mit der rechten Maustaste auf den Reader.

8. Wählen Sie im Kontextmenü den Menübefehl "Gerätename zuweisen".

   Reaktion: Das Fenster "PROFINET-Gerätename vergeben" wird geöffnet.

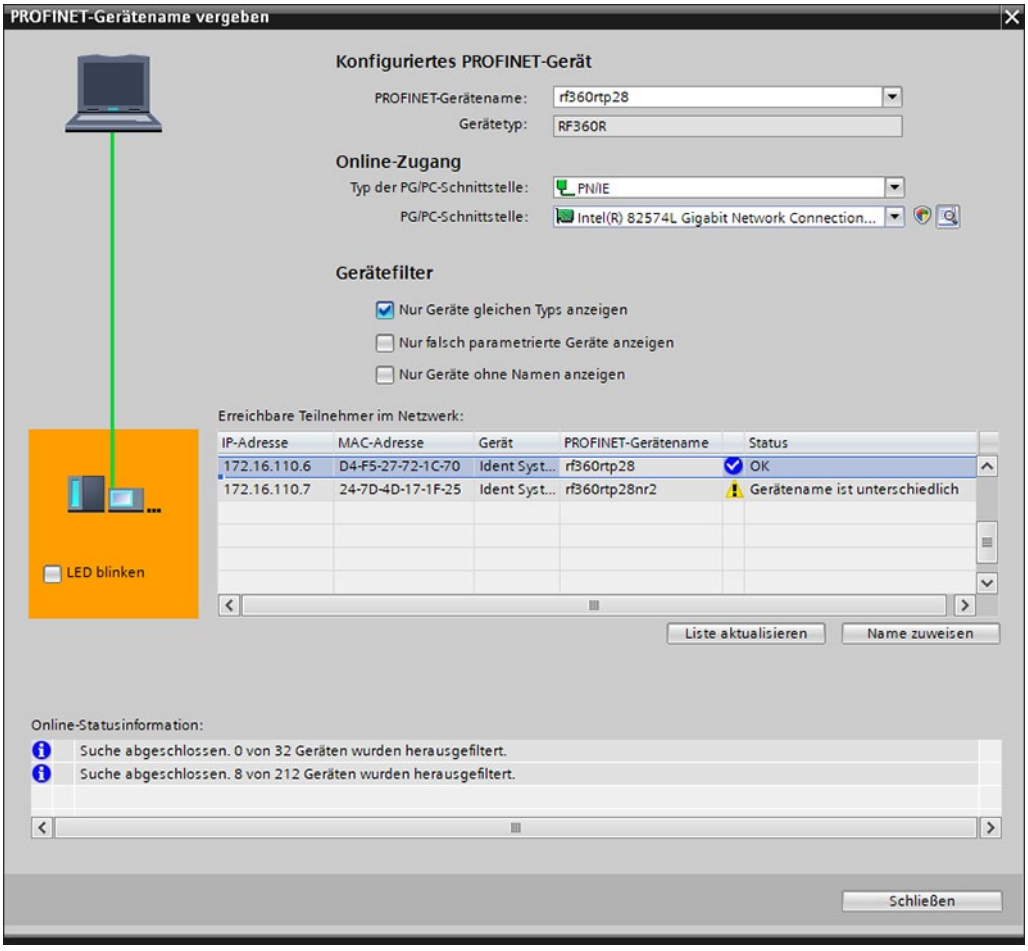


Bild 5-1 Gerätename zuweisen

9. Wählen Sie im Bereich "Online-Zugang" in der Klappliste "Typ der PG/PC-Schnittstelle" die Verbindungsart aus.
10. Wählen Sie im Bereich "Online-Zugang" in der Klappliste "PG/PC-Schnittstelle" die Netzwerkkarte aus, über die der Reader mit dem PG/PC verbunden ist.
11. Klicken Sie auf die Schaltfläche "Liste aktualisieren", um sich alle erreichbaren Teilnehmer im Netzwerk anzeigen zu lassen.
12. Wählen Sie aus der Liste den gewünschten Teilnehmer aus.
13. Klicken Sie auf die Schaltfläche "Name zuweisen", um dem Reader den PROFINET-Gerätename zuzuweisen.

Ergebnis: Dem Reader wird der projektierte PROFINET-Gerätename aus dem Projekt zugewiesen.

Hinweis

Gerätename beim Baugruppentausch vergeben

Bei einem Baugruppentausch können Sie die Gerätenamen automatisch vergeben. Weitere Informationen dazu, finden Sie im Kapitel "Baugruppentausch (Seite 114)".

Teilnehmer-Blinktest mit Hilfe des TIA Portals

Mit Hilfe des Teilnehmer-Blinktest können Sie den Reader schnell und einfach identifizieren, indem Sie die LEDs des Gerätes blinken lassen. Diese Funktion ist vor allem dann hilfreich, wenn mehrere Geräte an der Steuerung angeschlossen sind. Vergleichen Sie in diesem Fall die MAC-Adresse des Gerätes mit der angezeigten MAC-Adresse und wählen Sie dann das gewünschte Gerät aus.

Gehen Sie folgendermaßen vor, um das betreffende Geräte mit Hilfe des Blinktests zu identifizieren:

1. Wählen Sie in der Projektnavigation den Menübefehl "Online Zugänge > Ihren Online-Zugang > Erreichbare Teilnehmer aktualisieren".

   Die zur Verfügung stehenden Teilnehmer werden angezeigt.
2. Selektieren Sie den gewünschten Reader und klicken Sie auf den Eintrag "Online & Diagnose" im Ordner des ausgewählten Devices.
3. Wählen Sie die Option "Funktionen > Namen zuweisen".
4. Klicken Sie auf die Schaltfläche "LED blinken".

   Reaktion: Am ausgewählten Reader blinken die LEDs.
5. Klicken Sie erneut auf die Schaltfläche "LED blinken", um das Blinken wieder zu beenden.

5.1.2 IP-Adresse / Gerätename über SINEC PNI vergeben

Voraussetzungen

SINEC PNI ist installiert und der Reader ist angeschlossen und hochgelaufen. SINEC PNI finden Sie auf den Seiten des "Siemens Industry Online Support (https://support.industry.siemens.com/cs/ww/de/ps/26672/dl)".

Vorgehensweise

Gehen Sie folgendermaßen vor, um dem Reader eine neue, eindeutige IP-Adresse und einen eindeutigen Gerätenamen zuzuweisen:

1. Starten Sie SINEC PNI.
2. Wählen Sie im Menü "Einstellungen" den "Netzwerkadapter" aus, über den der Reader mit dem PC verbunden ist.
3. Stellen Sie sicher, dass das "Scan-Protokoll > PROFINET-Geräte" aktiviert ist.

   Hinweis: Beachten Sie, dass die Funktion "Zusätzliche Informationen auslesen" einige Zeit in Anspruch nehmen kann, wenn viele Geräte in dem Netzwerk enthalten sind.
4. Klicken Sie auf die Schaltfläche "Speichern".
5. Wechseln Sie in das Menü "Geräteliste".
6. Klicken Sie in der Funktionsleiste auf die Schaltfläche "Netzwerk-Scan starten".

   Reaktion: Das Netzwerk wird nach angeschlossenen Geräten durchsucht und alle erkannten Geräte werden in der Geräteliste angezeigt.
7. Markieren Sie den gewünschten Reader in der Geräteliste.
8. Klicken Sie in der Funktionsleiste auf die Schaltfläche "Gerät konfigurieren".

   Reaktion: Das Fenster "Gerätekonfiguration" wird geöffnet.
9. Tragen Sie im Eingabefeld "IP-Adresse" eine neue, eindeutige IP-Adresse des Readers ein.

   Hinweis: Ggf. müssen Sie zuvor die Funktion "DHCP" deaktivieren.
10. Tragen Sie im Eingabefeld "Subnetzmaske" die Subnetzmaske Ihres Netzwerkes ein.
11. Wechseln Sie in das Register "PROFINET".
12. Tragen Sie im Eingabefeld "PROFINET-Gerätename" einen Gerätenamen ein.
13. Klicken Sie auf das Symbol "Laden", um die Einstellungen auf den Reader zu übertragen.

Ergebnis: Dem Reader werden die neue IP-Adresse, Subnetzmaske sowie ein neuer Gerätename zugewiesen.

Teilnehmer-Blinktest mit Hilfe von SINEC PNI

Mit Hilfe des Teilnehmer-Blinktest können Sie den Reader schnell und einfach identifizieren, indem Sie die LEDs des Gerätes blinken lassen. Diese Funktion ist vor allem dann hilfreich, wenn mehrere Geräte am Netzwerk/PC angeschlossen sind.

Gehen Sie folgendermaßen vor, um den betreffenden Reader mit Hilfe des Blinktests zu identifizieren:

1. Wählen Sie im Menü "Geräteliste" aus der Geräteliste die gewünschte Baugruppe aus.
2. Klicken Sie in der Funktionsleiste auf die Schaltfläche "LED blinken".

   Reaktion: Am ausgewählten Reader blinken die LEDs.
3. Klicken Sie auf die Schaltfläche "Stop", um das Blinken wieder zu beenden.

5.1.3 IP-Adresse über DHCP vergeben

Dieses Kapitel richtet sich an alle Anwendertypen in erster Linie an Rockwell-Anwender.

Im Rockwell-Umfeld wird die IP-Adresse mit Hilfe von BOOTP/DHCP vergeben. Der Reader fungiert dabei als DHCP-Client. Rockwell Automation™ stellt hierfür einen BOOTP-/DHCP-Server für Windows zur Verfügung, um der MAC-Adresse des Readers IP-Adressdaten zuzuordnen.

Voraussetzung

Eine aktuelle Version des BOOTP-/DHCP-Servers ist installiert, der Reader ist eingebunden, angeschlossen und hochgelaufen. Der BOOTP-/DHCP-Server ist vorkonfiguriert und steht zur Verfügung.

Informationen zum Einbinden der Reader in Studio 5000 Logix Designer finden Sie im Kapitel "Projektieren über Studio 5000 Logix Designer (Seite 35)".

Vorgehensweise

Gehen Sie folgendermaßen vor, um dem Reader einen eindeutigen Gerätenamen zuzuweisen:

1. Rufen Sie den BOOTP-/DHCP-Server auf.
2. Wählen Sie die gewünschte Netzwerkschnittstelle aus.
3. Doppelklicken Sie im Bereich "Discovery History" auf einen Eintrag.

   Die Eingabemaske "New Entry" wird geöffnet.
4. Tragen Sie im Eingabefeld "IP Adress" eine neue, eindeutige IP-Adresse des Readers ein.

5. Bestätigen Sie die Eingabe mit "OK".

   Im Bereich "Discovery History" wurde dem Eintrag die IP-Adresse zugewiesen.

   Zusätzlich wird im Bereich "Relation List" der Eintrag angezeigt.

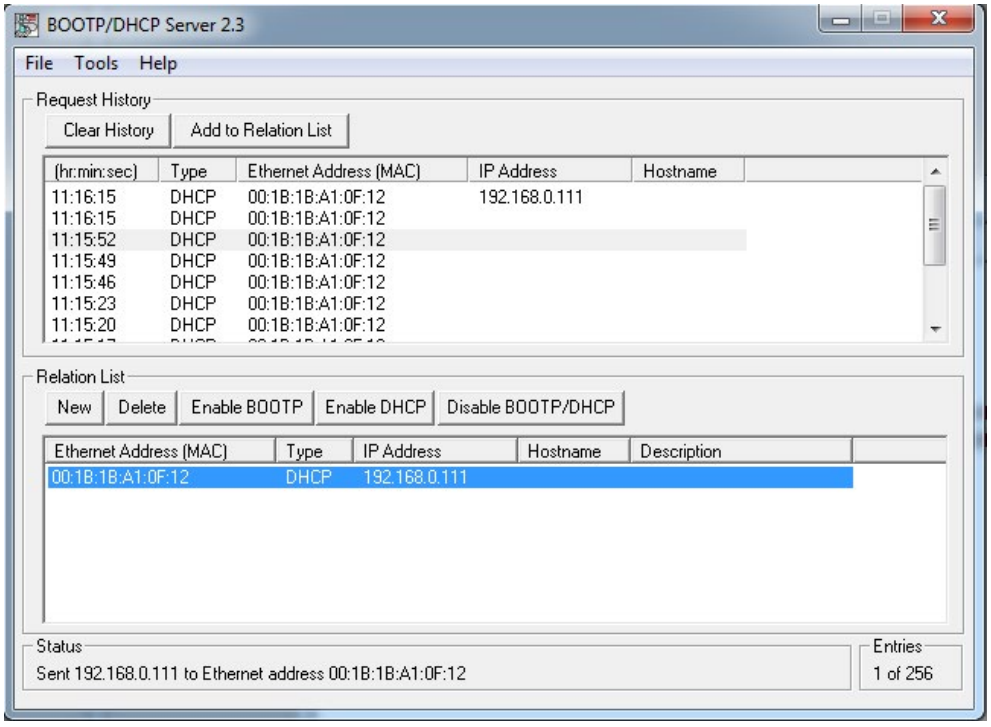


Bild 5-2 BOOTP-/DHCP-Server-Software

6. Klicken Sie auf die Schaltfläche "Disable BOOTP/DHCP", um die IP-Adresse im Reader zu speichern.

Ergebnis: Dem Reader wird die IP-Adresse statisch zugewiesen.

5.2 Projektierung über PROFINET IO (STEP 7)

Ab STEP 7 Basic / Professional V17 ist der Reader RF360R im TIA Portal integriert und kann in SIMATIC-Automatisierungssysteme eingebunden werden. Ab STEP 7 Basic / Professional V16 kann der Reader über eine HSP-Datei, in ältere Versionen (< V16) kann der Reader über eine GSDML-Datei ins TIA Portal integriert werden. Die Anbindung erfolgt über PROFINET, die Konfiguration über das TIA Portal und das Arbeiten über die Ident-Bausteine des TIA Portals. Eine weitergehende Konfiguration des Readers können Sie mit Hilfe des WBM vornehmen.

Beachten Sie, dass bei der Integration über die GSDML-Datei bei TIA Portal-Versionen < V16 die Projektierung nicht über das Technologieobjekt "SIMATIC Ident" erfolgen kann.

Die zu dem Reader passende GSDML-Datei ist auf dem Reader gespeichert und kann mit Hilfe des WBM von diesem heruntergeladen werden ("Der Menüpunkt "System - Geräteeinstellungen" (Seite 84)"). Alternativ finden Sie die GSDML-Datei auf den Seiten des Siemens Industry Online Supports.

Voraussetzungen

STEP 7 Basic / Professional ist installiert, gestartet und ein Projekt ist geöffnet. Der Reader ist über Industrial Ethernet oder PROFINET mit der Steuerung bzw. dem PC verbunden und hochgelaufen.

Der Reader besitzt einen gültigen PROFINET-Gerätenamen.

Vorgehensweise

Gehen Sie folgendermaßen vor, um den Reader über PROFINET IO mit Hilfe des TIA Portals zu projektieren:

1. Wechseln Sie in die Projektansicht.
2. Fügen Sie über die Projektnavigation über den Menübefehl "Neues Gerät hinzufügen" eine SIMATIC-Steuerung in das Projekt ein.

   Die Gerätesicht wird geöffnet und die Steuerung wird angezeigt.
3. Wechseln Sie in die Netzsicht und ziehen Sie den Reader aus dem Hardware-Katalog in das Projekt.
4. Verbinden Sie den Reader mit der Steuerung.
5. Konfigurieren Sie den Reader (z. B. Gerätename, Adressbereich).
6. Parametrieren Sie den Reader (z. B. Baugruppenparameter).
7. Speichern Sie die Konfiguration ab bzw. laden Sie diese in den PROFINET IO-Controller.

Weitere Informationen zur Basis-Konfiguration finden Sie in dem Kapitel "IP-Adresse / Gerätename vergeben (Seite 25)".

Parametrierung über die Gerätekonfiguration

Sie können die Parameter des Readers über das Eigenschaftenfenster des Readers parametrieren. Über die nachfolgenden Parametergruppen können Sie alle baugruppenspezifischen Parameter einstellen.

Parametergruppe "Web Based Management"

In dieser Parametergruppe können Sie das Web Based Management starten.

Tabelle 5- 1 Parameter der Parametergruppe "Web Based Management"

Parameter	Beschreibung
Web Based Management	Web Based Management des Readers starten. Das Web Based Management (WBM) bietet umfangreiche Funktionen, um den Reader zu konfigurieren. Hinweis: Das WBM kann erst gestartet werden, wenn entweder die PROFINET-Verbindung zwischen CPU und Reader aufgebaut ist oder dem Reader die im Projekt hinterlegte IP-Adresse zugewiesen wurde. D. h. der Gerätename muss vergeben sein und die TIA-Projektierung muss in die SIMATIC-Steuerung geladen sein.

Parametergruppe "Konfigurationsmanagement"

In dieser Parametergruppe können Sie Konfigurationsdaten laden oder speichern.

Tabelle 5- 2 Parameter der Parametergruppe "Konfigurationsmanagement"

Parameter	Beschreibung
Benutzername [1)]	Benutzername eines auf dem Reader angelegten Benutzers Beachten Sie, dass der Benutzer über die benötigten Rechte verfügen muss.
Passwort [1)]	Eingabefeld für das Passwort des ausgewählten Benutzers
Konfiguration in Gerät laden	Konfigurationsdaten vom STEP 7-Projekt in den Reader laden.
Konfiguration im Projekt speichern	Konfigurationsdaten des Readers im aktuellen STEP 7-Projekt speichern.

1) Benutzername und Passwort müssen ausschließlich dann eingegeben werden, wenn die Benutzerverwaltung des Readers im WBM aktiviert ist.

Voraussetzung

Folgende Voraussetzungen müssen erfüllt sein, damit Konfigurationsdaten geladen oder gespeichert werden können:

- In dem Parameter "PROFINET-Schnittstelle [X1]" ist die korrekte IP-Adresse des Readers eingetragen.
- Der eingetragene Benutzer hat die nötigen Rechte, um den Down-/Upload durchzuführen.
- Beachten Sie, dass https mit TIA Portal Versionen ≤ V17 nicht unterstützt wird.

Parametergruppe "Baugruppenparameter"

In dieser Parametergruppe können Sie alle baugruppen-spezifischen Parameter des Readers projektieren.

Tabelle 5- 3 Parameter der Parametergruppe "Baugruppenparameter"

Parameter	Parameterwert	Default-Wert	Beschreibung
Diagnosealarm des Geräts	An Aus	An	Diagnosealarmmeldungen des Readers ein-/ausschalten.

Parametergruppe "Baugruppenparameter > Allgemeine Parameter" der Submodule

In dieser Parametergruppe können Sie alle baugruppen-spezifischen Parameter der angeschlossenen Geräte projektieren. Beachten Sie, dass einige der nachfolgenden Parameter modulspezifisch sind. Bei einigen Modultyp werden nicht alle Parameter angezeigt.

Mit Hilfe des Submoduls "Reader configuration_1" können Konfigurationen von dem oder auf das angeschlossene Gerät übertragen werden, sowie Statusabfrage über das Gerät durchgeführt werden. Mit Hilfe des Submoduls "RFID-Kommunikation_1" erfolgt die Kommunikation zwischen Reader und Transponder.

Tabelle 5- 4 Parameter der Parametergruppe "Baugruppenparameter > Allgemeine Parameter" der Submodule

Parameter	Parameterwert	Default-Wert	Beschreibung
User Mode	Ident-Profil/RFID-Normprofil	Ident-Profil/RFID-Normprofil	Mit diesem Parameter wählen Sie den Baustein aus: • Ident-Profil/RFID-Normprofil: Singletag-/Multitag-Betrieb. In der Steuerung kommt der Programmbaustein für das Ident-Profil zum Einsatz.
Diagnose-alarm	Keine Hard Errors Hard/Soft Errors	Keine	Mit diesem Parameter stellen Sie ein, in welchem Umfang readerbezogene Diagnosealarmmeldungen gemeldet werden sollen. • Keine: Es werden keine Alarme generiert. • Hard Errors: Schwerwiegende Hardware-Fehler werden über die S7-Diagnose gemeldet. • Hard/Soft Errors: Schwerwiegende Hardware-Fehler, sowie Fehler, die während der Befehlsbearbeitung auftreten, werden über die S7-Diagnose gemeldet.

Beschreibung der Baustein-Befehle

Eine Beschreibung der bausteinspezifischen Befehle finden Sie in den jeweiligen Baustein-Handbüchern:

- RFID-Normprofil; Standardfunktion für RFID-Systeme
- Ident-Profil und Ident-Bausteine, Standardfunktion für Ident-Systeme

5.3 Projektierung über XML

Dieses Kapitel richtet sich ausschließlich an XML-Anwender.

Bei der reinen XML-Arbeit ist eine Projektierung des Readers nicht notwendig. Sie können direkt mit der Konfiguration über das WBM und dem Programmieren über XML fortsetzen. Ausführliche Informationen hierzu finden Sie im Handbuch "XML-Programmierung für SIMATIC Ident (https://support.industry.siemens.com/cs/ww/de/view/109781631)".

5.4 Projektierung über OPC UA

Dieses Kapitel richtet sich ausschließlich an OPC UA-Anwender.

Bei der reinen OPC UA-Arbeit ist eine Projektierung des Readers nicht notwendig. Sie können direkt mit der Konfiguration über das WBM und dem Programmieren über OPC UA fortsetzen. Ausführliche Informationen hierzu Sie im Handbuch "OPC UA für SIMATIC Ident (https://support.industry.siemens.com/cs/ww/de/ps/14971/man)".

5.5 Projektieren über Studio 5000 Logix Designer

Dieses Kapitel richtet sich ausschließlich an Anwender von Rockwell-Steuerungen.

Sie können den Reader mit Hilfe von Add-On Instructions über eine Rockwell-Steuerung projektieren. Eine ausführliche Beschreibung des Ident-Profils und der Add-On Instructions finden Sie im Funktionshandbuch "Ident-Profil, Add-On Instructions für Rockwell-Systeme (https://support.industry.siemens.com/cs/ww/de/view/109781634/137304404619)".

Hinweis

Seriennummer im Studio 5000 Logix Designer

Beachten Sie, dass die im Studio 5000 Logix Designer angegebene Seriennummer nicht mit der Reader-Seriennummer übereinstimmt. Die im Logix Designer angegebene Seriennummer bildet die letzten 4 Byte der MAC-Adresse des Readers ab.

Hinweis

Getestete Programme

Die in diesem Kapitel beschriebenen Inhalte wurden mit den Programmen "Studio 5000 Logix Designer" (V21 bis V28) und "RSLogix 5000" (V20) getestet.

Konfigurieren über das WBM

6

Die Reader sind mit einem Webserver ausgestattet, der dem Web-Client ein Web Based Management (WBM) zur Konfiguration der Reader bereitstellt. Das WBM kann über den Webbrowser eines PCs/Laptops aufgerufen werden.

Der WBM-Server stellt dem Web-Client (PC/Laptop) die Parameterdaten des Readers bereit und nimmt Parameteränderungen von dem Web-Client entgegen. Beachten Sie, dass geänderte Parameterwerte nicht automatisch an den Reader übertragen werden. Änderungen in der Konfiguration müssen Sie immer manuell an den Reader übertragen.

Nachfolgend wird der Begriff "WBM" stellvertretend für die im Webbrowser angezeigte Oberfläche des WBM verwendet.

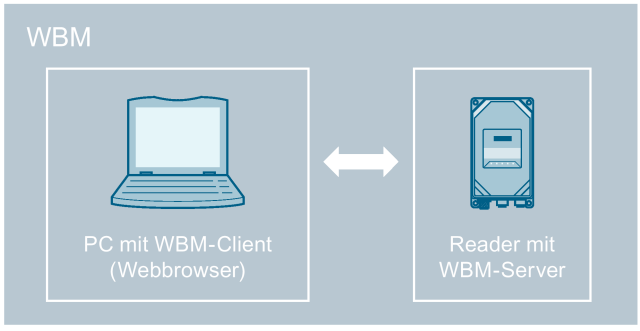


Bild 6-1 Aufbau und Funktionsweise des WBMs

6.1 WBM starten

Voraussetzung

Der Reader ist angeschlossen, eingeschaltet und betriebsbereit ("RUN"-LED leuchtet/blinkt grün) und dem Reader wurde eine IP-Adresse zugewiesen.

Um ein flüssiges Arbeiten mit dem WBM sicherzustellen, empfehlen wir Ihnen einen PC mit folgenden Mindestanforderungen:

- CPU: DualCore
- RAM: 2 GB

Sie können das WBM über die zum Veröffentlichungsdatum dieses Handbuchs aktuellen Versionen der folgenden Webbrowser aufrufen: Microsoft Edge, Mozilla Firefox und Google Chrome. Die Oberfläche des WBM ist auf eine Bildschirmauflösung von mindestens 1366 × 768 Pixel ausgelegt.

ACHTUNG
Abbruch von Diagnosen aufgrund geöffneter Browser-Register Beachten Sie, dass einige Webbrowser Webseiten nicht mehr aktualisieren, wenn andere Register (Tabs) im Vordergrund sind. Dieses Verhalten kann dazu führen, dass laufende Diagnosen beendet werden.

Vorgehensweise

Gehen Sie folgendermaßen vor, um das WBM zu starten:

1. Starten Sie Ihren Webbrowser.
2. Geben Sie die IP-Adresse des Readers mit vorangestelltem "https://" in das Adressfeld Ihres Browsers ein.
3. Bestätigen Sie die Eingabe durch Drücken der <Enter>-Taste.

Hinweis

HTTPS-Zertifikate aktualisieren

Beim erstmaligen Anmelden wird das HTTPS-Zertifikat des Readers als unsicher angezeigt. Beachten Sie, dass das in dem Reader hinterlegte Zertifikat ausschließlich sicherstellen soll, dass der erste Verbindungsaufbau zu dem Reader verschlüsselt wird. Bestätigen Sie die Sicherheit des Zertifikats. Übertragen Sie anschließend ein eigenes, sicheres Zertifikat auf den Reader.

Ergebnis: Das WBM des Readers öffnet sich.

Alternativ können Sie das WBM auch aus dem TIA Portal heraus öffnen.

Hinweis

Verbindung zum Reader kann nicht hergestellt werden

Kann keine Verbindung zu dem Reader hergestellt werden, prüfen Sie folgende Punkte:

- Stellen Sie sicher, dass alle Kabel richtig verbunden sind.
- Stellen Sie sicher, dass die Ethernet-Verbindung aufgebaut wurde ("LK"-LED leuchtet grün).
- Stellen Sie sicher, dass der Reader hochgelaufen ist ("RUN"-LED leuchtet/blinkt grün).
- Überprüfen Sie die IP-Adressen des PCs und des Readers sowie die Subnetzmaske. Beide IP-Adressen müssen sich im gleichen Subnetz befinden.
- Stellen Sie sicher, dass die Verbindung nicht durch eine Firewall blockiert wird.
- Überprüfen Sie die Verbindung zwischen PC und Reader mit Hilfe einer Ping-Anfrage.

Erstmaliges Anmelden im WBM

Beim erstmaligen Anmelden im WBM erscheint ein Popup-Fenster, in dem Sie dazu aufgefordert werden sich mit dem voreingestellten Default-Benutzer "admin" anzumelden.

1. Wählen Sie aus der Klappliste die gewünschte Oberflächensprache aus.
2. Tragen Sie im Eingabefeld "Benutzer" den voreingestellten Default-Benutzernamen "admin" ein.
3. Tragen Sie im Eingabefeld "Passwort" das voreingestellte Default-Passwort "admin" ein.
4. Klicken Sie auf die Schaltfläche "Anmelden".

   Reaktion: Das Popup-Fenster wird aktualisiert und Sie werden dazu aufgefordert das Default-Passwort für den Benutzer "admin" zu ändern.

   Hinweis: Alternativ können Sie über die Schaltfläche "Authentifizierung deaktivieren" die Authentifizierung deaktivieren.

ACHTUNG
Security-Empfehlung: Authentifizierung Um sicherzustellen, dass keine unbefugten Personen Zugriff auf die Reader-Einstellungen haben, empfehlen wir Ihnen, die Authentifizierung aktiviert zu lassen und neue Benutzerprofile anzulegen. Beachten Sie hierzu die Hinweise im Absatz "Passwörter" im Kapitel "Security-Empfehlungen (Seite 7)". Die Authentifizierung kann ausschließlich durch einen Administrator aktiviert/deaktiviert werden kann. Weitere Informationen zum Anmelden am WBM und dem Anlegen/Löschen von Benutzerprofilen, finden Sie im Kapitel "Der Menüpunkt "Benutzerverwaltung" (Seite 74)".

5. Wählen Sie ggf. aus der Klappliste "Einsatzumgebung" die primäre Schnittstellenverbindung aus, über die Sie den Reader betreiben.
6. Tragen Sie im Eingabefeld "Neues Passwort" Ihr neues Passwort für den Benutzer "admin" ein.
7. Tragen Sie im Eingabefeld "Passwort bestätigen" nochmals das neu gewählte Passwort ein.
8. Klicken Sie auf die Schaltfläche "Anmelden".

Ergebnis: Sie sind mit dem Profil "admin" am WBM angemeldet und können jetzt den Reader parametrieren.

Einsatzumgebung

Abhängig von der ausgewählten Einsatzumgebung werden vorab die zu dem Modus passenden Schnittstellen, Kommunikationskanäle, sowie die dazugehörigen Dienste freigeschaltet. Dabei werden die zu dem Modus gehörenden Parameterwerte auf die werkseitig festgelegten Standardwerte gesetzt.

Diese Funktion erhöht die Sicherheit ihres Geräts, da alle anderen Schnittstellen, Kommunikationskanäle und die dazugehörigen Dienste deaktiviert werden.

Reguläres Anmelden am WBM

Abhängig davon, ob die Authentifizierung aktiviert oder deaktiviert ist, müssen Sie sich ggf. mit Ihrem Benutzernamen und dem dazugehörigen Passwort anmelden. Nach der Anmeldung, und auch bei deaktivierter Authentifizierung, wird die Startseite des WBM geöffnet.

Über den Link "Readme OSS" können Sie die Readme OSS-Datei mit den Copyright-Hinweisen und Lizenzbedingungen zu der in dieser Firmware enthaltenen Open Source Software öffnen. Über den Link "Handbuch" können Sie das zu dem Reader bzw. WBM gehörige Handbuch öffnen.

6.2 Das WBM

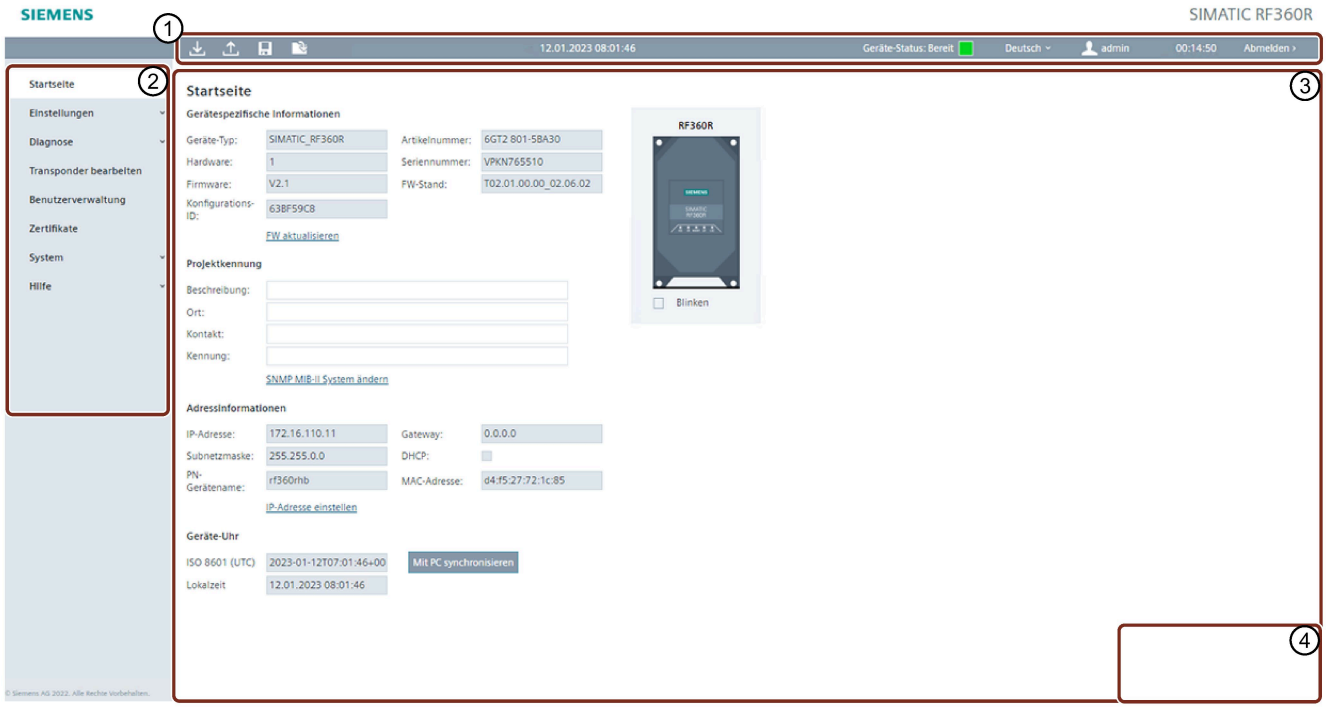
Mit Hilfe des WBM können Sie die Reader SIMATIC RF360R konfigurieren.

Nachdem Sie neue Benutzerprofile angelegt haben, müssen Sie sich beim erneuten Starten des WBM mit einem dieser Benutzerprofile anmelden.

ACHTUNG
Zugriff auf den Reader Beachten Sie, dass der zeitgleiche Zugriff auf einen Reader über zwei WBM-Clients (Webbrowser) möglich ist, jedoch nicht empfohlen wird. Werden bei einem zeitgleichen Zugriff über zwei WBM-Clients parallel Änderungen durchgeführt, kann dies zu Fehlern in der Konfiguration oder zu einem unerwünschten Ergebnis führen.

Der Aufbau des WBM

Nach erfolgreichem Verbindungsaufbau zum Reader und Anmeldung (bei aktiver Authentifizierung) erscheint das Startfenster des WBM:



Das Startfenster des WBM ist in folgende Bereiche eingeteilt:

① Funktions-/Statusleiste (inkl. Abmeldebereich)
② Menübaum
③ Hauptfenster
④ Meldebereich

Bild 6-2 Startfenster des WBM

Funktions- und Statusleiste ①

Funktionsleiste

Links oberhalb des Hauptfensters befinden sich vier Schaltflächen zum Übertragen/Laden/Speichern der angezeigten Konfiguration. Sie können diese Schaltflächen auch über Tastenkombinationen direkt bedienen.

Tabelle 6- 1 Die Funktionsleiste des WBM

Symbol	Beschreibung
	Konfiguration auf den Reader übertragen Mit Hilfe dieser Schaltfläche können Sie die im WBM eingestellten Konfigurationsdaten an den Reader übertragen. Tastenkombination: Strg + L **Hinweis** Beachten Sie, dass durch das Übertragen einer Konfiguration aktuell laufende Anwenderapplikationen gestört werden können. Im WBM werden Sie durch einen orangenen Balken in der Hinweisleiste gewarnt, wenn dies der Fall ist.
	Konfiguration vom Reader laden Mit Hilfe dieser Schaltfläche können Sie die im Reader eingestellten Konfigurationsdaten in das WBM laden. Tastenkombination: Strg + G **Hinweis** Beachten Sie, dass Sie mit Hilfe der Konfigurationsdatei keine Benutzerprofile und Passwörter auf andere Reader übertragen können. Nach dem Laden der Konfigurationsdatei in einen neuen Reader müssen Sie ggf. die Authentifizierung aktivieren und neue Benutzerprofile und Passwörter anlegen.
	Konfiguration speichern unter Mit Hilfe dieser Schaltfläche können Sie die im WBM eingestellten Konfigurationsdaten auf dem PC speichern. Tastenkombination: Strg + S
	Konfiguration vom PC laden Mit Hilfe dieser Schaltfläche können Sie die auf dem PC gespeicherten Konfigurationsdaten in das WBM laden. Beachten Sie, dass diese Daten nur in das WBM geladen werden. Zum Übertragen der Daten an den Reader, müssen Sie zusätzlich die Schaltfläche "Konfiguration auf den Reader übertragen" klicken. Tastenkombination: Strg + O

Statusleiste

Rechts oberhalb des Hauptfensters befindet sich die Statusleiste mit folgenden Informationen:

- Datum-/Uhrzeitanzeige des Readers

  Beachten Sie, dass der Zeitstempel von der Geräte-Uhr (UTC-Zeit) erzeugt wird. Diese Uhrzeit wird mit dem/der im PC eingestellten Zeitformat und Zeitzone abgeglichen und im entsprechenden Format angezeigt.

- Anzeige des Geräte-Status

  Folgende Geräte-Stati sind möglich:

	Bereit Der Reader ist betriebsbereit.
	In Betrieb Der Reader ist in Betrieb und hat eine Verbindung aufgebaut.
	In Betrieb Der Reader ist in Betrieb und hat mehrere Verbindungen aufgebaut (z. B. via PNIO und XML).
	Fehler (Bereit) Der Reader ist betriebsbereit und ein Fehler liegt vor.
	Fehler (In Betrieb) Der Reader ist in Betrieb, hat eine Verbindung aufgebaut und ein Fehler liegt vor.
	Fehler (In Betrieb) Der Reader ist in Betrieb, hat mehrere Verbindungen aufgebaut und ein Fehler liegt vor.

- Klappliste zur Auswahl der Oberflächensprache
- Angemeldeter Benutzer (bei aktiver Authentifizierung)
- Anzeige der Zeit bis zur automatischen Abmeldung, sowie Klappliste zur Auswahl der Zeitspanne
- Abmeldebereich (bei aktiver Authentifizierung)

Änderungshinweise in der Oberfläche

Abweichungen zwischen den Einstellungen in der Oberfläche des WBM zu der im angeschlossenen Reader gespeicherten Konfiguration werden durch ein Symbol in der Oberfläche angezeigt. Wird ein Wert in der Oberfläche des WBMs geändert, dann wird das betreffende Feld durch ein Symbol markiert. Zusätzlich dazu wird ggf. auch das Register, sowie der Menüpunkt in dem sich der geänderte Wert befindet und die Schaltfläche "Konfiguration auf Reader übertragen" durch ein Symbol markiert. Dabei wird zwischen den folgenden Symbolen unterschieden:

- Dieses Symbol zeigt an, dass es sich um eine einfache Änderung handelt.
- Dieses Symbol zeigt an, dass während des Zugriffs auf dem Reader über das WBM parallel durch eine andere Applikation eine Änderung durchgeführt wurde. Um sicherzustellen, dass die Änderung nicht verloren geht, sollten Sie die Konfiguration vom Reader laden.
- Dieses Symbol zeigt an, dass es sich um eine Änderung handelt, die beim Übertragen zu einem Neustart des Readers führt.

Menübaum ②

Am linken Rand des WBM befindet sich der Menübaum. Der aktuell ausgewählte Menüpunkt wird farblich hervorgehoben.

Die nachfolgende Tabelle gibt Ihnen einen Überblick über die Menüpunkte und die enthaltenen Funktionalitäten.

Tabelle 6- 2 Die Menüstruktur des WBM

Menüpunkte		**Funktionalitäten**
Startseite		• Systemüberblick • Gerätespezifische Informationen einsehen • Kundenspezifische Anlagenkennzeichen eintragen
Einstellungen		
	Allgemein	Kategorien der Logbuch-Ereignisse aktivieren/deaktivieren
	Reader-Schnittstelle	Reader konfigurieren
	Kommunikation	Kommunikationseinstellungen vornehmen
Diagnose		
	Hardware-Diagnose	Schnittstellen-spezifische Diagnosefunktion
	Logbuch	Übersicht der Logbuch-Einträge
	Service-Logbuch	Informationen für den Service-Fall
	Syslog-Logbuch	Übersicht der Syslog-Meldungen

Menüpunkte		Funktionalitäten
Transponder bearbeiten		Transponder-Daten auslesen und beschreiben
Benutzerverwaltung		• Authentifizierung aktivieren/deaktivieren • Benutzerprofile anlegen und löschen • Passwörter ändern • Sicherheitseinstellungen konfigurieren
Zertifikate		• HTTPS-Zertifikate importieren • OPC UA-Zertifikate importieren
System		
	Geräteeinstellungen	• Firmware-Update durchführen • Reader zurücksetzen • Gerätebeschreibungsdateien herunterladen
Hilfe		Reader-relevante Dokumentationen
	Service und Support	Weiterführende Informationen zu dem Reader
	Handbuch	Handbuch des Readers

Wenn Sie mit der Rolle "Benutzer" angemeldet sind, sind einige Menüpunkte nur eingeschränkt nutzbar. Eine Auflistung der Einschränkungen finden Sie im Kapitel "Der Menüpunkt "Benutzerverwaltung" (Seite 74)".

Hauptfenster ③

Das Hauptfenster zeigt die Inhalte der ausgewählten Menüpunkte an. Hier können Sie die verschiedenen, menüabhängigen Parameter konfigurieren.

Meldebereich ④

Im Meldebereich werden alle WBM bezogenen Fehlermeldungen und Warnungen angezeigt (z. B. Übertragungsfehler).

Bedienung des WBM über die Tastatur

Neben der Bedienung mit der Maus, können Sie die Oberflächenobjekte/Eingabefelder auch mit Hilfe der Tastatur ansteuern:

- TAB

  Sprung zum nächsten Oberflächenobjekt/Eingabefeld

- SHIFT + TAB

  Sprung zum vorherigen Oberflächenobjekt/Eingabefeld

Neben der manuellen Eingabe von Werten können Sie die Werte in den Eingabefeldern auch über folgende Tasten ändern:

- Pfeil nach oben / nach unten

  Wert wird um eine Schrittweite erhöht bzw. verringert.

- Bild hoch / Bild runter

  Wert wird um zehn Schrittweiten erhöht bzw. verringert.

- Pos1 / Ende

  Wert wird auf den Minimal- bzw. Maximalwert gesetzt.

6.3 Die Menüpunkte des WBM

6.3.1 Der Menüpunkt "Startseite"

Der Menüpunkt "Startseite" ist in folgende Bereiche unterteilt:

- Gerätespezifische Informationen
- Projektkennung
- Adressinformationen
- Geräte-Uhr
- Konfigurationsdarstellung

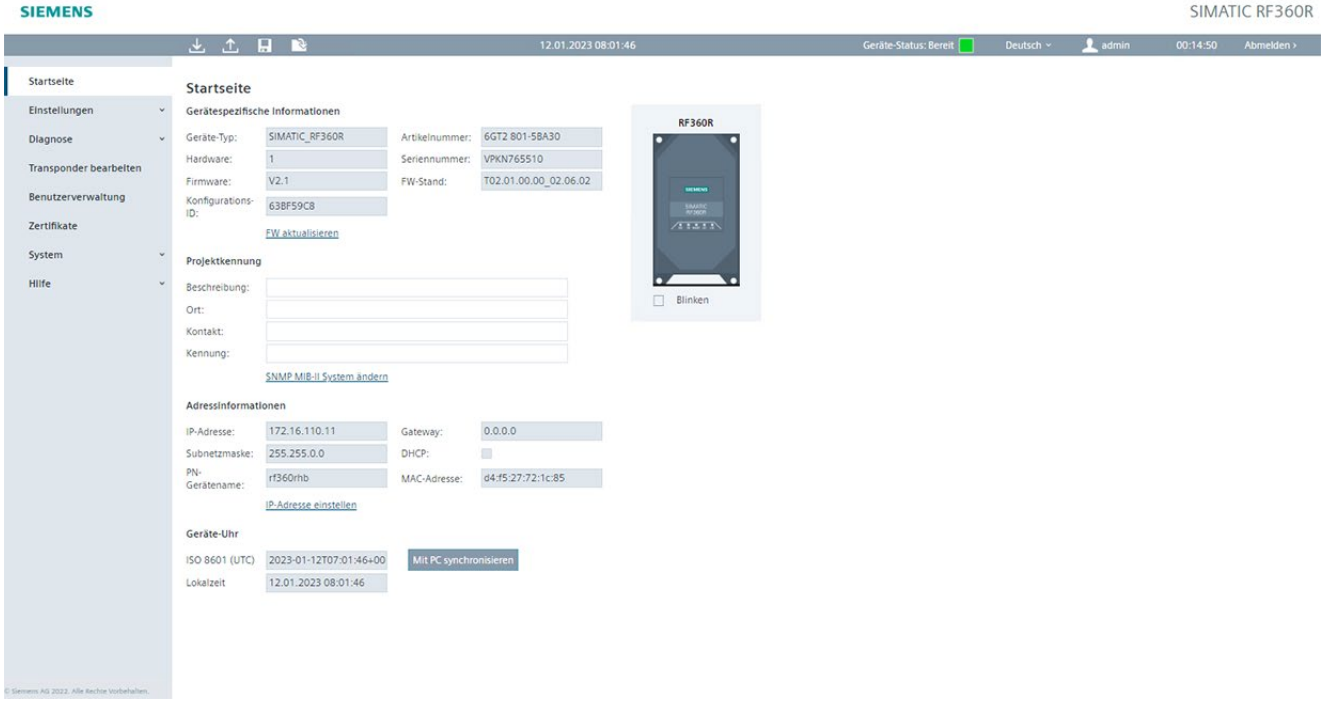


Bild 6-3 Der Menüpunkt "Startseite"

Gerätespezifische Informationen

Der erste Bereich enthält gerätespezifische Informationen. Die Felder "Geräte-Typ", "Artikelnummer", "Hardware" und "Seriennummer" sind werkseitig festgelegt. Die Inhalte der Felder "Firmware" und "FW-Stand" sind abhängig von der auf dem Reader hinterlegten Firmware. Über den Link "FW aktualisieren" springen Sie in den Menüpunkt "System", in dem Sie ein Firmware-Update durchführen können. Das Feld "Konfigurations-ID" enthält eine eindeutige Kennung der Konfiguration, die zuletzt im Reader aktiviert bzw. in den Reader geladen wurde. Klicken Sie auf die Schaltfläche "Standardkonfiguration", um die in der Benutzeroberfläche angezeigten Parameter auf die Standardwerte zurückzusetzen. Beim Wiederherstellen der Standardkonfiguration bleiben die Adressinformationen (IP-Adresse, PN-Gerätename) erhalten.

Projektkennung

Der zweite Bereich enthält Eingabefelder, über die Sie eigene, gerätespezifische Informationen im Reader hinterlegen können. Diese sollen Ihnen u. A. dabei helfen, die einzelnen Reader leichter zu identifizieren. Über den Link "SNMP MIB-II System" springen Sie in den Menüpunkt "Kommunikation", in dem Sie die MIB-Variablen einsehen und ändern können.

Adressinformationen

Der dritte Bereich enthält alle wichtigen Adressinformationen, über die der PC oder die Steuerung den Reader erreichen kann. Die IP-Adresse, sowie PN-Gerätenamen können Sie mit Hilfe von "SINEC PNI" und "STEP 7" dem Reader zuweisen. Über den Link "IP-Adresse" springen Sie in den Menüpunkt "System", in dem Sie ebenfalls die IP-Adresse neu zuweisen können.

Geräte-Uhr

In diesem Bereich wird die Geräte-Uhrzeit nach ISO 8601 (UTC), sowie die die umgerechnete lokale Uhrzeit angezeigt. Über die Schaltfläche "Mit PC synchronisieren" können Sie die angezeigte Lokalzeit mit der in Ihrem Betriebssystem hinterlegten Uhrzeit synchronisieren.

Hinweis

Geräte-Uhrzeit entspricht immer der UTC-Zeit (ISO 8601)

Beachten Sie, dass die Geräte-Uhrzeit immer der UTC-Zeit entspricht (ISO 8601) und nicht an Zeitzonen angepasst werden kann. Durch Klicken der Schaltfläche wird die in Ihrem Betriebssystem hinterlegte lokale Uhrzeit in das WBM übertragen. Da bei einem Abbruch der Spannungsversorgung die mit dem PC synchronisierte Uhrzeit verloren geht, empfehlen wir Ihnen die Uhrzeit mit einem NTP-Server zu synchronisieren.

Konfigurationsdarstellung

Rechts neben den Bereichen wird der Reader schematisch darstellt. Mit Hilfe des Optionskästchens "Blinken" können Sie die LEDs des Readers blinken lassen. Dies ermöglicht Ihnen eine schnelle und einfache Sicht-Identifizierung des Readers.

6.3.2 Der Menüpunkt "Einstellungen - Allgemein"

Der Menüpunkt "Einstellungen - Allgemein" ist in folgende Bereiche unterteilt:

- Logbuch-Einstellungen
- Service-Logbuch-Einstellungen

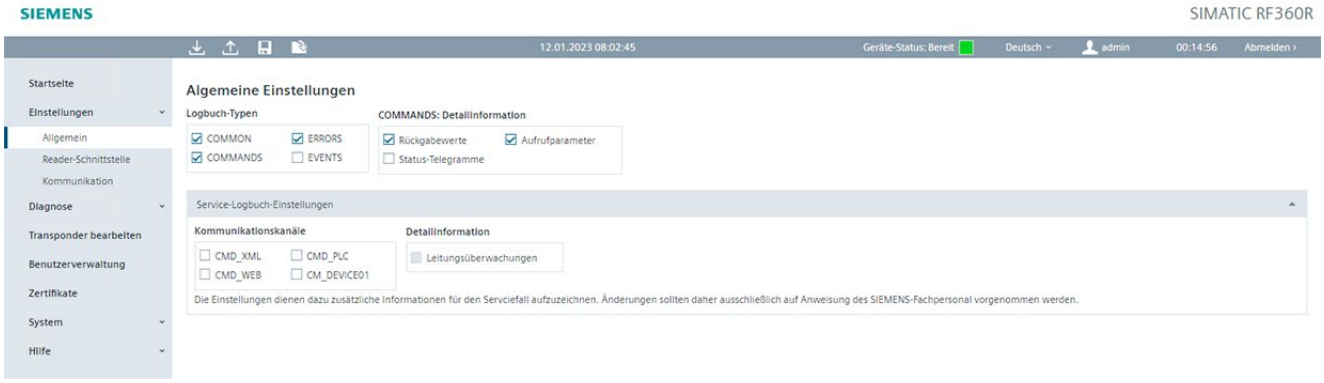


Bild 6-4 Der Menüpunkt "Einstellungen - Allgemein"

Logbuch-Einstellungen

In dem Bereich "Logbuch-Einstellungen" können Sie durch Aktivieren der Optionskästchen festlegen, welche Ereignisse in das Logbuch eingetragen werden. Das Logbuch ist als Ringpuffer aufgebaut. Bedenken Sie, dass durch einen hohen Detailgrad der Daten der Ringpuffer schneller befüllt wird und die Performance des Gerätes negativ beeinflusst werden kann.

Tabelle 6- 3 Beschreibung der Parameter des Logbuchs

Parameter	Beschreibung
Logbuch-Typen	
COMMON	Meldungen zu allgemeinen Ereignissen: z. B. Reader-Hochlauf, Login am WBM, ...
ERRORS	Fehler und Alarmmeldungen des Readers
COMMANDS	Befehle der Anwenderapplikation
EVENTS	Aufzeichnung aller Tag-Events
COMMANDS: Detailinformationen	
Rückgabewert	Rückgabewerte zu den Befehlen der Anwenderapplikation sowie zu den geschriebenen bzw. gelesenen Transponder-Daten.
Aufrufparameter	Aufrufparameter zu den Befehlen der Anwenderapplikation
Status-Telegramme	Aufzeichnung der Status-Telegramme bei der PLC-Kommunikation. Kann ausgeschaltet werden, falls die Status-Telegramme als Leitungsüberwachung verwendet werden. Dadurch wird das Logbuch für Nutzdaten freigehalten.

Service-Logbuch-Einstellungen

In dem Bereich "Service-Logbuch-Einstellungen" können Sie durch Aktivieren der Optionskästchen festlegen, welche Ereignisse in das Service-Logbuch eingetragen werden. Das Service-Logbuch ist als Ringpuffer aufgebaut. Bedenken Sie, dass durch einen hohen Detailgrad der Daten der Ringpuffer schneller befüllt wird und die Performance des Gerätes negativ beeinflusst werden kann.

Tabelle 6- 4 Beschreibung der Parameter des Service-Logbuchs

Parameter	Beschreibung
Kommunikationskanäle	
CMD_XML	Telegramme auf der XML-Schnittstelle
CMD_PLC	Interne Telegramme auf der PLC-Schnittstelle
CMD_WEB	Interne Telegramme zum Webserver
CM_DEVICE01	Telegramme auf der internen Schnittstelle
Detailinformationen	
Leitungs-überwachung	Aufzeichnung der Leitungsüberwachungstelegramme (CMD_XML und CMD_PLC) bei den Service-Informationen. Kann ausgeschaltet werden, um das Logbuch für Nutzdaten freizuhalten.

6.3.3 Der Menüpunkt "Einstellungen - Reader-Schnittstelle"

In dem Menüpunkt "Einstellungen - Reader-Schnittstelle" können Sie die Reader-Parameter (Reset-Parameter) konfigurieren. Ist der Reader an eine S7-Steuerung angeschlossen, dann wird die Konfiguration über die Steuerung vorgenommen. In diesem Fall werden die Parameter im Bereich "Reader-Parameter" nicht angezeigt.

Diese Seite ist in folgende Bereiche unterteilt:

- Basiseinstellungen
- Reader-Parameter

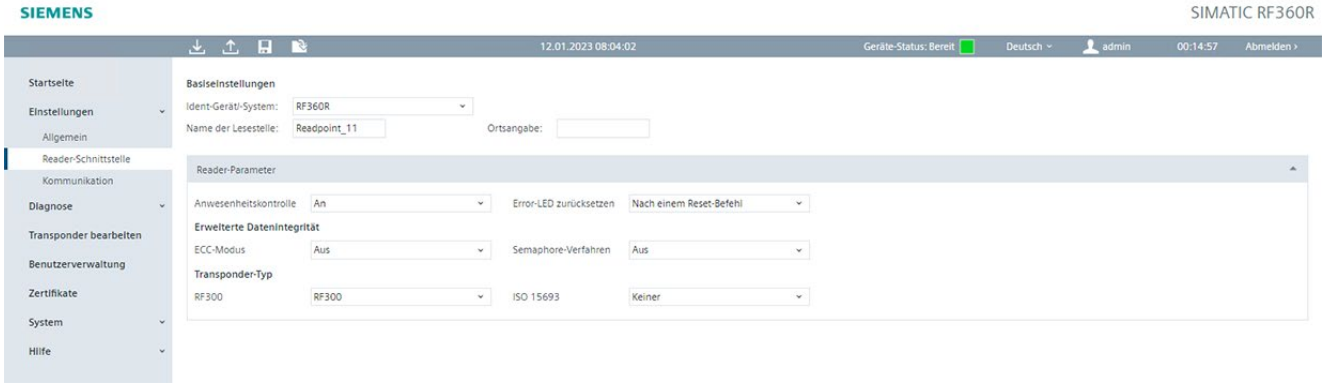


Bild 6-5 Der Menüpunkt "Einstellungen - Reader-Schnittstelle"

Basiseinstellungen

In diesem Bereich legen Sie die Basiseinstellungen für die Lesestelle fest.

Tabelle 6- 5 Parameter der Parametergruppe "Basiseinstellungen"

Parameter	Parameterwert	Default-Wert	Beschreibung
Ident-Geräte/-System	RF360R Allgemeiner Reader	RF360R	Auswahl des an dem Reader angeschlossenen Geräts/Systems. Abhängig von der getroffenen Auswahl, werden in dem nachfolgenden Bereich "Reader-Parameter" unterschiedliche Parameter ein-/ausgeblendet.
Name der Lesestelle	--	--	Eingabefeld, um den Namen der Lesestelle festzulegen.
Ortsangabe	--	--	Eingabefeld, um Informationen zum Standort der Lesestelle einzugeben. Diese Information wird bei den OPC UA Scan-Events ausgegeben.

Reader-Parameter

Haben Sie in dem Parameter "Ident-Geräte/-System" den Parameterwert "Allgemeiner Reader" ausgewählt, dann werden in diesem Bereich die Reset-Parameter des Readers in hexadezimaler Darstellung angezeigt. Ausführliche Informationen dazu finden Sie in dem Handbuch "Ident-Profil und Ident-Bausteine, Standardfunktionen für Ident-Systeme (https://support.industry.siemens.com/cs/ww/de/view/109793329)".

Haben Sie in dem Parameter "Ident-Geräte/-System" den Parameterwert "RF360R" ausgewählt, dann können Sie nachfolgende Reader-Parameter konfigurieren.

Tabelle 6- 6 Parameter der Parametergruppe "Reader-Parameter"

Parameter	Parameterwert	Default-Wert	Beschreibung
Anwesenheitskontrolle	An Aus (HF-Feld an) Aus (HF-Feld aus)	An	An = Sobald sich ein Transponder im Antennenfeld des Readers befindet, wird dessen Anwesenheit gemeldet. Aus (HF-Feld an) = Die Anwesenheitsanzeige am FB wird unterdrückt. Die Antenne am Reader ist jedoch eingeschaltet, solange diese nicht durch einen Befehl abgeschaltet wurde. Aus (HF-Feld aus) = Die Antenne wird nur eingeschaltet, wenn ein Befehl abgeschickt wird und schaltet sich danach wieder ab.
Error-LED zurücksetzen	Aus An	An	Aus = An der Error-LED wird immer der letzte Fehler angezeigt. Ein Rücksetzen der Anzeige ist nur durch Ausschalten des Readers möglich. An = Das Blinken der Error-LED am Reader wird durch jeden Reset, sowie durch einen neuen OPC-Befehl zurückgesetzt.

Parameter	Parameterwert	Default-Wert	Beschreibung
	Aus Nach einem erfolgreichen Befehl Nach einem Reset-Befehl Nach einem Reset- oder einem erfolgreichen Befehl		Aus = Das Blinken der LED im Fehlerfall wird nicht zurückgesetzt, auch nicht durch Abschalten der Versorgungsspannung am Reader. Nach einem erfolgreichen Befehl = Das Blinken der LED im Fehlerfall wird nach dem erfolgreichen Ausführen eines Befehls zurückgesetzt. Dies betrifft ausschließlich Kommunikationsfehler. Nach einem Reset-Befehl = Das Blinken der LED im Fehlerfall wird durch einen "init_run" bzw. "WRITE-CONFIG" mit "Init" (RESET) zurückgesetzt. Nach einem Reset- oder einem erfolgreichen Befehl = Das Blinken der LED im Fehlerfall wird durch einen "init_run" bzw. "WRITE-CONFIG" mit "Init" (RESET) oder nach dem erfolgreichen Ausführen eines Befehls zurückgesetzt.
ECC-Modus	An Aus	Aus	Aktivierung/Deaktivierung des ECC-Modus. Ausführliche Informationen zu dem Modus finden Sie in der Produktinformation "Input-Parameter für das RF300-System für die Programmierung über Kommunikationsmodule". Voraussetzung: Transponder-Typ: ISO 15693 = Keiner
Semaphore-Verfahren	An Aus	Aus	Aktivierung/Deaktivierung des Semaphore-Verfahrens. Ausführliche Informationen zu dem Verfahren finden Sie in der Produktinformation "Input-Parameter für das RF300-System für die Programmierung über Kommunikationsmodule". Voraussetzung: Transponder-Typ: ISO 15693 = Keiner
Transponder-Typ	[1]	[1]	Auswahl der verwendeten Transponder-Typen.

[1] Eine ausführliche Beschreibung zu diesen Parametern finden Sie in den nachfolgenden Absätzen.

Der Parameter "Transponder-Typ"

Auswahl der verwendeten Transponder. Es können folgende Transponder-Typen ausgewählt werden:

Reader-Parametrierung	Werte
RF300	Keiner RF300
ISO 15693	Keiner Allgemein MDS D1xx, NXP MDS D2xx, TI MDS D3xx, Infineon MDS D4xx, Fujitsu - 2 kB MDS D5xx, Fujitsu - 8 kB

6.3.4 Der Menüpunkt "Einstellungen - Kommunikation"

Der Menüpunkt "Einstellungen - Kommunikation" ist in folgende Register unterteilt.

- Netzwerkschnittstellen
- PLC
- XML
- OPC UA

Im Register "Netzwerkschnittstellen" können Sie die Netzwerk-Ports, SNMP- und NTP-Protokolle, sowie Syslog-Meldungen aktivieren/deaktivieren. Im Register "PLC" können Sie die PLC-Zugriffe sperren. Im Register "XML" können Sie festlegen, welche Daten über die XML-Schnittstelle gesendet werden. Im Register "OPC UA" können Sie die OPC UA-Server-Funktion des Readers aktivieren und bearbeiten.

Zugriff über die Kommunikationsprotokolle

Die Reader verfügen über verschiedene Netzwerkschnittstellen. Dies ermöglicht es Ihnen über unterschiedliche Kommunikationsprotokolle auf die Reader zuzugreifen. Im Auslieferungszustand sind alle Kommunikationsprotokolle freigeschaltet.

Um eine simultane Ansteuerung der Reader zu vermeiden, werden alle anderen Kommunikationsprotokolle verriegelt, sobald ein Kommunikationsprotokoll eine Verbindung zum Gerät hergestellt hat. Aus sicherheitsrelevanten Gründen wird empfohlen, bei der Erstinbetriebnahme alle nicht verwendeten Kommunikationsprotokolle zu verriegeln.

Eine Ausnahme bilden die Kommunikationsprotokolle "XML" und "OPC UA", die für einen parallelen Diagnose-Zugriff aktiviert werden können. Über die Diagnose- bzw. Parallelkommunikation kann jedoch nur lesend auf die Reader zugegriffen werden.

Das Register "Netzwerkschnittstellen"

Das Register "Netzwerkschnittstellen" ist in folgende Bereiche unterteilt:

- Netzwerk-Basiseinstellungen
- SNMP
- NTP
- Syslog-Meldungen

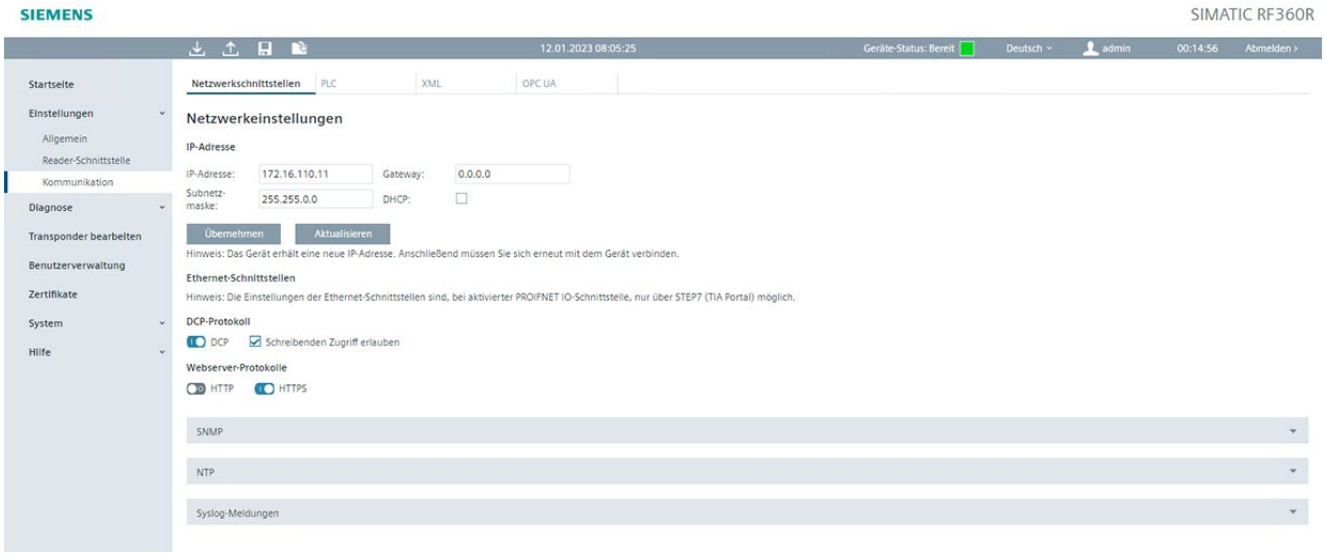


Bild 6-6 Der Menüpunkt "Einstellungen - Kommunikation"; Register "Netzwerkschnittstellen"

Netzwerk-Basiseinstellungen

In dem Bereich "Netzwerk-Basiseinstellungen" können Sie die Netzwerk-Ports des Readers aktivieren/deaktivieren, den Zugriff über DCP-Protokolle erlauben/verbieten und festlegen, über welche Webserver-Protokolle die Kommunikation mit dem WBM erlaubt wird.

Tabelle 6- 7 Beschreibung der Netzwerk-Basisparameter

Parameter	Beschreibung
IP-Adresse	In diesem Bereich können Sie die IP-Adresse, Subnetzmaske, sowie Gateway des Readers ändern. Alternativ kann die Konfiguration der IP-Daten von einem DHCP-Server bezogen werden. Mit Hilfe der Schaltfläche "Übernehmen" können Sie die im WBM geänderten Adressdaten auf den Reader übertragen. Mit Hilfe der Schaltfläche "Aktualisieren" können Sie die im WBM angezeigten Adressdaten aktualisieren bzw. neu von dem Reader laden. **Hinweis** Bei der Adressenvergabe über DHCP wird auch die Option "12" (hostname) unterstützt. Der hostname kann aus der SNMP-Variablen "sysName" entnommen werden. Die Variable kann über SNMP-Tools beschrieben werden.
Ethernet-Schnittstellen	Dieser Bereich wird nur angezeigt, wenn im Register "PLC" die Funktion "PROFINET IO-Schnittstelle" deaktiviert wurde. In diesem Bereich können Sie die Netzwerk-Ports der Reader aktivieren/deaktivieren. Zusätzlich können Sie das Kommunikationsprotokoll LLDP für die jeweilige Schnittstelle aktivieren/deaktivieren. LLDP ist ein Protokoll zur Nachbarschaftsüberwachung. Hinweis: Stellen Sie sicher, dass Sie nicht den Port deaktivieren, über den Sie gerade mit dem Reader kommunizieren.

Parameter	Beschreibung
DCP-Protokoll	In diesem Bereich können Sie die Kommunikation via DCP-Protokolle aktivieren/deaktivieren. Dabei können Sie festlegen, ob über die DCP-Protokolle ausschließlich schreibend oder auch lesend auf den Reader zugegriffen werden darf. Abhängig von der hier getroffenen Entscheidung kann beispielsweise über SINEC PNI der Reader auf die Werkseinstellungen zurückgesetzt werden oder nicht.
Webserver-Protokolle	In diesem Bereich können Sie festlegen, über welche Webserver-Protokolle Sie auf das WBM des Readers zugreifen können. Aus Sicherheitsgründen wird empfohlen die Funktion "HTTP" zu deaktivieren, da bei diesem Protokoll die Daten nicht verschlüsselt werden.

Deaktivieren Sie die Funktion "Schreibenden Zugriff erlauben", wenn Sie sicherstellen wollen, dass nicht über DCP auf den Reader zugegriffen wird. Durch diese Einstellung wird verhindert, dass beispielsweise über SINEC PNI der Reader auf die Werkseinstellungen zurückgesetzt werden kann.

Hinweis

Deaktivieren der Netzwerk-Ports

Stellen Sie sicher, dass Sie nicht den Port deaktivieren, über den Sie gerade mit dem Gerät kommunizieren.

Hinweis

Voraussetzung für die Port-Statistik

Mithilfe der PROFINET-Diagnose oder über SNMP können Sie eine Port-Statistik auslesen.

SNMP

In dem Bereich "SNMP" können Sie das Netzwerkprotokoll aktivieren/deaktivieren. "SNMP" ist ein Protokoll zur Überwachung von Netzwerkkomponenten.

Die Einstellung "SNMPv1" ist ab Werk aktiviert. Prüfen Sie die Notwendigkeit der Nutzung von SNMPv1. SNMPv1 ist als unsicher eingestuft. Verwenden Sie, wenn möglich, ausschließlich SNMPv3. Wenn Sie das Protokoll nicht verwenden, empfehlen wir Ihnen aus Sicherheitsgründen die Einstellung zu deaktivieren.

Tabelle 6- 8 Beschreibung der SNMP-Parameter

Parameter	Beschreibung
SNMPv1-Einstellungen	
Community string lesend	Eingabefeld, um den Benutzername für lesende Zugriffe auf SNMP-Variablen festzulegen. Typischer weise wird diese Eigenschaft mit dem Wert mit "public" belegt.
Community string schreibend	Eingabefeld, um den Benutzernamen für schreibende Zugriffe auf SNMP-Variablen festzulegen. Typischer weise wird diese Eigenschaft mit dem Wert mit "private" belegt. In diesem Feld können nur dann Änderungen vorgenommen werden, wenn der Schreibende Zugriff erlaubt wurde. Schreibender Zugriff ist nur für die SNMP-Variablen "sysName", "sysLocation" und "sysContact" der Gruppe "system" der MIB-II möglich.
Schreibender Zugriff erlauben	Optionskästchen, um den Schreibschutz für SNMP-Variablen zu aktivieren/deaktivieren.
SNMPv3-Einstellungen	
Benutzer	Liste der bereits angelegen SNMP-Benutzer. Mit Hilfe der Schaltfläche "Benutzer hinzufügen" können Sie neue Benutzerprofile anlegen und diese hinzufügen. Über die Schaltfläche "Löschen" können Sie selektierte Benutzerprofile löschen.
Benutzereigenschaften	Eingabefeld und Klappliste Tragen Sie in dem Eingabefeld den Namen des neu erstellten Benutzerprofils ein und weisen Sie dem Benutzer Lese- oder Lese-/Schreibrechte zu.
Authentifizierung	Klappliste und Eingabefelder Legen Sie fest, ob der Benutzer sich authentifizieren muss und wenn, mit welchem Protokoll. Tragen Sie ggf. in die Eingabefelder das Authentifizierungspasswort des neu erstellten Benutzerprofils fest.
Verschlüsselung	Klappliste und Eingabefelder Legen Sie fest, ob die SNMP-Kommunikation des Benutzers verschlüsselt werden muss und wenn, mit welchem Protokoll. Tragen Sie ggf. in die Eingabefelder das Verschlüsselungspasswort des neu erstellten Benutzerprofils fest.
Speichern	Mit Hilfe der Schaltfläche können Sie durchgeführte Änderungen an bestehenden Benutzerprofilen speichern.
SNMP MIB-II System	
sysName sysLocation sysContact	Felder zum Auslesen ("Aktualisieren") und Ändern ("Übernehmen") der MIB-II Systeminformationen. Diese werden i.d.R. über Netzwerkmanagement-Systeme (z. B. SINEC PNI) vergeben. Hier durchgeführte Änderungen werden entsprechend in dem Netzwerkmanagement-System angezeigt und umgekehrt. Diese Informationen werden ausschließlich bei der Nutzung von Netzwerkmanagement-Systemen benötigt.

NTP

In dem Bereich "NTP" können Sie das Netzwerkprotokoll aktivieren. "NTP" ist ein Protokoll zur Synchronisierung der UTC-Uhrzeit in Netzwerksystemen.

Diese Einstellung ist ab Werk deaktiviert und muss vor der ersten Benutzung von NTP hier aktiviert werden.

Tabelle 6- 9 Beschreibung der NTP-Parameter

Parameter	Beschreibung
IP-Adresse des NTP-Servers x	Eingabefeld, um die Adresse des NTP-Servers einzugeben, von dem der angeschlossene Reader seine Uhrzeit synchronisiert. Es können bis zu vier NTP-Server angegeben werden, um mögliche Serverausfällen zu kompensieren.
Aktualisierungsintervall in Sekunden	Eingabefeld, um festzulegen, in welchen Zeitintervallen der Reader automatisch seine Uhrzeit synchronisiert.
Uhrzeit von nicht synchronisierten NTP-Server annehmen	Optionskästchen, um sicherzustellen, dass der Reader auch die Uhrzeit von nicht synchronisierten NTP-Servern annimmt.

Syslog-Meldungen

In dem Bereich "Syslog-Meldungen" können Sie die Syslog-Meldungen aktivieren. Wenn die Syslog-Funktion aktiviert ist, generiert die Baugruppe Syslog-Meldungen an den voreingestellten UDP-Port gemäß RFC 5424 bzw. RFC 5426. Syslog-Meldungen protokollieren Informationen beim Zugriff auf die Baugruppe, sowie Konfigurationsänderungen. Diese werden standardmäßig in einem Log-Datei gespeichert und im Menü "Der Menüpunkt "Diagnose - Syslog-Logbuch" (Seite 72)" ausgegeben. Die Log-Datei ist als Umlaufpuffer angelegt. Sind alle Einträge in der Log-Datei belegt, wird bei einem neuen Eintrag der älteste Eintrag gelöscht.

Diese Einstellung ist ab Werk deaktiviert und muss ggf. hier aktiviert werden.

Tabelle 6- 10 Beschreibung der Syslog-Parameter

Parameter	Beschreibung
IP-Adresse des Syslog-Servers	Eingabefeld, um die Adresse des Syslog-Servers einzugeben, an den die Syslog-Meldungen übertragen werden.
Default-Port	Eingabefeld, um den Default-Port des Syslog-Servers einzugeben, über den die Syslog-Meldungen übertragen werden.

Das Register "PLC"

Das Register "PLC" ist in folgenden Bereich unterteilt:

- PLC-Basiseinstellungen

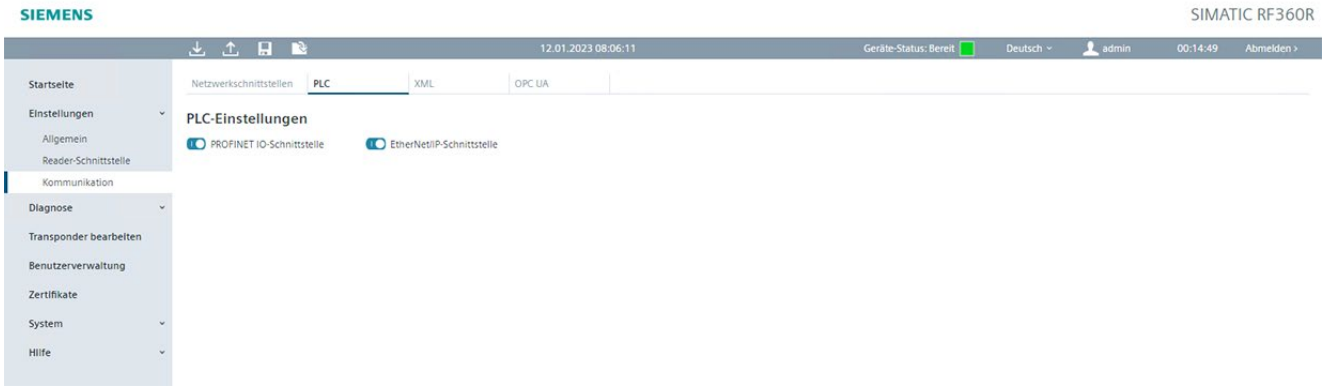


Bild 6-7 Der Menüpunkt "Einstellungen - Kommunikation"; Register "PLC"

PLC-Basiseinstellungen

In dem Bereich "PLC-Basiseinstellungen" können Sie festlegen, über welche Schnittstellen eine Kommunikation mit der Steuerung stattfinden darf.

Tabelle 6- 11 Beschreibung der PLC-Basisparameter

Parameter	Beschreibung
PROFINET IO-Schnittstelle	In diesem Bereich können Sie festlegen, ob über die Steuerung (STEP 7) auf den Reader zugegriffen werden darf. Durch diese Einstellung wird die Ethernet-Schnittstelle für die Kommunikation mit der Steuerung geschlossen.
EtherNet/IP-Schnittstelle	In diesem Bereich können Sie festlegen, ob über EtherNet/IP auf den Reader zugegriffen werden darf. Durch diese Einstellung wird die Ethernet-Schnittstelle für die EtherNet/IP-Kommunikation mit der Steuerung geschlossen.

Das Register "XML"

Das Register "XML" ist in folgende Bereiche unterteilt:

- XML-Basiseinstellungen
- Diagnose-Events des XML-Kanal 1

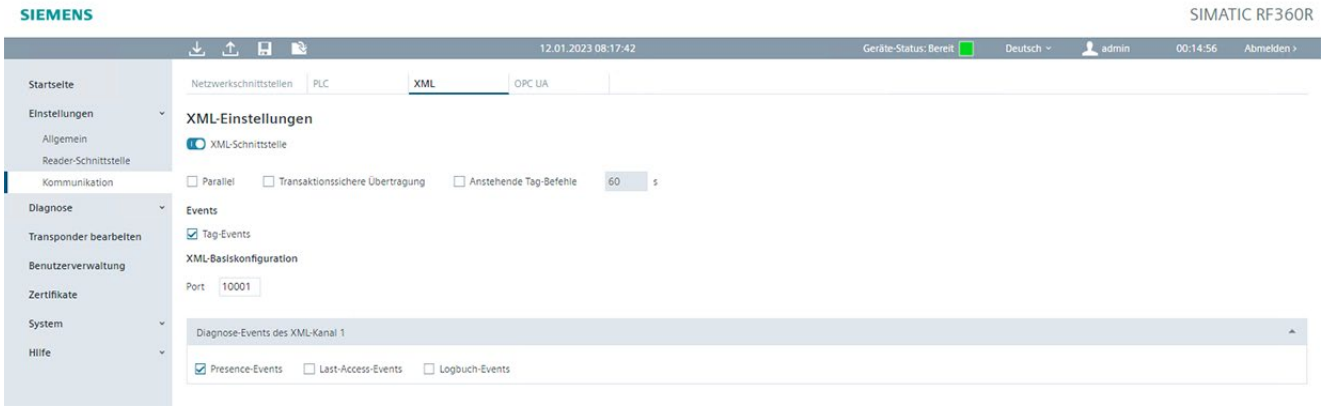


Bild 6-8 Der Menüpunkt "Einstellungen - Kommunikation"; Register "XML"

XML-Basiseinstellungen

In dem Bereich "XML-Basiseinstellungen" können Sie die XML-Kommunikation über die XML-Schnittstelle des Readers aktivieren/deaktivieren. Zusätzlich können Sie festlegen, welche Ereignisse über alle XML-Kanäle an die Anwenderapplikation übertragen werden und über welche XML-Kanäle die Kommunikation zu den Schnittstellen übermittelt wird.

Tabelle 6- 12 Beschreibung der XML-Basisparameter

Parameter	Beschreibung
Parallel	Bei aktivem Optionskästchen kann zusätzlich zu einer bestehenden Verbindung z. B. zu einer Steuerung (PLC), ein paralleler Diagnose-Zugriff über den XML-Kanal aktiviert werden. Beachten Sie, dass bei einem parallelen Zugriff die XML-Applikation ausschließlich lesend auf den Reader zugreifen kann. Wird bereits über eine andere Applikation parallel auf das Kommunikationsmodul zugegriffen, kann diese Option nicht ausgewählt werden. Ist die Funktion deaktiviert, kann ausschließlich über einen Kommunikationskanal auf den Reader zugegriffen werden. Wenn über einen Kommunikationskanal bereits eine Verbindung aufgebaut ist, dann wird ein weiterer Verbindungsversuch von einem anderen Kommunikationskanal abgelehnt.
Transaktionsgesicherte Übertragung	Bei aktivem Optionskästchen wird jedes von der Anwenderapplikation empfangene Telegramm (XML-Bericht) des Readers mit einem Antworttelegramm bestätigt. Geht innerhalb von 10 Sekunden kein Antworttelegramm beim Reader ein, sendet dieses den Bericht erneut an die Applikation. Nicht übertragene Berichte werden im Reader gepuffert. Mit dieser Funktion können Sie sicherstellen, dass auch bei einer instabilen Verbindung (z. B. WLAN-Verbindung reißt gelegentlich ab), keine Telegramme vom Reader verloren gehen. Diese Funktion ermöglicht auch einen Batch-Betrieb des Readers, bei dem nur zeitweise eine Verbindung zu einer Anwenderapplikation besteht. Der Reader sammelt die Telegramme und diese können bei Bedarf über eine PC-Applikation abgerufen werden.

Parameter	Beschreibung
Anstehende Tag-Befehle	Festlegung der Zeitspanne, wie lange XML-Befehle bestehen bleiben, wenn sich zum Zeitpunkt der Befehlsübertragung kein Transponder im Antennenfeld befindet. Betritt innerhalb der angegebenen Zeitspanne ein Transponder das Antennenfeld wird der Befehl ausgeführt. Aktivieren Sie diese Funktion, wenn sehr schnelle Transponder-Zugriffe notwendig sind (z. B. aufgrund hoher Transponder-Geschwindigkeiten). Zeitspanne = 0 s: Gleichbedeutend mit unendlich. Die Befehle bleiben solange bestehen, bis ein Transponder das Antennenfeld betritt und der Befehl ausgeführt wurde. Voreinstellung: 60 s
Events	
Tag-Events	Bei aktivem Optionskästchen wird jedes Mal, wenn ein Transponder zuverlässig erfasst wurde, ein Tag-Event-Telegramm (Observed) erzeugt. Verlässt der Transponder das Antennenfeld, wird ein weiteres Tag-Event-Telegramm (LOST) erzeugt.
XML-Basiskonfiguration	
Port	Eingabefeld für den Ethernet-Port des XML-Kanals.

Diagnose-Events des XML-Kanal 1

In dem Bereich "Diagnose-Events des XML-Kanal 1" können Sie festlegen, welche Ereignisse über den ausgewählten XML-Kanal an die Steuerung übertragen werden.

Tabelle 6- 13 Beschreibung der Diagnose-Event-Daten für den XML-Kanal

Events	Beschreibung
Presence-Events	Bei aktivem Optionskästchen werden Informationen über Anwesenheitszustände bzw. -änderungen übertragen.
Last-Access-Events	Bei aktivem Optionskästchen werden alle Zugriffe auf die Transponder, sowie die dabei gelesenen/geschriebenen Daten übertragen.
Logbuch-Events	Bei aktivem Optionskästchen werden alle Logbuch-Einträge übertragen.

Das Register "OPC UA"

Das Register "OPC UA" ist in folgende Bereiche unterteilt:

- OPC UA-Basisparameter
- Diagnose-Events und -Items
- Security-Einstellungen

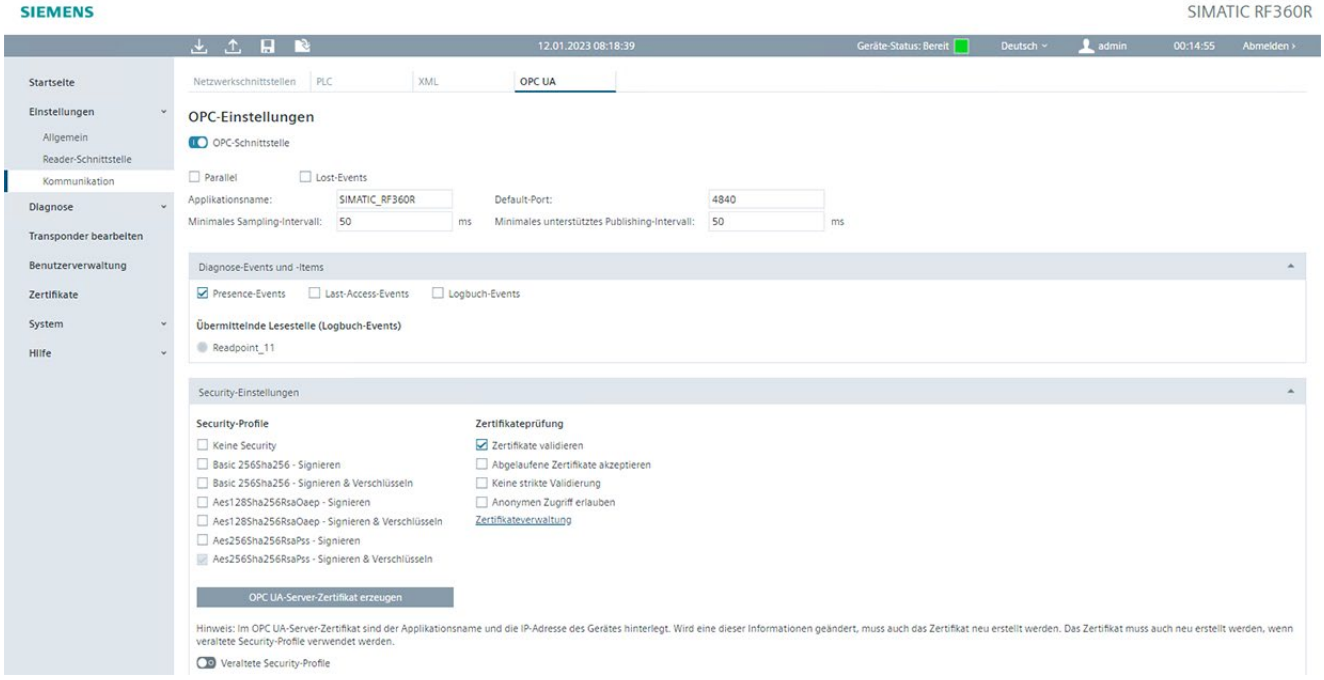


Bild 6-9 Der Menüpunkt "Einstellungen - Kommunikation"; Register "OPC UA"

OPC UA-Basiseinstellungen

In dem Bereich "OPC UA-Basiseinstellungen" können Sie die Kommunikation über die OPC UA-Schnittstelle aktivieren/deaktivieren und Basiseinstellungen für die OPC UA-Schnittstelle vornehmen.

Tabelle 6- 14 Beschreibung der OPC UA-Basisparameter

Parameter	Beschreibung
Parallel	Bei aktivem Optionskästchen kann zusätzlich zu einer bestehenden Verbindung z. B. zu einer Steuerung (PLC), ein paralleler Diagnose-Zugriff über den OPC UA-Kanal aktiviert werden. Beachten Sie, dass bei einem parallelen Zugriff der OPC UA-Client ausschließlich lesend auf den Reader zugreifen kann. Wird bereits über eine andere Applikation parallel auf das Kommunikationsmodul zugegriffen, kann diese Option nicht ausgewählt werden. Ist die Funktion deaktiviert, kann ausschließlich über einen Kommunikationskanal auf den Reader zugegriffen werden. Wenn über einen Kommunikationskanal bereits eine Verbindung aufgebaut ist, dann wird ein weiterer Verbindungsversuch von einem anderen Kommunikationskanal abgelehnt.
Lost-Events	Bei aktivem Optionskästchen wird jedes Mal, wenn ein Transponder das Antennenfeld verlässt, ein Lost-Event erzeugt.

Parameter	Beschreibung
Applikationsname	Name der OPC UA-Applikation des Servers. Der Applikationsname wird für die Identifizierung des OPC UA-Namensraums des Readers benötigt und sollte innerhalb des Projekts für jeden Reader eindeutig sein. Der Applikationsname ist Bestandteil der URL des OPC UA-Servers des Readers.
Default-Port	Hier können Sie die Portnummer der Applikation verändern. In der Voreinstellung wird die Portnummer 4840 verwendet, der Standard-TCP-Port für das OPC UA-Binärprotokoll.
Minimales Sampling-Intervall	Minimales Sampling-Intervall in dem der Reader die Prozessdaten abtastet. Das Sampling-Intervall ist auf einen Minimalwert von 10 Millisekunden begrenzt, um anderen Prozessen ausreichend Zeit zu reservieren. Wertebereich: 10 .. 50 ms Voreinstellung: 50 ms
Minimales unterstütztes Publishing-Intervall	Minimales von der Server-Applikation unterstütztes Publishing-Intervall, in dem die Prozessdaten für angemeldete OPC UA-Clients veröffentlicht werden. Von einem OPC UA-Client vorgegebene kleinere Werte werden nicht berücksichtigt. Wertebereich: 10 .. 65535 ms Voreinstellung: 50 ms

Diagnose-Events

In dem Bereich "Diagnose-Events" können Sie festlegen, welche Ereignisse übertragen werden.

Tabelle 6- 15 Beschreibung der Diagnose-Events

Daten	Beschreibung
Presence-Events	Bei aktivem Optionskästchen werden Informationen über Anwesenheitszustände bzw. -änderungen übertragen.
Last-Access-Events	Bei aktivem Optionskästchen werden alle Zugriffe auf die Transponder, sowie die dabei gelesenen/geschriebenen Daten übertragen. Die Aktivierung dieses Events ist die Voraussetzung dafür, dass in den OPC UA-Variablen der Gruppe "Diagnostics" Werte eingetragen werden.
Logbuch-Events	Bei aktivem Optionskästchen werden alle Logbuch-Einträge übertragen.
Übermittelnde Lesestelle (Logbuch-Events)	
Lesestelle 1	Auswahl ob und über welche Lesestelle die Logbuch-Einträge übermittelt werden.

Security-Einstellungen

In dem Bereich "Security-Einstellungen" können Sie Sicherheitseinstellungen für die OPC UA-Schnittstelle vornehmen.

Tabelle 6- 16 Beschreibung der Security-Parameter

Parameter	Beschreibung
Security-Profile	Festlegung des Security-Profils und der Zugriffsoptionen für den UA-Server des Kommunikationsmoduls. • Keine Security • Basic 256 / Sha 256 - Signieren • Basic 256 / Sha 256 - Signieren & Verschlüsseln • Aes128 / Sha256 Rsa Oaep - Signieren • Aes128 / Sha256 Rsa Oaep - Signieren & Verschlüsseln • Aes128 / Sha256 Rsa Pss - Signieren • Aes128 / Sha256 Rsa Pss - Signieren & Verschlüsseln "Kein Security" entspricht dem Security-Profil "None" verwendet. Dieses Profil bietet keinerlei Sicherheitsmechanismen (Verschlüsselungen). Wurde ein "Signieren"-Profil ausgewählt, dann erlaubt das Kommunikationsmodul ausschließlich die Kommunikation mit signierten Telegrammen unter Nutzung des jeweiligen Hash-Algorithmus. Wurde ein "Signieren & Verschlüsseln"-Profil ausgewählt, dann erlaubt das Kommunikationsmodul ausschließlich die Kommunikation mit signierten und verschlüsselten Telegrammen unter Nutzung des jeweiligen Hash-Algorithmus. Die Profile sind nach ihren Sicherheitsstufen aufsteigend angeordnet. Es wird empfohlen die höchste Sicherheitsstufe (Aes128 / Sha256 Rsa Pss) zu verwenden.
Zertifikateprüfung	
Zertifikate validieren	Bei aktivem Optionskästchen prüft der Reader generell das Zertifikat des Kommunikationspartners. Falls das Partnerzertifikat ungültig oder nicht vertrauenswürdig ist, wird die Kommunikation abgebrochen.
Abgelaufene Zertifikate akzeptieren	Der Reader prüft grundsätzlich die Gültigkeitsdauer des Zertifikats des Kommunikationspartners. Bei aktivem Optionskästchen werden Zertifikat auch dann akzeptiert und die Kommunikation aufgebaut, wenn der reader-interne aktuelle Zeitpunkt außerhalb der Gültigkeitsdauer des Partnerzertifikats liegt.
Keine strikte Validierung	Bei aktivem Optionskästchen lässt der Reader die Kommunikation auch in den folgenden Fällen zu: • Wenn die IP-Adresse des Kommunikationspartners nicht mit der IP-Adresse in dessen Zertifikat identisch ist. Hinweis: Der OPC UA-Server prüft nicht die IP-Adresse seines Kommunikationspartners (Client). • Wenn für die CA des Partnerzertifikats keine Sperrliste auf dem Reader hinterlegt ist. Unabhängig von diesen Ausnahmen müssen für den Aufbau einer Verbindung mindestens folgende Voraussetzungen erfüllt sein: • Wenn das Partnerzertifikat nicht vertrauenswürdig ist, muss der Reader zumindest ein selbstsigniertes Zertifikat des Partners gespeichert haben. • Wenn das Partnerzertifikat von mehreren CAs (Certification Authorities) ausgestellt wurde, müssen alle CA Root-Zertifikate im Zertifikatspeicher des Readers gespeichert sein.

Parameter	Beschreibung
Anonymen Zugriff erlauben	Bei aktivem Optionskästchen erlaubt der Reader anonymen Benutzern den Zugriff auf die Daten seines OPC UA-Servers. Anonyme Benutzer müssen beim Verbindungsaufbau keinen Benutzernamen/Passwort angeben. Ist der anonyme Zugriff nicht erlaubt, muss ein OPC UA-Client bzw. ein Benutzer eine gültige Benutzername/-Passwort-Kombination eines Benutzers mit OPC UA-Rechten angeben. Ein Benutzer mit OPC UA-Rechten kann über das WBM angelegt werden. Das werksseitig vorinstallierte Benutzerprofil (Benutzername: "admin" Passwort: "admin") besitzt ebenfalls OPC UA-Rechte. Es wird empfohlen den anonymen Zugriff zu deaktivieren.
Zertifikate-verwaltung	Link in den Menüpunkt "System - Zertifikate", in dem Sie vorhandene Zertifikate einsehen, neue Zertifikate importieren, sowie Zertifikatsignierungsanforderungen erstellen und Zertifikat-Dateien und Zertifikat-Schlüsseldateien auf den Reader übertragen können.
OPC UA-Server-Zertifikat erzeugen	Schaltfläche, um ein OPC UA-Server-Zertifikat zu erstellen. Das Server-Zertifikat dient unter anderem zum Ausweisen des OPC UA-Servers gegenüber einem OPC UA-Client. Im OPC UA-Server-Zertifikat sind der Applikationsname, das Security-Profil und die IP-Adresse des Readers hinterlegt. Wird eine dieser Informationen geändert, muss auch das Server-Zertifikat neu erstellt werden. Hinweis: Beachten Sie, dass der Vorgang bis zu mehreren Minuten dauern kann.
Veraltete Security-Profile	Mit diesem Schalter können Sie veraltete und als unsicher eingestufte Security-Profile einblenden und verwenden. Diese Profile sollten ausschließlich dann verwendet werden, wenn aus Kompatibilitätsgründen kein anderes Security-Profil verwendet werden kann.

6.3.5 Der Menüpunkt "Diagnose - Hardware-Diagnose"

In dem Menüpunkt "Diagnose - Hardware-Diagnose" können Sie sich die Status-Parameter des Readers und des sich aktuell im Antennenfeld befindlichen Transponders anzeigen lassen.

Diese Seite ist in folgende Bereiche unterteilt:

- Monitoring-Status
- Status
- Fehlerzähler

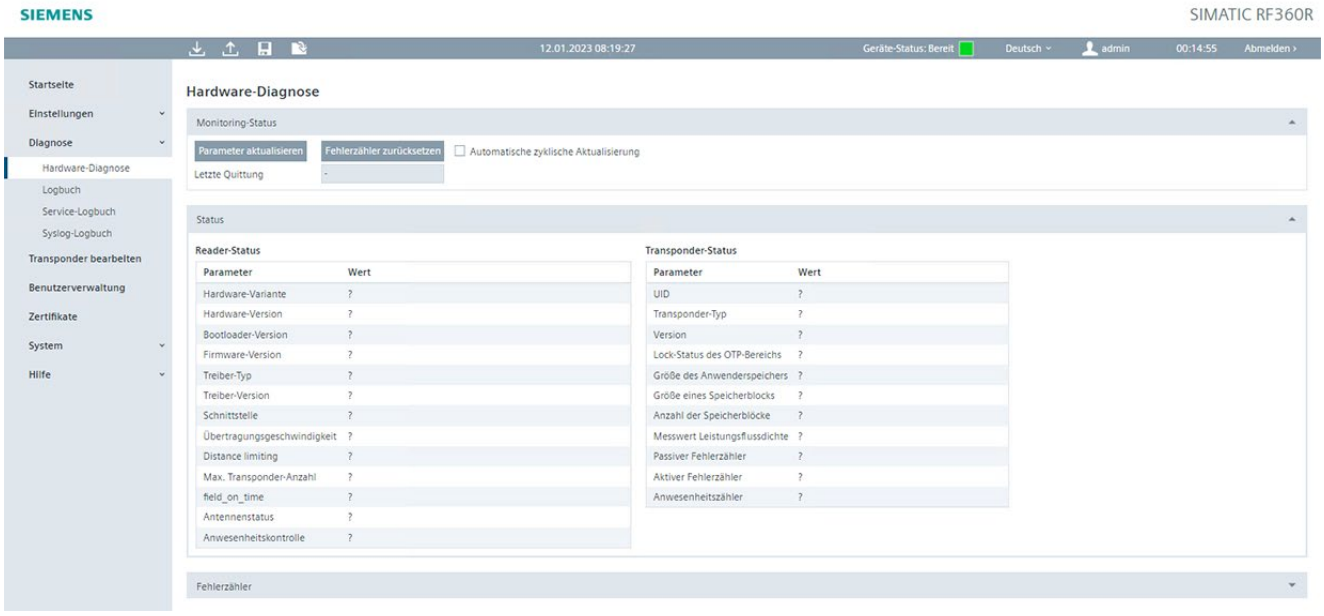


Bild 6-10 Der Menüpunkt "Diagnose - Hardware-Diagnose"

Monitoring-Status

In diesem Bereich können Sie die Reader- und Transponder-Parameter aktualisieren und die Fehlerzähler-Stände des Readers zurücksetzen.

Aktivieren Sie das Optionskästchen "Automatische zyklische Aktualisierung", um die Parameterwerte automatisch und zyklisch aktualisieren zu lassen.

Die Datums- und Uhrzeitangabe der letzten Quittung bezieht sich auf das Datum bzw. die Uhrzeit des angeschlossenen PCs.

Status

Folgende Parameter werden gelesen und angezeigt:

Tabelle 6- 17 Angezeigte Parameter des Bereichs "Reader-Status"

Angezeigte Parameter	Beschreibung
Hardware-Variante	Hardware-Variante des Readers
Hardware-Version	Hardware-Version des Readers
Bootloader-Version	Bootloader-Version des Readers
Firmware-Version	Firmware-Version des Readers
Treiber-Typ	Treiber-Typ der internen Schnittstelle des Readers
Treiber-Version	Treiber-Version der internen Schnittstelle des Readers
Schnittstelle	Verwendete Schnittstelle des Readers Dieser Parameter hat für RF360R keine Relevanz (Fixwert: RS422).
Übertragungs-geschwindigkeit	Verwendete Übertragungsgeschwindigkeit des Readers Dieser Parameter hat für RF360R keine Relevanz (Fixwert: 921,6 kBd).
Distance limiting	Dieser Parameter hat für RF360R keine Relevanz (Fixwert: 0).

Angezeigte Parameter	Beschreibung	
Max. Transponder-Anzahl	Maximale Anzahl der zu erwartenden Transponder, die sich zeitgleich im Antennenfeld des Readers befinden dürfen. Aufgrund des Singletag-Betriebs darf sich bei RF360R maximal ein Transponder im Antennenfeld befinden.	
Transponder-Typ	Eingestelltes Transponder-Typen-Profil Folgende Werte sind möglich:	
	Wert	Bedeutung
	0x00	RF300 (RF3xxT)
	0x01	ISO 15693 allgemein
	0x03	MDS D3xx, Infineon
	0x04	MDS D4xx, Fujitsu - 2 kB
	0x05	MDS D1xx, NXP
	0x06	MDS D2xx, TI
	0x08	MDS D5xx, Fujitsu - 8 kB
	0x10	RF300 (RF3xxT)
	0x11	General Mode
Antennenstatus	Status der Antenne	
Anwesenheitskontrolle	Eingestelltes Anwesenheitskontroll-Profil	

Tabelle 6- 18 Angezeigte Parameter des Bereichs "Transponder-Status"

Angezeigte Parameter	Beschreibung
UID	Unique Identifier des Transponders
Transponder-Typ	Transponder-Typ (Hersteller, Bezeichnung)
Version	Version des Transponder-Chips
Lock-Status des OTP-Bereichs	Gesperrte Blöcke des OTP-Bereichs auf dem Chip
Größe des Anwenderspeichers	Speichergröße des Anwenderspeichers in Byte
Größe eines Speicherblocks	Größe der Speicherblöcke des Transponder-Chips
Anzahl der Speicherblöcke	Anzahl der Speicherblöcke des Transponder-Chips
Messwert Leistungsflussdichte	Strahlungsleistung die beim Transponder ankommt. Je niedriger der Wert ist, umso mehr Leistung erhält der Transponder.
Passiver Fehlerzähler	Anzahl der aufgetretenen Ruhefehler
Aktiver Fehlerzähler	Anzahl der aufgetretenen Fehler Summe der Signatur- und CRC-Fehler
Anwesenheitszähler	Dauer in [ms] die der Transponder sich im Antennenfeld befunden hat.

Fehlerzähler

Folgende Fehlertypen werden gelesen und angezeigt:

Tabelle 6- 19 Angezeigte Fehlertypen des Bereichs "Fehlerzähler"

Angezeigte Fehlertypen	Beschreibung
FZP	Passiver Fehlerzähler (Ruhefehlerzähler) Dieser Fehlerzähler ist ein Indikator für eine gestörte Umgebung (Interferenzen).
ABZ	Abbruchszähler Zähler für Protokollfehler auf der Luftschnittstelle, bei denen der Transponder die Kommunikation abgebrochen hat.
CFZ	Codefehlerzähler Zähler für Störungen oder Kollisionen auf der Luftschnittstelle, durch die die Kommunikation gestört wurde.
SFZ	Signaturfehlerzähler Zähler für fehlgeschlagene Signaturverschlüsselungen von geschriebenen Datenblöcken. Ausschließlich für den Transponder-Typ "RF300" relevant.
CRCFZ	CRC-Fehlerzähler Zähler für fehlgeschlagene CRC-Überprüfungen
ASMFZ	Fehlerzähler für Schnittstellenprobleme der internen Schnittstelle Zähler für Fehler auf der seriellen Schnittstelle.
Signalstärke	
AMLI	AM-Leistungsindikator Empfangssignalstärke [dB] für die Amplituden-Modulation mit der der Transponder erkannt wurde.
PMLI	PM-Leistungsindikator Empfangssignalstärke [dB] für die Phasen-Modulation mit der der Transponder erkannt wurde.

Hinweis

Fehlerzähler-Stände

Die angezeigten Fehlerzähler-Stände werden ab dem letzten Neustart des Readers bzw. dem letzten manuellen Zurücksetzen der Fehlerzähler-Stände gezählt.

6.3.6 Der Menüpunkt "Diagnose - Logbuch"

In dem Menüpunkt "Diagnose - Logbuch" wird das Logbuch des Readers angezeigt.

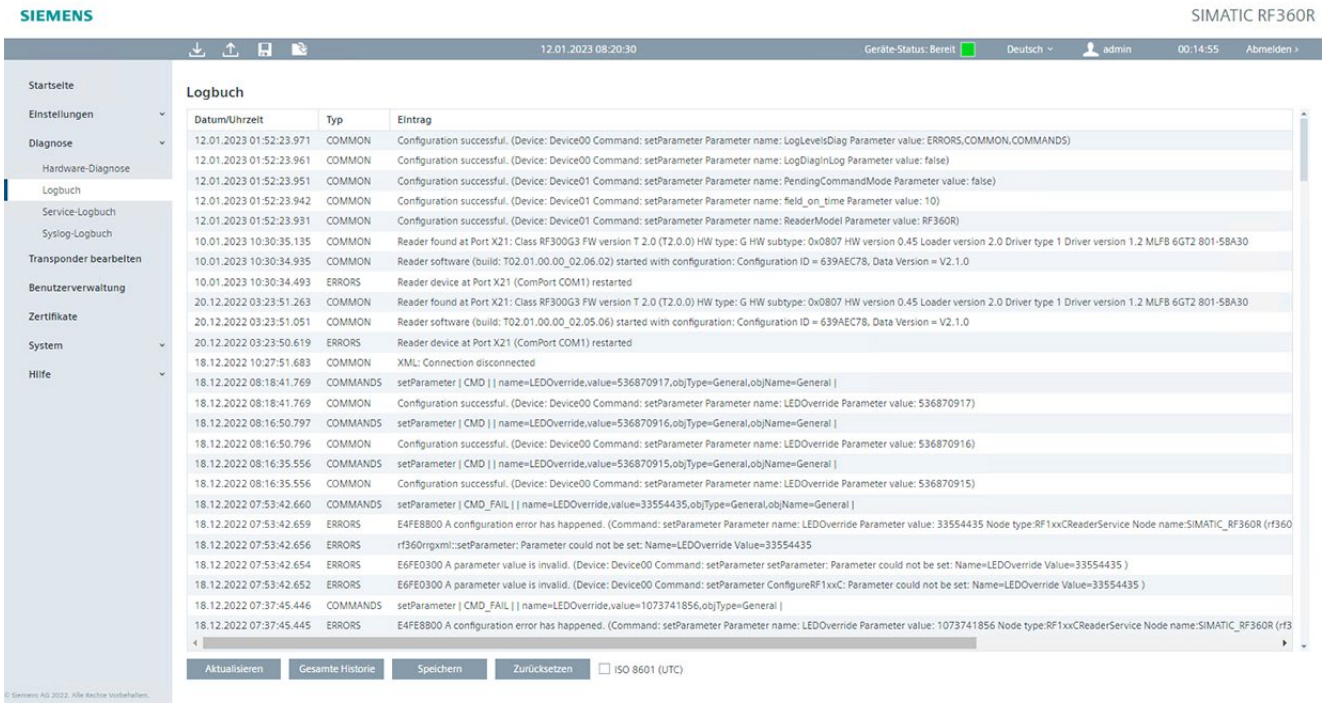


Bild 6-11 Der Menüpunkt "Diagnose - Logbuch"

Im Menüpunkt "Logbuch" werden alle Meldungstypen angezeigt, die im Menüpunkt "Einstellungen - Allgemein" im Bereich "Logbuch-Einstellungen" aktiviert wurden. In diesem Menüpunkt werden die vom Reader durchgeführten Aktionen dokumentiert.

Die Einträge enthalten folgende Eigenschaften:

Tabelle 6- 20 Angezeigte Eigenschaften der Logbuch-Meldungen

Eigenschaft	Beschreibung
Datum/Uhrzeit	Zeitstempel, wann der Eintrag vom Reader eingetragen wurde. Beachten Sie, dass der Zeitstempel von der Geräte-Uhr (UTC-Zeit) erzeugt wird. Diese Uhrzeit wird mit dem/der im PC eingestellten Zeitformat und Zeitzone abgeglichen und im entsprechenden Format angezeigt.
Typ	Typ der Meldung Welche Meldungstypen gemeldet werden, ist abhängig von den im Menüpunkt "Einstellungen - Allgemein" im Bereich "Logbuch-Einstellungen" aktivierten Optionskästchen.
Eintrag	Text der Meldung

Über die Schaltflächen können Sie die Einträge steuern:

- Aktualisieren

  Das Logbuch wird erneut vom Reader eingelesen und die Liste aktualisiert. Die angezeigten Logbuch-Einträge umfassen die aktuellsten Daten (200 kB).

- Gesamte Historie

  Das komplette gespeicherte Logbuch des Readers wird eingelesen. Die angezeigten Logbuch-Einträge umfassen alle gespeicherten Daten (10 MB).

- Speichern unter

  Das vom Reader ausgelesene Logbuch wird als *.csv-Datei auf dem PC gespeichert. Beachten Sie, dass der Zeitstempel von der Geräte-Uhr nach ISO 8601 (UTC-Zeit) erzeugt wird.

- Zurücksetzen

  Das Logbuch wird im Reader gelöscht.

Mit dem Optionskästchen "ISO 8601 (UTC)" können Sie die Datumsanzeige in der Spalte "Datum/Uhrzeit" auf UTC-Zeit umstellen, identisch zu der Ausgabe in dem exportierten Logbuch.

Bei einer großen Anzahl von Logbucheinträgen in der Historie kann es bis zu mehreren Minuten dauern, bis diese angezeigt werden.

6.3.7 Der Menüpunkt "Diagnose - Service-Logbuch"

In dem Menüpunkt "Diagnose - Service-Logbuch" wird das Service-Logbuch des Readers angezeigt. Das Logbuch zeichnet interne Abläufe des Readers auf und wird für Service-Unterstützungen durch SIEMENS-Fachpersonal benötigt. Nehmen Sie auf dieser Seite nur Einstellungen vor, wenn Sie dazu vom SIEMENS-Fachpersonal aufgefordert werden. Die Auswertung der Logbucheinträge obliegt ebenfalls dem SIEMENS-Fachpersonal.

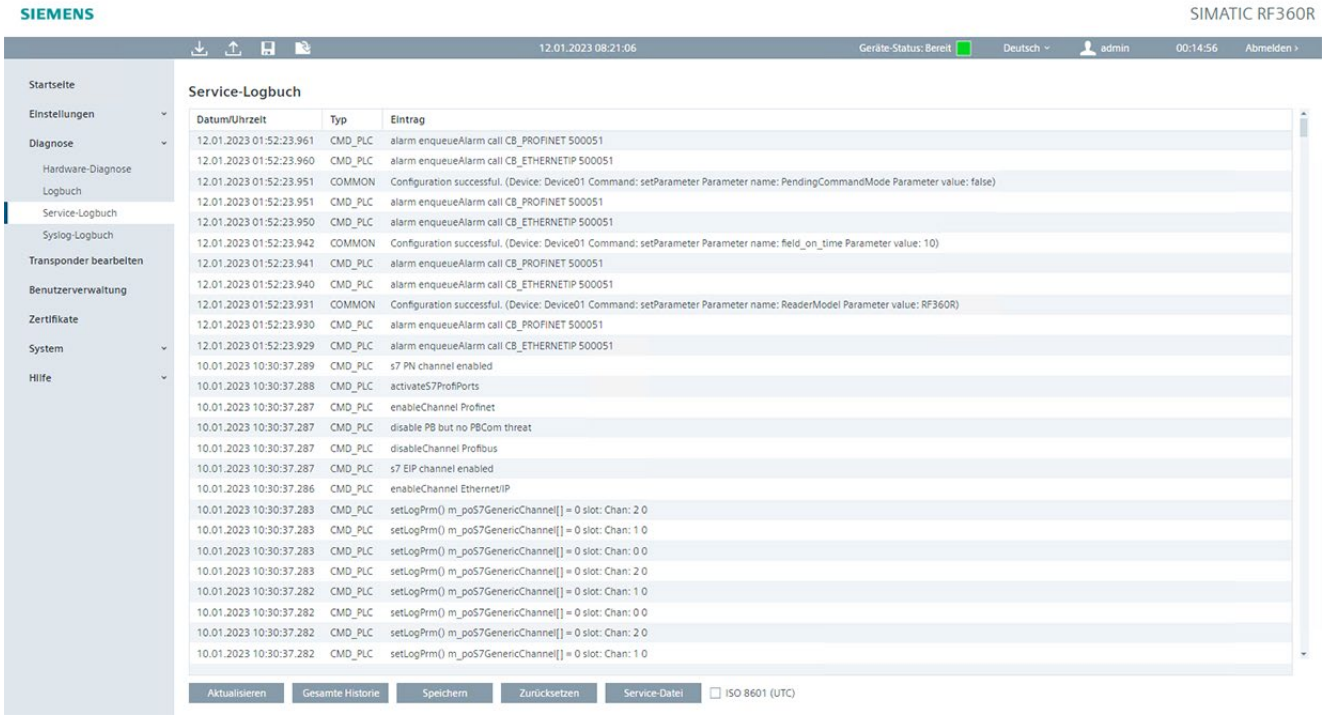


Bild 6-12 Der Menüpunkt "Diagnose - Service-Logbuch"

Auf dieser Seite werden all die Meldungstypen angezeigt, die im Menü "Einstellungen - Allgemein > Service-Logbuch-Einstellungen" festgelegt wurden.

Die Einträge enthalten folgende Eigenschaften:

Tabelle 6- 21 Angezeigte Eigenschaften der Logbuch-Meldungen

Eigenschaft	Beschreibung
Datum/Uhrzeit	Zeitstempel, wann der Eintrag vom Reader eingetragen wurde. Beachten Sie, dass der Zeitstempel von der Geräte-Uhr (UTC-Zeit) erzeugt wird. Diese Uhrzeit wird mit dem/der im PC eingestellten Zeitformat und Zeitzone abgeglichen und entsprechend angezeigt.
Typ	Typ der Meldung Welche Meldungstypen gemeldet werden, ist abhängig von den im Menüpunkt "Einstellungen - Allgemein" im Bereich "Logbuch-Einstellungen" aktivierten Optionskästchen.
Eintrag	Text der Meldung

Über die Schaltflächen "Aktualisieren", "Speichern unter" und "Zurücksetzen" können Sie die Einträge steuern:

- Aktualisieren

  Das Logbuch wird erneut vom Reader eingelesen und die Liste aktualisiert. Die angezeigten Logbuch-Einträge umfassen die aktuellsten Daten (200 kB).

- Speichern unter

  Das vom Reader ausgelesene Logbuch wird als *.csv-Datei gespeichert.

- Zurücksetzen

  Das Logbuch wird im Reader gelöscht.

- Service-Datei

  Alle diagnose-relevante Daten des Readers werden als *.slf-Datei gespeichert. Die Datei enthält ausschließlich für Siemens-Service-Personal relevante Informationen und kann nur von diesem ausgewertet werden.

Mit dem Optionskästchen "ISO 8601 (UTC)" können Sie die Datumsanzeige in der Spalte "Datum/Uhrzeit" auf UTC-Zeit umstellen, identisch zu der Ausgabe in dem exportierten Logbuch.

Bei einer großen Anzahl von Logbucheinträgen in der Historie kann es bis zu mehreren Minuten dauern, bis diese angezeigt werden.

6.3.8 Der Menüpunkt "Diagnose - Syslog-Logbuch"

In dem Menüpunkt "Diagnose - Syslog-Logbuch" werden bei aktivierter Syslog-Funktion das Logbuch der Syslog-Meldungen angezeigt. Diese Seite kann ausschließlich von Nutzern mit Administrator-Rechten aufgerufen werden.

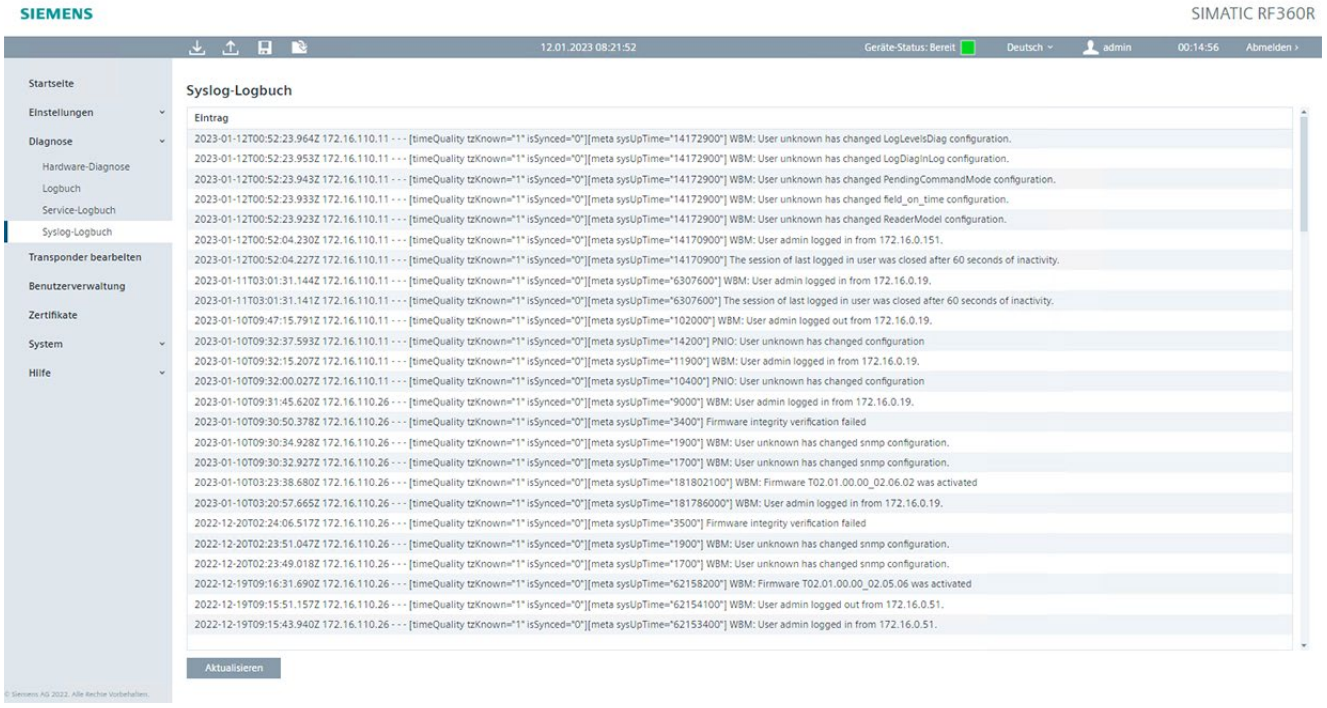


Bild 6-13 Der Menüpunkt "Diagnose - Syslog-Logbuch"

Im Menüpunkt "Syslog-Logbuch" werden alle Syslog-Meldungen angezeigt. In diesem Menüpunkt werden alle sicherheitsrelevanten Zugriffe auf den Reader und durchgeführten Aktionen dokumentiert. Ausführliche Informationen zu den Syslog-Meldungen, deren Aufbau und Inhalte finden Sie im Kapitel "Syslog-Meldungen".

Über die Schaltfläche "Aktualisieren" können Sie die Einträge erneut vom Reader einlesen und die Liste aktualisieren. Die angezeigten Logbuch-Einträge umfassen 128 kB Daten.

6.3.9 Der Menüpunkt "Transponder bearbeiten"

In dem Menüpunkt "Transponder bearbeiten" können Sie Transponder-Daten auslesen und beschreiben.

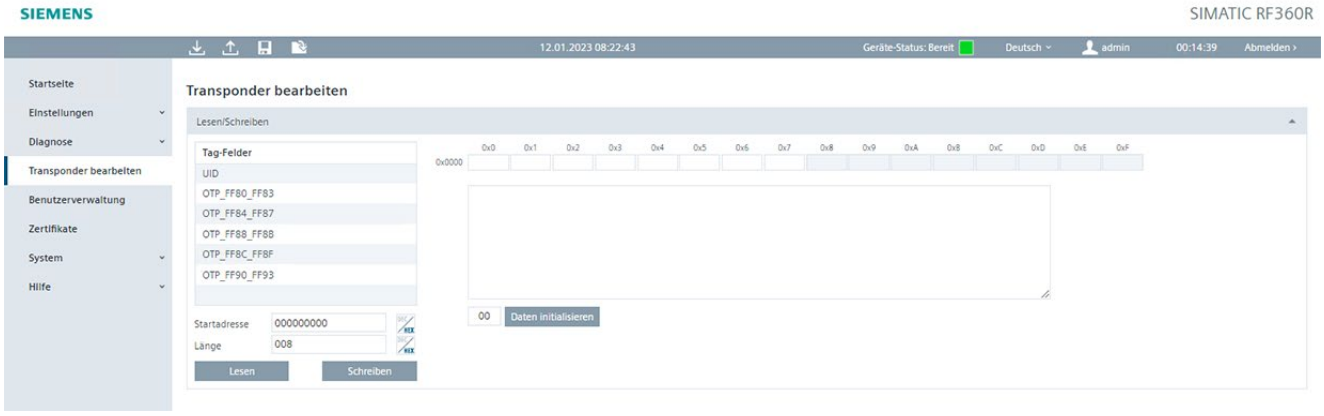


Bild 6-14 Der Menüpunkt "Transponder bearbeiten"

In dem Bereich "Lesen/Schreiben" können Sie Speicherbereiche auslesen und überschreiben. Dabei können Sie auf vordefinierte Adressen (Tag-Felder) zugreifen. Den Speicherbereich können Sie mit Hilfe der Parameter manuell anpassen.

Tabelle 6- 22 Beschreibung der Parameter der Tag-Felder

Parameter	Beschreibung
Tag-Felder	Liste mit vordefinierten Adressen.
Startadresse	Eingabefeld zur Eingabe der Startadresse innerhalb des ausgewählten Tag-Felds, ab der Sie die Daten des Ziel-Transponders lesen oder verändern bzw. beschreiben wollen. Mit Hilfe der Schaltfläche können Sie das Ein-/Ausgabeformat ändern (dezimal oder hexadezimal). Wertebereich: 0 ... 65535
Länge	Eingabefeld zur Eingabe der Länge innerhalb des ausgewählten Tag-Felds und ausgehend von der Startadresse, innerhalb der Sie die Daten des Ziel-Transponders lesen oder verändern bzw. beschreiben wollen. Mit Hilfe der Schaltfläche können Sie das Ein-/Ausgabeformat ändern (dezimal oder hexadezimal). Wertebereich: 1 ... 1024 Byte
Daten	Ein-/Ausgabefelder für die Werte (dezimal oder hexadezimal). Mögliche Zeichen: 0 ... 9, A ... F
ASCII	In dem ASCII-Feld werden die Daten zusätzlich in ASCII-Schreibweise angezeigt. Sie können die Daten sowohl in dem Daten-Feld als auch in dem ASCII-Feld bearbeiten.
Daten initialisieren	Schaltfläche zum Initialisieren der Daten. Mithilfe der Initialisierungsfunktion können Sie die Datenfelder vorbelegen.

Neben der Liste der Tag-Felder werden die Daten des ausgewählten Speicherbereichs angezeigt (dezimal oder hexadezimal und in ASCII).

Mit Hilfe der Schaltfläche "Lesen" werden die Daten vom Transponder gelesen. Um die vom Transponder gelesene Daten gegenüber den manuell eingegebenen Daten abzuheben,

werden diese rot dargestellt. Wenn keine Werte angezeigt werden, bedeutet dies, dass noch keine Werte vom Transponder ausgelesen wurden.

Klicken Sie auf die Schaltfläche "Schreiben", um die geänderten Daten auf den Transponder zu übertragen.

ACHTUNG
Transponder-Daten lesen/schreiben bei bestehender Verbindung zur Steuerung Beachten Sie, dass bei einer bestehenden Verbindung zur Steuerung die Konfiguration des Readers über die Steuerung vorgenommen wird. Damit Transponder-Daten über das WBM gelesen/geschrieben werden können, muss zuvor der Reader korrekt initialisiert worden sein.

6.3.10 Der Menüpunkt "Benutzerverwaltung"

In dem Menüpunkt "Benutzerverwaltung" können Sie die Authentifizierung aktivieren/deaktivieren, Benutzerprofile anlegen, löschen und bearbeiten sowie Passwörter ändern.

Diese Seite ist in folgende Bereiche unterteilt:

- Benutzerprofile
- Benutzereigenschaften
- Passwort
- Rollen
- Automatische Abmeldung
- Authentifizierung
- Sicherheitseinstellungen

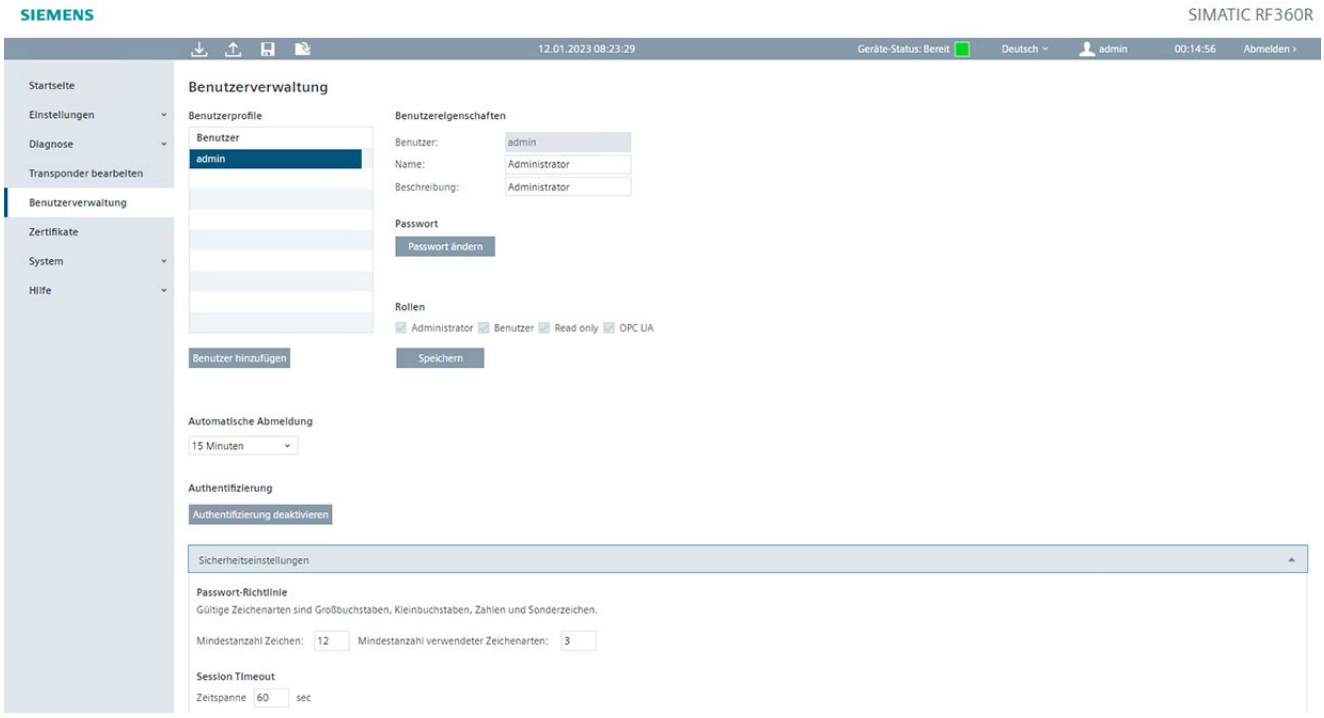


Bild 6-15 Der Menüpunkt "Benutzerverwaltung"

Benutzerprofile

Der Bereich "Benutzerprofile" enthält eine Liste aller vorhandenen Benutzerprofile. Es können maximal 30 Benutzerprofile angelegt werden. Um ein Benutzerprofil zu bearbeiten, selektieren Sie den gewünschten Benutzernamen in der Liste. Der selektierte Benutzername wird farblich hervorgehoben.

Klicken Sie auf die Schaltfläche "Neuen Benutzer hinzufügen", um einen neuen Benutzer anzulegen. Klicken Sie auf die Schaltfläche "Löschen", um ein selektiertes Benutzerprofil zu löschen.

Benutzereigenschaften

Tragen Sie in dem Eingabefeld "Benutzer" den Namen des neu erstellten Benutzerprofils ein. Den Benutzernamen benötigen Sie, genauso wie das Passwort, zum Anmelden am WBM. Der Benutzername kann nicht nachträglich bearbeitet werden.

In dem Eingabefeld "Name" können Sie den Namen der Person oder die Gruppenbezeichnung der Gruppe eintragen, die mit dem Benutzerprofil arbeitet. In dem Eingabefeld "Beschreibung" können Sie weitere Informationen zu dem Benutzerprofil hinterlegen.

Passwort

Tragen Sie in dem Eingabefeld "Passwort" und "Passwort wiederholen" das Passwort des Benutzerprofils ein. Den Benutzernamen und das Passwort benötigen Sie zum Anmelden am WBM. Benutzer-Passwörter können von dem jeweiligen Benutzer oder einem Administrator geändert werden. Die Passwortstärke Ihres Passworts wird Ihnen farb- und textlich angezeigt.

ACHTUNG
Security-Empfehlung: Passwörter Beachten Sie hierzu die Hinweise im Absatz "Passwörter" im Kapitel "Security-Empfehlungen (Seite 7)".

Sollten Sie Ihr Administrator-Passwort verlieren, müssen Sie den Reader, wie im Kapitel "Werkseinstellungen hardware-seitig zurücksetzen (Seite 113)" beschrieben, auf die Werkseinstellungen zurücksetzen.

Rollen

In dem Bereich "Rollen" können Sie dem Benutzerprofil Rollen zuweisen. Klicken Sie auf die betreffenden Optionskästchen, um dem Benutzerprofil die gewünschten Rollen zuzuweisen. Die Rolle "Administrator" beinhaltet alle Lese-/Schreibrechte.

- Administrator

  Benutzerprofil mit allen Lese-/Schreibrechten

- Benutzer

  Eingeschränktes Benutzerprofil mit Lese-/Schreibrechten. Mit der Rolle "Benutzer" können Sie keine neuen Benutzerprofile erstellen oder andere Benutzerprofile bearbeiten. Außerdem können Sie im Geräte-Status "Im Betrieb" keine schreibenden Zugriffe auf den Reader durchführen.

- Read only

  Eingeschränktes Benutzerprofil mit Leserechten. Mit der Rolle "Read only" können Sie keine neuen Benutzerprofile erstellen oder andere Benutzerprofile bearbeiten. Außerdem können Sie keine schreibenden Zugriffe auf den Reader durchführen.

- OPC UA

  Eingeschränktes Benutzerprofil mit OPC UA-Rechten. Mit der Rolle "OPC UA" können Sie ausschließlich OPC UA-Verbindung anmelden. Diese Rolle hat keinerlei Rechte im WBM und kann damit auch nicht zur Anmeldung im WBM verwendet werden.

Klicken Sie auf die Schaltfläche "Speichern", um die Änderungen zu speichern bzw. um das neue Benutzerprofil anzulegen.

Hinweis

Einschränkungen beim Übertragen der Konfiguration

Beachten Sie, dass Sie als "Benutzer" nur im Geräte-Status "Bereit" Änderungen an den Reader übertragen können. Als "Administrator" können Sie auch im Geräte-Status "Im Betrieb" Änderungen übertragen.

Die nachfolgende Tabelle gibt Ihnen einen Überblick, welche Menüpunkte für die Rolle "Benutzer" eingeschränkt sind:

Tabelle 6- 23 Einschränkungen der Rolle "Benutzer"

Menüpunkte		Einschränkungen
Startseite		• Eingeschränkt: Eingabefelder können nicht befüllt werden. • Im Geräte-Status "Im Betrieb" ist keine Bedienung möglich.
Diagnose		
	Hardware-Diagnose	Im Geräte-Status "Im Betrieb" ist keine Bedienung möglich.
	Logbuch	Eingeschränkt: Das Logbuch kann nicht zurückgesetzt werden.
	Syslog-Logbuch	Die Seite wird nicht angezeigt.
Transponder bearbeiten		Im Geräte-Status "Im Betrieb" ist keine Bedienung möglich.
Benutzerverwaltung		Eingeschränkt: Es kann ausschließlich das eigene Passwort geändert werden.
System		Im Geräte-Status "Im Betrieb" ist keine Bedienung möglich.

Außerdem können Änderungen nicht mithilfe der Schaltfläche "Konfiguration auf Reader übertragen" auf den Reader übertragen werden, solange eine aktive Kommunikationsverbindung besteht.

Automatische Abmeldung

In diesem Bereich können Sie die Zeitspanne festlegen, nach deren Ablauf Sie automatisch vom WBM abgemeldet werden. Diese Zeitspanne läuft durch Inaktivität ab und wird durch Eingaben automatisch auf den von Ihnen eingestellten Wert zurückgesetzt. Sobald die eingestellte Zeitspanne abgelaufen ist, wird die Verbindung zum Reader automatisch getrennt. Dadurch wird sichergestellt, dass die Verbindung zu dem Reader nicht durch einen inaktiven Anwender blockiert und diese für andere Nutzer freigegeben wird.

Authentifizierung

In diesem Bereich können Sie die Authentifizierung ein-/ausschalten. Beachten Sie, dass bei einer deaktivierten Authentifizierung jeder Anwender über alle Lese-/Schreibrechte verfügt (Administrator-Rechte).

ACHTUNG
Security-Empfehlung: Authentifizierung Um sicherzustellen, dass keine unbefugten Personen Zugriff auf die Reader-Einstellungen haben, empfehlen wir Ihnen, die Authentifizierung aktiviert zu lassen und neue Benutzerprofile anzulegen. Beachten Sie, dass die Authentifizierung ausschließlich durch einen Administrator aktiviert/deaktiviert werden kann.

Sicherheitseinstellungen

In dem Bereich "Sicherheitseinstellungen" können Sie die Bedingungen für die Passwort-Richtlinien, Session Timeout und Brute Force Prevention (BFP) festlegen.

Unter einer Brute-Force-Attacke versteht man eine Angriffsmethode, bei der auf Basis leistungsstarker Computersysteme sowie automatisierter Software passwortgeschützte Zugänge durch wiederholte und systematische Eingabe von Benutzer-Passwort-Varianten und -Kombinationen entschlüsselt werden. Mit dieser Angriffsmethode können maximalst viele Benutzer-Passwort-Varianten/-Kombinationen mit einer hohen Performanz abgearbeitet werden.

Durch die Brute Force Prevention (BFP) wird dieses Vorgehen ausgebremst, indem die Anzahl ungültiger Login-Versuche begrenzt werden, wodurch die Erfolgsaussichten von Brute-Force-Angriffen deutlich gesenkt werden. Bei den SIMATIC Ident-Geräten kommt der Leaky Bucket-Algorithmus zum Einsatz. Das bedeutet, dass bei einem ungültigen Login-Versuch der BFP-Level um den eingestellten Wert erhöht wird. Überschreitet der BFP-Level den festgelegten BFP-Schwellwert, werden alle weiteren Login-Versuche ignoriert. Zeitgleich wird pro Sekunde der BFP-Level um den eingestellten Wert reduziert.

Tabelle 6- 24 Beschreibung der Sicherheitseinstellungen

Parameter	Beschreibung
Passwort-Richtlinie	
Mindestanzahl Zeichen	In dem Eingabefeld können Sie die Mindestanzahl der Zeichen festlegen, aus denen die Passwörter der Benutzerprofile bestehen müssen. Wertebereich: 1 ... 32 Voreinstellung: 12
Mindestanzahl verwendeter Zeichenarten	In dem Eingabefeld können Sie die Mindestanzahl der verwendeten Zeichenarten festlegen, die die Passwörter der Benutzerprofile enthalten müssen. Wertebereich: 1 ... 4 Voreinstellung: 3
Session Timeout	
Zeitspanne	In dem Eingabefeld können Sie die Zeitspanne festlegen, nach deren Ablauf die Verbindung zu dem Reader automatisch getrennt wird (z. B. aufgrund einer getrennten Ethernet-Verbindung). Wertebereich: 30 ... 3 600 s Voreinstellung: 60 s
Brute Force Prevention (BFP)	
Erhöhung BFP-Level (pro ungültigem Login-Versuch)	In dem Eingabefeld können Sie den Wert festlegen, um den das BFP-Level bei jeder falschen Passworteingabe bzw. bei jedem ungültigen Login-Versuch erhöht wird. Wertebereich: 1 ... 10 000 Voreinstellung: 200
BFP-Schwellwert	In dem Eingabefeld können Sie den BFP-Schwellwert festlegen. Sobald der BFP-Schwellwert aufgrund mehrfach falsch eingegangener Passwörter bzw. ungültigen Login-Versuchen überschritten wird, werden alle weiteren Login-Versuche ignoriert. Erst wenn der aktuelle BFP-Level wieder unter den BFP-Schwellwert sinkt, können erneut Login-Versuche erfolgreich durchgeführt werden. Wertebereich: 1 ... 10 000 Voreinstellung: 4 000
Maximalwert des BFP-Levels	In dem Eingabefeld können Sie den Maximalwert des BFP-Levels festlegen. Bis zu dem hier angegebenen Wert wird das BFP-Level maximal erhöht. Wertebereich: 1 ... 10 000 Voreinstellung: 10 000

Parameter	Beschreibung
Reduzierung BFP-Level (pro Sekunde)	In dem Eingabefeld können Sie den Wert festlegen, um den das aktuelle BFP-Level jede Sekunde reduziert wird. Das BFP-Level wird so lange sekündlich reduziert, bis das BFP-Level auf "0" abgesenkt wurde. Wertebereich: 1 ... 10 000 s Voreinstellung: 50 s
Anzahl ungültiger Login-Versuche	Ausgabefeld/Anzeige, der Anzahl von ungültigen Login-Versuchen, die innerhalb von x Sekunden durchgeführt werden können, bis der BFP-Schwellwert erreicht wird und infolgedessen alle weiteren Login-Versuche ignoriert werden. Die Werte in diesen Feldern werden auf Basis der Eingabefelder "Erhöhung BFP-Level (pro ungültigem Login-Versuch)" und "BFP-Schwellwert" bzw. "Erhöhung BFP-Level (pro ungültigem Login-Versuch)" und "Reduzierung BFP-Level (pro Sekunde)" berechnet.
Maximale Wartezeit	Ausgabefeld/Anzeige, der maximalen Wartezeit, die vergeht - nachdem der Maximalwert des BFP-Levels erreicht wurde - bis erneut Login-Versuche erfolgreich durchgeführt werden können. Vorausgesetzt, dass in der Zwischenzeit keine weiteren ungültigen Login-Versuche durchgeführt werden. Der Wert in diesem Feld wird auf Basis der Eingabefelder "Maximalwert des BFP-Levels", "BFP-Schwellwert" und "Reduzierung BFP-Level (pro Sekunde)" berechnet.

Mit Hilfe der Schaltfläche "Speichern" können Sie die im WBM geänderten BFP-Werte auf das Kommunikationsmodul übertragen. Mit Hilfe der Schaltfläche "Aktualisieren" können Sie die im WBM angezeigten BFP-Werte aktualisieren bzw. neu von dem Reader laden.

6.3.11 Der Menüpunkt "Zertifikate"

In dem Menüpunkt "Zertifikate" können Sie vorhandene Zertifikate einsehen, neue Zertifikate importieren, sowie Zertifikatsignierungsanforderungen erstellen und Zertifikat-Dateien und Zertifikat-Schlüsseldateien auf den Reader übertragen.

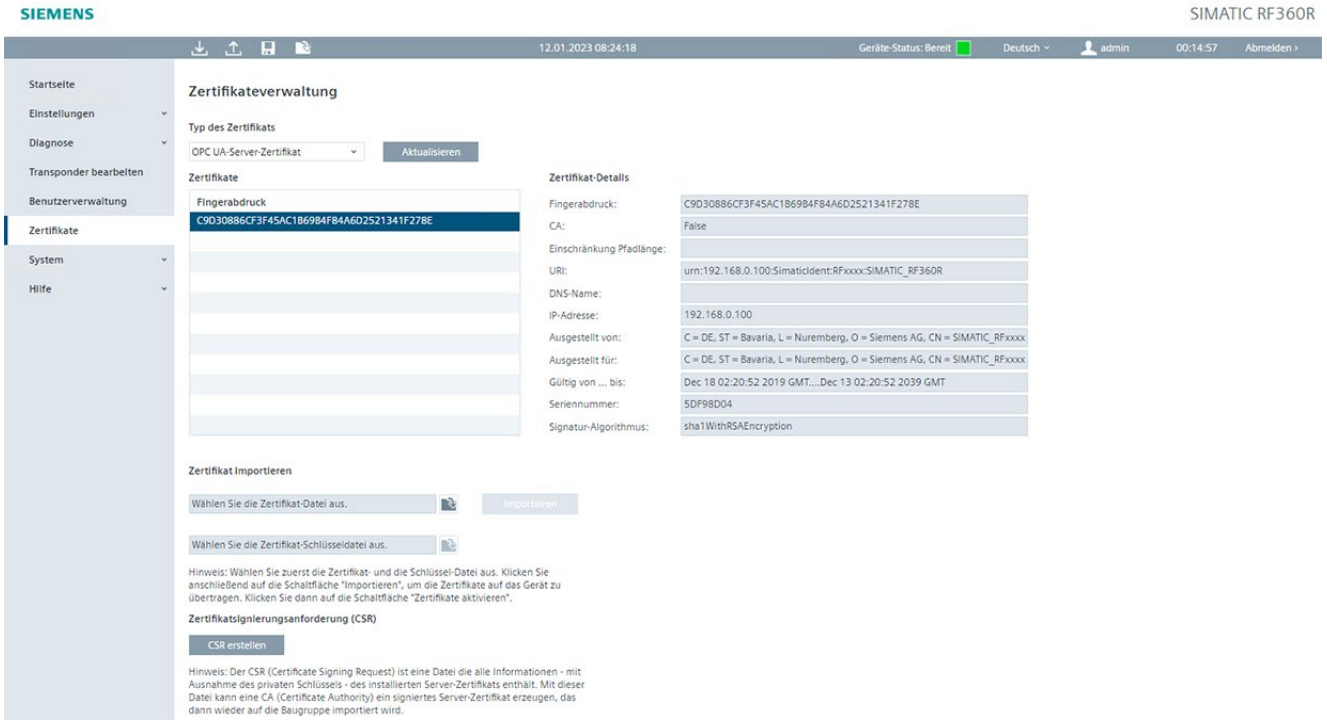


Bild 6-16 Der Menüpunkt "Zertifikate"

Mit Hilfe von Zertifikaten können Sie den Reader in Ihre jeweilige Sicherheitsinfrastruktur integrieren. Zertifikate dienen zur Überprüfung der Identität einer Person oder eines Gerätes, zum Authentifizieren eines Dienstes oder zum Verschlüsseln von Dateien. Sie können sich eigene Zertifikate anlegen oder offizielle von einer Zertifizierungsstelle erstellte Zertifikate verwenden. Sie haben die Möglichkeit Zertifikate zu importieren, die sowohl Zertifikat als auch privaten Schlüssel enthalten (PKCS#12). Wenn Sie Zertifikate und die dazugehörigen privaten Schlüssel in getrennten Dateien importieren, dann müssen beide Dateien entweder in "ASN.1" oder "Base64" codiert sein.

Zertifikate bestehen immer aus einer Zertifikat-Datei und einer Zertifikat-Schlüsseldatei, die Sie auf den Reader übertragen müssen. Beachten Sie, dass Sie die Daten erst auf den Reader importieren müssen, bevor Sie diese aktivieren können.

Wenden Sie sich an Ihre administrative IT-Abteilung, um weitere Informationen zu dem Thema zu erhalten.

Parameterübersicht

Beachten Sie, dass die nachfolgend genannten Parameter abhängig von dem ausgewählten Zertifikatetyp sind und nicht alle Parameter bei allen Zertifikatetypen angezeigt werden.

Tabelle 6- 25 Beschreibung der Parameter

Parameter	Beschreibung
Typ des Zertifikats	Auswahl des Zertifikatstyps Wählen Sie aus der Klappliste den gewünschten Zertifikattyp aus und klicken Sie auf die Schaltfläche "Aktualisieren", um die zu dem ausgewählten Zertifikattyp passenden Zertifikate angezeigt zu bekommen. • HTTPS-Zertifikat HTTPS-Zertifikat des Readers. • OPC UA-Server-Zertifikate OPC UA-Server-Zertifikat des Readers. • OPC UA-Client-Zertifikate OPC UA-Client-Zertifikate der Kommunikationspartner des Readers. • OPC UA-CA-Zertifikate Wurzelzertifikate von Zertifizierungsstellen. Zertifizierungsstellen sind Organisationen, die von ihren Zertifikaten abgeleitete signierte Zertifikate für Netzwerk-Teilnehmer ausgeben. Folglich handelt es sich bei den CA-Zertifikaten um Wurzelzertifikate für die Client-Zertifikate. Client-Zertifikate - für die ein gültiges CA-Zertifikat vorliegt - werden beim Verbindungsaufbau automatisch akzeptiert. • OPC UA-Aussteller-Zertifikate Wurzelzertifikate von Zertifizierungsstellen. Im Gegensatz zu den CA-Zertifikaten müssen hiervon abgeleitete Client-Zertifikate zusätzlich noch von einem Administrator über die Schaltfläche "Annehmen" akzeptiert und zugelassen werden. Beachten Sie, dass sich die Auswahl des Zertifikattyps auf die Anzeige der nachfolgenden Parameter auswirkt.
Aktualisieren	Schaltfläche zum Aktualisieren der in der Liste angezeigten Zertifikate Durch das Aktualisieren werden alle aktuell im Reader hinterlegten Zertifikate geladen und angezeigt.
Zertifikate	Liste aller vorhandenen Zertifikate Die in dieser Liste eingetragenen, schwarz hinterlegten Zertifikate werden von dem Reader als vertrauenswürdig eingestuft. Um die Details eines Zertifikats angezeigt zu bekommen, selektieren Sie das gewünschte Zertifikat in der Liste. Das selektierte Zertifikat wird farblich hervorgehoben. Rot dargestellte Zertifikate werden noch nicht als vertrauenswürdig eingestuft. Ein Client, der solch ein Zertifikat verwendet, kann noch keine Verbindung zum OPC UA-Partner aufbauen. Diese Zertifikate können von einem Administrator über die Schaltfläche "Annehmen" akzeptiert und zugelassen werden. Schwarz dargestellte Zertifikate wurden bereits angenommen und werden als vertrauenswürdig eingestuft. Abhängig vom ausgewählten Zertifikattyp können Sie vorhandene Zertifikate löschen. Wählen Sie dazu das gewünschte Zertifikat aus der Liste aus und klicken Sie auf die Schaltfläche "Löschen".

Parameter	Beschreibung
Zertifikat-Details	Liste mit Detail-Informationen zu dem ausgewählten Zertifikat Ausführliche Informationen zu den Zertifikat-Details entnehmen Sie den X.509-Spezifikationen.
Sperrlisten	Liste aller Sperrlisten Dieser Bereich wird angezeigt, wenn die Zertifikattypen "CA-Zertifikate" oder "Aussteller-Zertifikate" ausgewählt wurden. Eine Sperrliste wird von einer Zertifizierungsstelle herausgegeben. Für jedes CA-Zertifikat und Aussteller-Zertifikat muss eine Sperrliste hinterlegt werden. Über Sperrlisten haben Zertifizierungsstellen die Möglichkeit, von Ihnen ausgestellte und signierte Client-Zertifikate wieder zu sperren. Die in einer Sperrliste eingetragenen Zertifikate werden für die Kommunikation mit dem Reader gesperrt. Um die Details einer Sperrliste angezeigt zu bekommen, selektieren Sie die gewünschte Sperrliste in der Liste. Die selektierte Sperrliste wird farblich hervorgehoben. Um Sperrlisten aus der Liste zu löschen, wählen Sie die gewünschte Sperrliste aus der Liste aus und klicken Sie auf die Schaltfläche "Löschen".
Sperrlisten-Details	Liste mit Detail-Informationen zu der ausgewählten Sperrliste Ausführliche Informationen zu den Sperrlisten-Details entnehmen Sie entnehmen Sie den X.509-Spezifikationen.

Parameter	Beschreibung
Zertifikat importieren	In diesem Bereich können Zertifikat-Dateien auf den Reader übertragen. Zulässige Formate: • *.p12, *.pfx Binärcodiertes Dateiformat, in dem Zertifikat-Datei und Zertifikat-Schlüsseldatei in einer Datei gespeichert werden. Diese Datei ist in der Regel passwortgeschützt. Geben Sie das Passwort in dem unteren Eingabefeld ein. Beachten Sie, dass dieses Format ausschließlich für Server-Zertifikate verwendet werden kann. • *.cer, *.crt, *.der, *.pem Binär- oder textcodiertes Dateiformat, in dem Zertifikat-Datei und Zertifikat-Schlüsseldatei in separaten Dateien gespeichert werden. Beachten Sie, dass Server-Zertifikate zwingend eine separate Zertifikat-Schlüsseldatei benötigen. Bei Client-Zertifikaten, CA-Zertifikaten und Aussteller-Zertifikaten wird ausschließlich die Zertifikat-Datei angegeben. Sowohl die Zertifikat-Datei als auch die Zertifikat-Schlüsseldatei können binär- oder textcodiert vorliegen. • *.crl Binär- oder textcodiertes Dateiformat für Sperrlisten-Dateien. Diese Sperrlisten werden von CA-Zertifikate und Aussteller-Zertifikate zwingend benötigt. Wählen Sie in diesem Fall die Zertifikat-Datei und die Sperrlisten-Datei aus, bevor Sie auf die Schaltfläche "Importieren" klicken. Ist auf dem Reader bereits eine passende Sperrliste hinterlegt, kann ein CA-Zertifikat oder Aussteller-Zertifikat auch allein übertragen werden. Beachten Sie, dass ausschließlich Dateien mit der Dateiendung *.crl für Sperrlisten verwendet werden können. Nachdem Sie ein Server-Zertifikat importiert haben, müssen Sie dieses noch aktivieren.
Zertifikatsignierungsanforderung (CSR)	Schaltfläche, um eine Zertifikatsignierungsanforderung zu erstellen. Dieser Bereich wird angezeigt, wenn der Zertifikattyp "Server-Zertifikate" ausgewählt wurde. Klicken Sie auf die Schaltfläche "CSR erstellen", um eine Zertifikatsignierungsanforderung (CSR) zu erstellen. Die CSR-Datei enthält alle relevanten Informationen des installierten Server-Zertifikats. Mit Hilfe dieser Datei kann ein CA (Certificate Authority) ein signiertes, baugruppen-spezifisches Server-Zertifikat erzeugen, das Sie anschließend in diese Baugruppe importiert wird.

Unterstütze Dateiformate

Die nachfolgende Tabelle gibt Ihnen einen Überblick über die von den verschiedenen Zertifikat-Typen unterstützten Dateiformate.

Tabelle 6- 26 Unterstützte Dateiformate der verschiedenen Zertifikat-Typen

Zertifikat-Typen	Unterstützte Dateiformate
HTTPS OPC UA-Server	*.p12 *.pfx *.pem [1] *.cer *.crt *.der
OPC UA-Client OPC UA-CA OPC UA-Aussteller	*.pem [1] *.cer *.crt *.der

[1] Kann ggf. privaten Schlüssel enthalten.

6.3.12 Der Menüpunkt "System - Geräteeinstellungen"

In dem Menüpunkt "System - Geräteeinstellungen" können Sie Firmware-Updates durchführen, den Reader auf Werkseinstellung zurücksetzen, die IP-Adresse des Readers ändern, Zertifikate auf den Reader laden und Steuerungsdateien auf den PC übertragen. Diese Seite ist in folgende Bereiche unterteilt:

- Firmware-Update
- Zurücksetzen
- Gerätebeschreibungsdateien

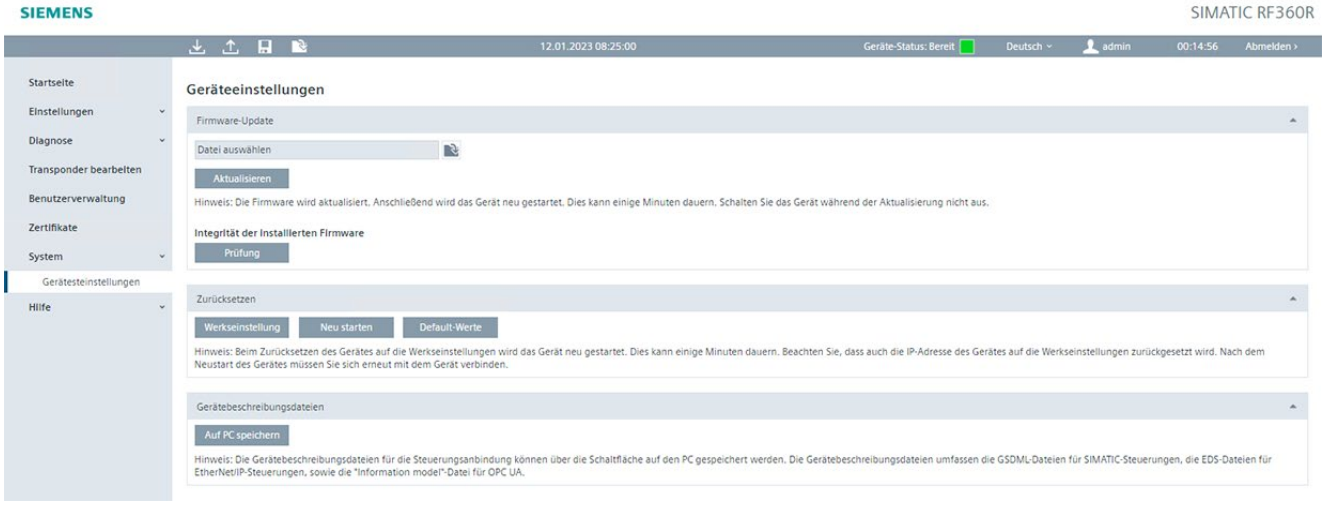


Bild 6-17 Der Menüpunkt "System - Geräteeinstellungen"

Firmware-Update

- Firmware-Update

  Mit Hilfe der Schaltfläche "Firmware-Update" können Sie die Firmware des Kommunikationsmoduls aktualisieren. Eine genaue Beschreibung des Firmware-Updates finden Sie im Kapitel "Firmware-Update (Seite 109)".

- Prüfen

  Mit Hilfe der Schaltfläche "Prüfen" können Sie die Integrität der Firmware überprüfen. Mit dieser Funktion können Sie prüfen, ob die Firmware mit der von Siemens veröffentlichten Firmware übereinstimmt oder die möglicherweise böswillig verändert wurde.

Werkseinstellung

In dem Bereich "Werkseinstellung" können Sie den Reader auf die Werkseinstellung oder auf die voreingestellten Default-Werte zurücksetzen oder diesen neu starten.

- Werkseinstellung

  Mit Hilfe der Schaltfläche "Werkseinstellung" können Sie den Reader auf die werkseitig eingestellten Konfigurationseinstellungen zurückzusetzen. Beim Zurücksetzen des Readers auf die Werkseinstellung gehen alle eingestellten Konfigurationsdaten, Einstellungen der Benutzerverwaltung, sowie Adressinformationen verloren. Nach dem Zurücksetzen wird der Reader automatisch neu gestartet. Beachten Sie, dass Sie anschließend dem Reader eine neue IP-Adressen zuweisen müssen.

  Sollten Sie Ihr Administrator-Passwort verlieren, müssen Sie den Reader, wie im Kapitel "Werkseinstellungen hardware-seitig zurücksetzen (Seite 113)" beschrieben, auf die Werkseinstellungen zurücksetzen.

- Neu starten

  Mit Hilfe der Schaltfläche "Neu starten" können Sie einen Neustart des Readers ausführen.

- Default-Werte

  Mit Hilfe der Schaltfläche "Default-Werte" können Sie die Parameterwerte des Readers auf die werkseitig eingestellten Konfigurationseinstellungen zurückzusetzen. Beim Zurücksetzen auf die Default-Werte gehen alle eingestellten Konfigurationsdaten verloren, Einstellungen der Benutzerverwaltung, sowie Adressinformationen bleiben jedoch erhalten.

Gerätebeschreibungsdateien

Auf dem Reader sind die zum Lieferzeitpunkt aktuellen GSDML- und ESD-Dateien, sowie OPC UA-Gerätebeschreibungsdatei hinterlegt. Klicken Sie auf die Schaltfläche "Auf PC speichern", um die Gerätebeschreibungsdateien auf den angeschlossenen PC zu übertragen. Mithilfe dieser Dateien können Sie die Reader in die Projektierungssoftware Ihrer Steuerungen integrieren.

6.3.13 Der Menüpunkt "Hilfe"

Service & Support

In dem Menüpunkt "Hilfe - Service & Support" erhalten Sie weiterführende Informationen zu dem Reader RF360R, sowie Links zu relevanten Dokumenten auf den Seiten des Siemens Industry Online Support. Zusätzlich können Sie über einen Link die Readme OSS-Datei mit den Copyright-Hinweisen und Lizenzbedingungen zu der in dieser Firmware enthaltenen Open Source Software öffnen.

Handbuch

In dem Menüpunkt "Hilfe - Handbuch" finden Sie das zu dem Reader gehörende Handbuch "SIMATIC RF360R".

Programmieren

7

7.1 Programmieren über SIMATIC-Steuerung

Dieses Kapitel richtet sich ausschließlich an S7-Anwender.

Voraussetzung: Die PLC-Schnittstelle wurde im WBM aktiviert.

Der Reader ist ab der TIA Portal-Version V17 in STEP 7 Basic / Professional integriert und kann über eine HSP-Datei ins TIA Portal V16 integriert werden. In beiden Fällen können Sie den Reader mit Hilfe des Technologieobjekts "SIMATIC Ident" programmieren und projektieren. Alternativ können Sie den Reader auch mit Hilfe der Ident-Anweisungen programmieren und projektieren. Das Ident-Profil und die Ident-Bausteinen sind ab der Version V13.1 in STEP 7 integriert.

In ältere TIA Portal-Versionen (< V16) kann der Reader über eine GSDML-Datei integriert werden. In diesem Fall müssen Sie bei dem Betrieb über SIMATIC Steuerung S7-1200/-1500 die Bibliotheksversion V4.0 der Ident-Anweisungen verwenden, um den Reader zu programmieren und projektieren.

Eine ausführliche Beschreibung der Ident Anweisungen (Ident-Profil und Ident-Bausteine) finden Sie im Funktionshandbuch "Ident-Profil und Ident-Bausteine, Standardfunktionen für Ident-Systeme (https://support.industry.siemens.com/cs/ww/de/view/109793329)".

Hinweis

Funktionsbaustein "FB 45" wird nicht unterstützt

Beachten Sie, dass der Funktionsbaustein "FB 45" von dem Reader nicht unterstützt wird.

7.2 Programmieren über XML

Dieses Kapitel richtet sich ausschließlich an XML-Anwender.

Voraussetzung: Die XML-Schnittstelle wurde im WBM aktiviert.

Sie können den Reader über die XML-Schnittstelle mit Hilfe von XML-Befehlen programmieren. Ausführliche Informationen hierzu finden Sie im Handbuch "XML-Programmierung für SIMATIC Ident (https://support.industry.siemens.com/cs/ww/de/view/109781631)".

7.3 Programmieren über OPC UA

Dieses Kapitel richtet sich ausschließlich an OPC UA-Anwender.

Voraussetzung: Die OPC UA-Schnittstelle wurde im WBM aktiviert.

Sie können die Reader über die OPC UA-Schnittstelle mit Hilfe von Variablen, Events und Methoden programmieren. Ausführliche Informationen hierzu finden Sie im Handbuch "OPC UA für SIMATIC Ident (https://support.industry.siemens.com/cs/ww/de/ps/14971/man)".

7.4 Programmieren über Rockwell-Steuerung

Dieses Kapitel richtet sich ausschließlich an Rockwell-Anwender.

Voraussetzung: Die PLC-Schnittstelle wurde im WBM aktiviert.

Sie können den Reader mit Hilfe von Add-On Instructions über eine Rockwell-Steuerung programmieren. Mithilfe der beschriebenen Funktionen können Sie Transponder-Daten über die Reader auslesen und beschreiben. Eine ausführliche Beschreibung des Ident-Profils und der Add-On Instructions finden Sie im Funktionshandbuch "Ident-Profil, Add-On Instructions für Rockwell-Systeme (https://support.industry.siemens.com/cs/ww/de/view/109781634/137304404619)".

Fehlermeldungen

8

Für die Baugruppen stehen Ihnen folgende Optionen zur Fehleranalyse zur Verfügung:

- über Fehlermeldungen des Readers
- über das WBM
- über XML-Fehlermeldungen
- über OPC UA-Fehlermeldungen

Im Folgenden werden diese alternativen Vorgehensweisen beschrieben.

8.1 Fehlermeldungen des Readers

Beachten Sie, dass abhängig von der Fehlerursache bei Fehlermeldungen immer die Status-LED "ERROR" (ER) blinken. Sie können den Fehler über die Fehlercodes oder alternativ über das Logbuch des WBMs auslesen.

In der folgenden Tabelle sind die Fehlercodes, sowie die Blinkmuster der Reader-LED aufgeführt.

Tabelle 8- 1 Fehlermeldungen der Reader

Blinken der Reader-LED	Baustein (hex)	Fehlerbeschreibung
12	0xE1FE0100	Der Speicher des Transponders kann nicht beschrieben werden. Mögliche Ursachen: • Speicher des Transponders ist defekt. • EEPROM-Transponder wurde zu oft beschrieben und hat sein Lebensende erreicht.
02	0xE1FE0200	Anwesenheitsfehler Der Transponder befindet sich nicht mehr im Übertragungsfenster des Readers. Der Befehl wurde nicht oder nur teilweise abgearbeitet. Lesebefehl: Es sind keine gültigen Daten in "IDENT_DATA" vorhanden. Schreibbefehl: Der Transponder, der gerade das Antennenfeld verlassen hat, beinhaltet einen unvollständigen Datensatz. Mögliche Ursachen: • Arbeitsabstand zwischen Reader und Transponder wird nicht eingehalten. • Projektierungsfehler: Der zu bearbeitende Datensatz ist zu groß (im dynamischen Betrieb).

Blinken der Reader-LED	Baustein (hex)	Fehlerbeschreibung
13	0xE1FE0300	Adressfehler Der Adressbereich des Transponders wird überschritten. Mögliche Ursachen: • Anfangsadresse beim Befehlsstart ist falsch aufgesetzt. • Falscher Transponder-Typ • Der zu schreibende Bereich ist schreibgeschützt.
--	0xE1FE0400	Initialisierungsfehler Der Transponder kann den Initialisierungsbefehl nicht durchführen Mögliche Ursachen: • Transponder ist defekt.
--	0xE1FE0500	Der Speicher des Transponders ist voll.
04	0xE1FE0600	RF300: Beim Semaphore-Verfahren wurde die Datenspeicherung nicht korrekt abgeschlossen.
11	0xE1FE0700	Passwort-Fehler
--	0xE1FE0900	Der Befehl wird von dem Transponder nicht unterstützt.
--	0xE1FE0A00	Der Transponder ist lese-/schreibgeschützt.
--	0xE1FE8100	Der Transponder antwortet nicht.
--	0xE1FE8200	Das Transponder-Passwort ist falsch. Zugriff wird verweigert.
--	0xE1FE8300	Die Verifikation der geschriebenen Transponder-Daten ist fehlgeschlagen. Mögliche Ursachen: • Transponder ist defekt. • Transponder befindet sich im Grenzbereich.
--	0xE1FE8400	Allgemeiner Transponder-Fehler
--	0xE1FE8500	Der Transponder hat zu wenig Leistung, um den Befehl auszuführen. Mögliche Ursachen: • Transponder befindet sich im Grenzbereich.

Blinken der Reader-LED	Baustein (hex)	Fehlerbeschreibung
06	0xE2FE0100	Feldstörung am Reader Mögliche Ursachen: • Der Reader empfängt Störimpulse aus der Umgebung. – Externes Störfeld; das Störfeld kann mit dem "induktiven Feldindikator" des mobilen Readers nachgewiesen werden. – Der Abstand zwischen zwei Readern ist zu klein und entspricht nicht den Projektierungsrichtlinien. – Das Verbindungskabel zum Reader wird gestört, ist zu lang oder entspricht nicht der Spezifikation. • Zu viele Sendefehler Der Transponder konnte den Befehl oder die Schreibdaten vom Kommunikationsmodul nach mehreren Versuchen nicht richtig empfangen. – Transponder steht genau im Grenzbereich des Übertragungsfensters. – Datenübertragung zum Transponder wird durch externe Störungen beeinflusst. • CRC-Sendefehler – Der Transponder meldet sehr oft CRC-Fehler (Transponder steht im Grenzbereich des Readers; Transponder und/oder Reader haben einen Hardwaredefekt). • Nur bei Initialisierung: CRC-Fehler beim Quittungsempfang vom Transponder (Ursache wie bei Feldstörung am Reader). • Bei der Formatierung muss der Transponder im Übertragungsfenster des Readers stehen, ansonsten erfolgt ein Timeout-Fehler, d. h.: – Der Transponder steht genau im Grenzbereich des Übertragungsfensters. – Der Transponder ist defekt und verbraucht zu viel Strom. – Der EEPROM-Transponder wurde durch "FORMAT" falsch parametriert. • RF300: ECC-Fehler Die Daten können nicht vom Transponder gelesen werden. Mögliche Ursachen: – Daten des Transponders sind verlorengegangen (Transponder defekt). – Der Transponder wurde nicht mit dem ECC-Treiber initialisiert. – Der EEPROM-Speicher des Transponders hat sein Lebensende erreicht und die Daten sind verloren gegangen. – Während des Schreibvorgangs hat der Transponder das Antennenfeld verlassen. – Der Befehl zum Kommunikationsmodul wurde falsch aufgesetzt.
--	0xE2FE0200	Es sind mehr Transponder im Übertragungsfenster, als der Reader gleichzeitig bearbeiten kann.
--	0xE2FE8100	Kein Transponder mit der gewünschten EPC-ID/UID befindet sich im Übertragungsfenster, bzw. es befindet sich gar kein Transponder im Antennenfeld.
--	0xE2FE8200	Die angeforderten Daten sind nicht verfügbar.
--	0xE2FE8300	CRC-Fehler in der Reader-Transponder-Kommunikation.
--	0xE2FE8400	Die ausgewählte Antenne ist nicht aktiviert.
--	0xE2FE8500	Die ausgewählte Frequenz ist nicht aktiviert.
--	0xE2FE8600	Das Trägersignal ist nicht aktiviert.
--	0xE2FE8700	Mehr als ein Transponder befindet sich im Übertragungsfenster.

Blinken der Reader-LED	Baustein (hex)	Fehlerbeschreibung
--	0xE3FE0100	Der Dateiname ist nicht zulässig.
--	0xE3FE0200	Die Datei existiert nicht.
--	0xE4FE0100	Warnung bei niedriger Spannungsversorgung Die Versorgungsspannung ist dem unteren Grenzwert sehr nahe.
--	0xE4FE0200	Hardware-Fehler
28	0xE4FE0300	Verbindungsproblem zum Reader Fehler in der Verbindung zum Reader; Reader antwortet nicht. Mögliche Ursachen / weiteres Vorgehen: • Das PROFINET- oder das Spannungsversorgungskabel ist falsch verdrahtet oder Kabelbruch. • Die 24 V-Versorgungsspannung ist nicht angeschlossen oder abgeschaltet bzw. kurzzeitig ausgefallen. • Die Hardware ist defekt. • RF300: Antenne wird nicht erkannt. Mögliche Ursachen: Antenne ist nicht angeschlossen oder Antennenkabel ist defekt. • Führen Sie nach der Fehlerbehebung einen "init_run" durch.
19	0xE4FE0400	Der Puffer im Kommunikationsmodul oder Reader zur Zwischenspeicherung des Befehls reicht nicht aus.
--	0xE4FE0500	Der Puffer im Kommunikationsmodul oder Reader zur Zwischenspeicherung der Daten reicht nicht aus.
--	0xE4FE0600	Dieser Befehl ist in diesem Status nicht erlaubt, bzw. wird nicht unterstützt. Mögliche Ursachen: • Der Befehl "INIT" wurde verkettet. • Die Befehlswiederholung wurde ohne "Presence-Mode" gestartet.
--	0xE4FE0700	Hochlaufmeldung vom Reader/Kommunikationsmodul Der Reader bzw. das Kommunikationsmodul war ausgeschaltet und hat noch keinen Befehl "Reset_Reader" ("WRITE-CONFIG") erhalten. Mögliche Ursachen / weiteres Vorgehen: • Führen Sie den Befehl "INIT" durch. • Die gleiche physikalische Adresse im Parameter "IID_HW_CONNECT" wird mehrmals verwendet. Überprüfen Sie ihre "IID_HW_CONNECT"-Parametrierungen. • Überprüfen Sie die Verbindung zum Reader. • Nachdem die Übertragungsgeschwindigkeit geändert wurde, wurde das Gerät noch nicht neu gestartet.
--	0xE4FE8100	Das angegebene Tag-Feld des Transponders ist nicht bekannt.
--	0xE4FE8A00	Allgemeiner Fehler
--	0xE4FE8B00	Es wurden keine oder fehlerhafte Konfigurationsdaten/Parameter übertragen. Mögliche Ursachen: • Sie greifen auf eine nicht projektierte Lesestelle zu.

Blinken der Reader-LED	Baustein (hex)	Fehlerbeschreibung
--	0xE4FE8C00	• Kommunikationsfehler zwischen Ident-Profil und Reader. Handshake-Fehler. Mögliche Ursachen / weiteres Vorgehen: – Der UDT dieses Geräts wurde durch andere Programmteile überschrieben. – Überprüfen Sie die Parametrierung des Geräts im UDT. – Überprüfen Sie den Befehl des Ident-Profil, der zu diesem Fehler führt. – Führen Sie nach der Fehlerbehebung den Befehl "INIT" durch.
20	0xE4FE8D00	• Kommunikationsfehler des Kommunikationsmoduls/Readers Mögliche Ursachen / weiteres Vorgehen: – Stecker-Kontaktproblem auf dem Kommunikationsmodul/Reader – Hardware des Kommunikationsmoduls/Readers hat einen Defekt; → Kommunikationsmodul/Reader zur Reparatur einschicken. – Führen Sie nach der Fehlerbehebung den Befehl "INIT" durch. • Überwachungsfehler des Kommunikationsmoduls/Readers Mögliche Ursachen / weiteres Vorgehen: – Programmablauffehler auf dem Kommunikationsmodul/Reader – Versorgungsspannung des Kommunikationsmoduls/Readers aus- und wieder einschalten. – Führen Sie nach der Fehlerbehebung den Befehl "INIT" durch. • Firmware-Fehler Mögliche Ursachen: Das Firmware-Update wurde nicht vollständig durchgeführt.
--	0xE4FE8E00	Der laufende Befehl wurde durch den Befehl "WRITE-CONFIG" ("INIT" oder "RESET") abgebrochen bzw. der Busstecker wurde abgezogen. Mögliche Ursachen: • Die Kommunikation mit dem Transponder wurde mit "INIT" abgebrochen. • Dieser Fehler kann nur bei einem "INIT" oder "RESET" zurückgemeldet werden.
--	0xE5FE0100	Falsche Sequenz-Nummernfolge (SN) im Reader/Kommunikationsmodul
--	0xE5FE0200	Falsche Sequenz-Nummernfolge (SN) im Ident-Profil
--	0xE5FE0400	Ungültige Datenblock-Nummer (DBN) im Reader/Kommunikationsmodul
--	0xE5FE0500	Ungültige Datenblock-Nummer (DBN) im Ident-Profil
--	0xE5FE0600	Ungültige Datenblock-Länge (DBL) im Reader/Kommunikationsmodul
--	0xE5FE0700	Ungültige Datenblock-Länge (DBL) im Ident-Profil

Blinken der Reader-LED	Baustein (hex)	Fehlerbeschreibung
25	0xE5FE0800	Vorheriger Befehl ist noch aktiv bzw. der Puffer ist voll. An den Reader bzw. das Kommunikationsmodul wurde ein neuer Befehl geschickt, obwohl der letzte Befehl noch aktiv ist. • Der aktive Befehl kann nur durch "INIT" abgebrochen werden. • Vor dem Start eines neuen Befehls muss das "DONE-Bit = 1" sein (Ausnahme "INIT"). • Zwei Ident-Profil-Aufrufe wurden mit den gleichen Parametern "HW_ID", "CM_CHANNEL" und "LADDR" parametriert. • Zwei Ident-Profil-Aufrufe arbeiten mit dem gleichen Zeiger. • Führen Sie nach der Fehlerbehebung den Befehl "INIT" durch. • Beim Arbeiten mit Befehlswiederholung (z. B. Festcode-Transponder) werden keine Daten vom Transponder abgeholt. Der Datenpuffer im Reader/Kommunikationsmodul ist übergelaufen. Es sind Transponder-Daten verloren gegangen.
--	0xE5FE0900	Der Reader bzw. das Kommunikationsmodul führt einen Hardware-Reset aus ("INIT_ACTIVE" auf "1" gesetzt). Das Ident-Profil erwartet einen "INIT" (Bit 15 im zyklischen Steuerwort).
--	0xE5FE0A00	Der Befehlscode "CMD" und die entsprechende Bestätigung stimmen nicht überein. Hierbei kann es sich um einen Software- oder Synchronisationsfehler handeln, der im Normalbetrieb nicht auftreten kann.
--	0xE5FE0B00	Falsche Reihenfolge der Quittungstelegramme (TDB / DBN)
--	0xE5FE0C00	Synchronisationsfehler (falsches Inkrement von "AC_H / AC_L" und "CC_H / CC_L" im zyklischen Steuerwort). "INIT" musste ausgeführt werden.
--	0xE5FE8100	Interner Kommunikationsfehler Zugriff verweigert
--	0xE5FE8200	Interner Kommunikationsfehler Ressource belegt
--	0xE5FE8300	Interner Kommunikationsfehler Funktionsfehler der Reader-Schnittstelle
--	0xE5FE8400	Interner Kommunikationsfehler Sonstige Fehler
05	0xE6FE0100	Unbekannter Befehl Ein nicht interpretierbarer XML-Befehl wurde an den Reader gesendet oder das Ident-Profil sendet einen nicht interpretierbaren Befehl an den Reader. Mögliche Ursachen: • Der Baustein "AdvancedCmd" wurde mit einem falschen "CMD" versorgt. • Der Eingang "CMD" des Bausteins "AdvancedCmd" wurde überschrieben.
--	0xE6FE0200	Ungültiger Kommandoindex (CI)

Blinken der Reader-LED	Baustein (hex)	Fehlerbeschreibung
21	0xE6FE0300	• Ein Parameter eines XML-Befehls hat einen ungültigen Wert oder das Kommunikationsmoduls bzw. der Reader wurde falsch parametriert. Mögliche Ursachen / weiteres Vorgehen: – Überprüfen Sie die Parameter im Ident-Profil. – Überprüfen Sie den entsprechenden XML-Befehl. – Überprüfen Sie die Parametrierung in HW-Konfig / STEP 7 (TIA Portal). – Der Befehl "WRITE-CONFIG" ist falsch parametriert. – Nach einem Hochlauf hat der Reader bzw. das Kommunikationsmodul noch keinen "INIT" erhalten. • Der Reader bzw. das Kommunikationsmodul am PROFIBUS/PROFINET wurde falsch parametriert und der Befehl kann nicht abgearbeitet werden. Mögliche Ursachen / weiteres Vorgehen: – Länge der Ein-/Ausgangsbereiche ist zu klein für das zyklische Wort E/A. – Überprüfen Sie, ob Sie die richtige GSD-Datei verwendet haben. – Der Befehl (z. B. "READ") mit zu großer Länge der Nutzdaten aufgesetzt. • Fehler beim Bearbeiten des Befehls. Mögliche Ursachen / weiteres Vorgehen: – Die Daten im "AdvancedCmd" bzw. "IID_CMD_STRUCT" sind fehlerhaft (z. B. "WRITE"-Befehl mit Länge = 0). Überprüfen Sie "AdvancedCmd" bzw. "IID_CMD_STRUCT" und führen Sie einen "INIT" durch. – Die Hardware des Readers/Kommunikationsmoduls ist defekt. Bei einem "INIT" erhält der Reader bzw. das Kommunikationsmodul falsche Daten. – Inkonsistente Längenangaben im Befehl • Der falsche Reset-Baustein wurde ausgewählt. Mögliche Ursachen / weiteres Vorgehen: – Verwenden Sie, unabhängig vom gewählten Reader-System, den Funktionsbaustein "Reset_Reader".
--	0xE6FE0400	Anwesenheitsfehler Ein Transponder hat das Übertragungsfenster eines Readers durchquert, ohne bearbeitet zu werden. • Diese Fehlermeldung wird nicht sofort gemeldet. Vielmehr wartet der Reader bzw. das Kommunikationsmodul auf den nächsten Schreib-/Lesebefehl. Dieser Befehl wird sofort mit diesem Fehler beantwortet und der Schreib-/Lesebefehl wird nicht bearbeitet. Erst der nächste Befehl wird wieder regulär vom Reader/Kommunikationsmodul ausgeführt. • Sie können diesen Fehlerzustand mit Hilfe eines "INIT" zurücksetzen. • Im Parameter "OPT1" ist das Bit 2 gesetzt und es befindet sich kein Transponder im Übertragungsfenster.

Blinken der Reader-LED	Baustein (hex)	Fehlerbeschreibung
24	0xE6FE0500	Es ist ein Fehler aufgetreten, der ein Reset_Reader ("WRITE-CONFIG" mit "Config = 3") erforderlich macht. Mögliche Ursachen / weiteres Vorgehen: • Der Befehl "WRITE-CONFIG" ist fehlerhaft. • Führen Sie nach der Fehlerbehebung einen "INIT" durch. • Überprüfen Sie den Parameter "IID_HW_CONNECT".
--	0xE6FE8100	Ein Parameter fehlt.
--	0xE6FE8200	Der Parameter hat ein ungültiges Format.
--	0xE6FE8300	Der Parameter-Typ ist ungültig.
--	0xE6FE8400	Unbekannter Parameter.
--	0xE6FE8500	Der Befehl bzw. das Telegramm hat ein ungültiges Format.
--	0xE6FE8600	Der Inventory-Befehl ist fehlgeschlagen.
--	0xE6FE8700	Der Lesezugriff auf den Transponder ist fehlgeschlagen.
--	0xE6FE8800	Der Schreibzugriff auf den Transponder ist fehlgeschlagen.
--	0xE6FE8900	Das Schreiben der EPC-ID/UID auf dem Transponder ist fehlgeschlagen.
--	0xE6FE8A00	Das Aktivieren des Schreibschutzes auf dem Transponder ist fehlgeschlagen.
--	0xE6FE8B00	Der "Kill"-Befehl ist fehlgeschlagen.
--	0xE7FE0100	In diesem Zustand ist nur der Befehl "Reset_Reader" ("WRITE-CONFIG") zulässig.
--	0xE7FE0200	Der Befehlscode "CMD" ist nicht zulässig.
--	0xE7FE0300	Der Parameter "LEN_DATA" des Befehls ist zu lang und passt nicht zu den globalen Daten, die innerhalb des Sendedaten-Puffers (TXBUF) reserviert wurden.
--	0xE7FE0400	Der Empfangsdaten-Puffer (RXBUF) oder der Sendedaten-Puffer (TXBUF) ist zu klein, der angelegte Puffer an TXBUF/RXBUF hat nicht den richtigen Datentypen oder der Parameter "LEN_DATA" hat einen negativen Wert. Mögliche Ursache / weiteres Vorgehen: • Überprüfen Sie, ob die Puffer TXBUF/RXBUF mindestens so groß sind wie bei "LEN_DATA" angegeben. • Bei S7-1200/1500: – Am Ident-Profil darf nur ein "Array of Byte" an TXBUF und RXBUF angelegt werden. – An dem Baustein "Reader_Status" dürfen nur ein "Array of Byte" oder die dazugehörigen Datentypen angelegt werden ("IID_TAG_STATUS_XX_XXX" oder "IID_READER_STATUS_XX_XXX")
--	0xE7FE0500	Fehlermeldung, die Sie darüber informiert, dass als nächster Befehl nur ein "INIT"-Befehl zulässig ist. Alle anderen Befehle werden zurückgewiesen.
--	0xE7FE0600	Falscher Datensatzindex eines azyklischen Datensatzes Erlaubter Index liegt in den Bereichen "101 ... 108" und "-20401 ... -20418".
--	0xE7FE0700	Der Reader bzw. das Kommunikationsmodul antwortet nicht auf "INIT" (in zyklischer Statusmeldung wird "INIT_ACTIVE" erwartet). Weiteres Vorgehen: • Überprüfen Sie den Adress-Parameter "LADDR".
--	0xE7FE0800	Zeitüberschreitung während des "INIT" (60 Sekunden)

Blinken der Reader-LED	Baustein (hex)	Fehlerbeschreibung
--	0xE7FE0900	Befehlswiederholung wird nicht unterstützt.
--	0xE7FE0A00	Fehler während der Übertragung der PDU (Protocol Data Unit).

"--" bedeutet, dass der Fehler nicht über die LEDs angezeigt wird.

8.2 Fehlermeldungen über das WBM auslesen

Im "Logbuch" werden alle aufgetretenen Diagnosemeldungen des Reader protokolliert, wenn in der WBM-Projektierung unter "Einstellungen - Allgemein" der Haken bei "ERRORS" gesetzt wurde. Weitere Informationen zum "Logbuch" finden Sie im Kapitel "Der Menüpunkt "Diagnose - Logbuch" (Seite 68)".

8.3 XML-Fehlermeldungen

Eine Liste der möglichen XML-Fehlercodes finden Sie im Handbuch "XML-Programmierung für SIMATIC Ident (https://support.industry.siemens.com/cs/ww/de/view/109781631)".

8.4 OPC UA-Fehlermeldungen

In der folgenden Tabelle werden die OPC UA-spezifischen Fehlercodes aufgeführt.

Tabelle 8- 2 OPC UA-Fehlermeldungen der Kommunikationsmodule/Reader

AutoId-Status	**OPC UA-Status**	**AutoId-Text**	**Fehlerbeschreibung**
1	good	MISC_ERROR_TOTAL	Allgemeiner Fehler
1	good	MISC_ERROR_TOTAL	• Firmware-Fehler Mögliche Ursache: Das Firmware-Update wurde nicht vollständig durchgeführt. • Interner Kommunikationsfehler des Kommunikationsmoduls/Reader – Stecker-Kontaktproblem auf dem Kommunikationsmodul/Reader – Hardware des Kommunikationsmoduls/Reader hat einen Defekt; → Kommunikationsmodul/Reader zur Reparatur einschicken – Nach Fehlerbehebung "INIT" starten • Interner Überwachungsfehler des Kommunikationsmoduls/Reader – Programmablauffehler auf dem Kommunikationsmodul/Reader – Versorgungsspannung des Kommunikationsmoduls/Reader aus- und wiedereinschalten – Nach Fehlerbehebung "INIT" starten
1	good	MISC_ERROR_TOTAL	Der "Inventory"-Befehl ist fehlgeschlagen.
1	good	MISC_ERROR_TOTAL	Das Aktivieren des Schreibschutzes auf dem Transponder ist fehlgeschlagen.
1	good	MISC_ERROR_TOTAL	Der "Kill"-Befehl ist fehlgeschlagen.
3	good	PERMISSON_ERROR	Der Transponder ist lese-/schreibgeschützt.
4	good	PASSWORD_ERROR	Das Transponder-Passwort ist falsch. Zugriff wird verweigert.
5	Bad Invalid Argument / good	REGION_NOT_FOUND_ERROR	Alle Befehle: Ein Parameter eines OPC UA-Befehls hat einen ungültigen Wert. "ReadTag"/"WriteTag"-Befehl: Der adressierte Speicherbereich ist beim aktuellen Transponder nicht verfügbar.

AutoId-Status	OPC UA-Status	AutoId-Text	Fehlerbeschreibung
7	good	OUT_OF_RANGE_ ERROR	Adressfehler Der Adressbereich des Transponders wird überschritten. Mögliche Ursachen: • Anfangsadresse beim Befehlsstart ist falsch aufgesetzt. • Falscher Transponder-Typ • Der zu schreibende Bereich ist schreibgeschützt.
7	good	OUT_OF_ RANGE_ERROR	Die angeforderten Daten sind nicht verfügbar.
8	good	NO_ IDENTIFIER	Kein Transponder mit der gewünschten EPC-ID/UID befindet sich im Übertragungsfenster, bzw. es befindet sich gar kein Transponder im Antennenfeld.
9	good	MULTIPLE_ IDENTIFIERS	Es sind mehr Transponder im Übertragungsfenster, als der Reader gleichzeitig bearbeiten kann.
9	good	MULTIPLE_ IDENTIFIERS	Mehr als ein Transponder befinden sich im Übertragungsfenster.
10	good	READ_ ERROR	Der Lesezugriff auf den Transponder ist fehlgeschlagen.
14	good	WRITE_ ERROR	Der Schreibzugriff auf den Transponder ist fehlgeschlagen.
14	good	WRITE_ ERROR	Das Schreiben der EPC-ID/UID auf dem Transponder ist fehlgeschlagen.
15	good	NOT_SUPPORTED_ BY_DEVICE	Unbekannter Befehl Ein nicht interpretierbarer XML-Befehl wurde an den Reader gesendet oder das Ident-Profil sendet einen nicht interpretierbaren Befehl an den Reader. Mögliche Ursachen: • Der Baustein "AdvancedCmd" wurde mit einem falschen "CMD" versorgt. • Der Eingang "CMD" des Bausteins "AdvancedCmd" wurde überschrieben.
17	good	DEVICE_NOT_ READY	Die angegebene Lesestelle ist nicht aktiv, da dieser keine Antennen zugewiesen wurden.
18	good	INVALID_ CONFIGURATION	Das angegebene Tag-Feld des Transponders ist nicht bekannt.
19	good	RF_COMMUNICATION_ ERROR	Der Transponder antwortet nicht.
19	good	RF_COMMUNICATION_ ERROR	Die Verifikation der geschriebenen Transponder-Daten ist fehlgeschlagen.
19	good	RF_COMMUNICATION_ ERROR	Allgemeiner Transponder-Fehler
19	good	RF_COMMUNICATION_ ERROR	Der Transponder hat zu wenig Leistung, um den Befehl auszuführen.
19	good	RF_COMMUNICATION_ ERROR	Der Transponder meldet einen CRC-Fehler.
19	good	RF_COMMUNICATION_ ERROR	Die ausgewählte Frequenz ist nicht aktiviert.
19	good	RF_COMMUNICATION_ ERROR	Das Trägersignal ist nicht aktiviert.

AutoId-Status	OPC UA-Status	AutoId-Text	Fehlerbeschreibung
19	good	RF_COMMUNICATION_ERROR	Allgemeiner Funkprotokoll-Fehler
20	good	DEVICE_FAULT	Fehler bei der Spannungsversorgung Die Versorgungsspannung ist dem unteren Grenzwert sehr nahe.
20	good	DEVICE_FAULT	Antennenfehler • Die Antenne oder das Antennenkabel ist defekt. • Fehler in der Verbindung zum Reader; Reader antwortet nicht (bei PROFIBUS-Betrieb). – Kabel zwischen Kommunikationsmodul und Reader ist falsch verdrahtet oder Kabelbruch – 24 V-Versorgungsspannung ist nicht angeschlossen oder abgeschaltet bzw. kurzzeitig ausgefallen – Automatische Sicherung auf dem Kommunikationsmodul hat angesprochen – Hardware defekt – Anderer Reader ist in der Nähe und ist aktiv geschaltet – Eine reflektierende Metallfläche ist in der Nähe und stört das Antennenfeld – nach der Fehlerbehebung "init_run" durchführen
--	--	--	Die ausgewählte Antenne ist nicht aktiviert.
--	OpcUa_BadInvalidState	--	Dieser Befehl ist in diesem Status nicht erlaubt, bzw. wird nicht unterstützt. Mögliche Ursache: • "INIT" wurde verkettet. • Befehlswiederholung wurde ohne "Presence-Mode" gestartet.
--	OpcUa_BadOutOfRange / OpcUa_BadConfigurationError	--	Es wurden keine oder fehlerhafte Konfigurationsdaten/Parameter übertragen. Mögliche Ursache: • Sie greifen auf eine nicht projektierte Lesestelle zu.
--	BadInvalidArgument	--	Ein Parameter fehlt.
--	BadInvalidArgument	--	Der Parameter hat ein ungültiges Format.
--	BadInvalidArgument	--	Der Parameter-Typ ist ungültig.
--	BadInvalidArgument	--	Unbekannter Parameter.
--	Bad	--	Der Befehl bzw. das Telegramm hat ein ungültiges Format.

Instandhalten und Warten

9

9.1 Diagnose

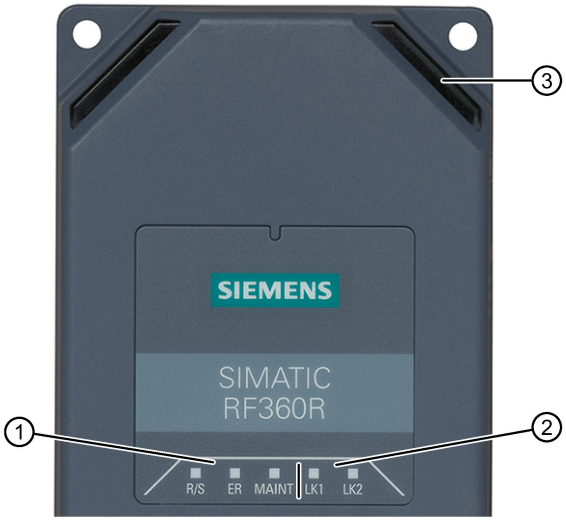
Für die Reader stehen Ihnen folgende Diagnosemöglichkeiten zur Verfügung:

- über die LED-Anzeigen der Reader
- über SNMP
- über das WBM
- über das TIA Portal (STEP 7 Basic / Professional)
- über XML
- über OPC UA

Im Folgenden werden diese alternativen Vorgehensweisen beschrieben.

9.1.1 Diagnose über die LED-Anzeige

Im folgenden Bild sind die Leuchtdioden des RF360R detailliert dargestellt.



① Status-LED-Anzeige

- RUN/STOP (R/S) — Zeigt an, ob der Reader betriebsbereit ist.
- ERROR (ER) — Zeigt an, ob ein Fehler vorliegt.
- MAINTENANCE (MAINT) — Zeigt an, ob der Reader gewartet werden muss.

② PROFINET-/Ethernet-LED-Anzeige

- LINK P1 (LK1) — Zeigt an, dass ein Link über die Ethernet-Schnittstelle "1" anliegt.
- LINK P2 (LK1) — Zeigt an, dass ein Link über die Ethernet-Schnittstelle "2" anliegt.

③ Reader-LED-Anzeige

- Zeigt an, ob sich ein oder mehrere Transponder im Antennenfeld befinden.
- Zeigt an, ob eine Kommunikation zum Reader stattfindet und ob ein Reader-Fehler vorliegt.
- Zeit im Modus "Einrichten" an, wie gut die Kommunikationsqualität zwischen Reader und Transponder ist.

Bild 9-1 LED-Anzeigen des Readers

Status-LED-Anzeige (inkl. PROFINET-/Ethernet-LEDs)

Der Reader-Status wird durch die LEDs "R/S", "ER" und "MAINT" angezeigt. Die LEDs können die Farben Grün, Rot oder Gelb und die Zustände aus, an, blinkt annehmen:

Tabelle 9- 1 Anzeige des Reader-Status über die Status-LED-Anzeige

R/S	ER	MAINT	Bedeutung
☐	☐	☐	Der Reader ist ausgeschaltet.
			• LED-Test während der Reader sich im Hochlauf befindet. • Der Reader wird manuell auf die Werkseinstellungen zurückgesetzt. • Ein angeschlossenes Kabel ist defekt.
	☐	☐	• Es findet kein Datenaustausch zwischen Reader und Anwenderapplikation statt. Der Reader hat noch keinen Anwenderbefehl erhalten. • Die Verbindung zur Anwenderapplikation ist abgebrochen.
	--	--	Ein Datenaustausch zwischen Reader und Anwenderapplikation findet statt. Der Reader hat einen Anwenderbefehl erhalten und ausgeführt.
		--	Die Ethernet-Verbindung wurde getrennt.
--	--		Ein Firmware-Update wird durchgeführt.
--	--		Die Spannung am Reader ist zu niedrig.
			• Der Blinktest zur Reader-Identifizierung wird durchgeführt. Gleichzeitig blinken auch die LEDs der Reader- und PROFINET-/Ethernet-LED-Anzeige. • Die Firmware ist defekt.
--		--	Es liegt ein Fehler vor. Ggf. wurde ein PROFINET-Alarm gemeldet. Die LED blinkt solange der Fehler/Alarm ansteht, mindestens jedoch für 3 Sekunden. Weitere Informationen zu den Fehlermeldungen finden Sie im Kapitel "Fehlermeldungen (Seite 89)".

Die Zustände der PROFINET-/Ethernet-Verbindungen werden durch die LEDs "LK1" für die Schnittstelle "X1 P1R" und "LK2" für die Schnittstelle "X1 P2R" angezeigt. Die LEDs können die Farben Grün, Rot oder Gelb und die Zustände aus, an, blinkt annehmen:

Tabelle 9- 2 Anzeige der PROFINET-/Ethernet-Zustände über die PROFINET-/Ethernet-LED-Anzeige

LK*	Bedeutung
☐	• Es liegt keine Verbindung vor. • Es wurde kein Verbindungskabel angeschlossen.
	Der Blinktest zur Reader-Identifizierung wird durchgeführt. Gleichzeitig blinken auch die LEDs der Betriebs- und Status-LED-Anzeige.
	• LED-Test während der Reader sich im Hochlauf befindet. • Es liegt eine Verbindung vor.

Reader-LED-Anzeige

Die Betriebszustände des Readers werden durch zwei LEDs angezeigt. Die LEDs können die Farben Weiß, Grün, Rot, Gelb oder Blau und die Zustände aus, an, blinkt annehmen:

Tabelle 9- 3 Anzeige der Betriebszustände über die Reader-LED-Anzeige

LEDs	Bedeutung
	Der Reader ist ausgeschaltet.
	Der Reader ist eingeschaltet und sucht nach Transpondern. Der Reader ist in dem "Einrichten"-Modus, im Zustand "Transponder suchen", hat noch keinen "RESET"-Befehl erhalten und ist nicht bereit. Ausführliche Informationen zum Modus "Einrichten", finden Sie im Kapitel "Einrichthilfe der Reader der zweiten Generation" des Systemhandbuchs "SIMATIC RF300 (https://support.industry.siemens.com/cs/ww/de/ps/15003/man)".
	Ein Transponder befindet sich im Antennenfeld. Der Reader ist in dem "Einrichten"-Modus, im Zustand "Qualität anzeigen", hat noch keinen "RESET"-Befehl erhalten und ist nicht bereit. Abhängig von der Signalstärke flackert die LED oder leuchtet durchgehend.
	Der Reader hat einen "RESET"-Befehl erhalten.
	Der Reader ist eingeschaltet, die Antenne ist ausgeschaltet.
	• Betriebsart "mit Anwesenheit": Transponder anwesend • Betriebsart "ohne Anwesenheit": Transponder anwesend und Befehl wird aktuell abgearbeitet
	Ein Fehler liegt vor. Die Blinkanzahl gibt Auskunft über den aktuell vorliegenden Fehler. Weitere Informationen zu den Fehlermeldungen finden Sie im Kapitel "Fehlermeldungen (Seite 89)".

9.1.2 Diagnose über SNMP

Über SNMP stehen Ihnen umfassende Diagnosemöglichkeiten der Netzwerkfunktionen des Readers zur Verfügung. Folgende Diagnosemöglichkeiten (MIBs) werden von den Readern unterstützt:

- RFC 2863: IF-MIB
- RFC 3418: SNMPv2-MIB
- RFC 4022: TCP-MIB
- RFC 4113: UDP-MIB

- RFC 4292: IP-MIB
- SIEMENS:
  - AUTOMATION-SN-SYSTEM-MIB
  - AUTOMATION-SYSTEM-MIB
  - IEC-62439-2-MIB
  - IEEE 802.1AB 2005 LLDP-MIB
  - LLDP-EXT-DOT1-MIB
  - LLDP-EXT-DOT3-MIB
  - LLDP-EXT-PNO-MIB

Die zu den Readern passenden MIB-Dateien finden Sie auf den Seiten des Siemens Industry Online Supports (https://support.industry.siemens.com/cs/ww/de/view/67637278), Informationen zu den MIB-Dateien finden Sie unter "PROFINET-Nutzerorganisation (https://www.profibus.com/download/profinet-specification/)".

Die Reader unterstützen das SNMPv3- und SNMPv1-Protokoll. SNMPv1 ist ab Werk aktiviert, jedoch als unsicher eingestuft. Deaktivieren Sie SNMP, wenn dieses nicht benötigt wird oder verwenden Sie SNMPv3. Informationen zu SNMP finden Sie im Kapitel "Der Menüpunkt "Einstellungen - Kommunikation" (Seite 53)".
Ausführliche Informationen zur Anwendung von SNMP und insbesondere auch zur Struktur der automation.mib finden Sie im Diagnosehandbuch "Netzwerkmanagement Diagnose und Projektierung mit SNMP (https://support.industry.siemens.com/cs/ww/de/view/103949062)".

9.1.3 Diagnose über das WBM

Über das WBM stehen Ihnen umfangreiche Diagnosemöglichkeiten zur Verfügung.

Im "Logbuch" werden alle aufgetretenen Diagnosemeldungen des Readers angezeigt. Das "Service-Logbuch" unterstützt SIEMENS-Fachpersonal bei der Fehleranalyse. Über das "Syslog-Logbuch" können Sie die Syslog-Melungen und mit Hilfe der "Hardware-Diagnose" können Sie die "Status-Parameter" des Readers und der Transponder auslesen.

Weitere Informationen zum "Logbuch" finden Sie im Kapitel "Der Menüpunkt "Diagnose - Logbuch" (Seite 68)".

9.1.4 Diagnose über das TIA Portal (STEP 7 Basic / Professional)

Dieses Kapitel richtet sich ausschließlich an S7-Anwender.

Voraussetzungen

STEP 7 Basic / Professional ist installiert, gestartet und ein Projekt ist geöffnet. Der Reader ist über Industrial Ethernet oder PROFINET mit der Steuerung bzw. dem PC verbunden und hochgelaufen.

Vorgehensweise

Diagnoseinformationen des Readers auslesen

Gehen Sie folgendermaßen vor, um Diagnoseinformationen des Readers mit Hilfe von STEP 7 Basic / Professional (TIA Portal) auszulesen:

1. Wechseln Sie in die Netzsicht.
2. Klicken Sie mit der rechten Maustaste auf den gewünschten Reader und klicken Sie im Kontextmenü auf den Eintrag "Online & Diagnose".
3. Wählen Sie die Parametergruppe "Diagnose".

   Im Diagnose-Fenster haben Sie folgende Optionen zur Diagnose des Readers:

   - Unter dem Eintrag "Allgemein" werden allgemein Informationen wie z. B. die Bezeichnung, Artikelnummer oder Firmware-Version des Readers angezeigt.
   - Unter dem Eintrag "Diagnosestatus" werden aktuelle Status-Informationen des Readers angezeigt.
   - Unter dem Eintrag "Kanaldiagnose" werden aktuelle Diagnose-Informationen der Reader-Schnittstelle angezeigt.
   - Unter dem Eintrag "PROFINET-Schnittstelle" werden Status-Informationen und weitere Informationen der PROFINET-Schnittstelle angezeigt.

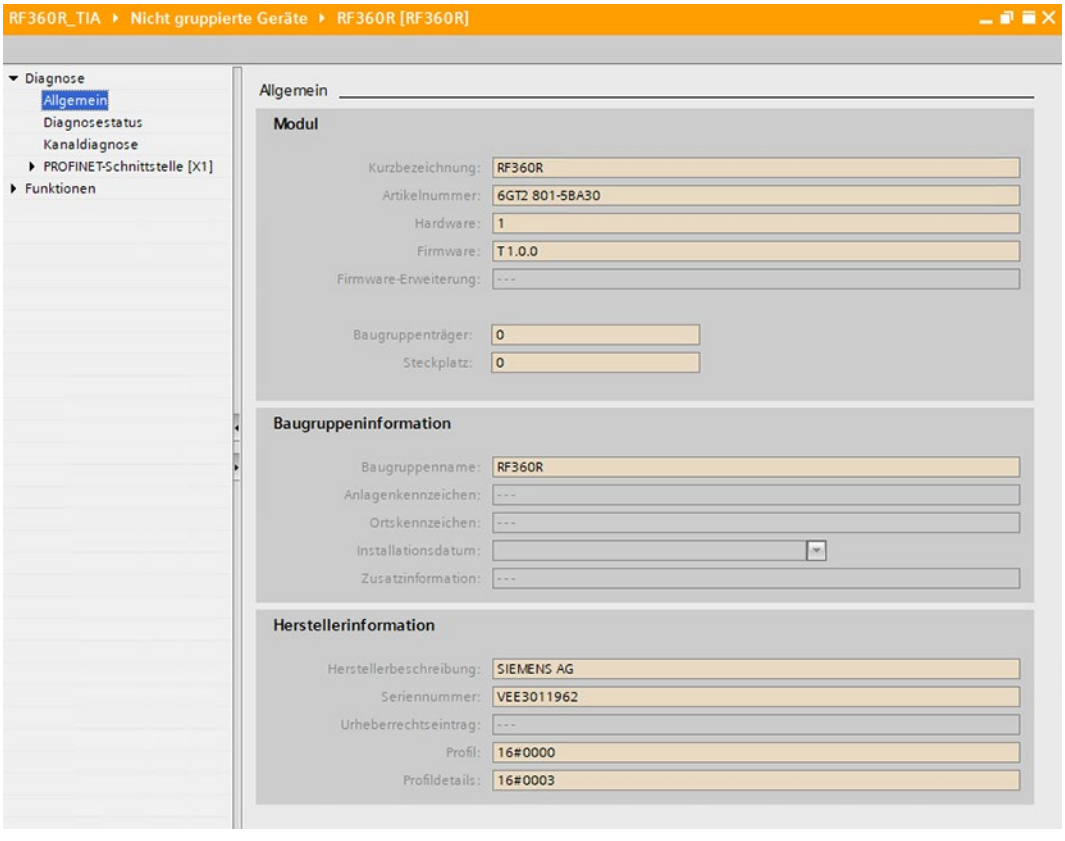


Bild 9-2 Anzeige der Diagnoseinformationen des Readers

Diagnose mit aktivierten Diagnosealarmmeldungen

Bei aktivierten Diagnosealarmmeldungen werden die Fehlermeldungen im Klartext im CPU-Diagnosepuffer abgelegt. Diese Meldungen können Sie mit den entsprechenden Funktionsbausteinen weiterverarbeiten, z. B. so, dass diese an ein HMI weitergeleitet werden.

Bei aktivierten Diagnosealarmmeldungen werden in der Online-Gerätesicht Fehlerzustände durch einen rotes Werkzeugsymbol angezeigt. Klicken Sie mit der rechten Maustaste auf die betreffende Baugruppe und klicken Sie im Kontextmenü auf den Eintrag "Online & Diagnose", um unterhalb des Eintrags "Kanaldiagnose" den Fehlertext angezeigt zu bekommen.

Diagnose über das Technologieobjekt "TO_Ident"

Alternativ können Sie die Reader auch mit Hilfe des Technologieobjekts "TO_Ident" diagnostizieren. Ausführliche Informationen dazu finden Sie in der Hilfe des TIA Portals.

9.1.5 Diagnose über XML

Dieses Kapitel richtet sich ausschließlich an XML-Anwender.

Über XML stehen Ihnen umfassende Diagnosemöglichkeiten zur Verfügung. Ausführliche Informationen zu den Diagnosemöglichkeiten finden Sie im Handbuch "XML-Programmierung für SIMATIC Ident (https://support.industry.siemens.com/cs/ww/de/view/109781631)".

9.1.6 Diagnose über OPC UA

Über OPC UA stehen Ihnen umfassende Diagnosemöglichkeiten zur Verfügung. Die verschiedenen Diagnosemöglichkeiten werden nachfolgend beschrieben.

Mithilfe der OPC UA-Variablen und -Events können Sie Diagnosemeldungen auslesen und gezielt abfragen. Ausführliche Informationen zu den Diagnosemöglichkeiten finden Sie im Handbuch "OPC UA für SIMATIC Ident (https://support.industry.siemens.com/cs/ww/de/ps/14971/man)".

9.1.7 Diagnose über Studio 5000 Logix Designer

Dieses Kapitel richtet sich ausschließlich an Anwender von Rockwell-Steuerungen.

Informationen zur Diagnose mit Hilfe des Studio 5000 Logix Designer entnehmen Sie bitte dem Studio 5000 Logix Designer-Handbuch.

9.1.8 Parametrierung der Diagnose

Mithilfe von STEP 7 Basic / Professional können Sie auswählen, welche Diagnosealarme/-meldungen Ihnen angezeigt werden sollen. Um die Diagnosealarme/-meldungen zu aktivierten/deaktivieren, gehen Sie wie folgt vor:

"Gerätesicht > Geräteübersicht > Reader-Modul > Allgemein > Baugruppenparameter > Diagnosemeldungen"

Diagnosemeldungen

Folgende Einstellungen der Diagnosemeldungen stehen Ihnen zur Verfügung:

- **Keine**

  Es werden keine weiteren Diagnosedaten gemeldet.

- **Hard Errors**

  Schwerwiegende Hardware-Fehler werden über die S7-Diagnose gemeldet. Es werden bei folgenden Ereignissen erweiterte Diagnosemeldungen generiert.

  - Hardware-Fehler (Speichertest)
  - Firmware-Fehler (Checksumme)
  - Verbindungsunterbrechung
  - Fehler bei der Spannungsversorgung
  - Kurzschlussfehler/Unterbrechung, soweit von Hardware unterstützt
  - Firmware-Update (Meldung bei Start/Ende)

- **Hard / Soft Errors**

  Zusätzlich zu den Hard Errors werden hier auch Fehler gemeldet, die während der Befehlsbearbeitung auftreten.

  Beachten Sie, dass Meldungen, die durch die Befehlsbearbeitung ausgelöst werden, automatisch nach 3 Sekunden zurückgenommen werden.

Unterscheidung der Diagnosealarmmeldungen

Bei den Diagnosealarmmeldungen wird zwischen kommendem und gehendem Diagnosealarm unterschieden.

- **Kommender Diagnosealarm**

  Ein Ereignis tritt ein und löst einen Alarm aus.

- **Gehender Diagnosealarm**

  Das Ereignis steht nicht mehr an. Bei Ereignissen, die nur einen Augenblick anstehen - z. B. Soft Errors -, wird die Rücknahme um 3 Sekunden verzögert.

Weitere Informationen

Detaillierte Informationen zur Diagnose am PROFINET IO sind im Handbuch "SIMATIC PROFINET Systembeschreibung (https://support.industry.siemens.com/cs/ww/de/view/19292127)".

9.2 Firmware-Update

Um die Firmware des Readers upzudaten, stehen Ihnen folgende Möglichkeiten zur Verfügung:

- über das WBM
- über das TIA Portal (ab STEP 7 Basic / Professional V17)

Im Folgenden werden diese alternativen Vorgehensweisen beschrieben.

9.2.1 Firmware-Update über das WBM durchführen

Voraussetzungen

- Der Reader ist über Industrial Ethernet oder PROFINET mit dem PC verbunden.
- Der Reader wurde vom laufenden Betrieb getrennt.
- Alle Anwenderapplikationen sind beendet.
- Die erforderliche Update-Datei (*.sfw) ist lokal gespeichert.

Vorgehensweise

Gehen Sie folgendermaßen vor, um das Firmware-Update mit Hilfe des WBM durchzuführen:

1. Starten Sie Ihren Webbrowser.
2. Geben Sie die IP-Adresse des Readers in das Adressfeld Ihres Browsers ein.
3. Melden Sie sich ggf. am WBM an.

   Beachten Sie, dass Sie als "Benutzer" ein Firmware-Update nur durchführen können, wenn sich der Reader im Zustand "Bereit" befindet.
4. Klicken Sie auf den Menüpunkt "System - Geräteeinstellungen".
5. Klicken Sie im Bereich "Firmware-Update" auf das Symbol "Firmware-Datei auswählen" .
6. Wählen Sie die Update-Datei (*.sfw) aus.
7. Klicken Sie auf die Schaltfläche "Öffnen".
8. Klicken Sie auf die Schaltfläche "Aktualisieren".

Ergebnis: Die Firmware wird aktualisiert. Der Update-Prozess wird Ihnen in der Hinweisleiste angezeigt.

Nachdem das Update abgeschlossen ist, wird der Reader neu gestartet. Der Reader ist betriebsbereit, wenn die "RUN"-LED grün leuchtet/blinkt. Beachten Sie, dass nach einem Firmware-Update der Hochlaufprozess ca. 1 Minute dauert.

Nach dem Neustart ist die aktualisierte Firmware aktiv.

9.2.2 Firmware-Update über TIA Portal (STEP 7 Basic / Professional) durchführen

Dieses Kapitel richtet sich ausschließlich an S7-Anwender.

Voraussetzungen

- Der Reader ist über Industrial Ethernet oder PROFINET mit der Steuerung bzw. dem PC verbunden.
- Die IP-Adresse des Readers ist in den Baugruppenparametern hinterlegt.
- Der Reader ist vom laufenden Betrieb getrennt.

  Beachten Sie, dass die Durchführung des Updates bei laufender Applikation sowohl das Update als auch die Befehlsabarbeitung verlangsamen kann.
- Die erforderlichen Update-Dateien wurden lokal gespeichert.

Vorgehensweise

Gehen Sie folgendermaßen vor, um ein Firmware-Update des Readers über STEP 7 Basic / Professional (TIA Portal) durchzuführen:

1. Starten Sie das TIA Portal.
2. Öffnen Sie Ihr bestehendes Projekt und wechseln Sie in die Projektansicht.
3. Wechseln Sie in die Netzsicht.
4. Klicken Sie mit der rechten Maustaste auf den gewünschten Reader und klicken Sie im Kontextmenü auf den Eintrag "Online & Diagnose".
5. Wählen Sie den Eintrag "Funktionen > Firmware-Update via Web Interface".
6. Klicken Sie auf die Schaltfläche "Starte Aktualisierung der Firmware".

   Reaktion: Das WBM des Readers wird in Ihrem Webbrowser geöffnet.
7. Setzen Sie das Firmware-Update fort, wie im Kapitel "Firmware-Update über das WBM durchführen (Seite 109)" beschrieben.

9.3 Werkseinstellungen

Sie können jederzeit die Konfiguration der Reader auf die Werkseinstellungen zurücksetzen. Um die Werkseinstellungen zurückzusetzen, stehen ihnen folgende Optionen zur Verfügung:

- über das WBM
- über SINEC PNI
- über XML
- hardware-seitig über die Spannungsversorgungsschnittstelle

Im Folgenden werden diese alternativen Vorgehensweisen beschrieben.

9.3.1 Werkseinstellungen über das WBM zurücksetzen

Voraussetzung

Dar Reader ist über Industrial Ethernet oder PROFINET mit dem PC verbunden.

Vorgehensweise

Gehen Sie folgendermaßen vor, um alle Einstellungen mit Hilfe des WBM auf die Werkseinstellungen zurückzusetzen:

1. Starten Sie Ihren Webbrowser.
2. Geben Sie die IP-Adresse des Readers in das Adressfeld Ihres Browsers ein.
3. Melden Sie sich ggf. am WBM an.
4. Öffnen Sie den Menüpunkt "System".
5. Klicken Sie im Bereich "Zurücksetzen" auf die Schaltfläche "Zurücksetzen".

Ergebnis: Der Reader wird auf die ursprüngliche Werkseinstellung zurückgesetzt. Der Wiederherstellungsprozess wird Ihnen in der Hinweisleiste angezeigt.

Beachten Sie, dass durch das Zurücksetzen auf die Werkseinstellungen auch die IP-Adresse des Readers zurückgesetzt wird. In den Werkseinstellungen wird die IP-Adresse über einen DHCP-Server bezogen. Sie erkennen nur anhand der "R/S"-LED, wann das Zurücksetzen abgeschlossen ist. Nach dem Zurücksetzen wird der Reader neu gestartet. Der Reader ist betriebsbereit, wenn die "R/S"-LED grün leuchtet/blinkt.

Nach dem Neustart des Readers müssen Sie dem Reader ggf. eine neue IP-Adresse bzw. einen neuen Gerätenamen zuweisen.

9.3.2 Werkseinstellungen über SINEC PNI zurücksetzen

Voraussetzung

Der Reader ist über Industrial Ethernet oder PROFINET mit dem PC verbunden.

Vorgehensweise

Gehen Sie folgendermaßen vor, um alle Einstellungen mit Hilfe von SINEC PNI auf die Werkseinstellungen zurückzusetzen:

1. Starten Sie SINEC PNI.
2. Klicken Sie in der Funktionsleiste auf die Schaltfläche "Netzwerk-Scan starten".

   Reaktion: Das Netzwerk wird nach angeschlossenen Geräten durchsucht und alle erkannten Geräte werden in der Geräteliste angezeigt.
3. Markieren Sie den gewünschten Reader in der Geräteliste.
4. Klicken Sie in der Funktionsleiste in der Klappliste "Geräteverwaltung" auf den Eintrag "Gerät zurücksetzen".

Ergebnis: Der Reader wird auf die ursprüngliche Werkseinstellung zurückgesetzt.

Beachten Sie, dass durch das Zurücksetzen auf die Werkseinstellungen auch die IP-Adresse des Readers zurückgesetzt wird. In den Werkseinstellungen wird die IP-Adresse über einen DHCP-Server bezogen. Sie erkennen nur anhand der "R/S"-LED, wann das Zurücksetzen abgeschlossen ist. Nach dem Zurücksetzen wird der Reader neu gestartet. Der Reader ist betriebsbereit, wenn die "R/S"-LED grün leuchtet/blinkt.

Nach dem Neustart des Readers müssen Sie dem Reader ggf. eine neue IP-Adresse bzw. einen neuen Gerätenamen zuweisen.

9.3.3 Werkseinstellungen über XML zurücksetzen

Mit Hilfe der XML-Schnittstelle und dem Befehl "resetDevice" können Sie alle Einstellungen auf die Werkseinstellungen zurückzusetzen.

Beachten Sie, dass durch das Zurücksetzen auf die Werkseinstellungen auch die IP-Adresse des Readers zurückgesetzt wird. In den Werkseinstellungen wird die IP-Adresse über einen DHCP-Server bezogen. Sie erkennen nur anhand der "R/S"-LED, wann das Zurücksetzen abgeschlossen ist. Nach dem Zurücksetzen wird der Reader neu gestartet. Der Reader ist betriebsbereit, wenn die "R/S"-LED grün leuchtet/blinkt.

Nach dem Neustart des Readers müssen Sie dem Reader ggf. eine neue IP-Adresse bzw. einen neuen Gerätenamen zuweisen.

9.3.4 Werkseinstellungen hardware-seitig zurücksetzen

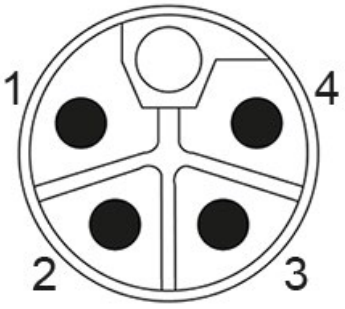
Voraussetzung

Der Reader wurde von der Spannungsversorgung getrennt.

Vorgehensweise

Gehen Sie folgendermaßen vor, um alle Einstellungen mit Hilfe der Spannungsversorgungsschnittstelle auf die Werkseinstellungen zurückzusetzen:

1. Stellen Sie ein Spannungsversorgungskabel mit offenen Kabelenden her, indem Sie die Kabelenden/Aderenden (spannungsversorgungsseitig) abisolieren.
2. Schließen Sie das Spannungsversorgungskabel an dem Reader an.
3. Verbinden Sie die Adernenden der Pins 3 (DC 0 V) und 4 (Reset To Factory) mit Hilfe einer Lüsterklemme und verbinden Sie diese mit DC 0 V der Spannungsversorgung.

Pin	Belegung	Ansicht der Spannungsversorgungsschnittstelle
1	Spannung (DC 24 V, braun)	
2	Nicht belegt (weiß)	
3	Funktionserde/Schirm (DC 0 V, blau)	
4	Reset to Factory (schwarz)	

4. Verbinden Sie den Pin 1 (DC 24 V) mit dem Pluspol der Spannungsversorgung.

   Reaktion: Die Reader-LED-Anzeige, sowie die Status-LED-Anzeigen (R/S, ER, MAINT) leuchten durchgängig.
5. Warten Sie ca. 60 Sekunden und entfernen Sie dann das Spannungsversorgungskabel mit den offenen Kabelenden.
6. Schließen Sie den Reader erneut, über ein reguläres Spannungsversorgungskabel, an der Spannungsversorgung an.

Ergebnis: Der Reader wurde auf die ursprüngliche Werkseinstellung zurückgesetzt.

Beachten Sie, dass durch das Zurücksetzen auf die Werkseinstellungen auch die IP-Adresse des Readers zurückgesetzt wird. In den Werkseinstellungen wird die IP-Adresse über einen DHCP-Server bezogen.

Nach dem Neustart des Readers müssen Sie dem Reader ggf. eine neue IP-Adresse bzw. einen neuen Gerätenamen zuweisen.

9.4 Baugruppentausch

ACHTUNG
Konfigurierung sichern Beachten Sie, dass Sie vor einem Baugruppentausch die auf dem Reader hinterlegte Konfiguration sichern, um diese nach dem Baugruppentausch auf den neu angeschlossenen Reader übertragen zu können.

ACHTUNG
Konfiguration laden Beachten Sie, dass Sie mit Hilfe der Konfigurationsdatei keine Benutzerprofile und Passwörter auf andere Reader übertragen können. Nach dem Laden der Konfigurationsdatei in einen neuen Reader müssen Sie ggf. die Authentifizierung aktivieren und neue Benutzerprofile und Passwörter anlegen.

Um die aktuelle Konfiguration des Readers zu sichern und nach dem Baugruppentausch auf den neu angeschlossenen Reader wiederherzustellen, stehen Ihnen folgende Optionen zur Verfügung:

- mit Hilfe des TIA Portal (ab STEP 7 Basic / Professional V17) in einem STEP 7-Projekt
- mit Hilfe des WBM auf Ihrem PC

Im Folgenden werden diese alternativen Vorgehensweisen beschrieben.

9.4.1 Konfiguration sichern

Tabelle 9- 4 Eigenschaften und Voraussetzungen der Sicherungsoptionen

Sicherungsoptionen	Eigenschaften
Sicherung in der Steuerung	• Baugruppentausch ohne PG möglich • Automatischer Ablauf möglich ⇒ Die Programmierung des automatischen Ablaufs muss von Ihnen durchgeführt werden.
Sicherung im STEP 7-Projekt	• Download zum Reader nur manuell über STEP 7 möglich • Kein Verwaltungsaufwand von Konfigurationsständen ⇒ Es wird immer nur der letzte Stand gespeichert (keine Speicherung alter Versionsstände). ⇒ Die Aktualisierung des Konfigurationstands im Projekt muss von Ihnen manuell angestoßen werden.
Sicherung über das WBM (als *.xml-Datei)	• Konfigurationsdaten werden unabhängig von Projekt und Steuerung gespeichert ⇒ Der Download zum Reader ist manuell über das WBM per Anwenderapplikation möglich. • Möglichkeit des Kopierens für weitere Reader des gleichen Typs • Ältere Konfigurationsstände können gespeichert werden (Versionierung) ⇒ Die Aktualisierung und Versionierung der Konfigurationsstände muss von Ihnen manuell angestoßen und verwaltet werden.

Sicherung in der Steuerung

Mit Hilfe der Bausteine "Config_Upload" und "Config_Download" können Sie über das Steuerungsprogramm die Konfiguration der Reader auslesen ("Config_Upload") oder schreiben ("Config_Download"). Da die Konfiguration dauerhaft gespeichert wird, müssen Sie dafür einen Datenbaustein / eine Variable in der Steuerung reservieren.

Zur Überprüfung der richtigen Konfiguration können Sie mit dem Reader-Status die Versionskennung (Config-ID) vom Reader auslesen und diese mit der Config-ID vergleichen, welche früher in der Steuerung mit dem Befehl "Config_Upload" im Datenbaustein / in der Variablen hinterlegt wurde.

Weitere Informationen zur Programmierung der Bausteine und dem Aufbau der Konfigurationsdaten finden Sie im Kapitel "Config_Upload/-_Download" im Handbuch "Ident-Profil und Ident-Bausteine, Standardfunktionen für Ident-Systeme (https://support.industry.siemens.com/cs/ww/de/view/109793329)".

Sicherung in einem STEP 7-Projekt

Über die Gerätesicht des TIA Portals gelangen Sie zu dem Register "Eigenschaften" des Readers. Bei der Projektierung über HSP können Sie in dem Eintrag "Konfigurationsmanagement" die Konfiguration des Readers in Ihrem Projekt speichern und diese auch wieder in den Reader laden.

Voraussetzung

- Im Eintrag "PROFINET-Schnittstelle [X1]" ist die korrekte IP-Adresse des Readers eingetragen.
- Benutzername und dazugehöriges Passwort sind korrekt eingetragen.
- Der eingetragene Benutzer hat die nötigen Rechte, um den Down-/Upload durchzuführen (siehe Kapitel "Der Menüpunkt "Benutzerverwaltung" (Seite 74)").

Hinweis

Benutzername und Passwort nur bei aktiver Authentifizierung nötig

Die Textfelder "Benutzername" und "Passwort" müssen nur ausgefüllt werden, wenn die Authentifizierung des WBM aktiviert ist.

Nach dem Up-/Download wird Ihnen über die Statusleiste angezeigt, ob der Vorgang erfolgreich durchgeführt wurde.

Sicherung über das WBM

Im WBM befinden sich auf der oberen Funktionsleiste zwei Schaltflächen zum Laden und Speichern von Konfigurationen. Mit Hilfe dieser Schaltflächen können Sie Konfigurationen sichern, neu laden und auf andere Reader übertragen. Weitere Informationen zum Speichern und Laden der Konfiguration auf bzw. von dem PC finden Sie im Kapitel "Das WBM (Seite 40)".

9.4.2 Baugruppentausch durchführen

Voraussetzungen

Der Reader RF360R ist montiert. Ein neuer Reader RF360R liegt bereit.

Vor dem Baugruppentausch

⚠WARNUNG

Lesen Sie das Handbuch der verwendeten SIMATIC-Steuerung

Lesen Sie vor der Montage, dem Anschließen und der Inbetriebnahme die entsprechenden Abschnitte in dem Handbuch der verwendeten SIMATIC-Steuerung. Gehen Sie bei der Montage und dem Anschließen entsprechend den darin enthaltenen Beschreibungen vor.

ACHTUNG

Konfigurierung sichern

Beachten Sie, dass Sie vor einem Baugruppentausch die auf dem Reader hinterlegte Konfiguration sichern, um diese nach dem Baugruppentausch auf den neu angeschlossenen Reader übertragen zu können.

ACHTUNG

Montage/Demontage im spannungslosen Zustand

Verdrahten Sie die SIMATIC-Steuerung und die anzuschaltenden Reader nur im spannungslosen Zustand. Stellen Sie sicher, dass während der Montage/Demontage der Geräte die Spannungsversorgung ausgeschaltet ist.

Vorgehensweise

Gehen Sie folgendermaßen vor, um einen Reader auszutauschen (Ethernet-/PROFINET-Anbindung):

1. Stellen Sie sicher, dass der Reader von der Spannungsversorgung getrennt ist.
2. Ziehen Sie die Kabel vom Reader ab.
3. Demontieren Sie den Reader.
4. Montieren Sie den neuen Reader.
5. Verbinden Sie den Reader mit Hilfe des vorhandenen Ethernet-Kabels mit dem PC bzw. mit der SIMATIC-Steuerung.
6. Verbinden Sie den Reader mit Hilfe des Anschlusskabels an der Spannungsversorgung.

   Warten Sie, bis der Reader hochgelaufen und betriebsbereit ist ("RUN"-LED leuchtet/blinkt grün).

7. Weisen Sie dem Reader ggf. eine eindeutige IP-Adresse und einen eindeutigen Gerätenamen zu.
8. Laden Sie ggf. die Konfiguration auf den Reader.
9. Parametrieren Sie die Benutzerverwaltung gemäß den Erfordernissen ihrer Applikation.

Baugruppentausch mit automatischer Gerätenamevergabe

Bei einem Baugruppentausch haben Sie die Möglichkeit die Gerätenamen automatisch anhand der projektierten PROFINET-Topologie zu vergeben. Diese Funktion ist ausschließlich bei einem Gerätetausch möglich.

Voraussetzung

- Die PROFINET-Topologie wurde projektiert.
- In den PROFINET-Einstellungen der Baugruppe ist die Option "Gerätetausch ohne Wechselmedium" aktiviert.
- Der neue Reader ist im Zustand der Werkseinstellung, d. h. es wurde kein Gerätename und keine IP-Adresse vergeben.

Anhang

A

A.1 Verschlüsselungsmethoden (Ciphers)

In den folgenden Tabellen sind die Verschlüsselungsmethoden (Ciphers) aufgeführt, die das Gerät verwendet.

SSL

Tabelle A- 1 Unterstützte Verschlüsselungsmethoden (Cipher-Suites) für HTTPS-WBM-Server

Kategorie	Verfahren	Wert (hex)	Per Default aktiviert
Verschlüsselungs-Suite	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	0xC02F	✓
Verschlüsselungs-Suite	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	0xC030	✓
Verschlüsselungs-Suite	TLS_AES_256_GCM_SHA384	0x1302	✓
Verschlüsselungs-Suite	TLS_CHACHA20_POLY1305_SHA256	0x1303	✓
Verschlüsselungs-Suite	TLS_AES_128_GCM_SHA256	0x1301	✓
Verschlüsselungs-Suite	TLS_AES_128_CCM_SHA256	0x1304	✓
Protokollversion	TLSv1.2	--	✓
Protokollversion	TLSv1.3	--	✓

SNMP

Tabelle A- 2 Unterstützte Verschlüsselungsmethoden (Cipher-Suites) für SNMP-Server

Kategorie	Verfahren	Wert (hex)	Per Default aktiviert
Authentifizierung	HMAC-MD5-96	--	--
Authentifizierung	HMAC-SHA-96	--	--
Verschlüsselung	aes128-cbc	--	--
Verschlüsselung	des-cbc	--	--

OPC UA

Tabelle A- 3 Unterstützte Verschlüsselungsmethoden (Cipher-Suites) für OPC UA-Server

Kategorie	Verfahren	Wert (hex)	Per Default aktiviert
Sicherheitsrichtlinie	None	--	--
Sicherheitsrichtlinie	Basic128Rsa15	--	--
Sicherheitsrichtlinie	Basic256	--	--
Sicherheitsrichtlinie	Basic256Sha256	--	--
Sicherheitsrichtlinie	Aes128-Sha256_RsaOaep	--	--
Sicherheitsrichtlinie	Aes256Sha256RsaPss	--	✓
Transport-Profil	UA-TCP	--	✓

Syslog-Meldungen

B

B.1 Aufbau der Syslog-Meldungen

Der Syslog-Server sammelt Log-Informationen der Geräte und informiert Sie über bestimmte Ereignisse. Die Syslog-Meldungen werden vom Syslog-Server über den eingestellten UDP-Port (Standard: 514) empfangen und gemäß RFC 5424 bzw. RFC 5426 ausgegeben.

Syslog-Meldungen protokollieren Informationen beim Zugriff auf das Gerät. Informationen können Statusinformationen wie z. B. die Herkunft der Meldung oder ein Zeitstempel sein. Das Syslog-Protokoll schreibt eine festgelegte Reihenfolge und Struktur der möglichen Parameter vor. Syslog-Meldungen sind gemäß RFC 5424 folgendermaßen aufgebaut:

Tabelle B- 1 Aufbau der Syslog-Meldungen

Parameter	Erläuterung
HEADER	
PRI	Innerhalb PRI steht codiert die Priorität der Syslog-Meldung, aufgeteilt in Severity (Schweregrad der Nachricht) und Facility (Herkunft der Nachricht).
VERSION	Versionsnummer der Syslog-Spezifikation.
TIMESTAMP	Das Gerät versendet den Zeitstempel im Format "2010-01-01T02:03:15.0003+02:00" als lokale Zeit.
HOSTNAME	Referenziert den Quell-Gerät mit seinem Namen oder der IP-Adresse. IPv4-Adresse nach RFC1035: Bytes in dezimaler Darstellung: XXX.XXX.XXX.XXX Bei fehlenden Angaben wird "-" ausgegeben.
APP-NAME	Gerät oder Anwendung, von dem die Meldung stammt. Dieser Parameter wird von dem Gerät nicht verwendet und es wird immer "-" ausgegeben.
PROCID	Die Prozess-ID dient z. B. bei der Analyse und Fehlersuche dazu, die einzelnen Prozesse eindeutig zu identifizieren. Dieser Parameter wird von dem Gerät nicht verwendet und es wird immer "-" ausgegeben.
MSGID	ID zur Identifizierung der Nachricht. Dieser Parameter wird von dem Gerät nicht verwendet und es wird immer "-" ausgegeben.
STRUCTURED-DATA	
timeQuality	Das strukturierte Datenelement "timeQuality" liefert Informationen zur Systemzeit. Der Parameter "tzKnown" gibt an, ob der Sender seine Zeitzone kennt (Wert "1" = bekannt; Wert "0" = unbekannt). Der Parameter "isSynced" gibt an, ob der Sender mit einer zuverlässigen externen Zeitquelle synchronisiert ist, z. B. über NTP (Wert "1" = synchronisiert; Wert "0" = nicht synchronisiert).
sysUpTime	Der Parameter "sysUpTime" ist eine Metainformation über die Meldung. Er gibt die Zeit (in Hundertstelsekunden) seit der letzten Neuinitialisierung des Netzwerkverwaltungsteils des Systems an.
MSG	
MESSAGE	Meldung als ASCII-String (Englisch)

Hinweis

Weiterführende Informationen

Weiterführende Informationen zu dem Aufbau der Syslog-Meldungen und über die Bedeutung der Parameter können Sie in den RFCs nachlesen:

https://tools.ietf.org/html/rfc5424

https://tools.ietf.org/html/rfc5426

B.2 Variablen in Syslog-Meldungen

Die Variablen werden im Kapitel "Syslog-Meldungen" im Feld "Meldungstext" mit geschweiften Klammern {variable} dargestellt.

Die ausgegebenen Meldungen können folgende Variablen enthalten:

Tabelle B- 2 Mögliche Variablen innerhalb der Syslog-Meldungen

Variable	Beschreibung	Format	Mögliche Werte oder Beispiel
{Ip address}	IPv4-Adresse nach RFC1035	%d.%d.%d.%d XXX.XXX.XXX.XXX	192.168.1.105
{Protocol}	Verwendetes Protokoll oder Dienst, der das Ereignis generiert hat.	%s	TCP | WBM | PNIO | PB | OPC | EIP
{User name}	Zeichenkette (ohne Leerzeichen), die den authentifizierten Benutzer anhand seines Namens identifiziert.	%s	<name>
{Action user name} oder {Destination user name}	Identifiziert den Benutzer anhand seines Namens. Dies ist nicht der authentifizierte Benutzer.	%s	<Vorname>.<Name>
{Role}	Symbolischer Name für die Gruppenrolle.	%s	Administrator | User | OPC UA
{Time second}	Sekundenanzahl	%d	44
{Max sessions}	Maximale Anzahl der Sitzungen	%d	10
{Url}	URL des Webservers, auf den zugegriffen wurde.	%s	/Engineering/Reset2Factory?r=0.6856445562508033
{Config detail}	Zeichenkette (mit Leerzeichen) für die Konfiguration.	%s	Power

B.3 Liste der Syslog-Meldungen

In diesem Kapitel werden die Syslog-Meldungen beschrieben. Der Aufbau der Meldungen orientiert sich an der IEC 62443-3-3.

Identifizierung und Authentifizierung von menschlichen Nutzern

Meldungstext	{protocol}: User {user name} logged in from {ip address}.
Beispiel	WBM: User admin logged in from 192.168.0.1.
Erläuterung	Gültige Anmeldeinformationen, die bei der Anmeldung angegeben werden.
Severity	Info
Facility	local0
Norm	IEC 62443-3-3 Reference: SR 1.1

Meldungstext	{protocol}: User {user name} failed to log in from {ip address}.
Beispiel	WBM: User admin failed to log in from 192.168.0.1.
Erläuterung	Falscher Benutzername oder falsches Kennwort bei der Anmeldung angegeben.
Severity	Error
Facility	local0
Norm	IEC 62443-3-3 Reference: SR 1.1

Meldungstext	{protocol}: User {user name} logged out from {ip address}.
Beispiel	WBM: User admin logged out from 192.168.0.1.
Erläuterung	Benutzersitzung beendet - Abmeldung erfolgt.
Severity	Info
Facility	local0
Norm	IEC 62443-3-3 Reference: SR 1.1

Meldungstext	{protocol}: Default user {user name} logged in from {ip address}.
Beispiel	PNIO: Default user admin logged in from 192.168.0.1.
Erläuterung	Standardnutzer ist angemeldet über die IP-Adresse.
Severity	Info
Facility	local0
Norm	IEC 62443-3-3 Reference: n/a (NERC-CIP 007-R5)

Nutzerkontenverwaltung

Meldungstext	Authentication was enabled.
Beispiel	Authentication was enabled.
Erläuterung	Authentifizierung wurde aktiviert.
Severity	Notice
Facility	local0
Norm	IEC 62443-3-3 Reference: SR 1.3

Meldungstext	Authentication was disabled.
Beispiel	Authentication was disabled.
Erläuterung	Authentifizierung wurde deaktiviert.
Severity	Notice
Facility	local0
Norm	IEC 62443-3-3 Reference: SR 1.3

Meldungstext	{Protocol}: User {User name} has changed the password.
Beispiel	WBM: User admin has changed the password.
Erläuterung	Benutzer hat sein Passwort geändert.
Severity	Notice
Facility	local0
Norm	IEC 62443-3-3 Reference: SR 1.3

Meldungstext	{Protocol}: User {User name} has changed the password of user {Destination user name}.
Beispiel	WBM: User admin has changed the password of user user1.
Erläuterung	Benutzer hat das Passwort eines anderen Benutzers geändert.
Severity	Notice
Facility	local0
Norm	IEC 62443-3-3 Reference: SR 1.3

Meldungstext	{Protocol}: User {User name} created user-account {Destination user name} with role {Role}.
Beispiel	WBM: User admin created user-account admin2 with role Administrator.
Erläuterung	Der Administrator hat ein Konto erstellt.
Severity	Notice
Facility	local0
Norm	IEC 62443-3-3 Reference: SR 1.3

Meldungstext	{Protocol}: User {User name} deleted user-account {Destination user name}.
Beispiel	WBM: User admin deleted user-account admin2.
Erläuterung	Der Administrator hat ein vorhandenes Konto gelöscht.
Severity	Notice
Facility	local0
Norm	IEC 62443-3-3 Reference: SR 1.3

Durchsetzung der Autorisierung

Meldungstext	{Protocol}: User {User}: Access to url {url} denied.
Beispiel	WBM: User admin: Access to url /Engineering/Reset2Factory?r=0.6856445562508033 denied.
Erläuterung	Zugriff auf Web-Ressource wurde verweigert.
Severity	Error
Facility	local0
Norm	IEC 62443-3-3 Reference: SR 2.1

Erfolglose Anmeldeversuche

Meldungstext	• Brute force protection activated. • Brute force protection deactivated.
Beispiel	Brute force protection activated.
Erläuterung	Bei zu vielen fehlgeschlagenen Anmeldungen wurde das entsprechende Benutzerkonto für einen bestimmten Zeitraum gesperrt.
Severity	Warning
Facility	local0
Norm	IEC 62443-3-3 Reference: SR 1.11

Sitzungssperrung

Meldungstext	{Protocol}: The session of user {User name} was closed after {Time second} seconds of inactivity.
Beispiel	WBM: The session of user admin was closed after 310 seconds of inactivity.
Erläuterung	Die aktuelle Sitzung wurde aufgrund der Inaktivität gesperrt.
Severity	Warning
Facility	local0
Norm	IEC 62443-3-3 Reference: SR 2.5

Begrenzung der Anzahl gleichzeitiger Sitzungen

Meldungstext	{Protocol}: The maximum number of {Max sessions} concurrent login session exceeded.
Beispiel	WBM: The maximum number of 10 concurrent login sessions exceeded.
Erläuterung	Die maximale Anzahl gleichzeitiger Sitzungen ist überschritten.
Severity	Warning
Facility	local0
Norm	IEC 62443-3-3 Reference: SR 2.7

Nicht-Abstreitbarkeit

Meldungstext	{Protocol}: User {User name} has changed configuration.
Beispiel	OPC: User unknown has changed configuration.
Erläuterung	Benutzer hat komplette Konfiguration geändert. Der Benutzer konnte nicht ermittelt werden. Es wird immer der Benutzer "unkonwn" ausgegeben.
Severity	Info
Facility	local0
Norm	IEC 62443-3-3 Reference: SR 2.12

Meldungstext	{Protocol}: User {User name} has changed {Config detail} configuration.
Beispiel	OPC: User admin has changed Power configuration.
Erläuterung	Benutzer hat bestimmte Konfiguration geändert.
Severity	Info
Facility	local0
Norm	IEC 62443-3-3 Reference: SR 2.12

Meldungstext	{Protocol}: User {User name} has initiated a reset to factory defaults.
Beispiel	WBM: User admin has initiated a reset to factory defaults.
Erläuterung	Benutzer hat ein Rücksetzen auf Werkseinstellungen initiert.
Severity	Info
Facility	local0
Norm	IEC 62443-3-3 Reference: SR 2.12

Software- und Informationsintegrität

Meldungstext	Configuration integrity verification failed.
Beispiel	Configuration integrity verification failed.
Erläuterung	Konfiguration Integritätsnachweis fehlgeschlagen.
Severity	Error
Facility	local0
Norm	IEC 62443-3-3 Reference: SR 3.4

Sitzungsintegrität

Meldungstext	{Protocol}: Session ID verification failed.
Beispiel	WBM: Session ID verification failed.
Erläuterung	Sitzungs-ID ist ungültig.
Severity	Error
Facility	local0
Norm	IEC 62443-3-3 Reference: SR 3.8

Wiederherstellung des Automatisierungssystems

Meldungstext	{Protocol}: Firmware {Version} was activated.
Beispiel	WBM: Firmware V2 was activated.
Erläuterung	Firmware erfolgreich aktiviert.
Severity	Notice
Facility	local0
Norm	IEC 62443-3-3 Reference: SR 7.4

Meldungstext	{Protocol}: Firmware activation failed.
Beispiel	WBM: Firmware activation failed.
Erläuterung	Firmware-Aktivierung fehlgeschlagen.
Severity	Error
Facility	local0
Norm	IEC 62443-3-3 Reference: SR 7.4

Service & Support

C

Industry Online Support

Zusätzlich zur Produktdokumentation unterstützt Sie die umfassende Online-Plattform des Siemens Industry Online Support unter folgender Internet-Adresse:
Link: (https://support.industry.siemens.com/cs/de/de/)

Neben Neuigkeiten finden Sie dort:

- Produktinformationen: Handbücher, FAQs, Downloads, Anwendungsbeispiele etc.
- Ansprechpartner, Technisches Forum
- Die Möglichkeit, eine Support-Anfrage zu stellen:
  Link: (https://support.industry.siemens.com/My/ww/de/requests)
- Unser Service-Angebot:

  Rund um unsere Produkte und Systeme bieten wir eine Vielzahl von Dienstleistungen an, die Sie in jeder Lebensphase Ihrer Maschine oder Anlage unterstützen - von der Planung und Realisierung über die Inbetriebnahme bis zur Instandhaltung und Modernisierung.

Kontaktdaten finden Sie im Internet unter folgender Adresse:
Link: (https://www.automation.siemens.com/aspa_app/?ci=yes&lang=de)

Homepage "Industrielle Identifikation"

Allgemeine Neuigkeiten zu unseren Identifikationssystemen finden Sie im Internet auf unserer Homepage (www.siemens.com/ident).

Online-Katalog und -Bestellsystem

Den Online-Katalog und das Online-Bestellsystem finden Sie ebenfalls auf der Industry Mall-Homepage (https://mall.industry.siemens.com).

SITRAIN - Training for Industry

Das Schulungsangebot umfasst mehr als 300 Kurse zu Grundlagenthemen, Aufbauwissen und Spezialwissen, sowie Weiterbildungsmaßnahmen zu einzelnen Branchen - verfügbar an über 130 Standorten weltweit. Zudem können die Kurse individuell gestaltet und bei Ihnen vor Ort abgehalten werden.

Ausführliche Informationen zum Schulungsangebot und Kontaktdaten unserer Kundenberater finden Sie unter folgender Internet-Adresse:

Link: (https://new.siemens.com/global/de/produkte/services/industrie/sitrain.html)