

BIS U-6127-081-1_4-06-ST36



deutsch Betriebsanleitung
english User's guide

www.balluff.com

BIS U-6127-081-1_4-06-ST36

Betriebsanleitung



www.balluff.com

1	Benutzerhinweise	6
1.1	Zu dieser Anleitung	6
1.2	Verwendete Symbole und Konventionen	6
1.3	Lieferumfang	6
1.4	Verwendete Abkürzungen	6
2	Sicherheit	7
2.1	Bestimmungsgemäße Verwendung	7
2.2	Vernünftigerweise vorhersehbare Fehlanwendung	7
2.3	Bedeutung der Warnhinweise	7
2.4	Allgemeine Sicherheitshinweise	7
2.5	Zulassungen und Kennzeichnungen	8
2.6	Entsorgung	8
3	Produktbeschreibung	9
3.1	Allgemeines zur Auswerteeinheit	9
3.2	Produktmerkmale	9
3.3	Systemübersicht	9
3.4	Geräteübersicht	10
3.5	Kundenspezifische Anwendungen und Erweiterungen	10
3.6	Datensicherheit	11
3.7	Tagdaten signieren	12
3.8	Anzeigeelemente	12
3.9	Ethernet TCP/IP	13
3.10	OPC UA	13
3.11	IO-Link Master	13
3.12	UHF-Datenträger (nicht im Lieferumfang enthalten)	14
4	Montage	15
4.1	Auswahl des Montageorts	15
4.2	Montage der Auswerteeinheit	15
4.3	Anschlussbelegung	16
4.4	Montage der UHF-Antennen (nicht im Lieferumfang enthalten)	17
4.5	Montage der UHF-Datenträger (nicht im Lieferumfang enthalten)	17
5	Technische Daten	18
5.1	Abmessungen	18
5.2	Mechanische Daten	18
5.3	Elektrische Daten	18
5.4	Umgebungsbedingungen	19
5.5	Anschlüsse ANT1...ANT4	19
5.6	Anschluss IO-Link	19
5.7	Anschluss Ethernet TCP/IP	19
5.8	Anschluss Service (USB)	19
5.9	Datenträger	19
5.10	Anzeigeelemente im Überblick	19
5.11	Uhrzeit und Datum	20
6	Applikationsplanung	21
6.1	Allgemeine Einsatzbedingungen	21
6.2	Antennenkonfigurationen	21
6.3	Datenträgerauswahl	21
6.4	UHF-Eigenschaften in der Praxis	22
6.5	Betriebsarten	23

7	Inbetriebnahme und Betrieb	29
7.1	Konfigurationssoftware UHF-Manager	29
7.1.1	Konfigurationssoftware installieren und starten	29
7.1.2	Benutzeroberfläche	29
7.1.3	Schnittstelleneinstellungen	30
7.1.4	Datenträger erfassen/erkennen	31
7.1.5	Datenträger lesen/schreiben	32
7.1.6	Parametereinstellung	32
7.2	Webserver	33
7.2.1	Home	33
7.2.2	Einloggen/Ausloggen	33
7.2.3	Spracheinstellungen	34
7.2.4	RFID	35
7.2.5	Konfiguration	36
7.2.6	Logbuch	48
7.2.7	Rechtliche und allgemeine Informationen	48
7.3	Parametrierung	49
7.3.1	Vorüberlegungen zur Parametrierung	49
7.3.2	Parameterübersicht	50
7.3.3	Beschreibung der Parameter für Standardbenutzer	53
7.3.4	Beschreibung der Parameter für Experten	56
7.3.5	Beschreibung der Parameter für Administratoren	72
7.3.6	Erzeugen eines Schlüssels zum Signieren von Tagdaten	82
7.4	Systemdiagnose	85
7.5	Betrieb	88
8	007-Protokoll	89
8.1	Protokollablauf	89
8.2	Steuerzeichen	90
8.3	Block Check Character (BCC)	90
8.4	Datenformat EPC/TID	90
8.5	Befehlsübersicht	91
8.6	Statuscodes	94
8.7	Allgemeine Befehle	95
8.8	Datenträger erfassen	99
8.9	Datenträger erfassen, asynchron	104
8.10	Datenträger bearbeiten	105
8.11	Universeller Datenträgerzugriff (Formatierte Tagdaten)	121
8.12	IO-Link	125

9	OPC UA	132
9.1	Grundlagen OPC UA	132
9.1.1	Beschreibung OPC UA	132
9.1.2	Systemschaubild	132
9.1.3	Sicherheitsmechanismen	132
9.2	Sicherheitsmechanismen OPC UA bei BIS U-6127	133
9.3	Verbindungsaufbau über OPC UA mit UaExpert	135
9.3.1	Unsicherer Verbindungsaufbau zwischen PC (OPC-UA-Client) und dem BIS U-6127-Gerät (OPC-UA-Server)	135
9.3.2	Sicherer Verbindungsaufbau zwischen PC (OPC-UA-Client) und dem BIS U-6127-Gerät (OPC-UA-Server)	136
9.4	Datenmodell Objekt: BIS_U_6127_Rfid_Provider	138
9.5	Methoden	139
9.5.1	Methoden Geräteeinstellung	140
9.5.2	Methoden zum Tag schreiben/lesen	141
9.5.3	Methoden für Scan-Einstellungen	148
9.6	Variablen und Konstanten	156
9.6.1	Geräteinformation /-einstellungen	156
9.6.2	Scan-Einstellungen	159
9.7	Datentypen	161
9.7.1	AntennaNameIdPair	161
9.7.2	AutoldOperationStatusEnumeration	161
9.7.3	BalluffFilterOperationEnumeration	162
9.7.4	CodeTypeDataType	162
9.7.5	DeviceStatusEnumeration	162
9.7.6	Location	162
9.7.7	LocationName	162
9.7.8	LocationTypeEnumeration	162
9.7.9	RfidLockOperationEnumeration	163
9.7.10	RfidLockRegionEnumeration	163
9.7.11	RfidPasswordTypeEnumeration	163
9.7.12	RfidScanResult	163
9.7.13	RfidSighting	164
9.7.14	ScanData	164
9.7.15	ScanDataEpc	164
9.7.16	ScanSettings	165
9.8	Events	165
9.9	Beispiele	166
9.9.1	Verbindungsaufbau	166
9.9.2	Lesen und Schreiben von Variablen	166
9.9.3	Methodenaufrufe	166
9.9.4	Read formatted Tag Data	167
9.9.5	Read Multiple Tag Data Formatted	168
9.9.6	Write Tag Data with Signature	168
9.9.7	Umgang mit statischen Filtern	169
9.9.8	Umgang mit Events	170
9.9.9	Global Session Mechanismus	171
10	Zubehör	173
10.1	UHF-Antennen	173
10.2	Antennenkabel	173
10.3	Anschlusskabel	173
10.4	Spannungsversorgung/Netzteil	173
10.5	Mechanisches Zubehör	173

1.1 Zu dieser Anleitung

Dieses Handbuch beschreibt die UHF-RFID-Auswerteeinheit BIS U-6127-081-1_4-06-ST36 sowie deren Handhabung für einen sicheren Betrieb.

Die Anleitung richtet sich an qualifizierte Fachkräfte. Lesen Sie diese Anleitung, bevor Sie die Auswerteeinheit installieren und betreiben.

1.2 Verwendete Symbole und Konventionen

Einzelne **Handlungsanweisungen** werden durch ein vorangestelltes Dreieck angezeigt.

- ▶ Handlungsanweisung 1
⇒ Resultat Handlung.

Handlungsabfolgen werden nummeriert dargestellt:

1. Handlungsanweisung 1
2. Handlungsanweisung 2

Zahlen ohne weitere Kennzeichnung sind Dezimalzahlen (z. B. 23). Hexadezimale Zahlen werden mit der Zusatzbezeichnung hex dargestellt (z. B. 00_{hex}).

Im **ASCII-Code** zu übertragende Zeichen sind in Hochkomma gesetzt (z. B. 'L').

Zu sendende **Steuerzeichen** sind in spitze Klammern gesetzt (z. B. <ACK>).

Schaltflächen oder auswählbare Menüeinträge werden kursiv und in Kapitälchen geschrieben, z. B. *SPEICHERN*.

Menübefehle werden mit einem Größerzeichen verbunden, z. B. „Einstellungen > Optionen“ steht für den Menübefehl „Optionen“ aus dem Menü „Einstellungen“.



Hinweis, Tipp

Dieses Symbol kennzeichnet allgemeine Hinweise.

1.3 Lieferumfang

- Auswerteeinheit BIS U-6127
- 5 x Verschlusskappe
- Sicherheitshinweise – Informationsblatt zu Konformität und Zulassung



Zugehörige technische Unterlagen sowie weitere Informationen zu lieferbarer Software und Zubehör siehe **www.balluff.com**.

1.4 Verwendete Abkürzungen

BCC	Block Check Character
BIS	Balluff Identifikationssystem
CRC	Cyclic Redundancy Check
DC	Gleichstrom
E/A-Port	Digitaler Eingang- bzw. Ausgangsport
EEPROM	Electrical Erasable and Programmable ROM
EIRP	Equivalent Isotropically Radiated Power
EMV	Elektromagnetische Verträglichkeit
EPC™	Electronic Product Code
ERP	Effective Radiated Power
FCC	Federal Communications Commission
FE	Funktionserde
IC	Industry Canada
IP	Internet Protocol
ISO	Internationale Organisation für Normung
kB	Kilobyte
LAN	Local Area Network
MAC-ID	Media Access Control Identifier
MB	Megabyte
OPC UA	Open Platform Communications Unified Architecture
PC	Personal Computer
RFID	Radio Frequency Identification
RFU	Reserved for Future Use
RSSI	Receive Signal Strength Indicator
SPS	Speicherprogrammierbare Steuerung
Tag	Datenträger mit Antenne/Transponder
TCP	Transmission Control Protocol
TID	Tag-Identifizier
UID	Unique Identifier
UHF	Ultrahoch-Frequenz
USB	Universal Serial BUS

2.1 Bestimmungsgemäße Verwendung

Die UHF-Auswerteeinheit BIS U-6127-... bildet zusammen mit maximal 4 anschließbaren UHF-Antennen das Identifikationssystem BIS U.

Die Auswerteeinheit stellt Netzwerkfunktionen zur Anbindung an ein übergeordnetes Ethernet-TCP/IP-Netzwerk bereit und ist für die kontaktlose Erfassung und Bearbeitung von UHF-RFID-Datenträgern in einem industriellen Umfeld vorgesehen. Die Auswerteeinheit darf nur zu diesem Zweck verwendet werden.

Die UHF-RFID-Auswerteeinheit BIS U darf nur innerhalb der freigegebenen Länder (siehe Informationsblatt zu Konformität und Zulassung) und unter Einhaltung der national gültigen gesetzlichen Bestimmungen betrieben werden.

Die einwandfreie Funktion gemäß den Angaben in den technischen Daten wird nur mit Original Balluff Zubehör zugesichert, die Verwendung anderer Komponenten bewirkt Haftungsausschluss.

Bei Schäden, die aus unbefugten Eingriffen oder nicht-bestimmungsgemäßer Verwendung, Installation oder Handhabung entgegen den Vorschriften dieser Betriebsanleitung entstehen, erlischt der Garantie-, Gewährleistungs- und Haftungsanspruch gegenüber dem Hersteller.

2.2 Vernünftigerweise vorhersehbare Fehlanwendung

Die Produkte sind für folgende Anwendungen und Bereiche nicht bestimmt und dürfen dort nicht eingesetzt werden:

- in sicherheitsgerichteten Anwendungen, in denen die Personensicherheit von der Gerätefunktion abhängt
- in explosionsgefährdeten Bereichen
- im Lebensmittelbereich

2.3 Bedeutung der Warnhinweise

Beachten Sie unbedingt die Warnhinweise in dieser Anleitung und die beschriebenen Maßnahmen zur Vermeidung von Gefahren.

Die verwendeten Warnhinweise enthalten verschiedene Signalwörter und sind nach folgendem Schema aufgebaut:

SIGNALWORT
Art und Quelle der Gefahr Folgen bei Nichtbeachtung der Gefahr ► Maßnahmen zur Gefahrenabwehr

Die Signalwörter bedeuten im Einzelnen:

ACHTUNG Kennzeichnet eine Gefahr, die zur Beschädigung oder Zerstörung des Produkts führen kann.
 VORSICHT Das allgemeine Warnsymbol in Verbindung mit dem Signalwort VORSICHT kennzeichnet eine Gefahr, die zu leichten oder mittelschweren Verletzungen führen kann.

2.4 Allgemeine Sicherheitshinweise

Die **Installation** und die **Inbetriebnahme** darf nur durch geschulte Fachkräfte mit grundlegenden elektrischen Kenntnissen erfolgen.

Eine **geschulte Fachkraft** ist, wer aufgrund seiner fachlichen Ausbildung, seiner Kenntnisse und Erfahrungen sowie seiner Kenntnisse der einschlägigen Bestimmungen die ihm übertragenen Arbeiten beurteilen, mögliche Gefahren erkennen und geeignete Sicherheitsmaßnahmen treffen kann.

Der **Betreiber** hat die Verantwortung, dass die örtlich geltenden Sicherheitsvorschriften eingehalten werden. Insbesondere muss der Betreiber Maßnahmen treffen, dass bei einem Defekt des Geräts keine Gefahren für Personen und Sachen entstehen können. Bei Defekten und nicht behebbaren Störungen des Geräts ist dieses außer Betrieb zu nehmen und gegen unbefugte Benutzung zu sichern.

Das Produkt darf nicht geöffnet, umgebaut oder verändert werden. Bei Defekten und nichtbehebaren Störungen des Produkts ist dieses außer Betrieb zu nehmen und gegen unbefugte Benutzung zu sichern.

Die Antennen des BIS U-Identifikationssystems senden ultrahochfrequente elektromagnetische Wellen aus. Nach IEC 62369 dürfen sich Personen nicht längere Zeit (über mehrere Stunden) im Nahbereich der UHF-Antenne aufhalten.

Die Auswerteeinheit und angeschlossenes Zubehör darf nur mit begrenzter Energie versorgt werden, entsprechend UL 61010-1 Third Edition, Sub. Clauses 9.4 oder LPS entsprechend UL 60950-1 oder Class 2 entsprechend UL 1310 oder UL 1585.

Bei Überschreiten der maximalen Stromaufnahme kann es zu Schäden an der Auswerteeinheit und an angeschlossenen Systemkomponenten kommen. Beim Betrieb muss darauf geachtet werden, dass der Gesamtstrom, der über den Anschluss Power geführt wird, 3 A nicht übersteigt. Der Spannungsausgang (L+) am IO-Link-Port sowie digitale Ausgänge (E/A) werden über den Anschluss Power versorgt. Die Summe der Teilströme dieser Pins, darf einen maximalen Strom von 2 A nicht übersteigen.

2

Sicherheit (Fortsetzung)

2.5 Zulassungen und Kennzeichnungen



Siehe beiliegendes Informationsblatt zu Konformität und Zulassung.



Nähere Informationen zu Richtlinien, Zulassungen und Normen finden Sie unter **www.balluff.com** auf der Produktseite.

2.6 Entsorgung

- Befolgen Sie die nationalen Vorschriften zur Entsorgung.



Weitere Informationen finden Sie unter **www.balluff.com** auf der Produktseite.

3.1 Allgemeines zur Auswerteeinheit

Die Auswerteeinheit BIS U-6127 bildet zusammen mit maximal vier anschließbaren UHF-Antennen der Baureihe BIS U-3... und UHF-RFID-Datenträgern der Baureihe BIS U-1... das Balluff Identifikationssystem BIS U.

Je nach verwendeter Ländervariante (siehe Informationsblatt zu Konformität und Zulassung) senden die Antennen Signale in einem Frequenzbereich von 865 MHz...930 MHz und kommunizieren drahtlos mit Datenträgern, die sich im Erfassungsbereich der Antennen befinden. Vier Antennen ermöglichen die bedarfsgerechte Erfassung und Bearbeitung von Datenträgern in unterschiedlichen Bereichen. Werden z. B. alle Antennen auf denselben Erfassungsbereich ausgerichtet (Tor-Anwendung), kann dieser vergrößert und die Erfassungssicherheit (je nach Betriebsart) gesteigert werden.

Über die Gigabit-Ethernet-TCP/IP-Schnittstelle kann die Auswerteeinheit in ein lokales Netzwerk (LAN) eingebunden und durch ein übergeordnetes System gesteuert werden. Zur Konfiguration steht ein Webserver zur Verfügung.

Das BIS U-6127 unterstützt über die TCP/IP-Schnittstelle das Protokoll OPC UA für RFID-Lesegeräte. Dieser Standard unterstützt vor allem den automatisierten Informationsaustausch zwischen industriellen Geräten (M2M) (siehe Kapitel 9 auf Seite 132).

Als zusätzliche Schnittstelle ist eine IO-Link-Master-Schnittstelle vorhanden, die ein direktes Einbinden von IO-Link-Komponenten sowie die Ein- und Ausgabe von Schaltsignalen ermöglicht.

Die USB-Service-Schnittstelle stellt einen Service-Zugang direkt am Einbauort bereit, ohne die Auswerteeinheit physisch vom Netzwerk zu trennen.

Funktionsanzeigen an der Geräteoberfläche geben jederzeit Aufschluss über Funktion und Status des Geräts.

3.2 Produktmerkmale

- Robustes Metallgehäuse mit Schutzklasse IP65
- Betrieb von bis zu 4 Antennen mit Direktanwahl und Multiplexbetrieb
- RFID-UHF-Betriebsfrequenzen: 865 MHz...930 MHz (Länderspezifisch)
- Sendeleistung einstellbar im Bereich 7 dBm...30 dBm (5 mW...1 W)
- Schreib-/Leseabstand bis zu 6 Meter (typ.)
- Unterstützte Datenträgertypen gemäß ISO 18000-63 und EPCglobal™ Class1 Generation2
- Ethernet-TCP/IP (1000BASE-T, 100BASE-TX, 10BASE-T) nach IEEE 802.3-2008
- Steuerung über OPC UA-Protokoll nach AIM AutoID Companion Specification 1.0
- Erhöhte Datensicherheit durch Zugriffsbeschränkungen über Benutzerkonten
- Verschlüsselte Netzwerkverbindungen über OPC UA
- Automatische Erzeugung von Signaturen auf Datenträgern, um Daten gegen Manipulation abzusichern
- Speicherung der geheimen Schlüssel in einem *Secure Element*-Chip
- IO-Link-Master-Schnittstelle, frei konfigurierbar als IO-Link- und E/A-Port oder 2 E/A-Ports
- Kontrollanzeigen für Funktion und Status
- Konfiguration und Überwachung via Webserver
- USB-Schnittstelle für Servicefunktionen

3.3 Systemübersicht

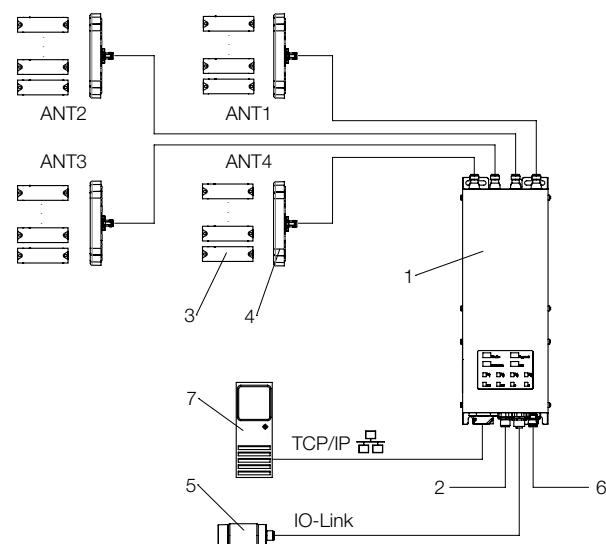


Bild 3-1: Systemübersicht

1 BIS U-6127	5 O-Link-Device
2 Service (USB)	6 Power
3 UHF-Datenträger	7 Ethernet-Host
4 UHF-Antennen	



Um Fehlfunktionen zu vermeiden, nicht verwendete Antennenports über die Parametrierung abschalten (siehe Kapitel 7.3 auf Seite 49).

3

Produktbeschreibung (Fortsetzung)

3.4 Geräteübersicht

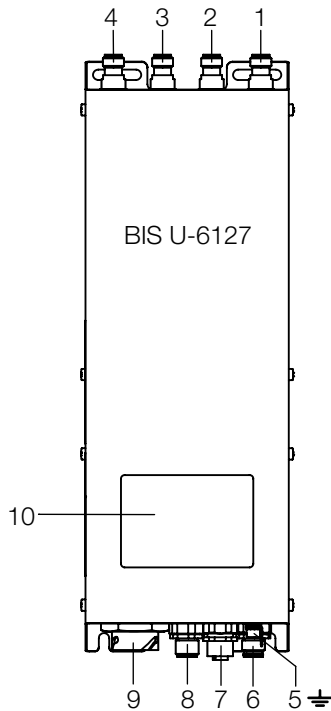


Bild 3-2: Geräteübersicht

1 Antennenport 1	6 X1 Power
2 Antennenport 2	7 X2 IO-Link
3 Antennenport 3	8 X3 Service (USB)
4 Antennenport 4	9 X4 Ethernet TCP/IP
5 Funktionserde FE	10 Funktionsanzeigen



Um die Schutzart IP65 zu gewährleisten, müssen nicht verwendete Anschlüsse mit Verschlusskappen versehen werden.

3.5 Kundenspezifische Anwendungen und Erweiterungen

Die Auswerteeinheit BIS U-6127 bietet viele Möglichkeiten zur Anpassung an kundenindividuelle Aufgabenstellungen, wie z. B. autonomer Betrieb, einstellbare Datenaus- und -eingabeformate und Filterfunktionen. Darüber hinaus ermöglicht der IO-Link-Master-Port die Ansteuerung von weiteren Geräten.

Dennoch kann es sinnvoll sein, weitere Verarbeitungsschritte der Datenaufbereitung oder von den Daten abhängige Abläufe im Gerät durchzuführen, und so zusätzliche Systemkomponenten, Steuer-PCs oder ähnliches einzusparen und die Handhabung und Wartung zu vereinfachen.

Das Linux-basierte Betriebssystem und die Balluff Systemarchitektur des Geräts ermöglichen es, auch kundenindividuelle Erweiterungen durch zusätzliche Applikationen im Gerät zu integrieren, um z. B. den Scanvorgang mit Sensorik am IO-Link-Port zu synchronisieren, Anzeigen anzu-steuern, direkt mit Ihren ERP-Systemen zu kommunizieren, einen vollständig autonomen Betrieb in einer Anwendung zu realisieren und vieles mehr.

Die Erweiterungsapplikationen können die Vorteile und das Sicherheitskonzept des Geräts optimal nutzen.



Kontaktieren Sie unsere Anwendungsspezialisten für individuelle Beratungen und die Erstellung kundenindividueller Apps.

3.6 Datensicherheit

Die Auswerteeinheit BIS U-6127 wurde konzipiert, um auch in verteilten Installationen und größeren Netzwerken betrieben zu werden. Mit zunehmender Verteilung der vernetzten Geräte steigt das Risiko einer unbeabsichtigten oder absichtlichen Veränderung der gespeicherten oder übertragenen Daten.

Das betrifft sowohl die Daten auf den genutzten Datenträgern und deren Übertragung von und zur Auswerteeinheit als auch die Daten in der Auswerteeinheit selbst und deren Übertragung zum übergeordneten verarbeitenden System.

Um Risiken zu minimieren, bietet das Gerät einige Sicherheitsfunktionen:

- Die Nutzung eines etablierten Linux-basierten Betriebssystems.
- Eine durchgängige Benutzerverwaltung bietet Zugriffsschutz auf Geräteeinstellungen in mehreren Stufen. Essentielle Einstellungen (z. B. IP-Adresse oder Antennenkonfiguration), Firmwareupdates oder ein Geräte-neustart können nur mit der Benutzerrolle *Admin* durchgeführt werden.
- Ansteuerung des Geräts über OPC UA mit optionaler Verschlüsselung der Daten und beidseitiger Endpunktauthentifizierung erlaubt auch die Steuerung über ausgedehnte Netzwerke.
- Nicht genutzte Kommunikationsprotokolle und Zugänge können gesperrt werden.
- Daten auf Standard-UHF-Datenträgern können automatisch mit einer Signatur versehen werden, um die Unversehrtheit und Echtheit der Daten zu prüfen.
- Die Verwaltung der sicherheitskritischen privaten Schlüssel für OPC UA und Tagsignaturen kann im Speicher des eingebauten *Secure Elements* erfolgen. Von dort können sie auch dann nicht ausgelesen werden, wenn das Gerät geöffnet wird oder aus dem Netzwerk angegriffen wird.

Empfohlene Maßnahmen für Datensicherheit

Um die bestmögliche Datensicherheit zu gewährleisten, empfehlen wir folgende Maßnahmen:

Allgemein

- Jedem Gerät im Netzwerk einen anderen Gerätenamen zuweisen.
- Mit dem Internet verbundene Netzwerke über Firewalls etc. abschotten.
- Von Balluff bereitgestellte Sicherheitsupdates einspielen.

Benutzerkonten

- Das Default-Administrator-Konto *admin_default* sollte möglichst nur zum initialen Einrichten anderer Benutzerkonten genutzt werden.
- Das gerätespezifische Kennwort für *admin_default* kann nicht geändert werden. Das auf dem Typschild aufgedruckte Kennwort abschneiden und sicher aufbewahren!
- Weitere Konten können mit selbstgewählten Kennwörtern versehen werden (auch solche mit Administrator-Rechten). Sichere Kennwörter sollten Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen beinhalten und mindestens acht Zeichen lang sein.
- Benutzerrechte und Kennwörter personengebunden vergeben und die Rechte nur soweit erteilen, wie sie für die Aufgaben der Personen notwendig sind.
- Kennwörter, die in unbefugte Hände gelangt sind, schnellstmöglich ändern.

Nähere Informationen zu Benutzerkonten und damit verbundenen Berechtigungen siehe Kapitel 7.2.5 auf Seite 36.

OPC UA

- OPC UA als Kommunikationsprotokoll verwenden. Die Auswerteeinheit BIS U-6127 implementiert einen erweiterten Funktionsumfang der OPC UA AutoID Companion Specification 1.0.
- Beim OPC UA Protokoll die Einstellungen *UNSICHERE CLIENTVERBINDUNGEN ZURÜCKWEISEN* und *NUR VERTRAUENS-WÜRDIGE CLIENTZERTIFIKATE AKZEPTIEREN* nutzen.
- Nicht benötigte Clientzertifikate blockieren oder löschen.
- Die Schlüssel- und Zertifikatsverwaltung des *Secure Elements* nutzen.
- Jedem Gerät im Netzwerk einen anderen Gerätenamen zuweisen.
- Bei Änderung des Netzwerknamens oder der IP-Adresse neue Gerätezertifikate erstellen.
- Auch im OPC-UA-Client nur geprüfte Gerätezertifikate freigeben und unbekannte Zertifikate ablehnen.
- Die Erstverbindung und den Zertifikatsaustausch bei einem neuen Gerät oder Gerätezertifikat in einer sicheren Netzwerkumgebung herstellen, damit sichergestellt werden kann, dass das Zertifikat zum verbundenen Gerät gehört.

007-Protokoll

- Das 007-Protokoll (wird auch vom UHF-Manager als Verbindungsprotokoll genutzt) nur in einer sicheren, geschlossenen Netzwerkumgebung oder über USB verwenden, da Kennwörter unverschlüsselt übertragen werden.
- Das 007-Protokoll kann über die Weboberfläche deaktiviert werden, wenn es nicht genutzt wird.

Weboberfläche

Die Weboberfläche zur Konfiguration des Geräts nur in einem lokalen Netzwerk betreiben, da die http-Übertragung nicht verschlüsselt ist und eingegebene Kennwörter von Dritten abgefangen werden könnten.

3

Produktbeschreibung (Fortsetzung)

3.7 Tagdaten signieren

Wenn Daten auf Datenträgern signiert werden, werden zu den eigentlichen Daten (TID, EPC, User-Daten) weitere Daten mit Hilfe eines geheimen Schlüssels und einem Rechenalgorithmus hinzugefügt, die später dazu dienen, die Echtheit der Daten zu prüfen.

Verwendet wird ein 224 Bit langer, geheimer (privater) Schlüssel und ein sog. *Elliptic Curve*-Algorithmus, der eine hohe Sicherheit bietet.

Beim Lesen der Datenträger werden die Daten nur dann als gültig akzeptiert, wenn folgende Voraussetzungen gegeben sind:

1. Es ist eine Signatur vorhanden.
2. Die Signatur mit dem richtigen geheimen Schlüssel des Betreibers wurde erzeugt.
3. Weder Daten noch Signatur wurden nachträglich geändert.

UHF-Datenträger (Tags), bei denen mindestens 64 Byte Speicher im User-Bereich verfügbar sind, die nicht für Anwendungsdaten genutzt werden müssen, können die Tag-Signatur verwenden. Für die Nutzung sind die Kommandos *FORMATIERTES LESEN/SCHREIBEN* zu verwenden. Dabei werden die ersten 64 Byte des User-Bereichs mit einer Signatur versehen, die üblicherweise den EPC und den TID des Tags sowie einen geheimen Schlüssel einbezieht und nur von Geräten erzeugt werden kann, die denselben geheimen Schlüssel besitzen.

Der Schlüssel muss vom Einrichtenden erzeugt und ins Gerät programmiert werden (siehe Kapitel 7.3.6 auf Seite 82). Der Schlüssel sollte sicher aufbewahrt und vor unbefugtem Zugriff geschützt werden. Im Gerät selbst ist der Schlüssel im *Secure Element* sicher verwahrt.

i Um Tagdaten zu signieren oder die Signatur zu prüfen, muss vom Kunden ein eigener privater Schlüssel in das *Secure Element* des Geräts eingespielt werden. Für das Einspielen eines Schlüssels muss eine spezielle Lizenz über den Balluff Vertrieb erworben werden: das Schlüssel-Update-Ticket.

3.8 Anzeigeelemente

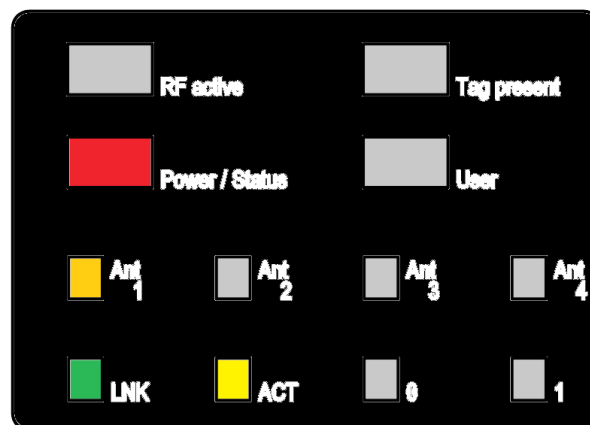


Bild 3-3: Anzeigeelemente

BIS U-Status

LED	Farbe	Bedeutung
RF active	Aus	Antennen Ant1...Ant4 inaktiv
	Blau	Aktive Kommunikation über eine der Antennen Ant1...Ant4
Tag present	Aus	Keine Datenträger im Erfassungsbereich von Ant1...Ant4
	Gelb (3 s)	Min. 1 Datenträger im Erfassungsbereich erkannt
Power/Status	Aus	Keine Versorgungsspannung
	Rot	Nicht betriebsbereit (siehe Kapitel 7.4 auf Seite 85)
	Gelb	Beim Einschalten: Versorgungsspannung vorhanden Im Betrieb: Warnstatus vorhanden (siehe Kapitel 7.4 auf Seite 85)
	Grün	Betriebsbereit
	Grün blinkend (1 s)	Bootmodus
User	Aus, Rot, Gelb, Grün	Über OPC UA frei programmierbar
Ant1...Ant4	Aus	Antennenport inaktiv
	Gelb	Antennenport aktiv

Ethernet TCP/IP Status

LED	Farbe	Bedeutung
LNK (Link)	Aus	Keine LAN-Verbindung
	Grün	LAN-Verbindung
ACT (Activity)	Aus	Keine Datenübertragung
	Gelb blinkend	Datenübertragung

IO-Link-Status

LED	Farbe	Bedeutung
0	Aus	Status des Eingangs/Ausgangs ist 0
	Gelb	Status des Eingangs/Ausgangs ist 1
	Grün	IO-Link-Kommunikation aktiv
	Grün blinkend (1 sek)	Keine IO-Link-Kommunikation oder falsches IO-Link-Device
	Grün blinkend (schnell)	IO-Link Preoperate während der Datenhaltung
	Rot	Kurzschluss IO-Link/Kurz- schluss Sensorversorgung/ Firmwareupdate
	Rot blinkend	Validierung fehlgeschlagen/ falsche Konfiguration der IO- Link Datenlänge/Selbsttest nach dem Einschalten
1	Aus	Status des Eingangs/Ausgangs ist 0
	Gelb	Status des Eingangs/Ausgangs ist 1
	Rot	Kurzschluss am Ausgang

3.9 Ethernet TCP/IP

Die TCP/IP-Schnittstelle erfüllt den Ethernet-Standard nach IEEE 802.3-2008 (bis 1 Gigabit) und unterstützt folgende Übertragungsmodi:

- 1000BASE-T
- 100BASE-TX
- 10BASE-T

Über die Ethernet-Schnittstelle kann die Auswerteeinheit in ein lokales Netzwerk (LAN) eingebunden werden. Ein Webserver bietet verschiedene Funktionen für Inbetriebnahme und Parametrierung.



Das Ethernetkabel sollte mindestens der Kategorie 5e nach EIA/TIA-568 entsprechen, um die Datensicherheit der Ethernetübertragung sicherzustellen. Die maximale Kabellänge darf 100 m nicht übersteigen. Bei längeren Kabelstrecken wird der Einsatz von Repeatern empfohlen.

3.10 OPC UA

Das BIS U-6127 kann über den Datenaustauschstandard OPC UA kommunizieren. Dieser Standard verwendet als physikalische Grundlage die Ethernet-Schnittstelle (siehe Kapitel 3.9 auf Seite 13). Alle physikalischen Eigenschaften der Ethernet-CP/IP-Schnittstelle gelten auch für den OPC-UA-Standard.

OPC-UA-Methoden erlauben Lesen und Schreiben von Prozessdaten sowie die Einstellung und Parametrierung unterschiedlichster UHF-Parameter.

Der Vorteil am industriellen Kommunikationsstandard OPC UA liegt darin, dass nicht nur spezielle Benutzer die Schnittstelle bedienen können, sondern jede OPC-UA-fähige Maschine kann anhand des Datenmodells eine Kommunikation mit dem BIS U-6127 aufbauen (Maschine-zu-Maschine-Kommunikation).

Das hier verwendete OPC-UA-Protokoll richtet sich nach der *Companion Specification for AutoID*, herausgegeben von AIM Deutschland und der OPC Foundation.

Für eine detaillierte Beschreibung zum Datenmodell mit allen unterstützten Methoden siehe Kapitel 9 auf Seite 132).

3.11 IO-Link Master

IO-Link ist als standardisierte Punkt-zu-Punkt-Verbindung zwischen Sensoren/Aktoren und dem E/A-Modul definiert. Über die IO-Link-Schnittstelle können Sensoren und Aktoren zusätzlich zu den binären Prozesssignalen weitere Kommunikationsdaten übertragen (z. B. Diagnosesignale). Die IO-Link-Schnittstelle eignet sich auch zum Anschluss einer externen Meldelampe (z. B. einer Smart Light – LED Signalsäule).

Kompatibilität zum Standard-E/A

- IO-Link-Sensoren/-Aktoren können an bestehende E/A-Module angeschlossen werden.
- Sensoren/Aktoren, die nicht IO-Link-fähig sind, können an ein IO-Link-Modul angeschlossen werden.
- Standardkabel für Sensoren/Aktoren verwendbar

Technische Eckdaten

- Serielle Punkt-zu-Punkt-Verbindung
- Kommunikation als Erweiterung zum Standard-E/A
- Standard-E/A-Anschlusstechnik, ungeschirmt, Leitungslänge max. 20 m
- Kommunikation durch 24-V-Pulsmodulation, Standard-UART-Protokoll

Standard-IO-Modus

- IO-Link-fähige Geräte werden über die IO-Link-Schnittstelle parametrierbar und dann in den SIO-Modus versetzt.
- Ab diesem Zeitpunkt funktioniert der IO-Link-Port-Pin als einfacher Schalteingang, der ein binäres Signal liefert.



Weitere Informationen zu lieferbaren IO-Link Geräten sowie Zubehör sind im Internet unter www.balluff.com zu finden.

3

Produktbeschreibung (Fortsetzung)

3.12 UHF-Datenträger (nicht im Lieferumfang enthalten)

Die Auswerteeinheit unterstützt UHF-Datenträger nach ISO 18000-63 und EPCglobal™ Class1 Generation2.

Wichtige Grundlagen zu Speicherbänken und deren Schutzstatus sind im Folgenden dargestellt. Tiefergehende Informationen zur Funktion von UHF-Datenträgern können den oben genannten UHF-RFID-Standards entnommen werden.

Die Speicherorganisation von UHF-Datenträgern sieht je nach Ausführung verschiedene Speicherbereiche (Speicherbänke) vor:

- Reserviert
- EPC
- TID
- USER

i Die Aufteilung bzw. die Größe der jeweiligen Speicherbänke können dem Datenblatt des verwendeten Datenträgers entnommen werden.

Die Speicherbereiche EPC und USER (sofern vorhanden) stehen der freien Bearbeitung zur Verfügung.

Die TID-Speicherbank ist schreibgeschützt und kann nur gelesen werden.

Der reservierte Speicherbereich ist für Passwörter vorgesehen. In ihm kann ein Zugriffspasswort (Access-Passwort) sowie ein Kill-Passwort gespeichert werden (siehe Befehle *Lock* und *Kill*).

Das Zugriffspasswort erlaubt das Lesen bzw. das Beschreiben von Speicherbereichen, deren Schutzstatus ein Passwort erfordert.

Der Sicherheitsstatus für die beiden Passwörter in der reservierten Speicherbank kann einzeln wie folgt festgelegt werden:

Operation	Unlock	Lock	Unlock Permanent	Lock Permanent
Lesen	Erlaubt	Access-Passwort	Erlaubt	Gesperrt
Schreiben	Erlaubt	Access-Passwort	Erlaubt	Gesperrt
Status Reversibel	Ja	Ja	Nein	Nein

Der Sicherheitsstatus für die Speicherbänke EPC, TID und USER kann wie folgt festgelegt werden:

Operation	Unlock	Lock	Unlock Permanent	Lock Permanent
Lesen (EPC, TID, USER)	Erlaubt	Erlaubt	Erlaubt	Erlaubt
Schreiben (EPC, USER)	Erlaubt	Access-Passwort	Erlaubt	Gesperrt
Status Reversibel	Ja	Ja	Nein	Nein

i Details zu den unterschiedlichen Speicherbänken sowie zu den Funktionen *Lock* und *Kill* können den UHF-RFID-Standards ISO/IEC 8000-63 und EPCglobal™ Class-1 Generation-2 entnommen werden.

4

Montage

4.1 Auswahl des Montageorts

Bei der Auswahl des Montageorts muss darauf geachtet werden, dass der Untergrund eine ausreichende Tragfähigkeit hat und dass an den Steckerseiten der Auswerteeinheit ausreichend Platz für die Kabelabgänge zur Verfügung steht. Dabei sollte der zulässige Biegeradius der verwendeten Kabel beachtet werden.

Die Montage des Geräts soll möglichst nahe am Einsatzort stattfinden, da die UHF-Antennenkabel in ihrer Länge begrenzt sind.

Um Fehlfunktionen oder Verletzungen zu vermeiden, muss das Gerät fest montiert werden. Der Montageort soll möglichst vibrationsarm, temperaturstabil und vor Stößen geschützt sein.



Befestigungsplatten und Halterungen sowie weiteres Montagezubehör finden Sie unter www.balluff.com.

Zur Montage der Auswerteeinheit sind vier Langlöcher für M5-Schrauben vorgesehen. Diese befinden sich an den Ecken des Gehäuserahmens im Bereich der Steckerfrontplatten.

4.2 Montage der Auswerteeinheit

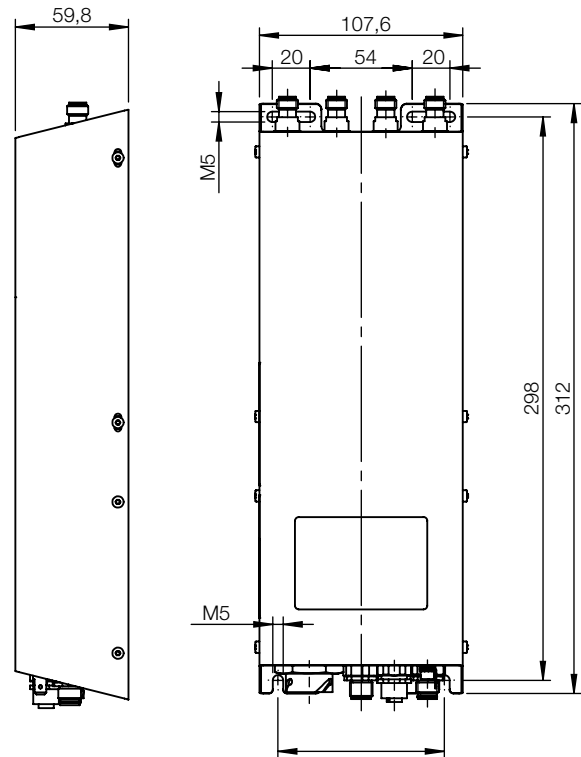


Bild 4-1: Montage

1. Geeignete Montageposition bestimmen.
2. Auswerteeinheit mit 4 Schrauben M5 befestigen (Festigkeitsklasse 8.8, leicht geölt, Anzugsmoment $M = 5,2 \text{ Nm}$).

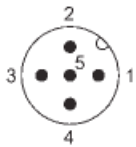
4

Montage (Fortsetzung)

4.3 Anschlussbelegung

Power

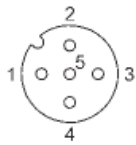
Stecker, M12, 5-polig, A-codiert



Pin	Beschreibung	Funktion
1	+24V DC	Versorgungsspannung
2	Nicht belegt	Keine
3	GND	Masse
4	Nicht belegt	Keine
5	Nicht belegt	Keine

O-Link

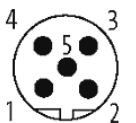
Buchse, M12, 5-polig, A-codiert



Pin	Beschreibung	Funktion
1	L+	Versorgungsspannung (Ausgang)
2	E/A	Eingang/Ausgang
3	L-	Masse
4	C/Q, E/A	IO-Link bzw. Eingang/Ausgang
5	Nicht belegt	Keine – nicht beschalten!

Service (USB)

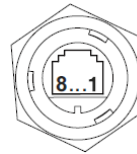
Stecker M12, 5-polig, B-codiert



Pin	Beschreibung	Funktion
1	+5V	Versorgungsspannung (Eingang)
2	D-	Bidirektionale Datenleitung –
3	D+	Bidirektionale Datenleitung +
4	GND	Masse
5	Shield	Kabelschirm

Ethernet TCP/IP

Buchse, RJ-45, 8-polig



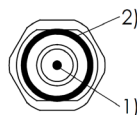
Pin	Beschreibung	Funktion
1	DA+	Bidirektionale Daten A+
2	DA-	Bidirektionale Daten A-
3	DB+	Bidirektionale Daten B+
4	DC+	Bidirektionale Daten C+
5	DC-	Bidirektionale Daten C-
6	DB-	Bidirektionale Daten B-
7	DD+	Bidirektionale Daten D+
8	DD-	Bidirektionale Daten D-



Das Ethernetkabel sollte mindestens der Kategorie 5e nach EIA/TIA-568 entsprechen, um die Datensicherheit der Ethernetübertragung sicherzustellen. Die maximale Kabellänge darf 100 m nicht übersteigen. Bei längeren Kabelstrecken wird der Einsatz von Repeatern empfohlen.

Antennen 1...4

Buchse, TNC-Reverse



Pin	Beschreibung	Funktion
1	RF	UHF-Signal
2	GND	Masse



Zum Verbinden der UHF-Antennen mit den Antennenports der Auswerteeinheit werden Koaxialkabel mit der Steckerkonfiguration *Stecker TNC Reverse* / *Stecker TNC* benötigt.

4

Montage (Fortsetzung)

4.4 Montage der UHF-Antennen (nicht im Lieferumfang enthalten)

Bei der Wahl des Einbauorts muss auf einen ausreichenden Abstand zu Arbeitsplätzen geachtet werden, an denen sich Personen dauerhaft aufhalten.

VORSICHT

Ultrahochfrequente elektromagnetische Wellen

Die Antennen des BIS U-Identifikationssystems senden ultrahochfrequente elektromagnetische Wellen aus. Um Gesundheitsgefährdungen auszuschließen, müssen zusätzliche Maßnahmen getroffen werden.

- ▶ Die Montageposition der Antennen so festlegen, dass ein Sicherheitsabstand von mindestens 20 cm zwischen den Antennen und Arbeitsplätzen von Personen gewährleistet wird.
- ▶ Bereiche, die explizit nicht erfasst werden sollen, durch geeignete Maßnahmen abschirmen.

Für Details zur Montage der Antennen siehe Datenblatt der verwendeten Antenne.

Die Antennen so ausrichten, dass die Hauptstrahlrichtung der Antenne auf den Ort ausgerichtet ist, an dem Datenträger erfasst werden sollen. Die maximale Größe des Erfassungsbereichs ist abhängig von der Sendeleistung und dem Öffnungswinkel der Antenne. Größere Erfassungsbereiche (wie z. B. Tordurchfahrten) können unter Umständen nur durch den Einsatz mehrerer Antennen vollständig abgedeckt werden.

Um die einwandfreie Funktion des Identifikationssystems zu gewährleisten, muss der Erfassungsbereich der Antenne und insbesondere die Sichtverbindung zwischen Antenne und Datenträger frei von elektromagnetisch wirksamen Materialien (z. B. Metall, Flüssigkeiten,...) sein, da diese Einfluss auf den Erfassungsbereich der Antenne haben und die maximale Reichweite des RFID-Systems reduzieren bzw. das Erfassen von Datenträgern erschweren können.

Bereiche, die explizit nicht erfasst werden sollen, müssen durch geeignete Maßnahmen abgeschirmt werden.

4.5 Montage der UHF-Datenträger (nicht im Lieferumfang enthalten)

Für Details zur Montage der Datenträger siehe Datenblatt der verwendeten Datenträger.

Bei der Montage von Datenträgern ist zu beachten, dass elektromagnetisch wirksame Materialien in der nahen Umgebung des Datenträgers die maximale Reichweite des RFID-Systems reduzieren bzw. das Erfassen von Datenträgern erschweren können. Dies gilt zum Beispiel bei der Montage von Datenträgern auf metallischen Oberflächen oder Behältern mit elektromagnetisch wirksamem Inhalt (z. B. Metall, Flüssigkeiten,...).

Ob die Montage auf metallischen Oberflächen zulässig ist, kann dem Datenblatt des Datenträgers entnommen werden. Gegebenenfalls sind geeignete Abstandshalter zu verwenden.

Auch eine hohe Datenträgerdichte erschwert das Identifizieren, z. B. wenn die Datenträger nur einen geringen Abstand zueinander haben oder sich überdecken.

5

Technische Daten

5.1 Abmessungen

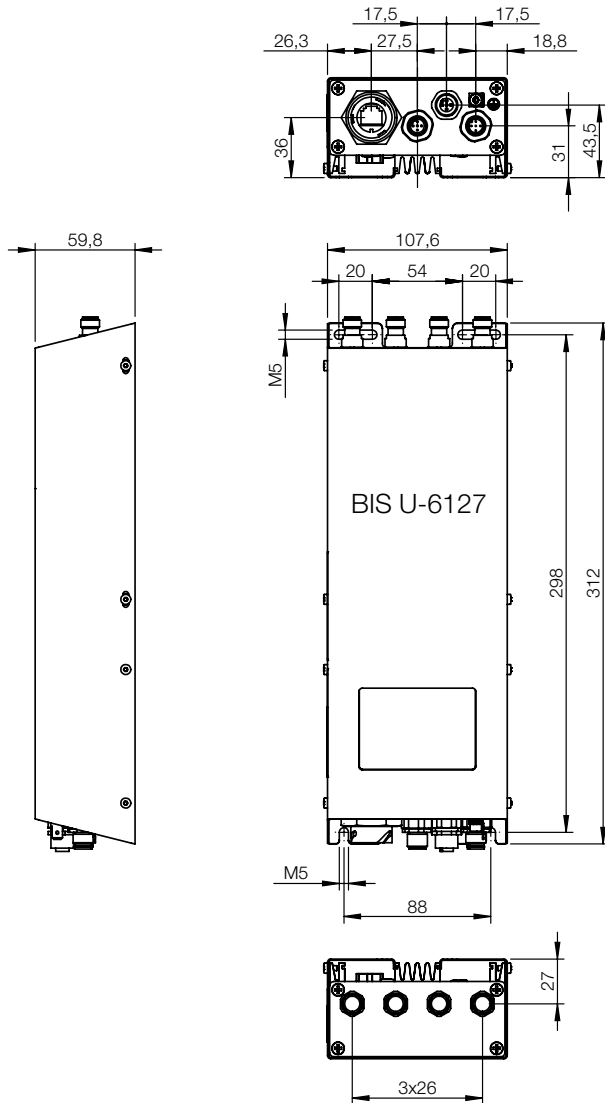


Bild 5-1: Abmessungen (mm)

5.2 Mechanische Daten

Gehäusematerial	Stahl beschichtet, Aluminium eloxiert
Abmessungen (L x B x H)	312 x 108 x 60 mm
Produktgewicht	ca. 2050 g
X1 Power	Einbaustecker M12, 5-polig, A-codiert
X2 IO-Link	Einbaubuchse M12, 5-polig, A-codiert
X3 Service	Einbaustecker M12, 5-polig, B-codiert
X4 Ethernet TCP/IP	Einbaubuchse RJ-45, 8-polig
1...4 Antennenports	Einbaustecker TNC-R

5.3 Elektrische Daten

Spannungsversorgung VS	+24 V DC $\pm 20\%$ (LPS Class 2)
Restwelligkeit	5 %
Stromaufnahme ohne Last	1 A
Maximale Stromaufnahme	3 A
Schnittstellen	Ethernet TCP/IP / OPC UA IO-Link-Master USB (Service)



Die Auswerteeinheit und angeschlossenes Zubehör darf nur mit begrenzter Energie versorgt werden, entsprechend UL 61010-1 Third Edition, Sub. Clauses 9.4 oder LPS entsprechend UL 60950-1 oder Class 2 entsprechend UL 1310 oder UL 1585.

ACHTUNG

Überschreiten der maximalen Stromaufnahme

Bei Überschreiten der maximalen Stromaufnahme kann es zu Schäden an der Auswerteeinheit und an angeschlossenen Systemkomponenten kommen.

- Beim Betrieb darauf achten, dass der Gesamtstrom, der über den Anschluss Power geführt wird, 3 A nicht übersteigt.
- Der Spannungsausgang (L+) am IO-Link-Port sowie digitale Ausgänge (E/A) werden über den Anschluss Power versorgt. Die Summe der Teilströme dieser Pins, darf einen maximalen Strom von 2 A nicht übersteigen.

5

Technische Daten (Fortsetzung)

5.4 Umgebungsbedingungen

Betriebstemperatur	–20...+55 °C
Lagertemperatur	–20...+60 °C
Schwing/Schock	EN 60068 Teil 2-6/27
Schutzart nach IEC 60529	IP65

5.5 Anschlüsse ANT1...ANT4

Wellenwiderstand	50 Ohm
Ausgangsleistung max.	1,4 W (31,5 dBm) oder 1 W (30 dBm), je nach Län- dervariante

5.6 Anschluss IO-Link

IO-Link Revision	1.1
Spannungsversorgung für IO-Link, E/A-Module (Ausgang)	VS – VD (VD = 0,5...3 V, lastabhängig) 1,7 A max. (abgesichert durch Überstromabschaltung)
Datenrate (IO-Link)	
COM1	4,8 kBit/s
COM2	38,4 kBit/s
COM3	230,4 kBit/s
Pin 2/Pin 4 (E/A-Modus) Eingang/Ausgang	VS – VD (VD = 0,5 V...3 V, lastabhängig) 2 A max.
Pin 4 (IO-Link-Modus)	C/Q IO-Link-Datenübertra- gung
Kabeltyp	Ungeschirmt, 4-adrig ¹⁾
Kabellänge max.	20 m (im IO-Link-Modus)

¹⁾ bei Einsatz von IO-Link-RFID-Schreibköpfen/-Leseköpfen in elektroma-
gnetisch gestörter Umgebung wird die Verwendung von geschirmten
Leitungen empfohlen.

ACHTUNG

Überschreiten der maximalen Stromaufnahme

Bei Überschreiten der maximalen Stromaufnahme kann es zu Schäden an der Auswerteeinheit und an ange-
schlossenen Systemkomponenten kommen.

- ▶ Beim Betrieb darauf achten, dass der Gesamtstrom, der über den Anschluss Power geführt wird, 3 A nicht übersteigt.
- ▶ Der Spannungsausgang (L+) am IO-Link-Port sowie digitale Ausgänge (E/A) werden über den Anschluss Power versorgt. Die Summe der Teilströme dieser Pins, darf einen maximalen Strom von 2 A nicht übersteigen.

5.7 Anschluss Ethernet TCP/IP

Ethernet-Standards nach IEEE 802.3-2008 (bis 1 Gigabit)	10BASE-T 100BASE-TX 1000BASE-T
Protokoll	TCP/IP OPC UA
Datenrate max.	10/100/1000 Mbit/s
Kabeltypen	CAT3 (nur 10BASE-T) CAT5
Kabellänge max.	100 m



Bei der Datenübertragung über größere Stre-
cken wird der Einsatz von Repeatern empfoh-
len.

5.8 Anschluss Service (USB)

USB-Version	2.0
Datenrate max.	480 Mbit/s
Kabeltyp	Geschirmt, 5-adrig
Kabellänge max.	5 m

5.9 Datenträger

ISO	18000-63
EPCglobal™	Class-1 Generation-2
Multitagging (maximale Anzahl der Datenträger)	500

5.10 Anzeigeelemente im Überblick

RF active	Blau
Tag Present	Gelb
Power/Status	Rot, Gelb, Grün
User	Rot, Gelb, Grün
Antenne 1...Antenne 4	Gelb
Link	Grün
Activity	Gelb
IO-Link 0	Rot, Gelb, Grün
IO-Link 1	Rot, Gelb



Für eine detaillierte Beschreibung der Anzeigeelemente siehe Kapitel 3.8 auf Seite 12.

5

Technische Daten (Fortsetzung)

5.11 Uhrzeit und Datum

Pufferung der Uhrzeit bei Stromausfall	> 2 Tage (bei voll aufgeladenem Speicherkondensator)
Ladezeit Speicherkondensator	8 h
Automatische Systemzeit	Network Time Protokoll Version 4

6.1 Allgemeine Einsatzbedingungen

Das BIS U-6127 kann an vielen Orten zum Einsatz kommen. Durch das IP65-Gehäuse und den Umgebungstemperaturbereich von $-20 \dots +55 \text{ }^{\circ}\text{C}$ ist es robust gegenüber Umwelteinflüssen konzipiert.

Details zur Montage und zur Planung des Montageorts siehe Kapitel 4 auf Seite 15.

6.2 Antennenkonfigurationen

Am Gerät BIS U-6127 können bis zu vier Antennen angeschlossen werden (Montage der Antennen siehe Kapitel 4.4 auf Seite 17).

Die vier Antennen können beliebig auf einzelne Erfassungsbereiche aufgeteilt werden und diese einzeln bedienen oder sie können in Kombination betrieben werden. Z. B. kann Antenne 1 eine Position auf einem Förderband vor der Verarbeitung überwachen, Antenne 2 eine weitere Position nach der Verarbeitung und die Antennen 3 und 4 überwachen gemeinsam eine Tordurchfahrt.

Bei der Ausrichtung der Antennen muss vor allem das Einsatzumfeld betrachtet werden. Der Erfassungsbereich, in dem sich Datenträger befinden, muss zu Beginn genau definiert sein. Anschließend müssen die Antennen so angebracht werden, dass eine möglichst gute *Ausleuchtung* des Erfassungsbereichs mit den Antennenkeulen gewährleistet ist.



Ist der gewünschte Erfassungsbereich klein und genau definiert (z. B. ein Bereich von $30 \times 30 \times 30 \text{ cm}$), kann *eine* Antenne ausreichend sein.

Soll eine Tordurchfahrt (Gate-Anwendung) mit variierenden Datenträgerpositionen erfasst werden, sind mehrere Antennen notwendig.

Nach Möglichkeit sind metallische Strukturen im Erfassungsbereich oder in unmittelbarer Nähe zu vermeiden. Metallflächen schatten die dahinterliegende Region ab. Ebene Metallflächen können durch Reflexion die Strahlrichtung der Funkwellen ändern und durch Überlagerung zu Auslöschungen oder Überreichweiten führen.

Die Antennenkeulen dürfen bzw. sollen sich überschneiden, um keine *Löcher* im Erfassungsbereich entstehen zu lassen. Kommen mehrere Antennen zum Einsatz, spielt es keine Rolle, ob diese nebeneinander, im Winkel oder gegenüberstehend angeordnet werden. Der einzige Fokus der Antennen muss auf dem Erfassungsbereich liegen.

Mit der Sendeleistung kann die Reichweite der Antenne gesteuert werden. Die Reichweiten sind auch abhängig vom Typ der verwendeten Datenträger. Die maximalen Lesereichweiten sind in der Regel deutlich größer als die maximalen Reichweiten beim Schreiben auf Datenträger. Zum Teil kann das durch die Angabe eines Write-Add-Ons (gezielte Erhöhung der Leistung) in den Parametereinstellungen ausgeglichen werden.

Ein weiterer Punkt bei der Antennenkonfiguration ist die Bewegungsgeschwindigkeit der Datenträger. Muss nur der EPC eines Datenträgers erkannt und müssen keine weiteren Daten auf dem Tag gelesen und geschrieben werden, dann kann der Erfassungsbereich in Bewegungsrichtung kleiner gewählt werden, da der Vorgang in kürzerer Zeit möglich ist.

Bewegen sich Datenträger relativ schnell durch das Antennenfeld und müssen weiteren Daten auf dem Tag gelesen oder geschrieben werden, müssen die Antennen so angeordnet werden, dass sich die Datenträger möglichst lange im Antennenfeld aufhalten, um z. B. die Daten vollständig auf die Datenträger zu schreiben.

Die Antenneneinstellungen können auf unterschiedliche Weise parametrisiert werden:

- im UHF Manager
- auf dem Webserver des Geräts
- über den 007-Befehlssatz
- über die OPC-UA-Kommandos

Für weitere Informationen siehe Kapitel 7.3 auf Seite 49.

6.3 Datenträgerauswahl

Korrekt ausgewählte Datenträger tragen einen großen Teil zum Erfolg der Applikation bei. Bei der Auswahl von Datenträgern sind folgende Faktoren zu berücksichtigen:

1. Speichergöße

Muss bei dieser Applikation nur der EPC gelesen werden, sind Datenträger mit kleiner Speichergöße (User Memory) ausreichend. Müssen jedoch mehrere Prozessdaten auf einen Datenträger geschrieben werden, muss die Mindestspeichergöße eines Datenträgers definiert werden.

2. Umgebungsbedingungen

Das Umfeld des Datenträgers spielt eine entscheidende Rolle für die Funktion der gesamten Applikation. Ist weder Feuchte noch mechanische Beanspruchung relevant, können preisgünstige *Label*-Datenträger verwendet werden. Wird der Datenträger mit Feuchtigkeit in Berührung kommen, muss ein Datenträger der Schutzart IP67 (oder höher) verwendet werden. Hauptunterscheidung bei den Datenträgern stellt allerdings das Medium dar, auf dem der Datenträger montiert wird. Müssen Datenträger auf Metall angebracht werden, muss der Einsatz von *On-Metal Tags* geprüft werden (siehe Kapitel 4.5 auf Seite 17).



On-Metal Tags haben generell eine schlechtere UHF-Performance (vor allem in der Schreib-/Lesereichweite) als vergleichbare Standard-Datenträger.

Jede UHF-Applikation muss so konfiguriert werden, dass die Datenträger prozesssicher erkannt werden. Dies betrifft besonders die Anordnung der Antennen und die Position der Datenträger auf den zu erfassenden Waren.

3. Schreib-/Lesereichweite

Ein entscheidender Faktor bei der UHF-Applikationsplanung ist der Schreib-/Leseabstand, d. h. der Abstand zwischen Datenträger und Antenne.

i Da große Datenträger eine größere Empfangsantenne in Ihrem Gehäuse unterbringen können und somit mehr elektrische Energie aus dem elektromagnetischen Feld entnehmen können, ist auch ihre Reichweite größer als die von kleinen Datenträgern (bei vergleichbaren übrigen Parametern).

Bei jeder Applikation muss die Auswahl des Datenträgers sorgfältig auf die Umgebungsbedingungen abgestimmt sein. Die Konfiguration des Gesamtsystems sollte immer auf maximale Prozesssicherheit ausgelegt sein.

i Passende Datenträger für eine Vielzahl von Applikationen finden Sie unter www.balluff.com.

6.4 UHF-Eigenschaften in der Praxis

Orientierung Datenträger zur Antenne (Polarisation)

Balluff bietet eine Vielzahl von Antennen für das BIS U-6127-Gerät an. Die angebotenen Antennen unterscheiden sich nicht nur in ihrer Größe, Reichweite und Frequenzband (FCC oder ETSI) sondern auch in Ihrer Polarisation.

Es gibt linear- und zirkularpolarisierte Antennen. Bei zirkularpolarisierten Antennen spielt es keine Rolle, ob der Datenträger horizontal oder vertikal zur Antenne ausgerichtet ist. Der Datenträger wird in allen Ausrichtungen erkannt.

Bei linearpolarisierten Antennen muss der Datenträger identisch zur Antenne ausgerichtet sein – horizontal oder vertikal (die Ausrichtung der Antenne ist auf dem Antennengehäuse gekennzeichnet). Ein Vorteil der linearpolarisierten Antennen ist die zielgenauere Erfassung. Sie können verwendet werden, wenn die Lage der Datenträger genau definiert ist.

Feldstärke und Abstand

Die Abnahme der elektrischen Feldstärke verläuft in der Theorie umgekehrt proportional zum Abstand von der Antenne ($1/x$). Ein Datenträger benötigt eine typische Mindestfeldstärke, um erkannt zu werden. Bis zur Unterschreitung dieser Mindestfeldstärke kann der Datenträger erkannt werden, bei größerem Abstand nicht mehr. Dieses Verhalten kann aber nur in homogenen Laborumgebungen verlässlich nachgestellt werden.

In der Praxis werden die emittierten elektromagnetischen Wellen der Antenne an verschiedenen Gegenständen im Raum reflektiert. In verschiedenen Abständen zur Antenne können durch Überlagerung mehrerer Wellen lokale Maxima oder Minima der Feldstärke entstehen. Die Feldstärke als Funktion des Abstands ist nicht mehr stetig abnehmend.

Das hat folgende Auswirkung:

Entfernt man den Datenträger von der Antenne, wird der Datenträger ab einem bestimmten Abstand nicht mehr erkannt. Bewegt man den Datenträger noch etwas weiter weg von der Antenne, kann der Datenträger plötzlich erneut erkannt werden. Diese *Löcher* im Grenzabstand sind auf das inhomogene elektromagnetische Feld zurückzuführen. Daher sollte ein Betrieb der UHF-Anlage im Grenzabstand vermieden werden.

Weiterhin gilt:

Eine Verdoppelung der Reichweite erfordert in etwa eine vierfache Sendeleistung. In der Einheit dBm bedeutet das, dass die Sendeleistung um 6 dBm höher eingestellt werden muss. Auch die Empfangsrichtung der Welle vom Tag zur Antenne kann an Grenzen geraten, was jedoch nicht nachgeregelt werden kann.

Durchdringung Elektromagnetische Welle

Ein Vorteil von UHF-RFID-Anlagen im Gegensatz zu optischen Lesegeräten ist die Durchdringung von undurchsichtigen Materialien. Die elektromagnetischen Wellen des UHF-Spektrums durchdringen Papier und Karton ohne nennenswerte Verluste. Ebenfalls können die meisten Kunststoffe durchdrungen werden, um die dahinter liegenden Datenträger zu lesen oder zu beschreiben.

Der Durchdringung der UHF-Wellen wird durch die Physik eine natürliche Grenze gesetzt. Ist die Absorption oder die Reflexion der UHF-Wellen zu groß, kann das entsprechende Medium nicht durchdrungen werden. Dies kommt vor allem bei leitenden Materialien wie Stahlblechen oder Aluminiumplatten vor. Befindet sich ein Datenträger hinter einer Stahlplatte ist dieser für das BIS U-6127-Gerät nicht erreichbar. Man spricht in diesem Fall auch von Abschattung eines Datenträgers.

Zwischen totaler Abschattung und freier Sichtbarkeit zwischen Antenne und Datenträger gibt es noch zahlreiche Zwischenstadien, in der die Durchdringung von Medien nur eingeschränkt gegeben ist.

Ein Beispiel hierfür sind ESD-Behälter. Kunststoffbehälter, die leicht leitfähig sind, um eine elektrostatische Aufladung zu unterbinden. Datenträger sind in diesen Behältern nur eingeschränkt sichtbar für die Antenne. Hier müssen in der Applikationsplanung Tests durchgeführt werden.

Ein zweites Beispiel für die erschwerte Durchdringung der elektromagnetischen Wellen ist Feuchtigkeit. Wasser ist je nach Reinheit leitfähig und absorbiert durch seine polare Struktur sehr stark UHF-Wellen. Andere Flüssigkeiten verhalten sich unterschiedlich, der Bereich variiert von nahezu neutral bis hin zu kompletter Abschattung.

Mit diesem Hintergrundwissen sollte man in jede Applikationsplanung gehen, z. B. bei Anwendungen, die Güter erkennen soll, die der Witterung ausgesetzt wurden. Nasse Kartonagen können das Lesen und Schreiben der innenliegenden Datenträger deutlich erschweren. Die Sendeleistung des BIS U-6127 sollte bei solchen Applikationen nicht grenzwertig niedrig eingestellt werden. Eine gewisse Sendeleistungsreserve sollte eingerechnet werden.

Zum Einrichten der anfänglichen Sendeleistung kann die Funktion *AutoSetup* verwendet werden.

SingleTag- oder MultiTag-Betrieb

Es gibt drei Zustände, die sich im Erfassungsbereich vor der Antenne abspielen können:

- kein Datenträger
- ein Datenträger
- mehrere Datenträger

Die vorhandenen Datenträger im Erfassungsbereich werden bei einem *Inventory* (z. B. *Scan*-Befehl) erkannt, in eine Tagliste eingetragen und ggf. an die Anwendung übermittelt.

Befindet sich nur ein einziger Datenträger im Erfassungsbereich der Antenne, kann sofort begonnen werden, auf den Datenträger Daten zu schreiben oder zu lesen. Diesen Betriebszustand nennt man *SingleTag-Betrieb*.

Befinden sich mehrere Datenträger im Erfassungsbereich der Antenne, muss die Tagliste ausgewertet werden. Bevor auf einen Datenträger Daten geschrieben oder vom Datenträger gelesen werden kann, muss ein Datenträger ausgewählt werden (*Select*-Befehl). Erst nach der Auswahl des Datenträgers, können Daten gelesen oder geschrieben werden.

Eine Ausnahme bilden *BulkRead*- und *BulkWrite*-Befehle, die alle diese Schritte für jeden einzelnen Tag durchführen sowie die Befehle *ReadMultipleTagDataFormatted* bzw. *UniversalTagList*.

Zugriffszeit auf einen Datenträger



Mit der hier beschriebenen Zugriffszeit wird die Zeitdauer bezeichnet, die während des Ausführens eines *Inventory*-Befehls abläuft.

Die vergehende Zeitspanne bis der BIS U-6127 auf Datenträger zugreifen kann, hängt vor allem von zwei Faktoren ab:

1. Verwendet man eine schnelle Codierung Miller 2 (RX: 320/160 kbps; TX: 80 kbps), ist die Zugriffszeit um ca. 29 % kürzer als mit der Standardcodierung Miller 4 (RX: 160/40 kbps; TX: 40 kbps). Allerdings nimmt die Zuverlässigkeit ab und zudem sind schnelle Codierungen nicht in allen Ländern zugelassen.
2. Entscheidender ist die Anzahl der Datenträger im Erfassungsbereich der Antenne. Befindet sich nur ein Datenträger vor der Antenne, ist die Zeitdauer eines *Inventory*-Befehls am kürzesten. Befinden sich z. B. 10 Datenträger im Erfassungsbereich kann die Zugriffszeit doppelt so lange dauern.

Typische Zugriffszeiten auf Datenträger (Standardeinstellung: RX: 160/40 kbps; TX: 40 kbps) zeigt nachfolgende Tabelle. Die angegebenen Zeiten sind beispielhaft und variieren statistisch. Sie hängen zudem von anderen Einstellungen, insbesondere dem initialen *Q-Wert* ab.

Anzahl Datenträger	Gemessene Zeitdauer, bis ein <i>Inventory</i> -Befehl abgearbeitet ist [ms]
1	109
3	129
7	180
10	219
20	371
31	508
52	891
71	1273
87	1590
100	1879
111	2168
119	2352

Pulk-Applikation

Sollen bei einem *Scan* mehrere Datenträger sicher erkannt werden, muss die Antennenleistung im Vergleich zum Lesen von einzelnen Datenträgern erhöht werden. Dies funktioniert auch dann, wenn sich die Datenträger mit geringer Geschwindigkeit bewegen.

Mit einer geschickten Antennenanordnung und der Auswertung mehrerer *Scans* ist es möglich, in einer Pulk-Applikation alle Datenträger zu erkennen.

Mit Verwendung des *Loop*-Filters (siehe Seite 25) kann die Zuverlässigkeit einer Applikation deutlich erhöht werden.

6.5 Betriebsarten

Die Auswerteeinheit BIS U-6127 unterstützt mehrere Betriebsarten, um eine optimale Einbindung in Ihre Steuerungs- oder IT-Umgebung herzustellen:

- Synchroner Betrieb
- Asynchroner Betrieb (mit *Loop*-Filter)
- Synchroner Betrieb mit *Loop*-Filter, *Live*- oder *Kumuliert*-Modus
- Autonomer Betrieb

Die Betriebsarten beziehen sich auf das Erfassen von einzelnen oder multiplen Datenträgern und das Auslesen von Daten. Sie unterscheiden sich darin, wie viel automatische Vorverarbeitung das Gerät durchführen soll und ob die gelesenen Daten der Datenträger vom Gerät abgerufen werden oder unaufgefordert bereitgestellt werden sollen.

Das Schreiben von Daten auf Datenträger erfolgt immer im synchronen Betrieb.

6

Applikationsplanung (Fortsetzung)

Synchroner Betrieb

Diese Betriebsart ermöglicht die direkte Kontrolle, wann und welche Aktionen auf der Luftschnittstelle mit den Datenträgern durchgeführt werden. Eine Suche nach Datenträgern oder ein Lesebefehl werden dann gestartet, wenn ein entsprechendes Kommando über 007 gesendet wird oder eine OPC-UA-Methode aufgerufen wird. Die gelesenen Daten werden dem steuernden Gerät nach erfolgreicher Abarbeitung unmittelbar zur Verfügung gestellt.

Befehle für synchronen Betrieb:

Befehl	007-Protokoll	OPC UA
Datenträger erfassen	<i>GetMultipleTags</i> -Kommando <i>GetMultipleTagsExtended</i> -Kommando	<i>Scan()</i> -Methode
Einzelnen Datenträger lesen	<i>Read</i> -Kommando <i>ExtendedRead</i> -Kommando	<i>ReadTag()</i> -Methode
Datenträger erfassen und beliebige Daten lesen, benutzerdefinierte Ausgabe	<i>UniversalTagList</i> -Kommando	<i>ReadMultipleTagDataFormatted()</i> -Methode
Einzelnen Datenträger lesen, benutzerdefinierte Ausgabe	<i>UniversalTagRead</i> -Kommando	<i>ReadFormattedTagData()</i> -Methode

Die Parameter und Rückgabewerte der Kommandos und Methoden sind bei den jeweiligen Befehlsbeschreibungen zu finden.

i Wenn mehrere Kommandos über verschiedenen Schnittstellen gleichzeitig angefordert werden, können Verzögerungen in der Befehlsausführung entstehen. Das Gerät wird diese nacheinander abarbeiten.

i Die Funktionen zur Suche von UHF-Datenträgern nutzen statistische Methoden. Die Verarbeitungsgeschwindigkeit der Befehle ist bei UHF-Datenträgern daher nicht immer exakt kalkulierbar und kann von Ausführung zu Ausführung schwanken.

Asynchroner Betrieb

In dieser Betriebsart sucht das Gerät in einstellbaren Abständen selbstständig nach Datenträgern. Werden neue Datenträger gefunden, wird ein *Event* erzeugt, d. h. das steuernde Gerät wird ohne weitere Aktionen mit einer Nachricht informiert:

- 007: mit einem spontanen Telegramm
- OPC UA: mit dem Auslösen eines Events

Befehle für asynchronen Betrieb:

Befehl	007-Protokoll	OPC UA
Datenträgererfassung starten	Parameters 1006 _{hex} auf den Wert 3 (wenn nur <i>Tag kommt</i> -Meldungen gewünscht werden) oder auf den Wert 7 (wenn sowohl <i>Tag kommt</i> als auch <i>Tag geht</i> signalisiert werden soll) setzen.	<i>ScanStart()</i> -Methode
Datenträgererfassung beenden	<i>Abort</i> -Kommando oder Parameter 1006 _{hex} auf den Wert 0 setzen.	<i>ScanStop()</i> -Methode
Benachrichtigung über neue Datenträger	<i>Tag kommt</i> -Telegramm	<i>RfidScanEvent-Type</i> -Event
Benachrichtigung über nicht mehr gefundene Datenträger	<i>Tag geht</i> -Telegramm (optional)	nicht möglich
Scan-Zykluszeit (Pause zwischen 2 Scans), globaler Parameter	Parameter 100C _{hex} (Wertebereich 1...255 = 10 ms...2,55 s)	Parameter 100C _{hex} (Wertebereich 1...255 = 10 ms...2,55 s) über UHF-Manager <i>Asynchronous Scan Loop Time</i>

Die Parameter und Rückgabewerte der Kommandos und Methoden sind bei den jeweiligen Befehlsbeschreibungen zu finden.

i Im asynchronen Betrieb ist das Loop-Filter (siehe Kapitel *Loop Filter* auf Seite 25) mit seinen Parametern immer wirksam.

i Der asynchrone Betrieb ist nach einem Gerätereustart inaktiv.

6

Applikationsplanung (Fortsetzung)

Loop Filter

Das Loop-Filter ermöglicht, die Liste der gefundenen Datenträger zu stabilisieren, indem mehrere Lesungen kombiniert werden. So können Fehllesungen korrigiert oder die Ergebnisse mehrerer Suchvorgänge in einer Liste zusammengefasst werden.

Das Loop-Filter legt folgende Parameter fest:

- *Mindestanzahl der erfolgreichen Lesungen*: wie oft ein Tag hintereinander erfolgreich erfasst oder gelesen werden muss, damit er an das steuernde Gerät als erfasst/gelesen gemeldet wird.

- *Anzahl der Nichtlesungen*: wie oft ein Tag hintereinander erfolglos gesucht werden muss, bevor er an das steuernde Gerät als nicht mehr vorhanden gemeldet wird.
- *Wartezeit*: die Zeitdauer, die ein Tag, nachdem er aus dem Lesefeld der Antennen verschwunden ist, ignoriert wird, bevor eine erneute Erfassung des Tags gemeldet werden kann (sofern die Bedingung *Mindestanzahl der erfolgreichen Lesungen* erfüllt ist).

Bild 6-1 veranschaulicht die Wirkungsweise des Filters:

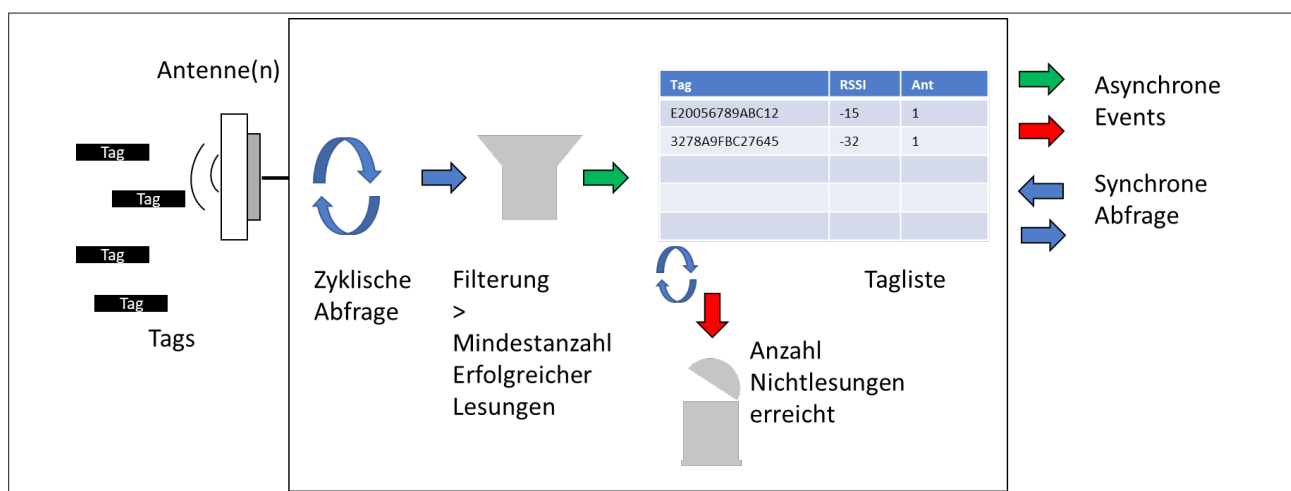


Bild 6-1: Wirkungsweise Loop-Filter

Die Parameter des Loop-Filters können für die aktuelle Verbindung wie folgt gesetzt werden:

Parameter	007-Protokoll	OPC UA
Parameter <i>Mindestanzahl der erfolgreichen Lesungen</i>	Parameter 100C _{hex} (Wertebereich 1...255 Scans)	SetASyncFilter() – Methode ¹⁾
Parameter <i>Anzahl der Nichtlesungen</i>	Parameter 100D _{hex} (Wertebereich 1...255 Scans)	SetASyncFilter() – Methode ¹⁾
Parameter <i>Wartezeit</i>	Parameter 100E _{hex} (Wertebereich 0...1000 s)	SetASyncFilter() – Methode ¹⁾
Scan-Zykluszeit (Pause zwischen 2 Scans), globaler Parameter	Parameter 100C _{hex} (Wertebereich 1...255 = 10 ms...2,55 s)	Parameter 100C _{hex} (Wertebereich 1...255 = 10 ms...2,55 s) über UHF-Manager <i>Asynchronous Scan Loop Time</i>

¹⁾ Zum Auslesen der eingestellten Parameter kann die *GetASyncFilter()*-Methode verwendet werden.

Die Parameter 0023_{hex}, 0024_{hex} und 0029_{hex} legen die jeweiligen Default-Werte für neue Verbindungen sowohl für 007 als auch OPC UA fest. Die Defaults können auch über den UHF-Manager eingestellt werden.



Das Loop-Filter und der asynchrone Betrieb unterstützen derzeit nur Datenträgererfassungen mit EPC-Ausgabe. Das Scannen mit Ausgabe von TID-Werten in Kombination mit dem Loop-Filter oder im Asynchron-Erkennen-Modus wird derzeit nicht unterstützt.

6

Applikationsplanung (Fortsetzung)

Loop-Filter im asynchronen Betrieb

Im asynchronen Betrieb ist das Loop-Filter unmittelbar aktiv. Ein Event für einen neuen Tag wird dann ausgelöst, wenn die Bedingung *Mindestanzahl der erfolgreichen Lesungen* erfüllt ist. Ein Event für einen nicht mehr gefundenen Tag wird erst ausgelöst, wenn die *Anzahl der Nichtlesungen* überschritten wird.

Loop-Filter im synchronen Betrieb

Im synchronen Betrieb kann das Loop-Filter wie folgt verwendet werden:

- **Live-Modus:** Scans und Filterbetrieb erfolgen im Hintergrund, Abfrage der momentanen Datenträgerliste (nach Filterung) über die normalen synchronen Kommandos. Der Modus eignet sich für laufend wiederholte Abfragen in kurzen Abständen.
- **Kumuliert-Modus:** Scans und Filterbetrieb erfolgen im Hintergrund, Abfrage aller neu gefundenen Datenträger (einschließlich solcher, die das Antennen-Lesefeld inzwischen wieder verlassen haben) über die normalen synchronen Kommandos. Der Modus eignet sich, um über getriggerte oder gelegentliche Abfragen eine vollständige Liste der Datenträger zu erhalten (z. B. in einer Gate-Anwendung).

Neben der eigentlichen Filterfunktion hat die Verbindung des Loop-Filters und des synchronen Betriebs folgende Vorteile:

- Die Antworten auf synchrone Kommandos und Methodenaufrufe erfolgen fast ohne Wartezeit, da die eigentliche Datenträgersuche davon unabhängig im Hintergrund läuft.
- Die Anwendung auf dem steuernden Gerät kann bestimmen, wann sie die Ergebnisse der Datenträgersuche abholen möchte, ohne dass die Gefahr besteht, Ergebnisse zu verlieren, da sie im Gerät gesammelt und zwischengespeichert (kumuliert) werden können.

Das Loop-Filter kann im synchronen Betrieb wie folgt genutzt werden:

Live-Modus

Befehl	007-Protokoll	OPC UA
Datenträgererfassung mit Loop-Filter starten, <i>Live-Modus</i>	Setzen des Parameters 1006 _{hex} auf den Wert 1	<i>ScanStart()</i> -Methode
Datenträgerliste auslesen <i>Live-Modus</i>	<i>GetMultipleTags</i> -Kommando <i>GetMultipleTagsExtended</i> -Kommando	<i>Scan()</i> -Methode
Datenträgerliste auslesen <i>Live-Modus</i> und beliebige Daten lesen, benutzerdefinierte Ausgabe	<i>UniversalTagList</i> -Kommando ¹	<i>ReadMultipleTagDataFormatted()</i> -Methode ¹
Momentane Anzahl Tags in der Datenträgerliste ausgeben	<i>GetTagCount</i> -Kommando	<i>Scan()</i> -Methode
Datenträgererfassung mit Loop-Filter beenden	<i>Abort</i> -Kommando oder Setzen des Parameters 1006 _{hex} auf den Wert 0.	<i>ScanStop()</i> -Methode

¹⁾ Die formatierte Ausgabe ist nur sinnvoll einsetzbar, wenn ausschließlich EPC-Daten und Statuswerte ausgegeben werden sollen, da Datenträger zum Zeitpunkt der Abfrage evtl. nicht mehr im Lesefeld der Antennen sind und weitere Daten dann nicht mehr zur Verfügung stehen und somit eine Ausgabe dann nicht erfolgt.

Kumuliert-Modus

Befehl	007-Protokoll	OPC UA
Datenträgererfassung mit Loop-Filter starten, <i>Kumuliert-Modus</i>	Setzen des Parameters 1006 _{hex} auf den Wert 9	Nicht möglich
Datenträgerliste auslesen <i>Kumuliert-Modus</i>	<i>GetMultipleTags</i> -Kommando <i>GetMultipleTagsExtended</i> -Kommando	Nicht möglich
Datenträgerliste auslesen <i>Kumuliert-Modus</i> und beliebige Daten lesen, benutzerdefinierte Ausgabe	<i>UniversalTagList</i> -Kommando ¹	Nicht möglich
Momentane Anzahl Tags in der Datenträgerliste ausgeben	<i>GetTagCount</i> -Kommando	<i>Scan()</i> -Methode
Datenträgererfassung mit Loop-Filter beenden	<i>Abort</i> -Kommando oder Setzen des Parameters 1006 _{hex} auf den Wert 0.	<i>ScanStop()</i> -Methode

¹⁾ Die formatierte Ausgabe ist nur sinnvoll einsetzbar, wenn ausschließlich EPC-Daten und Statuswerte ausgegeben werden sollen, da Datenträger zum Zeitpunkt der Abfrage evtl. nicht mehr im Lesefeld der Antennen sind und weitere Daten dann nicht mehr zur Verfügung stehen und somit eine Ausgabe dann nicht erfolgt.

6

Applikationsplanung (Fortsetzung)

Autonomer Betrieb

Im autonomen Betrieb führt das Gerät zyklische Datenträgererfassungen durch, ohne dass ein Kommando abgesetzt werden muss.

Diese Betriebsart eignet sich insbesondere für Anwendungen, die ohne zusätzliches steuerndes System auskommen sollen oder nur selten einzelne Datenträger erfassen sollen.

Befehl	007-Protokoll	OPC UA
Autonomen Betrieb starten	Den Parameter 000F _{hex} auf einen Wert zwischen 1 und 255 setzen, um das Scanintervall im Bereich 10 ms...2,55 s einzustellen. Diese Einstellung und der autonome Betrieb bleiben über einen Geräteeinstart hinaus erhalten und beziehen sich auf den TCP-Kanal, von dem aus der Betrieb gestartet wurde.	Aufruf der <i>SetAutoScan()</i> -Methode mit einem Wert zwischen 1 und 65535, um das Scanintervall im Bereich 1 ms...65 s einzustellen. Diese Einstellung und der autonome Betrieb bleiben über einen Geräteeinstart hinaus nicht erhalten.
Autonomen Betrieb beenden	Parameter 000F _{hex} auf den Wert 0 setzen.	Aufruf der <i>SetAutoScan()</i> -Methode mit einem Wert 0.
Scan-Daten erhalten	<i>USB-Service-Schnittstelle:</i> Keine Datenausgabe <i>Ethernet-Schnittstelle:</i> Die Ausgabe der Daten erfolgt immer auf einem separaten TCP-Kanal, abhängig vom 007-TCP-Kanal über den der Betrieb gestartet wurde. Das Verhalten entspricht einem zyklisch ausgeführten Kommando. <i>Befehlskennung '-L': Datenträger erfassen, universal</i> (siehe Seite 122) ohne Acknowledges. Die Parameter für Kopf(Antennen)-Auswahl und maximaler Taganzahl entsprechen dem zuletzt ausgeführten Kommando <i>UniversalTagList</i> . Wurde seit dem Gerätestart kein solches Kommando ausgeführt gelten folgende Defaultwerte: Head = 0 (alle aktiven Antennen) Max. Anzahl Tags = nur durch Gerät begrenzt	Keine selbsttätige Datenausgabe. Die Variable <i>LastScanData</i> zeigt die Daten eines Datenträgers an, wenn mindestens einer gefunden wurde. Die Variable <i>LastScanData</i> wird von allen OPC-UA-Sessions gemeinsam genutzt. Sind mehrere Sessions gleichzeitig aktiv, empfiehlt sich der Einsatz der Methode <i>GetLastScanData()</i> , die sessionbezogene Daten liefert. Wird eine selbsttätige Datenausgabe unter OPC UA erwünscht, empfiehlt sich der asynchronen Betrieb.



Der autonome Betrieb mit 007 ermöglicht, dass das Gerät ohne weitere Einwirkung von außen direkt nach dem Einschalten Datenträger zyklisch erfasst und die Ergebnisse selbsttätig an ein externes System über TCP meldet.

6

Applikationsplanung (Fortsetzung)

Betriebsart	Gerät scannt selbsttätig nach Tags	Verwendbar mit			Formatiertes Lesen nutzbar	2. Kanal möglich (007, formatiert)	2. Kanal benötigt
		007-Protokoll	OPC UA	Weboberfläche			
Synchron	–	+	+	+	+	+	–
Asynchron (incl. Loop-Filter)	+	+	+	–	–	–	–
Synchron + Loop-Filter, Live	+	+	+	–	+ ⁵⁾	+	–
Synchron + Loop-Filter, Kumuliert	+	+ ¹⁾	–	–	+ ⁵⁾	+	–
Autonomer Betrieb	+	+ ^{2), 3)}	+ ⁴⁾	–	+	+	+

¹⁾ Der Kumuliert-Modus kann über das Protokoll, aber nicht über den UHF-Manager eingestellt werden.

²⁾ Der UHF-Manager kann den autonomen Betrieb starten oder beenden. Er kann die Ausgaben des autonomen Betriebs aber nicht anzeigen, da sie auf einem 2. Kanal erfolgen.

³⁾ Falls im autonomen Betrieb ein Loop-Filter benötigt wird, muss es nach jedem Geräteneustart neu aktiviert werden, und der autonome Betrieb neu aktiviert werden.

⁴⁾ Bei OPC UA muss der autonome Betrieb nach jedem Geräteneustart neu aktiviert werden.

⁵⁾ Wenn das Loop-Filter aktiv ist, können in formatierter Ausgabe keine Werte aus dem TID, dem Passwort oder dem User-Daten-Bereich ausgegeben werden. Es können nur Daten aus der EPC-Bank (EPC, Protokollkontrollwort) und Statuswerte ausgegeben werden.

7.1 Konfigurationssoftware UHF-Manager

Die Konfigurationssoftware *Balluff UHF-Manager* bietet die Möglichkeit, das RFID-System vor dem Einbau auf einfache Weise in Betrieb zu nehmen, Grundfunktionen zu testen und Parametereinstellungen vorzunehmen.

7.1.1 Konfigurationssoftware installieren und starten



Die Konfigurationssoftware ist online unter **www.balluff.com** erhältlich. Für die Installation der Software können Administratorrechte erforderlich sein. Die Software wird unter dem voreingestellten Pfad installiert (sofern dieser nicht geändert wird):
C:\Program Files (x86)\Balluff\UHF Manager

1. Den Installationsassistenten durch Doppelklick auf die Installationsdatei (UhfManagerSetup_version.msi) starten und den Anweisungen des Assistenten folgen.
2. Mit Doppelklick auf die Datei *Balluff.Uhf.UhfManager.exe* im Installationsverzeichnis die Konfigurationssoftware starten.

7.1.2 Benutzeroberfläche

Nach dem Verbinden der Auswerteeinheit über TCP/IP bzw. USB (siehe Kapitel 7.1.3 auf Seite 30) wird das Hauptfenster wie folgt dargestellt (siehe Bild 7-1).

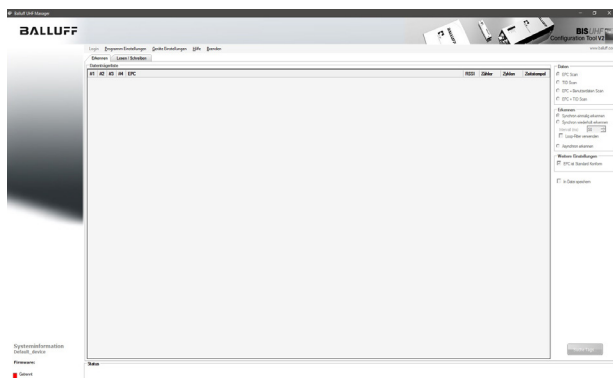


Bild 7-1: Hauptfenster

RFID Systeminformation

Im linken Fensterbereich wird die RFID-Systeminformation zu einer verbundenen BIS-Auswerteeinheit dargestellt. Diese zeigt eine schematische Darstellung der Auswerteeinheit und gibt Aufschluss über folgende Informationen:

- Typbezeichnung der verbundenen Auswerteeinheit
- Firmware-Version der Auswerteeinheit
- Verbindungsstatus der verwendeten Schnittstelle
- Aktuell ausgewählte Antenne über die Optionsflächen 1...4 bzw. ALL

Aktionsbereich

Der Aktionsbereich in der Fenstermitte zeigt die Daten der Datenträger, die im aktiven Feld der Antenne gefunden wurden und stellt die zur Interaktion mit einem Datenträger erforderlichen Bedienelemente zur Verfügung.

Statuszeile

In der Statuszeile unterhalb des Aktionsbereichs wird das Ergebnis der zuletzt ausgeführten Aktion dargestellt.



Informationen zur Bedienung des UHF-Managers bietet die Hilfefunktion. Diese kann über das Hilfe-Menü oder mit der F1-Taste aufgerufen werden.

Menü

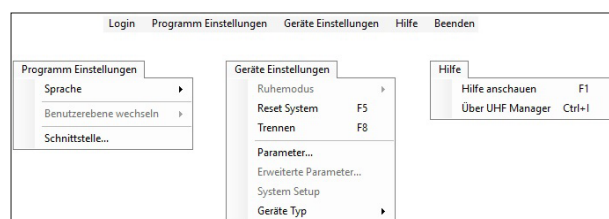


Bild 7-2: Menüdarstellung

Login/Logout

Die Auswerteeinheit BIS U-6127 verfügt über passwortgeschützte Sicherheitsebenen, die es verschiedenen Benutzergruppen erlauben, tiefergehende Einstellungen am Gerät vorzunehmen. Über *LOGIN/LOGOUT* können die Ebenen *USER/EXPERT/ADMIN* aktiviert bzw. deaktiviert werden. Höhere Sicherheitsebenen ermöglichen zusätzliche Einstellungen im Menüpunkt *GERÄTE EINSTELLUNGEN*.

Benutzer werden nach einer Zeit der Inaktivität von 15 Minuten automatisch aus dem System ausgeloggt und eine Neuanmeldung wird erforderlich. Spätestens nach 24 Stunden muss eine neue Anmeldung erfolgen.

Login (bei Auslieferung):

Sicherheits-ebene	Benutzername	Passwort
User	ohne	ohne
Admin (Standard)	admin_default	Siehe Typenschild auf dem Gerät



Benutzerrollen und Login-Daten können über Benutzerkonten verwaltet werden (siehe *Benutzerkonten* auf Seite 11 und *Benutzerverwaltung* auf Seite 45).

Wir empfehlen, folgende Benutzerrollen anzulegen:

Sicherheits-ebene	Benutzername	Passwort
Experte	expert	Frei festlegbar
Administrator	admin	Frei festlegbar

Programmeinstellungen

- *SPRACHE*
Umschalten der Menüsprache Deutsch/Englisch.
- *BENUTZEREbene WECHSELN*
Dieser Menüpunkt wurde beim BIS U-6127 durch den Login-Bereich abgelöst und dient nur der Kompatibilität zu anderen Auswerteeinheiten.
- *SCHNITTSTELLE...*
Öffnet das Fenster für die Schnittstelleneinstellungen RS232 / TCP/IP.

Geräteeinstellungen

- *RUHEMODUS*
Ist bei Verwendung der BIS U-Auswerteeinheit nicht verfügbar.
- *RESET SYSTEM* (Taste F5)
Veranlasst die BIS U-Auswerteeinheit, einen Neustart durchzuführen. Es ist ein vorheriges Login mit Administratorrechten erforderlich.
- *TRENNEN/VERBINDEN* (Taste F8)
Öffnet bzw. schließt die zuletzt verwendete Verbindung.
- *PARAMETER...*
Öffnet das Parameterfenster.
- *ERWEITERTE PARAMETER...*
Öffnet das Fenster für erweiterte Parameter (Bereich ist kennwortgeschützt, siehe Menüpunkt *Benutzerebene wechseln* auf Seite 30).
- *SYSTEM SETUP*
Bereich ist nur für Balluff Servicemitarbeiter zugänglich.
- *GERÄTE TYP*
Zeigt eine Liste der unterstützten Geräte und ermöglicht eine manuelle Auswahl. Je nach ausgewähltem Gerät verändert sich die Benutzeroberfläche.



Diese Funktion ist nur für den Offline-Modus vorgesehen. Der *GERÄTE TYP* wird beim Verbindungsaufbau automatisch gewählt.

Hilfe

- *HILFE ANSCHAUEN* (Taste F1)
Öffnet die Hilfefunktion für die Konfigurationssoftware
- *ÜBER UHF-MANAGER* (Taste Strg + I)
Öffnet das Fenster für die Benutzerinformation
 - Software-Version der Konfigurationssoftware
 - Kontaktdaten der Balluff GmbH

Beenden

Schließt die Konfigurationssoftware.

7.1.3 Schnittstelleneinstellungen

Über die *SCHNITTSTELLENEINSTELLUNGEN* kann die BIS U-Auswerteeinheit über eine TCP/IP-Verbindung mit einem Windows™-PC verbunden werden. Für Wartungs- bzw. Servicefunktionen steht auch ein Service-Port (USB) zur Verfügung, der über einen virtuellen COM-Port verbunden werden kann.

TCP/IP-Verbindung

Öffnen einer TCP/IP-Verbindung:

1. Menü: Programm Einstellungen > Schnittstelle...
⇒ Das Fenster Schnittstelleneinstellungen öffnet sich.
2. Tabellenreiter TCP/IP auswählen.

Bild 7-3: Schnittstelleneinstellungen

3. Im Pull-down-Menü *NETZWERKSCHNITTSTELLE* den Netzwerkadapter auswählen.
4. Klicken auf die Schaltfläche *BIS SUCHEN*.
⇒ BIS U-Auswerteeinheiten werden gesucht und in der Tabelle aufgelistet.
5. BIS U-Auswerteeinheit durch Klicken auf die entsprechende Zeile auswählen.
6. Mit *VERBINDEN/TRENNEN* wird die TCP/IP-Verbindung aufgebaut bzw. getrennt.

Im Bereich *NEUE IP-ADRESSE VERGEBEN* kann dem über TCP/IP oder USB verbundenen Gerät eine neue IP-Adresse oder ein neues Standard-Gateway zugewiesen werden. Über das Kontrollkästchen *DHCP VERWENDEN*, kann das Gerät auf DHCP zum automatischen Beziehen der IP-Adresse, umgestellt werden.

i DHCP kann nur in einem Netzwerk verwendet werden, das die dynamische Vergabe von IP-Adressen erlaubt. Dies muss vor dem Aktivieren von DHCP sichergestellt werden, da sonst unter Umständen nicht mehr über das Netzwerk auf die Auswerteeinheit zugegriffen werden kann. Im Notfall kann diese Einstellung über den Service-Port (USB) rückgängig gemacht werden. Dazu ist ein Servicekabel M12-USB erforderlich (siehe Kapitel 10.3 auf Seite 173).

USB-Verbindung (virtueller COM-Port)

Öffnen einer seriellen Verbindung über einen virtuellen COM-Port:

1. Menü: Programm Einstellungen > Schnittstelle...
⇒ Das Fenster Schnittstelleneinstellungen öffnet sich.
2. Tabellenreiter RS232 auswählen.
3. Port auswählen, über den der virtuelle COM-Port verbunden wird.
4. Über die Schaltfläche *SUCHEN* bzw. *VERBINDEN* wird die serielle Verbindung aufgebaut.

i Für die Verwendung von virtuellen COM-Ports ist die Installation eines Treibers (Download unter **www.balluff.com**) erforderlich. Zum Verbinden der Auswerteeinheit mit dem USB-Port des PCs wird ein M12-USB-Service-Kabel benötigt. Kabel und weiteres Zubehör siehe Kapitel 10.3 auf Seite 173.

7.1.4 Datenträger erfassen/erkennen

Mit der Schaltfläche *SUCHE TAGS...* im Reiter *ERKENNEN* des Aktionsbereichs kann eine Datenträgerliste erstellt werden, die die Datenträger auflistet, die sich im Erfassungsbereich der gewählten Antenne befinden.

1. Tabellenreiter *ERKENNEN* im Aktionsbereich wählen.
2. Antenne über die Optionsflächen *1...4* oder *ALL* im Infobereich wählen.
3. Auf *SUCHE TAGS...* klicken.
⇒ Datenträger im Erfassungsbereich der gewählten Antenne werden erfasst und in die Liste eingetragen.

Die Datenträgerliste enthält folgende Informationen:

- #1...#4: Antennen (1...4), die den gelisteten Datenträger erfasst haben
- *EPC/TID*: EPC oder TID des Datenträgers
- *RSSI*: höchster RSSI-Wert, der bei der Erfassung des Datenträgers gemessen wurde
- *ZÄHLER*: zählt, wie oft der Datenträger im zyklischen Betrieb erfasst wurde
- *ZYKLEN*: zählt die Erfassungsintervalle im zyklischen Betrieb

i Mit Rechtsklick auf einen Datenträger in der Liste kann direkt zum Tabellenreiter *LESEN/SCHREIBEN* gewechselt werden. Dort können weitere Interaktionen mit dem Datenträger durchgeführt werden.

Daten

Im Auswahlbereich *DATEN* kann ausgewählt werden, welche Daten (EPC oder TID) bei der Erfassung der Datenträger in die Liste eingetragen werden sollen.

i Die Länge des TID-Datenfelds ist parametrierbar, siehe Kapitel 7.3 auf Seite 49.

Erkennen

Im Auswahlbereich *ERKENNEN* kann die Betriebsart festgelegt werden, mit der die Datenträgererfassung durchgeführt wird.

SYNCHRON EINMALIG ERKENNEN

Über die Schaltfläche *SUCHE TAGS...* wird die Erfassung der Datenträger einmalig durchgeführt. Die Datenträgerliste wird vor jedem Vorgang gelöscht und mit dem neuen Ergebnis befüllt.

SYNCHRON WIEDERHOLT ERKENNEN

Über die Schaltfläche *SUCHE TAGS...* wird die Datenträgererfassung gestartet und zyklisch im angegebenen Intervall (ms) wiederholt. Dabei wird die Datenträgerliste kontinuierlich aktualisiert. Neue Datenträger werden der Liste hinzugefügt. Datenträger, die den Erfassungsbereich der Antenne verlassen haben, werden rot eingefärbt. Die zyklische Erfassung wird solange fortgeführt, bis sie über die Schaltfläche *STOPP* beendet wird.

Über das Kontrollkästchen *LOOP-FILTER VERWENDEN* kann gewählt werden, ob die Datenträgererfassung nach bestimmten Vorgaben erfolgen soll. Diese können durch verschiedene Parameter definiert werden (siehe Kapitel 6.5 auf Seite 25).

ASYNCHRON ERKENNEN

Der *ASYNCHRON ERKENNEN*-Modus wird einmalig über die Schaltfläche *SUCHE TAGS...* gestartet und läuft, bis er über die Schaltfläche *STOPP* beendet wird. Nach dem Start werden die Datenträger im Erfassungsbereich der aktiven Antenne erfasst und in die Liste eingetragen (nur EPC möglich). Datenträger, die neu erfasst werden, werden der Liste hinzugefügt. Datenträger, die den Erfassungsbereich der Antenne verlassen, werden aus der Liste entfernt, so dass die Liste stets die aktuelle Datenträgerpopulation widerspiegelt.

i Das Loop-Filter und der Asynchron-Erkennen-Modus unterstützen derzeit nur Datenträgererfassungen mit EPC-Ausgabe. Das Scannen mit Ausgabe von TID-Werten in Kombination mit dem Loop-Filter oder im Asynchron-Erkennen-Modus wird derzeit nicht unterstützt.

7.1.5 Datenträger lesen/schreiben

Der Reiter *LESEN/SCHREIBEN* stellt die Funktionen zum Auslesen sowie zum Beschreiben von Datenträgern zur Verfügung. Über die Schaltflächen *LESEN* und *SCHREIBEN* kann die gewünschte Aktion gestartet werden. Bevor ein einzelner Datenträger bearbeitet werden kann, muss dieser im Reiter *ERKENNEN* erfasst werden.

Speicherbereich, über den der TAG identifiziert werden soll

Zum Selektieren eines einzelnen Datenträgers können EPC und TID des Datenträgers verwendet werden. Über die jeweilige Aufklappliste kann ein einzelner Datenträger ausgewählt werden.



Mit Rechtsklick auf einen Datenträger in der Liste kann direkt zum Tabellenreiter *LESEN/SCHREIBEN* gewechselt werden. Dort können weitere Interaktionen mit dem ausgewählten Datenträger durchgeführt werden.

ACCESS PASSWORD

Durch Wählen des Kontrollkästchens *ACCESS PASSWORD* erscheint ein Eingabefeld, in das ein Zugriffspasswort eingetragen werden kann. Diese Funktion ist nur für Datenträger vorgesehen, die durch ein Zugriffspasswort gesichert sind.

Welcher Speicherbereich soll bearbeitet werden?

Auswahl des Speicherbereichs, der gelesen bzw. beschrieben werden soll.

Zur Auswahl stehen die Bereiche *EPC*, *TID*, *RESERVED* und *BENUTZERDATEN*. Details zu den Speicherbereichen und deren Größe können dem Datenblatt der verwendeten Datenträger entnommen werden.

Für die Daten *EPC* und *TID* sind *STARTADRESSE* und *LÄNGE* fest voreingestellt.

Für den direkten Zugriff auf die Speicherbänke *EPC*, *TID*, *RESERVED* sowie den Bereich *BENUTZERDATEN* können *STARTADRESSE* und *LÄNGE* (Anzahl Byte) über die vorgesehenen Eingabefelder festgelegt werden.

Speicherbereich	Lesen	Schreiben	Startadresse	Länge
<i>EPC</i>	Ja	Ja	Fest	Parameter
<i>TID</i>	Ja	Nein	Fest	Parameter
<i>BENUTZER-DATEN</i>	Ja	Ja	Feld <i>START-ADRESSE</i>	Feld <i>LÄNGE</i>

Daten

Im Feld *DATEN* werden die ausgelesenen Daten angezeigt. Im linken Bereich des Datenfelds werden die Startadressen der einzelnen Zeilen angezeigt. Der mittlere Bereich zeigt die Daten im Hex-Format. Der rechte Bereich gibt die ASCII-Repräsentation der Daten wieder. Zu schreibende Daten können direkt im Datenfeld per Tastatureingabe editiert werden (im Hex- oder ASCII-Format).

Daten manipulieren

Für einfache Datenwerte können die Schaltflächen *INKREMENT*, *DEKREMENT*, *FORTLAUFEND* und *FESTWERT* verwendet werden. Im Feld *STARTWERT/WERT* kann ein Startwert für die Funktion *FORTLAUFEND* oder ein Wert für die Funktion *FESTWERT* festgelegt werden.

Laden/Speichern von Daten

Über die Schaltflächen *ÖFFNEN* bzw. *SPEICHERN* können die Hex-Daten des Datenfelds in eine Datei (*.dat) exportiert bzw. aus einer Datei importiert werden.

7.1.6 Parametereinstellung

Abhängig von der aktiven Sicherheitsebene können unter *PARAMETER...* und *ERWEITERTE PARAMETER...* verschiedene Einstellungen vorgenommen werden. Die Bedeutung der einzelnen Parameter sowie deren Zuordnung zum UHF-Manager sind in Kapitel 7.3 auf Seite 49 beschrieben.

Über die Schaltflächen *AN BIS SENDEN* und *VON BIS EMPFANGEN* können die Parameter an die Auswerteeinheit übertragen oder von dieser gelesen werden.

Über die Schaltflächen *SPEICHERN UNTER...* und *ÖFFNEN...* können die Parametersätze in einer xml-Datei gespeichert bzw. aus einer xml-Datei eingelesen werden. Diese Vorgehensweise vereinfacht die Parametrierung, wenn mehrere Geräte dieselbe Parametrierung erhalten sollen.

Die Schaltfläche *STANDARDEINSTELLUNGEN* setzt zunächst nur die Benutzeroberfläche auf die Werte des Auslieferungszustands zurück. Durch die Schaltfläche *AN BIS SENDEN* können die Parameter auf die Auswerteeinheit übernommen werden.

7.2 Webserver

Um sich mit dem Webserver des Geräts über TCP/IP zu verbinden, wird ein Browser (z. B. Google Chrome) benötigt. In der Adresszeile die IP-Adresse des Geräts mit vorangestelltem „http://“ und nachfolgendem „/“ eingeben (z. B. http://192.168.10.2/).

Die Webserverapplikation von BIS U-6127 bietet eine Schnittstelle, über die man Zugang zur Geräteinformation erhält. Die Geräteeinstellungen können geändert und an die Bedürfnisse angepasst werden.

Bild 7-4 zeigt die Menüleiste des Webserver mit sieben Hauptmenüs, die nachfolgend beschrieben werden.

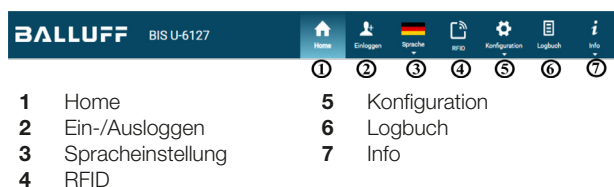


Bild 7-4: Hauptmenü

7.2.1 Home

Bild 7-5 zeigt die Homepage der Webserverapplikation.

Die Oberfläche ist in zwei Teile gegliedert:

- Auf der linken Seite stehen Geräteinformationen (nicht veränderbar).
- Auf der rechten Seite ist das Gerät abgebildet und zeigt den aktuellen Zustand der LEDs.

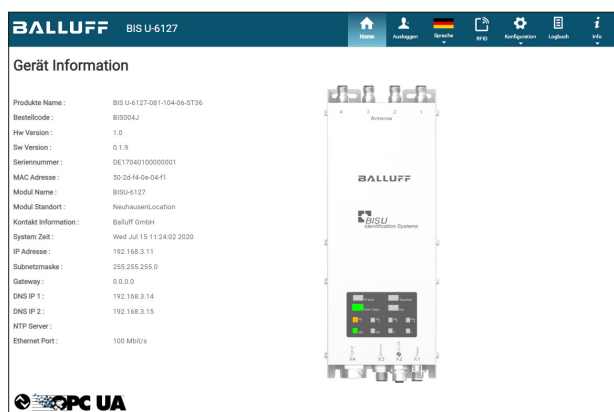


Bild 7-5: Startseite

7.2.2 Einloggen/Ausloggen

Ein Großteil der Anzeigefunktionen der Gerätewebseiten funktioniert auch ohne Anmeldung. Für die Änderung vieler Einstellungen ist aber die Rolle *EXPERT* oder *ADMIN* notwendig. Dann muss eine Anmeldung über den Menüpunkt *EINLOGGEN* erfolgen.

Einloggen

1. Im Feld *BENUTZERNAME* den Namen eintragen, unter dem man sich auf dem BIS U-6127-Gerät einloggen möchte.
2. Unter *PASSWORT* das für diesen Benutzer gültige Passwort eintragen.
Durch Klicken auf das Auge-Symbol neben dem Dialogfeld können die Zeichen sichtbar gemacht werden.

Bild 7-6: Eingabedialog zur Eingabe von Benutzername und Passwort

Ausloggen

War das Einloggen erfolgreich, zeigt das in Bild 7-4 dargestellte Feld (2) des Hauptmenüs den Text *AUSLOGGEN* an.

Benutzer werden nach einer Zeit der Inaktivität von 15 Minuten automatisch aus dem System ausgeloggt und eine Neuansmeldung wird erforderlich. Nach spätestens 24 Stunden muss eine neue Anmeldung erfolgen.

Werksseitig vorkonfigurierte Benutzer

Bei der ersten Inbetriebnahme sind dabei auf dem System werksseitig gewisse Standardbenutzerprofile vorhanden (siehe nachfolgende Tabelle).



Die Standardeinstellungen sollten aus Sicherheitsgründen bei der ersten Konfiguration verändert werden!

Es können eigene Benutzer hinzugefügt und mit entsprechenden Berechtigungen versehen werden.

7

Inbetriebnahme und Betrieb (Fortsetzung)

Diese Benutzer und die entsprechenden Passwörter sind in folgender Tabelle zusammengefasst:

Name	Standard-passwort	Beschreibung
user		Standardbenutzer ohne Konfigurationsberechtigung. In der Regel sind vor allem Prozessdaten und zusätzlich einige Einstellungen sichtbar. Eine Konfiguration kann aber nicht vorgenommen werden. Dies ist das Standardbenutzerlevel, das jeder Benutzer automatisch erhält, wenn er auf die Weboberfläche des BIS U zugreift. Ein Login wird nicht benötigt
admin_default	Siehe Aufdruck auf dem Typenschild	Administrativer Benutzer, der das Gerät in vollem Umfang konfigurieren kann. Um dieses Level zu erhalten ist ein Login nötig.

7.2.3 Spracheinstellungen

Für die Konfigurationsoberfläche von BIS U-6127 gibt es zwei Spracheinstellungen: Deutsch (Default) und Englisch.

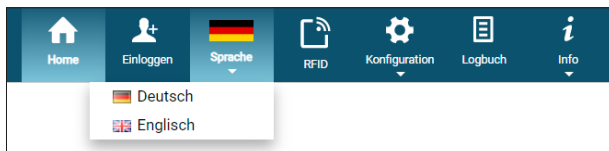


Bild 7-7: Spracheinstellungen

Die Sprache der Oberfläche kann wie folgt geändert werden:

- Die Sprachauswahl mit Klick auf den Menüpunkt *SPRACHE* im Hauptmenü öffnen und auf die gewünschte Sprachzeile klicken (siehe Bild 7-7).

7.2.4 RFID

Scan starten, Lesen/Schreiben

Das RFID-Menü kann über die Hauptmenüleiste aufgerufen werden (siehe Bild 7-4 auf Seite 33).

RFID

EPC	Count	RSSI	Antenna	
E2 00 90 51 32 05 01 72 22 80 2A F8	0	-29	1 ✓	3
E2 00 90 51 32 05 01 71 23 90 20 37	0	-35	1 ✓	3 ✓
E2 00 90 51 32 05 01 72 25 90 10 7F	0	-42	1 ✓	3
E2 00 90 51 32 05 01 72 24 00 20 3C	0	-32	1 ✓	3 ✓
E2 00 90 51 32 05 01 71 26 30 0D BB	0	-25	1 ✓	3
E2 00 90 51 32 05 01 71 26 90 08 B9	0	-60	1 ✓	3
E2 00 90 51 32 05 01 71 22 70 2A F3	0	-47	1 ✓	3 ✓
E2 00 90 51 32 05 01 71 27 50 06 87	0	-32	1 ✓	3
E2 00 90 51 32 05 01 72 26 50 0B 25	0	-43	1 ✓	3 ✓
E2 00 90 51 32 05 01 71 25 00 16 67	0	-31	1 ✓	3 ✓
E2 00 90 51 32 05 01 71 21 40 36 5E	0	-26	1 ✓	3
E2 00 90 51 32 05 01 71 24 40 1C D8	0	-36	1 ✓	3 ✓
E2 00 90 51 32 05 01 72 27 70 04 91	0	-34	1 ✓	3 ✓
E2 00 90 51 32 05 01 71 15 40 75 B6	0	-44	1 ✓	3 ✓

Herunterladen Tagliste

Info : Lesen erfolgreich abgeschlossen

Antennenstatus

Antenne 1: Ein 27 dBm
Antenne 2: Aus 27 dBm
Antenne 3: Ein 27 dBm
Antenne 4: Aus 27 dBm

Update Intervall: 2 Sek

Start Scan

Tag Parameter

Adresse: 0
Länge: 10
Access Passwort: 00000000
EPC Bank: ☒ User Data: ☐ TID Bank: ☐

E2 00 90 51 32 05 01 72 22 80 2A F8
4F 9E 30 00 E2 00 90 51 32 05

Daten Schreiben Daten Lesen

a Scan-Liste

b Antennenstatus

c Update-Intervall

d Startadresse

e Länge (Byte)

f Passwort

g Speicherbank

h EPC des ausgewählten Datenträgers

i Dateninhalt an ausgewählter Adresse und Speicherbank

Bild 7-8: RFID

Auf dieser Seite können Tag-Operationen wie *START SCAN*, *DATEN SCHREIBEN* und *DATEN LESEN* ausgeführt werden (siehe Bild 7-8).

Auf der rechten Seite zeigt der *ANTENNENSTATUS* (b) die global aktiven Antennen und ihre Leistungen. Diese Werte können für das Scannen von Tags auf dieser Seite geändert werden. Ferner zeigt das *UPDATE INTERVALL* (c) die Dauer zwischen zwei Scanvorgängen an. Der *ANTENNENSTATUS* und das *UPDATE INTERVALL* können geändert werden, um den gewünschten Scanvorgang auszuführen.

Auf der linken Seite der Seite wird die Scanliste (a) in tabellarischer Form mit EPC, Anzahl (wie oft der Tag gescannt wurde), RSSI und Antenne erstellt (ein Auswahlzeichen steht für jede Antenne, die den Tag gescannt hat).

Eingabeparameter für die Tag-Lese- und Tag-Schreibvorgänge:

- Die Startadresse (d), von der aus das Lesen/Schreiben beginnen muss.
- Länge der zu lesenden Byte (e).
- Passwort (f) zum Lesen/Schreiben des Tags.
- Die Speicherbank (g), aus der Daten gelesen/geschrieben werden müssen.

Darüber hinaus kann mit *HERUNTERLADEN TAGLISTE* die gescannte Tag-Liste als CSV-Datei (Comma Separated Values) heruntergeladen werden.

Rechts oben werden Informationen in roter Farbe angezeigt, z. B. *Lesen erfolgreich abgeschlossen*.

7.2.5 Konfiguration

Die Konfiguration ist das wichtigste Menü, mit dem die Einstellungen für das Gerät gelesen und geändert werden kann (siehe Bild 7-9).

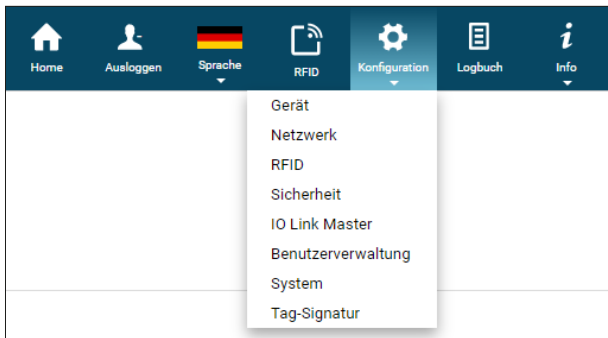


Bild 7-9: Konfiguration Untermenü

In den folgenden Abschnitten wird jedes Untermenü ausführlich erläutert.

Allgemeine Geräteeinstellungen

Die allgemeinen Geräteeinstellungen (siehe Bild 7-10) werden im Menü *KONFIGURATION* mit *GERÄT* (siehe Bild 7-9 auf Seite 36) aufgerufen. Hier vorgenommene Einstellungen kann das Gerät als Metainformation tragen.

Bild 7-10: Allgemeine Geräteeinstellungen

Der *GERÄTENAME* (a) kann frei gewählt werden. Auch ein *STANDORT* (b) kann dem Gerät als Information zur Verfügung gestellt werden.

Die Einstellung der Zeit erfolgt in der dargestellten Form. Das Datum besteht aus Tag und Monat als zweistellige Zahl, das Jahr muss als vierstellige Zahl eingegeben werden. Tag, Monat und Jahr müssen jeweils durch einen Punkt getrennt und in genau dieser Reihenfolge eingegeben werden. Die Uhrzeit wird in Stunden im 24-Stunden-Format und Minuten getrennt durch einen Doppelpunkt eingestellt. Unter *ZEITZONE* (d) erfolgt die Bezeichnung der Zeitzone in der das Datum eingegeben wurde. Der Zeitunterschied zur UTC (koordinierte Weltzeit, Coordinated Universal Time) muss dennoch manuell in das Feld *ZEITUNTERSCHIED ZUR UTC* (e) eingetragen werden. Der Zeitunterschied muss dabei in Stunden angegeben werden.

Zur Korrektur von Zeitstempeln kann die gewünschte Sommer/Winterzeiteinstellung eingetragen werden. Ein automatischer Wechsel von Sommer nach Winterzeit findet derzeit nicht statt, um in industriellen Prozessen durchgängige Zeitstempel zu gewährleisten.

Mit *SETZEN* werden vorgenommene Einstellungen auf das Gerät übertragen, mit *AKTUALISIEREN* verworfen bzw. aktualisiert.

Alle oben genannten Parameter benötigen einen *ADMIN*-Level, um Parameter zu ändern/aktualisieren.

Netzwerkeinstellung

Die Einstellungen für die Ethernet-Schnittstelle des BIS U-6127 (siehe Bild 7-11) werden im Menü *KONFIGURATION* mit *NETZWERK* (siehe Bild 7-9 auf Seite 36) aufgerufen.

Bild 7-11: Netzwerkeinstellungen

Im Auslieferungszustand ist die statische Vergabe einer IP-Adresse aktiviert (siehe Bild 7-11). Diese Einstellung kann aber auch auf eine automatische Vergabe einer IP-Adresse via DHCP umgestellt werden (a). Wenn die statische IP-Adressvergabe aktiviert ist, können die *IP ADRESSE* (b) und die *SUBNETZMASKE* (c) eingestellt werden. Die neu eingestellte IP-Adresse kann auf dem Typenschild des Geräts vom Anwender eingetragen werden. Darüber hinaus stehen auch die Einstellung der IP-Adressen eines *GATEWAYS* (d) für einen externen Netzwerkzugriff und des gewünschten primären (e) und sekundären (f) DNS-Namensservers zur Verfügung. Soll für die Einstellung der Uhrzeit ein Server mit NTP-Funktionalität (Netzwerk-Zeitprotokoll) verwendet werden, muss dieser in das Eingabefeld (g) eingetragen werden. Hier kann entweder eine IP-Adresse oder ein Domain-Name (z. B. time.google.com) eingetragen werden.

Mit *SETZEN* (h) werden die Einstellungen auf dem Gerät gespeichert, mit *AKTUALISIEREN* (i) verworfen bzw. aktualisiert. Um die vorgenommenen Einstellungen auf dem Gerät aktiv werden zu lassen, ist ein Neustart notwendig, der mit *NEUSTART* (k) ausgelöst werden kann. Alle oben genannten Parameter benötigen einen *ADMIN*-Level, um Parameter zu ändern/aktualisieren.

Als Konfigurationswerte werden in der Standardkonfiguration folgende Einstellung verwendet:

Konfigurationselement	Standardwert
IP-Vergabe	Static
IP-Adresse	192.168.10.2
Subnetzmaske	255.255.255.0
Gateway	0.0.0.0
DNS IP 1	0.0.0.0
DNS IP 2	0.0.0.0
NTP-Server	

RFID-Einstellungen

Die RFID-Einstellungen (siehe Bild 7-12) werden im Menü *KONFIGURATION* mit *RFID* (siehe Bild 7-9 auf Seite 36) aufgerufen.

Bild 7-12: RFID-Einstellungen

Es gibt fünf Tabs, unter denen jeweils andere RFID-Einstellungen vorgenommen werden können:

- Basis UHF
- Antennen & Leistung
- UHF erweitert
- Filteroptionen
- Formatierte Tagdaten

Alle Parameter können mit jeder Zugriffsberechtigung gelesen werden. Um Parameterwerte zu ändern, müssen jedoch bestimmte Zugriffsrechte vorliegen.

Basis UHF

Bild 7-13: Basis UHF

i Um die Einstellungen zu ändern, wird mindestens das Berechtigungslevel *EXPERT* vorausgesetzt.

Parameter für den allgemeinen Betrieb:

- (a) *Initialer Q-Wert/erwartete Anzahl Tags* (Parameter 0002_{hex}) siehe Seite 56
- (b) *TID-Länge* (Parameter 0004_{hex}) in Byte siehe Seite 61
- (c) *Anzahl Leseversuche* (Parameter 000A_{hex}) siehe Seite 61
- (d) *BlockWrite aktivieren* (Parameter 000D_{hex}) siehe Seite 61
- (e) *Max. Schreiblänge* (Parameter 000D_{hex}) siehe Seite 62
- (f) *Max. Leselänge* (Parameter 000E_{hex}) siehe Seite 62
- (g) *Aktive Kanäle* (Parameter 000B_{hex}) siehe Seite 59

Antennen & Leistung

Antennen und Leistung									
Aktiviert	Antennentyp	Gewinn	Kabeltyp	Dämpfung	Voreingestellt Ant. Leistung (ERP)	Voreingestellt Port Leistung	Leistungserhöhung Schreiben		
a	b	c	d	e	f	g	h	i	
Ant1 ☒	BIS U-302-C0	5.5 dBi	Benutzerspezifisch	1.75 dB	7 dBm	5.4 dBm	2 dB	Auto	
Ant2 ☒	BIS U-302-C0	5.5 dBi	Benutzerspezifisch	1.75 dB	17 dBm	15.4 dBm	2 dB	Auto	
Ant3 ☒	BIS U-300-C0	5.4 dBi	Benutzerspezifisch	1.75 dB	17 dBm	15.5 dBm	0 dB	Auto	
Ant4 ☒	BIS U-302-C0	5.5 dBi	Benutzerspezifisch	1.75 dB	17 dBm	15.4 dBm	2 dB	Auto	
Setzen Aktualisieren									

Bild 7-14: Antennen & Leistung

Parameter für Antennen & Leistung:

i Um Einstellungen der nachfolgenden Parameter zu ändern, wird das Berechtigungslevel *ADMIN* vorausgesetzt.

- (a) *Aktive Antennen* (Parameter 0012_{hex}) siehe Seite 74
- (b) Für *Antennentyp* siehe Abschnitt *UHF-Komponenten* auf Seite 73
- (c) *Antennengewinn* (Parameter 0013_{hex}) siehe Seite 74
- (d) Für *Kabeltyp* siehe Abschnitt *UHF-Komponenten* auf Seite 73
- (e) *Kabeldämpfung* (Parameter 0014_{hex}) siehe Seite 75

i Um Einstellungen der nachfolgenden Parameter zu ändern, wird mindestens das Berechtigungslevel *EXPERT* vorausgesetzt.

- (f) *Sendeleistung beim Lesen (default)* (Parameter 0008_{hex}) siehe Seite 58
- (h) *Automatische Erhöhung der Sendeleistung beim Schreiben* (Parameter 0009_{hex}) siehe Seite 59
- (i) Startet die Funktion *Auto-Setup* für die entsprechende Antenne (Parameter 1003_{hex}) siehe Seite 60

Der folgende Parameter wird aus den übrigen Parametern errechnet und ist nicht unmittelbar veränderbar:

- (g) Zeigt die errechnete Sendeleistung an der Antennenbuchse an.

UHF erweitert

Bild 7-15: UHF erweitert

Einstellungen für die Luftschnittstelle:

i Um Einstellungen der nachfolgenden Parameter zu ändern, wird mindestens das Berechtigungslevel *EXPERT* vorausgesetzt.

- (a) *Funkprofil* (Parameter 0001_{hex}) siehe Seite 56
- (b) *Session (Inventoried Flag)* (Parameter 0005_{hex}) siehe Seite 57
- (c) *Pilotton (lange Präambel)* (Parameter 0006_{hex}) siehe Seite 58
- (d) *Modulation* (Parameter 0007_{hex}) siehe Seite 58
- (e) *Initialer Q-Wert/erwartete Anzahl Tags* (Parameter 0002_{hex}) siehe Seite 57

Einstellungen für die Tag Signatur:

i Um Einstellungen der nachfolgenden Parameter zu ändern, wird das Berechtigungslevel *ADMIN* vorausgesetzt.

- (f) *SignatureType* (Parameter 002A_{hex}) siehe Seite 81
- (g) *Berechnungsformat für die Signaturerzeugung (default)* (Parameter 0028_{hex}) siehe Seite 80

Informationen zu *Tagdaten signieren* siehe Kapitel 3.7 auf Seite 12.

Filteroptionen

Bild 7-16: Statische Filter

Filteroptionen:

i Um Einstellungen der nachfolgenden Parameter zu ändern, wird mindestens das Berechtigungslevel *EXPERT* vorausgesetzt.

- TID Bit Adresse (a), TID Bit Länge (b) und TID Daten (c) siehe *TIDFilter (default)* (Parameter 002E_{hex}) auf Seite 66
- (d) *RSSIMinFilter (default)* (Parameter 002F_{hex}) siehe Seite 67
- (e) *RSSIMaxFilter (default)* (Parameter 0030_{hex}) siehe Seite 68
- EPC Bit Adresse (f), EPC Bit Länge (g) und EPC-Daten (h) siehe *EPCFilter (default)* (Parameter 002D_{hex}) auf Seite 65
- (i) *MinReads bzw. AsyncObserved-Threshold (default)* (Parameter 0023_{hex}) siehe Seite 62
- (j) *MinNoReads bzw. AsyncObserved-Timeout (default)* (Parameter 0024_{hex}) siehe Seite 63
- (k) *WaitTime (default)* (Parameter 0029_{hex}) siehe Seite 63

i Um Einstellungen der nachfolgenden Parameter zu ändern, wird das Berechtigungslevel *ADMIN* vorausgesetzt.

- (l) *AsyncScanDelay* (Parameter 0011_{hex}) siehe Seite 73

7

Inbetriebnahme und Betrieb (Fortsetzung)

Formatierte Tagdaten

Bild 7-17: Formatierte Tagdaten

i Um Einstellungen der nachfolgenden Parameter zu ändern, wird das Berechtigungslevel *ADMIN* vorausgesetzt.

Einstellungen für formatierte Tagdaten:

- (a) *Formatdefinition für ReadTagDataFormatted, ReadMultipleTagDataFormatted und WriteFormattedTagData (default)* (Parameter 0025_{hex}) siehe Seite 79
- (b) *Präfix für ReadMultipleTagDataFormatted (default)* (Parameter 0026_{hex}) siehe Seite 80
- (c) *Suffix für ReadMultipleTagDataFormatted (default)* (Parameter 0027_{hex}) siehe Seite 80

Mit *TEST* (d) können die definierten Tag-Parameter geprüft und im Textfeld (e) angezeigt (links: binär, rechts: ASCII-Format) werden.

Sicherheitseinstellungen

Die Sicherheitseinstellungen (siehe Bild 7-18) werden im Menü *KONFIGURATION* mit *SICHERHEIT* (siehe Bild 7-9 auf Seite 36) aufgerufen.

Bild 7-18: Sicherheitseinstellungen

Es gibt drei Tabs, unter denen jeweils andere Sicherheitseinstellungen vorgenommen werden können:

- OPC/UA
- Secure Element
- Allgemein

Weitere Informationen zu *Datensicherheit* siehe Kapitel 3.6 auf Seite 11.

OPC/UA

OPC/UA Einstellungen
 Unsichere Clientverbindungen zurückweisen ☒ **a**
 Nur vertrauenswürdige Clientzertifikate akzeptieren ☒ **b**
 Secure Element benutzen ☐ **c**

Zertifikatliste

Status	Name	Organisation	Gültig ab	Gültig bis	
Vertrauenswürdig	wibu2048.der	Balluff GmbH	Nov 30 12:15:09 2018 GMT	Nov 30 12:15:09 2023 GMT	d
Zurückgewiesen	UaExpert.der	Balluff GmbH	Oct 16 09:11:06 2018 GMT	Oct 15 09:11:06 2023 GMT	e

Setzen Aktualisieren Reboot

Zertifikat erzeugen/download
 Zertifikat erzeugen Download

f **g**

Bild 7-19: OPC/UA

OPC/UA Einstellungen:

- Mit *UNSICHERE CLIENTVERBINDUNGEN ZURÜCKWEISEN* (a) können unsichere Verbindungen abgelehnt werden.
- Mit *NUR VERTRAUENSWÜRDIGE CLIENTZERTIFIKATE AKZEPTIEREN* (b) werden nur Verbindungen mit autorisiertem Zertifikat gestattet und somit wird vor nicht autorisierter Verbindung zum OPC/UA-Server geschützt. Diese Einstellung ist mit der Einstellung *UNSICHERE CLIENTVERBINDUNGEN ZURÜCKWEISEN* (a) gekoppelt.
- Mit *SECURE ELEMENT BENUTZEN* (c) wird das eingebaute Hardwareelement zur Speicherung der geheimen Schlüssel genutzt, was die Sicherheit zusätzlich erhöht.

Zertifikatliste:

Die Zertifikatliste zeigt die verfügbaren Zertifikate auf dem Gerät an. Zusätzlich werden die Zertifikatdetails wie Status, Organisation und Gültigkeitsdauer des Zertifikats angezeigt. Der Status des Zertifikats gibt an, ob das Zertifikat vom autorisierten Benutzer oder Administrator als vertrauenswürdig eingestuft oder abgelehnt wird.

Mit *ADMIN*-Berechtigung kann die Liste mithilfe der Schaltflächen (d) und (e) geändert werden. Das Zertifikat, das bereits als vertrauenswürdig markiert ist, kann durch Klicken des Schlosssymbols in den abgelehnten Status versetzt oder durch Drücken des Abfallkorbsymbols vom Gerät gelöscht werden. Ebenso kann ein abgelehntes Zertifikat in den vertrauenswürdigen Zustand versetzt oder aus dem Gerät gelöscht werden.

Zertifikat erzeugen/download:

- Mit *ZERTIFIKAT ERZEUGEN* (f) kann ein Zertifikat für das Gerät selbst erstellt werden (z. B. nach Änderung der Netzwerkeinstellungen).
- Mit *DOWNLOAD* (g) kann ein Zertifikat heruntergeladen werden.



Um zu vermeiden, dass ungültige Zertifikate entstehen, beim Erzeugen eines Zertifikats Datum, Uhrzeit sowie Zeitzone korrekt einstellen. Zertifikate haben eine begrenzte Gültigkeit (typischerweise mehrere Jahre, die Gültigkeit kann z. B. auf einem Windows-PC angezeigt werden) und müssen nach Ablauf der Gültigkeit ersetzt werden.

Weitere Informationen zu *Datensicherheit* siehe *OPC UA* im Kapitel 3.6 auf Seite 11.

Secure Element

Secure Element

Secure Element Seriennummer (a)

Secure Element Lizenzen (b)

- Found license entry 0:0
- Found license entry 0:50
- Found license entry 0:60
- Found license entry 0:70
- Found license entry 0:1000
- Found license entry 10:40

Secure Element Kontext Datei

(c)

Secure Element Update Datei

(d)

(e)

Bild 7-20: Secure Element

In den Einstellungen *SECURE ELEMENT* werden die Details der Sicherheitslizenz angezeigt. Es ermöglicht auch die Aktualisierung der aktuellen Lizenz.

Secure Element (schreibgeschützte Felder):

- Secure Element Seriennummer (a) stellt die eindeutige Identifikationsnummer dar.
- Secure Element Lizenzen (b) steht für die verfügbare Lizenz.

Secure Element Kontext Datei:

Mit *DOWNLOAD KONTEXT DATEI* (c) kann die Remote-Kontext-Datei (*.WibuCmRaC) heruntergeladen werden.

Die Datei kann verwendet werden, um Update-Dateien für Secure-Element-Lizenzen zu generieren.

Secure Element Kontext Datei:

Sollen aktuellen Lizenzen aktualisieren oder erneuert werden, muss für diese Aktion ein Ticket beim Balluff Service erworben werden. Damit erhält man eine Remote-Update-Datei (*.WibuCmRaU) vom Balluff Service selbst oder von einer bestimmten Webseite. Diese Aktualisierungsdatei kann mit **.WIBUCMRAU DATEI AUSWÄHLEN* (d) hochgeladen werden, und die Aktualisierungen werden mit *UPLOAD UPDATE DATEI* (e) auf das sichere Element angewendet.

Weitere Informationen zu *Datensicherheit* siehe *OPC UA* im Kapitel 3.6 auf Seite 11.

7

Inbetriebnahme und Betrieb (Fortsetzung)

Allgemein

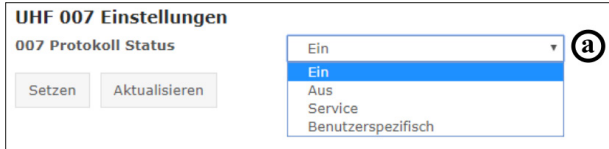


Bild 7-21: Allgemein

Auf der Seite *ALLGEMEIN* können die vom Kommunikationsprotokoll *UHF 007* verwendeten Ports geändert werden. Die Änderungen werden erst nach einem Gerätereustart übernommen.



007 sollte nur mit Bedacht für den USB-Anschluss deaktiviert werden!

Der USB-Port kann die einzige Möglichkeit sein, die IP-Adresse des Geräts abzurufen und zu ändern, wenn sie einmal verloren gegangen ist.

Das Kommunikationsprotokoll ermöglicht, eine Verbindung über fünf TCP/IP-Ports und einen USB-Port mit dem Gerät herzustellen:

- Anschluss 10001
- Anschluss 10002
- Anschluss 10003
- Anschluss 10004
- Anschluss 10005
- Tty USB-Anschluss

Vier Konfigurationen (a) stehen zur Verfügung:

- *Ein* öffnet alle verfügbaren Anschlüsse.
- *Aus* schließt alle verfügbaren Anschlüsse.
- *SERVICE* schließt alle Anschlüsse mit Ausnahme des USB-Anschlusses.
- *BENUTZERSPEZIFISCH* (schreibgeschützt) definiert die Port-Bedingung, die nicht mit einer der oben genannten von drei Optionen übereinstimmt.

IO-Link-Einstellungen (Webserver)

Die IO-Link-Einstellungen (siehe Bild 7-22) werden im Menü *KONFIGURATION* mit *IO LINK MASTER* (siehe Bild 7-9 auf Seite 36) aufgerufen.

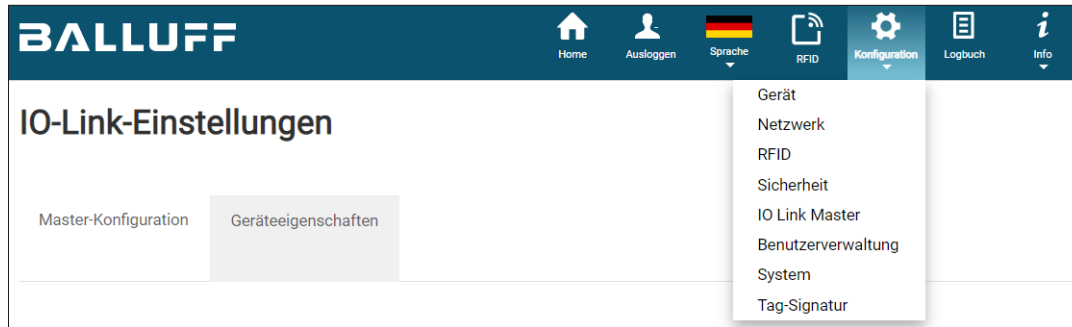


Bild 7-22: IO-Link-Einstellungen

Es gibt zwei Tabs, unter denen jeweils andere Einstellungen vorgenommen werden können:

- *MASTER-KONFIGURATION*
- *GERÄTEEIGENSCHAFTEN*

Alle Parameter können mit jeder Zugriffsberechtigung gelesen werden. Um Parameterwerte zu ändern, müssen jedoch bestimmte Zugriffsrechte vorliegen.

Master-Konfiguration



Um Einstellungen der nachfolgenden Parameter zu ändern, wird das Berechtigungslevel *ADMIN* vorausgesetzt.

Master-Parameter	
Vendor ID	0x0378
Device ID	0x000000
Serial Number	
Modus IO-Link Pin 2	Eingang NC
Modus IO-Link Pin 4	IOL
Safe State	0
Cycle Time Base	0
Cycle Time	0
Parameter Server	Deaktiviert
Parameter Download	Deaktiviert
Parameter Upload	Deaktiviert
Output Length	5
Input Length	0
Validierungs-Modus	Keine Validierung
Setzen Aktualisieren	

Bild 7-23: Master-Konfiguration

Geräteeigenschaften



Um Einstellungen der nachfolgenden Parameter zu ändern, wird das Berechtigungslevel *ADMIN* vorausgesetzt.

Geräteeigenschaften	
Prozessdaten	
Eingaben	00
Ausgaben	00 00 00 00 00
Ereignisse	
Aktuelles Ereignis	no event
Ausgabedaten setzen Aktualisieren	
Parameter	
Index	1062
Subindex	0
Daten	00 50 02 00 64 04 00 64
Setzen Daten Lesen	

Bild 7-24: Geräteeigenschaften

Mit *AKTUALISIEREN* können die Anzeigen der Prozessdaten und Ereignisse aktualisiert werden.

Daten können in einem bestimmtem Index und Subindex gelesen oder geschrieben werden.

Benutzerverwaltung

Zusätzlich zu den Standardbenutzerprofilen können eigene Benutzer mit individuellen Berechtigungen angelegt werden.

Die Benutzerverwaltung (siehe Bild 7-25) wird im Menü *KONFIGURATION* mit *BENUTZERVERWALTUNG* (siehe Bild 7-9 auf Seite 36) aufgerufen. Auf der Konfigurationsseite wird zunächst einen Überblick über die verfügbaren Benutzer im System gegeben. Werksseitig sind lediglich die (nicht sichtbaren) Benutzer *ADMIN_DEFAULT* und *USER* vorhanden.

Ohne Anmeldung sind keine Benutzerdaten sichtbar.

Benutzer, die nicht über die Rolle *ADMIN* verfügen, können nur ihre eigenen Daten sehen und ihr eigenes Passwort bearbeiten.

Nur Benutzer, die über die Rolle *ADMIN* verfügen, können alle Benutzer sehen, neue Benutzer anlegen und die Daten und Passwörter vorhandener Benutzer bearbeiten oder Benutzerkonten löschen.

Durch Löschen und Neuanlegen eines Benutzers kann auch bei einem unbekannten Passwort ein neues gesetzt werden.

Verfügbare Benutzerrollen

Rolle	Beschreibung
User	Benutzerrolle ohne Konfigurationsberechtigung. In der Regel sind vor allem Prozessdaten und zusätzlich einige Einstellungen sichtbar. Eine Konfiguration kann aber nicht vorgenommen werden.
Expert	Expertenbenutzer, der einige Einstellungen vornehmen kann.
Admin	Administrativer Benutzer, der das Gerät in vollem Umfang konfigurieren kann.

Benutzer Verwaltung			
Benutzerliste			
Benutzernamen	Benutzerrollen		
Balluff	☒ Admin	☒ Expert	☒ User
Gehard	☐ Admin	☒ Expert	☒ User
Tom	☐ Admin	☐ Expert	☒ User
expert	☐ Admin	☒ Expert	☒ User
Benutzer anlegen d			

- a** Geänderte Benutzerrollen übernehmen
- b** Passwort ändern
- c** Benutzer löschen
- d** Neue Benutzer anlegen

Bild 7-25: Benutzerliste Beispiel

System-Update

Das System-Update (siehe Bild 7-26) wird im Menü *KONFIGURATION* mit *SYSTEM* (siehe Bild 7-9 auf Seite 36) aufgerufen.

Bild 7-26: System

Bild 7-26 zeigt das Dialogfeld zum Firmware-Update mit den Schaltflächen zur Auswahl einer Firmware-Datei (a), zum Auslösen des Updateprozesses (c) und zum Abschließenden Gerätereustart (d) die durch Updates entstehen können.

Die Firmware-Update-Dateien sind signiert und auch nur solche können ins System eingespielt werden. Sollte ein Firmware-Upgrade fehlschlagen, verfügt das Gerät über ein Notfallsystem, über das eine neue, signierte Firmware eingespielt werden kann.

i Trotz eines Updates ist das Gerät zunächst normal funktionsfähig und läuft unverändert weiter (wenn der Update-Prozess stattfindet oder bereits abgeschlossen ist). Das Update wird erst nach einem Gerätereustart wirksam.

Nach erfolgtem Update, mit *NEUSTART* das Gerät neu starten.

Mit **.AML DATEI AUSWÄHLEN* (e) wird ein Dateidialog geöffnet, mit dem eine auf dem PC gesicherte Parameter-Konfigurationsdatei auf dem lokalen Rechner gesucht und ausgewählt werden kann. Nachdem eine Parameterdatei gewählt wurde, können die enthaltenen Parameter mit *HOCHLADEN* (f) in das Gerät eingespielt werden. Es wird empfohlen, anschließend das Gerät neu zu starten.

Mit *HERUNTERLADEN* (g) können die derzeitigen Einstellungen des Geräts auf einen lokalen Rechner gesichert werden.

7

Inbetriebnahme und Betrieb (Fortsetzung)

Tag-Signature

Tag Signature (siehe Bild 7-27) wird im Menü *KONFIGURATION* mit *TAG-SIGNATUR* (siehe Bild 7-9 auf Seite 36) aufgerufen.

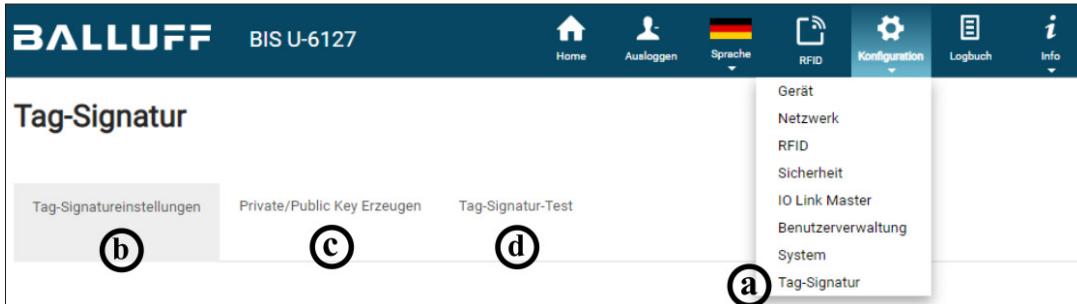


Bild 7-27: Tag-Signatur

Die 3 Tabs unter *TAG-SIGNATUR* enthalten die Funktionen, um die Tag-Signatur-Funktionalität zu konfigurieren (b), ein Schlüsselpaar zu erzeugen (c) und die Funktionalität zu testen (d) (siehe Kapitel 3.6 auf Seite 11).

Tag-Signatureinstellungen

Um die Parameter *TAG_SIGNATUR* und *SIGNATUR_BERECHNUNGSFORMAT* im Reiter *TAG-SIGNATUREEINSTELLUNGEN* zu ändern sind Administratorrechte erforderlich. Informationen zu *Tagdaten signieren* siehe Kapitel 3.7 auf Seite 12.

Private/Public Key Erzeugen

Bild 7-28: Private/Public Key Erzeugen

Mit *ERZEUGEN* (d) kann ein neues zufälliges Schlüsselpaar erzeugt werden. Die Ausgabe des Schlüsselpaares wird im Textformat angezeigt – *PRIVATE KEY* (a), *PRIVATE KEY FÜR DAS SECURE ELEMENT* (b) und *PUBLIC KEY* (c). Die Werte können nur gelesen und auf den lokalen PC kopiert werden.

Die Schlüssel werden nicht im Gerät gespeichert und müssen in das *Secure Element* übertragen werden (siehe Abschnitt *Erzeugen eines Schlüssels zum Signieren von Tagdaten* auf Seite 82).

Mit *LÖSCHEN* (e) kann die gesamte Textausgabe gelöscht werden.

Bild 7-29: Tag-Signature-Test

Tag Scannen kann ähnlich ausgeführt werden wie in Abschnitt *Scan starten, Lesen/Schreiben* auf Seite 35. Gescannte Tags werden in der linken Tabelle aufgelistet, in der ein Tag ausgewählt werden kann, um einen Tag-Test durchzuführen. Zuerst muss die Signatur erstellt und dann kann die Signatur getestet werden.

Um eine Signatur zu erstellen, muss der Benutzer prüfen, ob der Signaturtyp aktiviert ist (Parameter 002A_{hex}, siehe Seite 81), was über die Webseite *Tag Signature* (siehe Bild 7-27) erreicht werden kann. Ist er nicht aktiviert, kann die Meldung *TAG-SIGNATUR-FUNKTION DEAKTIVIERT* auf dem Bildschirm angezeigt werden. Als Ergebnis der Signaturerstellung werden die Daten auf dem Tag entsprechend geschrieben.

Nach erfolgreicher Erstellung der Signatur kann der Benutzer zum Testen die Schaltfläche *SIGNATUR PRÜFEN* (c) wählen. Daraufhin wird die Operation *Tag-Format lesen* durchgeführt und das Ergebnis der Signaturprüfung angezeigt.

7

Inbetriebnahme und Betrieb (Fortsetzung)

7.2.6 Logbuch

Generelle Statusinformationen können immer unter *HOME* eingesehen werden (siehe Kapitel 7.2.1 auf Seite 33). Dort stehen kompakte Informationen über den Betriebszustand des Geräts sowie einige Einstellungen, wie Namen und Uhrzeit. Außerdem findet sich hier auch die Typbezeichnung.

Gerätestatus und Funktionszustand

Das Logbuch kann unter *LOG* über die Hauptmenüleiste aufgerufen werden (siehe Bild 7-4 auf Seite 33). Dort stehen erweiterte Informationen für den Fehlerfall.

- Unter dem Reiter *ANWENDUNGSTATUS* kann hier detailliert der Fehlerzustand einzelner Funktionskomponenten ausgelesen werden, um festzustellen, wo Fehler aufgetreten sind.
 - Funktionskomponenten, die mit einem grünen Haken versehen sind, weisen keine Fehler auf.
 - Ist eine Funktionskomponente mit einem gelben Symbol versehen, dann sind im Ablauf kürzlich Probleme aufgetreten.
 - Ist eine Funktionskomponente mit einem roten Symbol versehen, dann ist sie nicht mehr ablauffähig und eine schwerwiegende Störung ist aufgetreten. Hinter dem Namen der Funktionskomponente steht auch eine Kurzbeschreibung des Status.
- Details über das aufgetretene Problem können unter dem Reiter *GERÄT LOGBUCH* ausgelesen werden. Hier befindet sich die Diagnosefunktion zur Fehlerbehebung. Diese Informationen sind wichtig, sollte Kontakt mit unserem Customer Service Team aufgenommen werden.

7.2.7 Rechtliche und allgemeine Informationen

Weitere Informationen stehen unter *INFO* (siehe Bild 7-30) bereit.

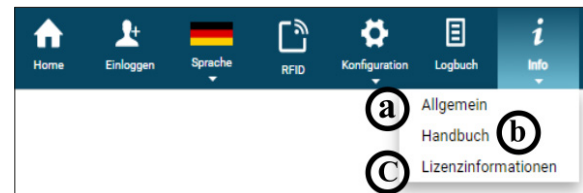


Bild 7-30: *INFO*-Menü

Mit *ALLGEMEIN* (a) ruft man eine Kurzerklärung zur Bedeutung der auf der Seite verwendeten Icons auf.

Unter *HANDBUCH* (b) kann die aktuelle Anleitung in allen verfügbaren Sprachen heruntergeladen werden.

LIZENZINFORMATIONEN (c) ruft Lizenztexte zu den auf dem Gerät verwendeten Open Source-Komponenten auf.

7.3 Parametrierung

Über verschiedene Parameter kann die Auswerteeinheit an die Gegebenheiten der Applikation und deren Umgebungsbedingungen angepasst werden. Die einzelnen Parameter und ihre Auswirkungen werden in den nachfolgenden Abschnitten erläutert.

Zur Durchführung der Parametrierung können folgende Kanäle verwendet werden:

- *007-Protokoll* (siehe Kapitel 8 auf Seite 89)
- *Konfigurationssoftware UHF-Manager* (siehe Kapitel 7.1 auf Seite 29)
- *OPC UA* (siehe Kapitel 9 auf Seite 132)
- *Webserver* (siehe Kapitel 7.2 auf Seite 33)

7.3.1 Vorüberlegungen zur Parametrierung



Der Zugang zu den verschiedenen Parametern ist über die Berechtigungen der Benutzerebenen *USER/EXPERT/ADMIN* geregelt. Diese können über den Webserver verwaltet werden (siehe *Datensicherheit* auf Seite 11 und *Benutzerverwaltung* auf Seite 45).

Sendeleistung

Um die Auswerteeinheit optimal für die vorliegende Applikation einzurichten, sind neben den Überlegungen zur Anordnung der Systemkomponenten (siehe Kapitel 6 auf Seite 21) auch Vorüberlegungen zur Parametrierung notwendig.

Über die Sendeleistung kann der gewünschte Schreib-/Leseabstand erhöht bzw. gesenkt werden. Eine höhere Sendeleistung bedeutet prinzipiell auch einen höheren Schreib-/Leseabstand. Dies gilt vor allem, wenn viele Datenträger auf engem Raum vorliegen oder auf elektromagnetisch wirksamen Materialien (z. B. Metall) montiert sind.

Allerdings kann eine zu hoch eingestellte Sendeleistung auch Nachteile mit sich bringen:

- Sind mehrere Auswerteeinheiten simultan im Einsatz und sind deren Antennen räumlich zu eng oder sogar im Erfassungsbereich anderer Antennen montiert, kommt es zu Beeinflussungen zwischen den Auswerteeinheiten. Ist eine räumliche Trennung nicht möglich, kann die Beeinflussung durch eine geringere Sendeleistung reduziert werden.
- Weiter entfernt angebrachte Datenträger können durch eine hohe Sendeleistung versehentlich von einer Antenne erfasst werden.
- Eine hohe Sendeleistung kann die Empfangsempfindlichkeit der Auswerteeinheit reduzieren.



Um die Beeinflussung der Auswerteeinheit sowie deren Umgebung so gering wie möglich zu halten, sollte die abgestrahlte elektromagnetische Energie grundsätzlich in der Umgebung minimiert werden. D. h., die Sendeleistung sollte nicht höher eingestellt werden, als es für die sichere Interaktion mit der gewünschten Datenträgerpopulation notwendig ist.

In Single-Tag-Anwendungen kann die Auto-Setup-Funktion zum Einstellen der optimalen Sendeleistung verwendet werden (siehe *Auto-Setup* auf Seite 60).

Funkparameter und elektromagnetisch gestörte Umgebung

Über Funkparameter kann der Übertragungskanal zwischen Antenne und Datenträger angepasst werden. Hier können z. B. Parameter wie Datenrate und Codierung an die Applikation und an die Umgebung angepasst werden. Höhere Datenraten ermöglichen einen schnelleren Datenaustausch zwischen Auswerteeinheit und Datenträger, können den Übertragungskanal jedoch anfälliger für Störungen durch eine elektromagnetisch belastete Umgebung machen. Über die Codierung kann dem zum Teil entgegengewirkt werden.

Grundsätzlich empfehlen wir, dass nur Experten die voreingestellten Funkparameter verändern und höhere Datenraten nur dann zu verwenden, wenn diese aufgrund der erforderlichen Prozessgeschwindigkeit notwendig sind.

Beim Einstellen der Funkprofile muss darauf geachtet werden, dass die verwendeten Datenträger das gewählte Funkprofil unterstützen.

Erfassungssicherheit vs. Geschwindigkeit

Durch verschiedene Parameter kann die Zuverlässigkeit des Identifikationssystems erhöht werden (z. B. durch wiederholtes Erfassen von Datenträgern), um sicherzustellen, dass nur Datenträger erfasst werden, die sich tatsächlich im gewünschten Erfassungsbereich befinden. Datenträger, die durch Feldschwankungen versehentlich erfasst wurden, können so ausgeblendet werden.

Die Erhöhung der Erfassungssicherheit geht unter Umständen zu Lasten der Erfassungsgeschwindigkeit, die in dynamischen Anwendungen erforderlich sein kann. Bei der Parametrierung kann es dann notwendig sein, eine Balance zwischen Zuverlässigkeit und Geschwindigkeit zu finden.

7

Inbetriebnahme und Betrieb (Fortsetzung)

7.3.2 Parameterübersicht

Die folgende Übersicht listet die verwendbaren Parameter auf und gibt Aufschluss über die erforderliche Sicherheitsebene *STANDARD/EXPERT/ADMIN* sowie über Geltungsbereich und Gültigkeitsdauer.

Global/Lokal/Antenne

Der Geltungsbereich sagt aus, ob ein Parameter global gültig ist oder nur für eine Session oder einen Antennenport.

GLOBAL: Parameter werden auf alle Antennen bzw. Sessions angewendet. Manche Parameter werden bei 007-Sessions erst beim Gerätereustart übernommen.

SESSION: Parameter gelten nur für die aktuelle Session (TCP-Verbindung) und können für jede Session unabhängig festgelegt werden.

ANTENNE: Parameter beziehen sich auf einen Antennenport und können für jeden Antennenport unabhängig festgelegt werden. Diese Werte gelten für alle Sessions.

Persistent/Temporär

Über die Gültigkeitsdauer ist festgelegt, ob ein Parameter dauerhaft gespeichert wird oder nur für die aktuelle TCP-Verbindung (Session) bzw. bis zu einem Neustart der Auswerteeinheit.

PERSISTENT: Parameter werden dauerhaft gespeichert und behalten ihren Wert auch nach einem Neustart der Auswerteeinheit.

TEMPORÄR: Parameter verlieren ihre Gültigkeit, wenn die aktuelle Session beendet oder die Auswerteeinheit neu gestartet wird.

Reset (Ja/Nein)

Bei der Änderung mancher Parameter ist ein Neustart der Auswerteeinheit erforderlich. Der Neustart muss manuell initiiert werden.



Einige Parameter sind mit dem Zusatz *default* gekennzeichnet. Diese Parameter sind persistent und behalten ihren Wert auch nach einem Neustart der Auswerteeinheit. Je nach Parameter kann ein höheres Berechtigungslevel notwendig sein.

Parameter für Standardbenutzer

Parameter-ID	Parameter	Global/Session/Antenne	Persistent/Temporär	Reset
0003 _{hex}	Max. EPC-Länge (read only)	Global	Persistent	Nein
1001 _{hex}	Sendeleistung beim Lesen (aktuell)	Session	Temporär	Nein
1002 _{hex}	Access Passwort	Session	Temporär	Nein
1004 _{hex}	Speicherbank	Session	Temporär	Nein
1006 _{hex}	AsyncOperation	Session	Temporär	Nein
1007 _{hex}	AdminLevel-Login	Session	Temporär	Nein

Parameter für Experten

Zum Einstellen von Expertenparametern ist der Zugriff auf die Sicherheitsebene *expert* notwendig (siehe *Datensicherheit* auf Seite 11 und *Benutzerverwaltung* auf Seite 45).

Air-Interface, Funkparameter

Parameter-ID	Parameter	Global/Session/Antenne	Persistent/Temporär	Reset
0001 _{hex}	Funkprofil	Global	Persistent	Nein
0002 _{hex}	Initialer Q-Wert/ erwartete Anzahl Tags	Global	Persistent	Nein
0005 _{hex}	Session	Global	Persistent	Nein
0006 _{hex}	Präambel (Pilotton)	Global	Persistent	Nein
0007 _{hex}	Modulation (ASK/PR-ASK)	Global	Persistent	Nein
0008 _{hex}	Sendeleistung beim Lesen (default), s. a. sessionbezogener Parameter 1001 _{hex}	Global	Persistent	Nein
0009 _{hex}	Automatische Erhöhung der Sendeleistung beim Schreiben	Global	Persistent	Nein
000B _{hex}	Aktive Kanäle (nur ETSI)	Global	Persistent	Nein
1003 _{hex}	Auto-Setup	Session	Persistent	Nein

Daten, Schreiben, Lesen, Erfassen

Parameter-ID	Parameter	Global/ Session/ Antenne	Persistent/ Temporär	Reset
0004 _{hex}	TID-Länge	Global	Persistent	Nein
000A _{hex}	Anzahl Leseversuche	Global	Persistent	Nein
000C _{hex}	BlockWrite-beim Schreiben	Global	Persistent	Nein
000D _{hex}	Max. Schreiblänge	Global	Persistent	Nein
000E _{hex}	Max. Leselänge	Global	Persistent	Nein

Loop-Filter

Parameter-ID	Parameter	Global/ Session/ Antenne	Persistent/ Temporär	Reset
0023 _{hex}	MinReads bzw. Async-Observed-Threshold (default)	Global	Persistent	Nein
100C _{hex}	MinReads bzw. Async-Observed-Threshold	Session	Temporär	Nein
0024 _{hex}	MinNoReads bzw. Async-ObservedTimeout (default)	Global	Persistent	Nein
100D _{hex}	MinNoReads bzw. Async-ObservedTimeout	Session	Temporär	Nein
0029 _{hex}	WaitTime (default)	Global	Persistent	Nein
100E _{hex}	WaitTime	Session	Temporär	Nein

Datenfilter

Parameter-ID	Parameter	Global/ Session/ Antenne	Persistent/ Temporär	Reset
002B _{hex}	EPCLength-Min (default)	Global	Persistent	Nein
100F _{hex}	EPCLength-Min	Session	Temporär	Nein
002C _{hex}	EPCLength-Max (default)	Global	Persistent	Nein
1010 _{hex}	EPCLength-Max	Session	Temporär	Nein
002D _{hex}	EPCFilter (default)	Global	Persistent	Nein
1011 _{hex}	EPCFilter	Session	Temporär	Nein
002E _{hex}	TIDFilter (default)	Global	Persistent	Nein
1012 _{hex}	TIDFilter	Session	Temporär	Nein

RSSI-Filter

Parameter-ID	Parameter	Global/ Session/ Antenne	Persistent/ Temporär	Reset
002F _{hex}	RSSIMinFilter (default)	Global	Persistent	Nein
1013 _{hex}	RSSIMinFilter	Session	Temporär	Nein
0030 _{hex}	RSSIMaxFilter (default)	Global	Persistent	Nein
1014 _{hex}	RSSIMaxFilter	Session	Temporär	Nein

FormattedTagData

Parameter-ID	Parameter	Global/ Session/ Antenne	Persistent/ Temporär	Reset
1008 _{hex}	Ausgabeformat für Formatierte Tagdaten	Session	Temporär	Nein
1009 _{hex}	Präfix für ReadMultiple-TagDataFormatted	Session	Temporär	Nein
100A _{hex}	Suffix für ReadMultiple-TagDataFormatted	Session	Temporär	Nein

7

Inbetriebnahme und Betrieb (Fortsetzung)

Tagsignatur

Parameter-ID	Parameter	Global/Session/Antenne	Persistent/Temporär	Reset
100B _{hex}	Berechnungsformat für die Signaturerzeugung	Session	Temporär	Nein

Parameter für Administratoren

Zum Einstellen der Parameter für Administratoren ist der Zugriff auf die Sicherheitsebene *Admin* notwendig (siehe *Datensicherheit* auf Seite 11 und *Benutzerverwaltung* auf Seite 45)

Autofunktionen

Parameter-ID	Parameter	Global/Session/Antenne	Persistent/Temporär	Reset
000F _{hex}	Automatisches Scannen	Session	Persistent	Nein
0011 _{hex}	AsyncScan-Delay	Global	Persistent	Nein

Aktive Antennen, Equipment (Antennen, Kabel)

Parameter-ID	Parameter	Global/Session/Antenne	Persistent/Temporär	Reset
0012 _{hex}	Aktive Antennen	Global	Persistent	Nein
0013 _{hex}	Antennengewinn	Antenne	Persistent	Nein
0014 _{hex}	Kabeldämpfung	Antenne	Persistent	Nein
0015 _{hex}	Antennenpolarisation	Antenne	Persistent	Nein
0016 _{hex}	Antennenöffnungswinkel	Antenne	Persistent	Nein

Netzwerk, System

Parameter-ID	Parameter	Global/Session/Antenne	Persistent/Temporär	Reset
0019 _{hex}	IP-Address	Global	Persistent	Nein
001A _{hex}	Netmask	Global	Persistent	Nein
001B _{hex}	DHCP	Global	Persistent	Nein
001C _{hex}	Hostname	Global	Persistent	Nein
001D _{hex}	Gateway	Global	Persistent	Nein
001E _{hex}	Nameserver	Global	Persistent	Nein
001F _{hex}	Gerätestandort	Global	Persistent	Nein
0020 _{hex}	Zeitzone	Global	Persistent	Nein
0021 _{hex}	NTP-Server	Global	Persistent	Nein
0022 _{hex}	Uhrzeit	Global	Persistent	Nein

Formatted Tag Data (defaults)

Parameter-ID	Parameter	Global/Session/Antenne	Persistent/Temporär	Reset
0025 _{hex}	Ausgabeformat für Formatierte Tagdaten (default)	Global	Persistent	Nein
0026 _{hex}	Präfix für ReadMultiple-TagDataFormatted (default)	Global	Persistent	Nein
0027 _{hex}	Suffix für ReadMultiple-TagDataFormatted (default)	Global	Persistent	Nein

Tagsignatur (defaults)

Parameter-ID	Parameter	Global/Session/Antenne	Persistent/Temporär	Reset
0028 _{hex}	Berechnungsformat für die Signaturerzeugung (default)	Global	Persistent	Nein
002A _{hex}	SignatureType	Global	Persistent	Nein

7.3.3 Beschreibung der Parameter für Standardbenutzer

Parameter für Standardbenutzer können von jedem Benutzer ohne Login verändert werden. Diese Parameter werden nur temporär von der Auswerteeinheit übernommen und sind nur für die aktuelle Session bzw. bis zum Neustart der Auswerteeinheit gültig.

Max. EPC-Länge (nur lesen)

Parameter-ID: 0003_{hex}

Der Parameter *Max. EPC-Länge* gibt an, welche maximale Anzahl Byte des EPC-Speicherbereichs von der Auswerteeinheit übertragen wird.

Werden Datenträger gelesen, deren EPC länger als die eingestellte *Max. EPC-Länge* ist, wird der gelesene EPC auf die eingestellt Anzahl Byte begrenzt.



Der Parameter *Max. EPC-Länge* dient nur der Kompatibilität zu anderen BIS U-Auswerteeinheiten und kann nicht verändert werden. Der Wert ist fest auf 496 Bit eingestellt.

Sendeleistung beim Lesen (aktuell)

Parameter-ID: 1001_{hex}

UHF-Manager: Menü: Geräteeinstellungen > Parameter... > Sendeleistung

OPC UA: GetRFPower/SetRFPower

Webserver: Menü: Konfiguration – RFID – Antennen & Leistung

Nach dem Einschalten bzw. nach einem Neustart der Auswerteeinheit wird die aktuelle Sendeleistung aus dem Expertenparameter *Sendeleistung beim Lesen (default)* übernommen. Je nach Anforderungen kann die Sendeleistung über den Parameter *Sendeleistung beim Lesen (aktuell)* temporär geändert werden. Die Einstellung bleibt erhalten, bis sie erneut geändert oder die Auswerteeinheit neu gestartet wird.

Die eingestellte Sendeleistung wird für den Lesebetrieb verwendet.

Als Parameterwert wird die gewünschte Leistung in Viertel-dBm übergeben.

$$\text{Parameterwert} = P(\text{dBm}) \times 4$$

Einstellbare Leistung: 7...36 dBm¹⁾ (entspricht 5...4000 mW)

0 schaltet die Antenne für diese Session ab

¹⁾ Die höchste mögliche Antennenleistung hängt von der Gerätevariante ab.

Länge [Bit]	Zulässige Werte	Werks-einstellung	Bedeutung
8	0, 28...144	108 27 dBm (500 mW)	Aktuelle Sendeleistung in ¼ dBm (ERP bzw. EIRP)



Die Angaben zur Sendeleistung sind je nach Gerätevariante als ERP-Werte (Equivalent Radiated Power) bzw. EIRP-Werte (Equivalent Isotropically Radiated Power) zu verstehen. Die jeweils gültige Angabe kann dem Informationsblatt zu Konformität und Zulassungen entnommen werden.

7

Inbetriebnahme und Betrieb (Fortsetzung)

Access Passwort

Parameter-ID: 1002_{hex}
 UHF-Manager: Aktionsbereich > Reiter *LESEN/SCHREIBEN*
 OPC UA: Wird bei den jeweiligen OPC UA-Methoden zum Schreiben und Lesen übergeben
 Webserver: Menü: RFID > Aktionsbereich: *TAG PARAMETER*

Soll auf einen passwortgeschützten Datenträger zugegriffen werden, kann der Datenträger mit dem Parameter *Access Passwort* zur weiteren Interaktion entsperrt werden.

Das Passwort muss im Format *LSB first* übergeben werden.

Sofern keine Datenträger mit unterschiedlichen Passwörtern im Einsatz sind, genügt es, den Parameter einmalig an die Auswerteeinheit zu senden.

Das Passwort bleibt in der Auswerteeinheit gespeichert, bis die aktuelle Session beendet oder die Auswerteeinheit neu gestartet wird.

Einstellbare Werte: 4-Byte Passwort (Standard 00 00 00 00_{hex})

Länge [Bit]	Zulässige Werte (hex)	Werks-einstellung (hex)	Bedeutung
32	00000000... FFFFFFFF	00000000	Zugriffspasswort

Speicherbank

Parameter-ID: 0x1004_{hex}
 UHF-Manager: Aktionsbereich > Reiter *LESEN/SCHREIBEN*
 OPC UA: Wird bei den jeweiligen OPC-UA-Methoden zum Schreiben und Lesen übergeben
 Webserver: Menü: *RFID* > Aktionsbereich: *TAG PARAMETER*

Über den Parameter *Speicherbank* kann gesteuert werden auf welchem Speicherbereich des Datenträgers Schreib-/Leseoperationen ausgeführt werden.

Je nach verwendetem Datenträger stehen die Speicherbereiche RFU (Reserved), EPC, TID und USER zur Verfügung.

Wird der Speicherbereich umgestellt, bleibt die Einstellung erhalten, bis sie erneut geändert oder die Session beendet wird.

Länge [Bit]	Zulässige Werte	Werks-einstellung	Bedeutung
8	0, 1, 2 oder 3	3 (USER)	Speicherbank des Datenträgers 0: RFU 1: EPC 2: TID 3: USER



Weiterführende Informationen zu den verschiedenen Speicherbereichen der Datenträger können dem Standard EPCglobal™ Class-1 Generation-2 für UHF-RFID-Systeme entnommen werden (www.epcglobal.de).

AsyncOperation

Parameter-ID: 1006_{hex}
 UHF-Manager: Aktionsbereich > Reiter *ERKENNEN*
 (nur Demo, kein kumulierter Betrieb)
 OPC UA: Wird bei den jeweiligen OPC-UA-
 Methoden zum Schreiben und Lesen
 übergeben
 Webserver: –

Zum Erfassen einer Datenträgerpopulation können ver-
 schiedene Betriebsarten gewählt werden. Diese sind in
 Kapitel 6.5 auf Seite 23 näher beschrieben.

- *SYNCHRON*
 Im synchronen Betrieb muss für jede Erfassung eine
 Anfrage an die Auswerteeinheit gesendet werden.
 Diese erfasst dann die Datenträger, die sich im Erfas-
 sungsbereich der angegebenen Antenne befinden und
 gibt diese in Form einer Liste an das steuernde System
 zurück.
- *ASYNCHRON*
 Im asynchronen Betrieb muss im Gegensatz zum
 synchronen Betrieb, die Erfassung nur einmal gestartet
 werden. Diese läuft dann permanent im Hintergrund,
 wodurch die Datenträgerliste aktuell gehalten wird.
 Über eine synchrone Anfrage kann dann die aktuelle
 Liste abgefragt werden.
- *KOMMT/GEHT-Meldungen*
 Alternativ zum asynchronen Betrieb mit synchroner
 Anfrage, können auch asynchrone Meldungen aktiviert
 werden. Diese melden dann lediglich Änderungen der
 Datenträgerpopulation. Neue Datenträger werden über
 eine *KOMMT*-Meldung angemeldet. Datenträger, die den
 Erfassungsbereich verlassen, werden über eine *GEHT*-
 Meldung abgemeldet.
- *KUMULIERT*
 Der kumulierte, asynchrone Betrieb erfasst kontinuier-
 lich alle Datenträger im Erfassungsbereich und fügt
 diese der Datenträgerliste hinzu. Erst durch das syn-
 chrone Abfragen der Liste wird diese gelöscht und
 erneut angelegt. So können alle Datenträger abgefragt
 werden, die den Erfassungsbereich seit der letzten
 Abfrage passiert haben.

Der Parameter *AsyncOperation* wird als Byte übergeben,
 wobei Optionen über die einzelnen Bit-Positionen aktiviert
 bzw. deaktiviert werden können.

Bit-Positionen:

Bit 0 0: *SYNCHRON* 1: *ASYNCHRON*
 Bit 1 0: *KOMMT*-Meldung 1: *KOMMT*-Meldung
 deaktiviert aktiviert
 Bit 2 0: *GEHT*-Meldung deakti- 1: *GEHT*-Meldung akti-
 viert viert
 Bit 3 0: *KUMULIEREN* deaktiviert 1: *KUMULIEREN* aktiviert

Länge [Bit]	Zulässige Werte	Werks- einstellung	Bedeutung
8	00 _{hex} ...0F _{hex}	00 _{hex} : Synchron	Synchrone Daten- trägererfassung

Beispiele:

Operation	Bit 3	Bit 2	Bit 1	Bit 0	Byte
<i>SYNCHRON</i>	0	0	0	0	00 _{hex}
<i>ASYNCHRON</i> mit syn- chrone Abfrage	0	0	0	1	01 _{hex}
<i>ASYNCHRON</i> mit <i>KOMMT/GEHT</i> -Meldung	0	1	1	1	07 _{hex}
<i>ASYNCHRON</i> , <i>KUMULIERT</i>	1	0	0	1	09 _{hex}

AdminLevelLogin

Parameter-ID: 1007_{hex}
 UHF-Manager: Menü: *Login*
 OPC UA:
 Webserver: Menü: *Einloggen*

Über den Parameter *AdminLevelLogin* kann zwischen den
 Sicherheitsebenen *STANDARDBENUTZER/EXPERT/ADMIN* gewech-
 selt werden. Die Sicherheitsebenen *EXPERT* und *ADMIN*
 werden benötigt, um Parameter mit höherer Sicherheitse-
 bene zu bearbeiten.

Die Auswerteeinheit wird nur mit einem Standard-Admin-
 Benutzer ausgeliefert. Weitere Benutzer können über den
 Webserver angelegt werden (siehe *Datensicherheit* auf
 Seite 11 und *Benutzerverwaltung* auf Seite 45).

Beim Setzen des Parameters müssen der Benutzername,
 ein Byte mit dem Wert 01_{hex} und das Passwort des Benut-
 zers gesetzt werden. Der String muss nicht mit einem
 0-Byte abgeschlossen werden.

Stimmt der Benutzername oder das Passwort nicht mit
 einem entsprechenden Eintrag der Benutzerdatenbank
 überein, wird ein Fehlerstatus zurückgegeben.

Beim Lesen des Parameters wird nur der Benutzername
 zurückgegeben.



Benutzer werden nach einer Zeit der Inaktivität
 von 15 Minuten automatisch aus dem System
 ausgeloggt und eine Neuansmeldung wird
 erforderlich. Nach spätestens 24 Stunden muss
 eine neue Anmeldung erfolgen.

Länge [Bit]	Zulässige Werte	Werks- einstellung	Bedeutung
Varia- bel	Benutzer- name + 01 _{hex} + Passwort	„user“	Logindaten werden als String überge- ben

7.3.4 Beschreibung der Parameter für Experten

Parameter für Experten können von Benutzern der Sicherheitsebenen *EXPERT* und *ADMIN* verändert werden. Dazu ist ein Login der entsprechenden Sicherheitsebenen erforderlich. Expertenparameter werden dauerhaft in der Auswerteeinheit gespeichert und behalten ihren Wert, bis sie überschrieben werden.

Folgende Gruppen von Experten-Parametern werden beschrieben:

- *Air-Interface/Funkparameter* (siehe Seite 56)
- *Schreiben, Lesen* (siehe Seite 61)
- *Loop-Filter* (siehe Seite 62)
- *Datenfilter* (siehe Seite 64)
- *RSSI-Filter* (siehe Seite 67)
- *FormattedTagData* (siehe Seite 69)

Air-Interface/Funkparameter

Über die Air-Interface/Funkparameter können Einstellungen vorgenommen werden, die das Funksignal zwischen Datenträger und Auswerteeinheit betreffen sowie Einstellungen, die das Verhalten von Datenträgern während dem Erfassungsvorgang betreffen.

Folgende Parameter sind wichtig für den optimalen Betrieb des RFID-Systems und sollten von allen Benutzern eingestellt werden:

- 0002_{hex}: Initialer Q-Wert/erwartete Anzahl Tags
- 0008_{hex}: Sendeleistung beim Lesen (default)
- 0009_{hex}: Automatische Erhöhung der Sendeleistung beim Schreiben
- 000B_{hex}: Aktive Kanäle



Die Einstellung weiterer Air-Interface/Funkparameter ist in den meisten Fällen nicht notwendig und sollte nur von erfahrenen Benutzern mit entsprechendem Fachwissen vorgenommen werden.

Funkprofil

Parameter-ID: 0001_{hex}
 UHF-Manager: Menü: *Geräte Einstellungen > Erweiterte Parameter... > HF Einstellungen*
 OPC UA: –
 Webserver: Menü: *Konfiguration > RFID > UHF erweitert*

Das Funkprofil legt fest, welche Verbindungsparameter auf der Luftschnittstelle zwischen Datenträger und Auswerteeinheit verwendet werden:

Tx: Bitrate vorwärts, d. h. von der Auswerteeinheit zum Datenträger: 40 kBit/s
 Rx: Bitrate rückwärts, d. h. vom Datenträger zur Auswerteeinheit: 62,5 kBit/s oder 75 kBit/s
 Codierung: Codierung rückwärts, d. h. mit welcher Codierung der Datenträger antwortet.
 Miller-4: Jedes Bit wird als vierfach Bit übertragen



Nicht alle Profile sind in jeder Ländervariante des Geräts verfügbar.

Folgende Funkprofile können eingestellt werden:

Profilnr.	Parameterwert	Tx [kBit/s]	Rx [kBit/s]	Codierung
1	00000902 _{hex}	40	62,5	Miller-4
2	00000B02 _{hex}	40	75	Miller-4

Einstellbare Werte:

Länge [Bit]	Zulässige Werte	Werkeinstellung	Bedeutung
32	Parameterwerte in Tabelle	0x00000902 40/62.5/Miller-4	Funkprofil

Initialer Q-Wert/erwartete Anzahl Tags

Parameter-ID: 0x0002_{hex}
 UHF-Manager: Menü: Geräte Einstellungen > Parameter... > Basic UHF (Erwartete Anzahl Tags) und Geräte Einstellungen > Erweiterte Parameter... > Luftschnittstelle (Q-Wert)
 OPC UA: –
 Webserver: Menü: Konfiguration > RFID > UHF erweitert

Der Q-Wert wird als Kennzahl für die Anzahl der Datenträger, die im Erfassungsbereich der Antenne erwartet werden, verwendet. Über den Q-Wert kann eine Zeitoptimierung hinsichtlich der Dauer, die die Datenträgererfassung in Anspruch nimmt, durchgeführt werden. Darüber hinaus kann die Erfassungsquote durch einen zu groß gewählten Q-Wert abnehmen.

Der eingestellte Q-Wert wird nur als Startwert während der Erfassung verwendet und kann von der Auswerteeinheit optimiert werden.

Folgende Tabelle zeigt eine Empfehlung zur Einstellung des Q-Werts, abhängig von der erwarteten Anzahl von Datenträgern:

Erwartete Anzahl Datenträger (ca.)	Empfohlener Q-Wert
1	1
2	2
5	3
10	4
25	5
50	6
100	7
200	8
500	9

Einstellbare Werte für den Q-Wert:

Länge [Bit]	Zulässige Werte	Werks-einstellung	Bedeutung
8	1...15	4 (Q-Wert = 4)	Anzahl der erwarteten Datenträger

Bei Einstellfeldern, die die erwartete Anzahl Tags angeben, wird stets auf eine aus dem Q-Wert errechnete Zahl gerundet.

Session (Inventoried Flag)

Parameter-ID: 0x0005_{hex}
 UHF-Manager: Menü: Geräte Einstellungen > Erweiterte Parameter... > Luftschnittstelle
 OPC UA: –
 Webserver: Menü: Konfiguration > RFID > UHF erweitert

Datenträger nach EPCglobal™ Class-1 Generation-2 unterstützen Session-Flags, um anzuzeigen, ob ein Datenträger bereits erfasst wurde. Dies erfolgt über den Status der Session-Flags (*ERFASST/NICHT ERFASST*). So kann gesteuert werden, ob und wann ein bereits erfasster Datenträger erneut erfasst werden kann. Für die 4 Sessions (0...3) gelten unterschiedliche Regeln in Bezug auf den Übergang vom Status *Erfasst* zurück in den Status *NICHT-ERFASST*.

Einstellbare Werte:

Länge [Bit]	Zulässige Werte	Werks-einstellung	Bedeutung
8	0: Session 0 1: Session 1 2: Session 2 3: Session 3	0	Session 0



Das Ändern der Session ist Experten vorbehalten und wird nur empfohlen, wenn die Voreinstellung keine zufriedenstellenden Ergebnisse bietet. Detailinformationen zum *SESSION*-Flag können dem Standard nach EPCglobal™ Class-1 Generation-2 entnommen werden.

7

Inbetriebnahme und Betrieb (Fortsetzung)

Pilotton (lange Präambel)

Parameter-ID: 0x0006_{hex}
 UHF-Manager: Menü: *Geräte Einstellungen > Erweiterte Parameter... > HF Einstellungen*
 OPC UA: –
 Webserver: Menü: *Konfiguration > RFID > UHF erweitert*

Datenträger, die auf Anfragen von der Auswerteeinheit antworten, stellen den Daten eine Präambel voran, die von der Auswerteeinheit zur Synchronisierung verwendet wird. Zusätzlich kann ein Pilotton übertragen werden, der in elektromagnetisch belasteter Umgebung die Synchronisation zwischen Datenträger und Auswerteeinheit verbessern kann.

Einstellbare Werte:

Länge [Bit]	Zulässige Werte	Werks-einstellung	Bedeutung
8	0 oder 1	1 (Pilotton ein)	Präambel mit oder ohne Pilotton 0: Pilotton aus 1: Pilotton ein

i Aus Gründen der Prozesssicherheit ist ratsam, den Pilotton eingeschaltet zu lassen. In sehr zeitkritischen Applikationen kann durch das Abschalten des Pilottones ein geringfügiger Zeitvorteil entstehen.

Modulation

Parameter-ID: 0x0007_{hex}
 UHF-Manager: Menü: *Geräte Einstellungen > Erweiterte Parameter... > HF Einstellungen*
 OPC UA: –
 Webserver: Menü: *Konfiguration > RFID > UHF erweitert*

Einstellen des Modulationsverfahrens, das zur Funkübertragung zwischen Auswerteeinheit und Datenträger verwendet wird.

i Nicht alle Modulationsverfahren sind in jeder Ländervariante des Geräts verfügbar.

Einstellbare Werte:

Länge [Bit]	Zulässige Werte	Werks-einstellung	Bedeutung
8	0 oder 1	1 (PR-ASK)	Modulationsverfahren 0: ASK 1: PR-ASK

i Die Umstellung des Modulationsverfahrens ist normalerweise nicht nötig. In elektromagnetisch belasteter Umgebung kann die Umstellung hilfreich sein, wenn die Voreinstellung keine zufriedenstellenden Ergebnisse bietet.

Sendeleistung beim Lesen (default)

Parameter-ID: 0008_{hex}
 UHF-Manager: Menü: *Geräte Einstellungen > Parameter... > Sendeleistung*
 OPC UA: Variable *RFPower*
 Webserver: Menü: *Konfiguration > RFID > Antennen & Leistung*

Über diesen Parameter wird festgelegt, welche Sendeleistung (in dBm) die Auswerteeinheit nach dem Einschalten bzw. nach einem Neustart für Leseoperationen einstellen soll. Die Sendeleistung ist als abgestrahlte Leistung (ERP bzw. EIRP) zu verstehen und wird als Parameterwert Viertel-dBm übergeben.

$$\text{Parameterwert} = P(\text{dBm}) \times 4$$

Zur korrekten Einstellung der abgestrahlten Sendeleistung müssen zudem folgende Parameter gesetzt werden. Die benötigten Daten können den Datenblättern der verwendeten UHF-Antenne und dem verwendeten Antennenkabel entnommen werden.

- Antennengewinn
- Antennenöffnungswinkel
- Antennenpolarisation
- Kabeldämpfung

Einstellbare Leistung: 7...36 dBm
 (entspricht 5 mW...4000 mW)

Länge [Bit]	Zulässige Werte	Werks-einstellung	Bedeutung
8	0, 28...144	108 (27 dBm (500 mW))	Standard Sendeleistung in ¼ dBm (ERP bzw. EIRP)

i Die maximale zulässige Sendeleistung (ERP/ EIRP) ist abhängig von national geltenden Vorschriften. Angaben zur maximal erlaubten Sendeleistung können dem Informationsblatt zu Konformität und Zulassungen entnommen werden.

i Die Angaben zur Sendeleistung sind je nach Gerätevariante als ERP (Equivalent Radiated Power) bzw. EIRP (Equivalent Isotropically Radiated Power) Werte zu verstehen. Die jeweils gültige Angabe kann dem Informationsblatt zu Konformität und Zulassungen entnommen werden.

Automatische Erhöhung der Sendeleistung beim Schreiben

Parameter-ID: 0009_{hex}
 UHF-Manager: Menü: *Geräte Einstellungen > Parameter... > Sendeleistung*
 OPC UA: –
 Webserver: Menü: *Konfiguration > RFID > Antennen & Leistung*

Mit diesem Parameter kann festgelegt werden, ob für Schreib- und Leseoperationen dieselbe Sendeleistung verwendet wird oder ob die Sendeleistung für Schreiboperationen um einen Offset-Wert angehoben wird. Viele Datenträger benötigen bei Schreiboperationen eine höhere Sendeleistung als bei Leseoperationen.

Leistung Schreiben (dBm) = Leistung Lesen (dBm) + Offset (dB)

Als Parameterwert wird die gewünschte Offset-Leistung in Viertel-dB übergeben.

Einstellbare Offset-Leistung: 0...20 dB
 (entspricht Faktor 1...100)

Länge [Bit]	Zulässige Werte	Werks-einstellung	Bedeutung
8	0...80	8 (2 dB (~Faktor 1.6))	Offset-Leistung in ¼ dB

Die resultierende Sendeleistung wird automatisch auf den maximal zulässigen Wert begrenzt.

i Die maximale zulässige Sendeleistung (ERP/ EIRP) ist abhängig von national geltenden Vorschriften. Angabe zur maximal erlaubten Sendeleistung können dem Informationsblatt zu Konformität und Zulassungen entnommen werden. Das Gerät stellt die Einhaltung der Vorschriften sicher, wenn die korrekten Daten der verwendeten Antennen und Kabel eingestellt wurden.

Aktive Kanäle

Parameter-ID: 000B_{hex}
 UHF-Manager: Menü: *Geräte Einstellungen > Parameter... > Basic UHF*
 OPC UA: –
 Webserver: Menü: *Konfiguration > RFID > Basis UHF*

Über den Parameter *Aktive Kanäle* kann festgelegt werden, welche Frequenzen bzw. Kanäle für die Kommunikation mit dem Datenträger verwendet werden. Die Einstellung ist global für alle Sessions.

i Die Einstellung der aktiven Kanäle ist nur für Geräte verfügbar, die nach dem Standard der Europäischen Union oder einer davon abgeleiteten Form arbeiten. Weiterführende Informationen können dem europäischen Standard ETSI EN 302 208 oder abgeleiteten nationalen Standards entnommen werden.

Folgende ETSI-Kanäle können verwendet werden:

ETSI-Kanal	Frequenz [MHz]
4	865,7
7	866,3
10	866,9
13	867,5

Bei Verwendung von 2...4 Kanälen werden diese über ein Frequenzsprungverfahren nacheinander angesteuert.

Einzelne Kanäle können über eine Bitmaske aktiviert (1) bzw. deaktiviert (0) werden.

Beispiel:

Kanal-belegung	Bit 7...Bit 4	Bit 3	Bit 2	Bit 1	Bit 0	Byte
4 und 10 aktiviert, 7 und 13 deaktiviert	0	0	1	0	1	05 _{hex}

Einstellbare Werte:

Länge [Bit]	Zulässige Werte	Werks-einstellung	Bedeutung
8	Bitmaske 0F _{hex} ...00 _{hex}	0F _{hex} Alle Kanäle ein	Bit 0: Kanal 4 Bit 1: Kanal 7 Bit 2: Kanal 10 Bit 3: Kanal 13

i

- Ist nur ein einzelner Kanal aktiv, kann es zu Verzögerungen beim Erfassen kommen, da ein einzelner Kanal nicht ununterbrochen in Betrieb sein darf. Ab 2 Kanälen besteht dieses Problem nicht mehr.
- Für statische Anwendungen kann das Frequenzsprungverfahren von Vorteil sein, da durch den Frequenzwechsel lokale Feldminima ausgeblendet werden können.
- Sind mehrere Auswerteeinheiten simultan auf engem Raum in Betrieb, kann es zu gegenseitiger Beeinflussung kommen, wenn diese auf denselben Kanälen arbeiten. In dem Fall wird empfohlen, die Auswerteeinheiten auf unterschiedlichen und weit entfernten Kanälen zu betreiben, z. B. Auswerteeinheit 1 auf Kanal 4 und Auswerteeinheit 2 auf Kanal 13.

7

Inbetriebnahme und Betrieb (Fortsetzung)

Auto-Setup

Parameter-ID: 1003_{hex}
 UHF-Manager: Menü: *Geräte Einstellungen > Parameter... > Sendeleistung*
 OPC UA: –
 Webserver: Menü: *Konfiguration > RFID > Antennen & Leistung*

Beim Setzen des Parameters *Auto-Setup* auf den Wert 1 beginnt die Auswerteeinheit direkt mit dem Auto-Setup über die angegebene Antenne. Während des Auto-Setups werden von der Auswerteeinheit keine weiteren Befehle angenommen, es kann aber zyklisch der Wert des Parameters abgefragt werden, um das Ende und das Resultat des Auto-Setups zu erkennen.

Das Auto-Setup wird verwendet, um in einer Single-Tag-Anwendung die optimale Sendeleistung einzustellen. Dazu wird die Sendeleistung so eingestellt, dass nur der vor der Antenne positionierte Datenträger erkannt und bearbeitet wird.

Während des Auto-Setups zeigt die LED RF (blau) an, dass das UHF-Feld eingeschaltet ist.

Um das Auto-Setup starten zu können, ist mindestens das Benutzerlevel *EXPERT* notwendig.

Das Auto-Setup kann und muss für jede Antenne einzeln aktiviert werden.

Das Auto-Setup modifiziert nach erfolgreichem Abschluss sowohl die globalen Parameter 0008_{hex} *Sendeleistung Antenne Lesen (default)* und 0009_{hex} *Automatische Erhöhung Sendeleistung beim Schreiben* als auch den session-bezogenen Parameter 1001_{hex} *Sendeleistung Antenne Lesen (aktuell)*.

Einstellbare Werte:

Länge [Bit]	Zulässige Werte	Werks-einstellung	Bedeutung
8	1 fällt nach Abschluss automatisch auf 0, 2, 3 oder 4 zurück	0 (Aus)	1: Auto-Setup 0: Inaktiv

Der zurückgelesene Wert bedeutet folgendes:

- 0: Auto-Setup noch nie gestartet oder erfolgreich abgeschlossen. Ein einzelner Tag konnte anhand der Leistung sicher alleine gelesen und beschrieben werden. Alle Parameter wurden gesetzt.
- 1: Auto-Setup noch nicht abgeschlossen.
- 2: Auto-Setup teilweise erfolgreich. Es konnten mehrere Tags erkannt werden, die Sendeleistung 0008_{hex} und 1001_{hex} wurden gesetzt, um zumindest einen Tag sicher erkennen und lesen zu können.
- 3: Auto-Setup komplett fehlgeschlagen. Es wurde kein Tag gefunden oder er konnte nicht gelesen werden. Es wurden keine Parameter verändert.
- 4: Auto-Setup teilweise erfolgreich. Ein einzelner Tag konnte anhand der Leistung sicher alleine gelesen werden, nicht aber beschrieben. Folgende Gründe sind möglich:
 - Tag enthält keine User-Daten.
 - Tags sind schreibgeschützt.
 - Die Maximalleistung des Geräts ist nicht ausreichend, um sicher zu schreiben.
 Die Sendeleistung 0008_{hex} und 1001_{hex} wurden gesetzt, um diesen Tag sicher erkennen und lesen zu können.

Schreiben, Lesen

Über die Parameter *Schreiben, Lesen* kann die Größe verschiedener Datenfelder festgelegt werden, ob zum Schreiben *BlockWrite* verwendet werden soll und wie oft ein Lesekommando bei einem fehlerhaften Zugriff wiederholt werden soll.

TID-Länge

Parameter-ID: 0004_{hex}
 UHF-Manager: Menü: *Geräte Einstellungen > Parameter... > Lesen-Schreiben*
 OPC UA: –
 Webserver: Menü: *Konfiguration > RFID > Basis UHF*

Über die TID-Länge wird bestimmt, wieviele Datenworte (16 Bit) der TID vom Datenträger an die Auswerteeinheit übertragen werden. Werden Datenträger gelesen, deren TID größer ist als die eingestellte TID-Länge, wird die gelesene TID auf die eingestellt Byte-Anzahl begrenzt. Werden Datenträger gelesen, deren TID kleiner ist als die eingestellte TID-Länge, wird die TID nicht an die Auswerteeinheit übertragen.

Einstellbare Werte:

Länge [Bit]	Zulässige Werte	Werks-einstellung	Bedeutung
8	1...31 Datenworte	4 (4 Worte (8 Byte))	Anzahl Datenworte (Byte) der TID

Anzahl Leseversuche

Parameter-ID: 000A_{hex}
 UHF-Manager: Menü: *Geräte Einstellungen > Parameter... > Basic UHF*
 OPC UA: –
 Webserver: Menü: *Konfiguration > RFID > Basic UHF*

Über den Parameter *Anzahl Leseversuche* wird festgelegt, wie oft die Auswerteeinheit versucht, einen gescheiterten Lesezugriff auf einen Datenträger zu wiederholen, bevor eine negative Statusmeldung an die Auswerteeinheit gesendet wird.

Einstellbare Werte:

Länge [Bit]	Zulässige Werte	Werks-einstellung	Bedeutung
8	0...255	0x05 (5 Wiederholungen)	Anzahl Leseversuche bzw. Wiederholungen

BlockWrite aktivieren

Parameter-ID: 000C_{hex}
 UHF-Manager: Menü: *Geräte Einstellungen > Parameter... > Luftschnittstelle*
 OPC UA: –
 Webserver: Menü: *Konfiguration > RFID > Basis UHF*

Bei gewöhnlichen Schreibzugriffen auf einen Datenträger, werden die Daten sequenziell über mehrere Schreiboperationen Wort für Wort auf den Datenträger geschrieben. Über *BlockWrite aktivieren*, können mehrere Datenworte (16 Bit) mit einem einzelnen Schreibzugriff auf den Datenträger geschrieben werden. Die maximale Anzahl der Datenworte kann über den Parameter *Max. Schreiblänge* festgelegt werden.

Bei Verwendung von *BlockWrite* sollte darauf geachtet werden, dass dieses Kommando von den verwendeten Datenträgern unterstützt wird.

Kann der *BlockWrite*-Befehl nicht erfolgreich auf einem Datenträger ausgeführt werden, weil dieser z. B. den Befehl nicht unterstützt, wird der Schreibvorgang mit dem gewöhnlichen Schreibbefehl wiederholt.



In zeitkritischen Applikationen kann *BlockWrite* einen Zeitvorteil bieten. Allerdings muss darauf geachtet werden, dass alle Datenträger dieses Kommando unterstützen. Ein Mischbetrieb von Datenträgern mit und ohne *BlockWrite*-Unterstützung kann zu höheren Schreib-/Lesezeiten führen.

Einstellbare Werte:

Länge [Bit]	Zulässige Werte	Werks-einstellung	Bedeutung
8	0 oder 1	0 (<i>BlockWrite</i> aus)	0: <i>BlockWrite</i> aus 1: <i>BlockWrite</i> ein

7

Inbetriebnahme und Betrieb (Fortsetzung)

Max. Schreiblänge

Parameter-ID: 000D_{hex}
 UHF-Manager: Menü: *Geräte Einstellungen > Parameter... > Luftschnittstelle*
 OPC UA: –
 Webserver: Menü: *Konfiguration > RFID > Basis UHF*

Die *Max. Schreiblänge* legt die maximale Anzahl der Datenworte (16 Bit) fest, die mit einem *BlockWrite*-Befehl übertragen werden kann.

Es können 1 bis 255 Datenworte übertragen werden, wobei die Einstellung von 0 oder 1 einem gewöhnlichen Schreibbefehl entspricht.

Einstellbare Werte:

Länge [Bit]	Zulässige Werte	Werks-einstellung	Bedeutung
8	1...255	16 (16 Worte (32 Byte))	Anzahl Datenworte beim Schreiben mit <i>BlockWrite</i>

i In einer elektromagnetisch stark gestörten Umgebung können unter Umständen bessere Ergebnisse erzielt werden, wenn weniger Datenworte in einem Kommando übertragen werden.

Max. Leselänge

Parameter-ID: 000E_{hex}
 UHF-Manager: Menü: *Geräte Einstellungen > Parameter... > Luftschnittstelle*
 OPC UA: –
 Webserver: Menü: *Konfiguration > RFID > Basis UHF*

Die *Max. Leselänge* legt die maximale Anzahl der Datenworte (16 Bit) fest, die mit einem Lesebefehl vom Datenträger zur Auswerteeinheit übertragen werden.

Einstellbare Werte

Länge [Bit]	Zulässige Werte	Werks-einstellung	Bedeutung
8	1...255	16 (16 Worte (32 Byte))	Anzahl Datenworte beim Lesen vom Datenträger

i In einer elektromagnetisch stark gestörten Umgebung können unter Umständen bessere Ergebnisse erzielt werden, wenn weniger Datenworte in einem Kommando übertragen werden.

Loop-Filter

Die UHF-RFID-Technologie arbeitet mit elektromagnetischen Wellen, die zur Kommunikation zwischen Datenträger und Auswerteeinheit über Antennen abgestrahlt werden. Diese Wellen werden an metallischen Gegenständen, Wänden und Böden reflektiert, wodurch unerwünschte Nebeneffekte (Auslöschungen oder Verstärkungen) entstehen können. So kann es vorkommen, dass weiter entfernte Datenträger oder Datenträger, die die Lesestelle bereits verlassen haben, versehentlich erfasst werden.

Über die Parameter *MinReads*, *MinNoReads* und *WaitTime* kann ein Loop-Filter definiert werden, der in der Betriebsart *ASYNCHRON ERKENNEN/ERFASSEN* festlegt, nach welchen Kriterien ein Datenträger als *KOMMT (ERFASST)* oder als *GEHT (ABWESEND)* gemeldet wird und nach welchem zeitlichen Abstand ein als *GEHT* gemeldeter Datenträger erneut erfasst werden kann. So kann verhindert werden, dass bereits erfasste Datenträger versehentlich erneut erfasst werden oder dass unerwünschte Datenträger erfasst werden, die nur sporadisch antworten.

MinReads bzw. AsyncObserved-Threshold (default)

Parameter-ID: 0023_{hex}
 UHF-Manager: Menü: *Geräte Einstellungen > Parameter... > Lesen-Schreiben*
 OPC UA: *Methoden SetASyncFilter/GetASyncFilter*
 Webserver: Menü: *Konfiguration > RFID > Filteroptionen*

Der Parameter *MinReads (default)* legt fest, wie oft ein Datenträger erfasst werden muss, damit dieser als *KOMMT* gemeldet wird. Dieser Wert wird nach dem Einschalten oder dem Neustart der Auswerteeinheit eingestellt.

Soll ein Datenträger z. B. zweimal hintereinander erfasst werden, bevor er als *KOMMT* gemeldet wird, muss als Parameterwert 2 eingestellt werden.

Einstellbare Werte:

Länge [Bit]	Zulässige Werte	Werks-einstellung	Bedeutung
8	1...255	1	Benötigte Erfassungen um einen Datenträger als <i>Kommt</i> zu melden.

MinReads bzw. AsyncObserved-Threshold

Parameter-ID: 100C_{hex}
 UHF-Manager: –
 OPC UA: Methoden
 SetASyncFilter/GetASyncFilter
 Webserver: –

Der Parameter *MinReads* legt fest, wie oft ein Datenträger erfasst werden muss, damit dieser als *KOMMT* gemeldet wird. Dieser Parameter überschreibt den Parameter *MinReads (default)* und ist gültig, bis die aktuelle TCP-Session beendet oder die Auswerteeinheit neu gestartet wird.

Soll ein Datenträger z. B. zweimal hintereinander erfasst werden, bevor er als *KOMMT* gemeldet wird, muss als Parameterwert 2 eingestellt werden.

Einstellbare Werte:

Länge [Bit]	Zulässige Werte	Werks-einstellung	Bedeutung
8	1...255	1	Benötigte Erfassungen um einen Datenträger als <i>KOMMT</i> zu melden.

MinNoReads bzw. AsyncObserved-Timeout (default)

Parameter-ID: 0024_{hex}
 UHF-Manager: Menü: Geräte Einstellungen > Parameter... > Lesen-Schreiben
 OPC UA: Methoden
 SetASyncFilter/GetASyncFilter
 Webserver: Menü: Konfiguration > RFID > Filteroptionen

Der Parameter *MinNoReads (default)* legt fest, wie oft ein als *Kommt* gemeldeter Datenträger nicht erfasst werden muss, damit dieser als *GEHT* gemeldet wird. Dieser Wert wird nach dem Einschalten oder dem Neustart der Auswerteeinheit eingestellt.

Soll ein Datenträger z. B. erst dann als *GEHT* gemeldet werden, wenn er zweimal hintereinander nicht erfasst wurde, muss als Parameterwert 2 eingestellt werden.

Einstellbare Werte:

Länge [Bit]	Zulässige Werte	Werks-einstellung	Bedeutung
8	1...255	1	Benötigte Fehlerfassungen um einen Datenträger als <i>GEHT</i> zu melden.

MinNoReads bzw. AsyncObserved-Timeout

Parameter-ID: 100D_{hex}
 UHF-Manager: –
 OPC UA: Methoden
 SetASyncFilter/GetASyncFilter
 Webserver: –

Der Parameter *MinNoReads (default)* legt fest, wie oft ein als *KOMMT* gemeldeter Datenträger nicht erfasst werden muss, damit dieser als *GEHT* gemeldet wird. Dieser Parameter überschreibt den Parameter *MinNoReads (default)* und ist gültig, bis die aktuelle TCP-Session beendet oder die Auswerteeinheit neu gestartet wird.

Soll ein Datenträger z. B. erst dann als *GEHT* gemeldet werden, wenn er zweimal hintereinander nicht erfasst wurde, muss als Parameterwert 2 eingestellt werden.

Einstellbare Werte:

Länge [Bit]	Zulässige Werte	Werks-einstellung	Bedeutung
8	1...255	1	Benötigte Fehlerfassungen um einen Datenträger als <i>GEHT</i> zu melden.

WaitTime (default)

Parameter-ID: 0029_{hex}
 UHF-Manager: Menü: Geräte Einstellungen > Parameter... > Lesen-Schreiben
 OPC UA: Methoden
 SetASyncFilter/GetASyncFilter
 Webserver: Menü: Konfiguration > RFID > Filteroptionen

Der Parameter *WaitTime (default)* legt fest, nach welchem zeitlichen Abstand ein als *GEHT* gemeldeter Datenträger erneut erfasst werden kann. Dieser Wert wird nach dem Einschalten oder dem Neustart der Auswerteeinheit eingestellt.

Der 16-Bit-Wert wird in 2 Byte in der Reihenfolge Low-High codiert.

Einstellbare Werte:

Länge [Bit]	Zulässige Werte	Werks-einstellung	Bedeutung
16	0...1000	0	Zeit in Sekunden, die ein Datenträger ignoriert wird.

7

Inbetriebnahme und Betrieb (Fortsetzung)

WaitTime

Parameter-ID: 100E_{hex}
 UHF-Manager: –
 OPC UA: Methoden
 SetASyncFilter/GetASyncFilter
 Webserver: –

Der Parameter *WaitTime* legt fest, nach welchem zeitlichen Abstand ein als *Geht* gemeldeter Datenträger erneut erfasst werden kann. Dieser Parameter überschreibt den Parameter *WaitTime (default)* und ist gültig, bis die aktuelle TCP-Session beendet oder die Auswerteeinheit neu gestartet wird.

Der 16-Bit-Wert wird in 2 Byte in der Reihenfolge Low – High codiert.

Einstellbare Werte:

Länge [Bit]	Zulässige Werte	Werks-einstellung	Bedeutung
16	0...1000	0	Zeit in Sekunden, die ein Datenträger ignoriert wird

Datenfilter

Datenfilter können verwendet werden, wenn nur eine Untermenge aus einer Datenträgerpopulation erfasst werden soll. Dazu können verschiedene Kriterien festgelegt werden, die die gewünschte Untermenge beschreiben. So können zum Beispiel nur Datenträger erfasst werden, deren EPC einer gewissen Länge entspricht oder deren TID eine besondere Datensequenz enthält.

EPCLengthMin (default)

Parameter-ID: 002B_{hex}
 UHF-Manager: –
 OPC UA: Methoden SetFilter/GetFilter
 Webserver: –

Über die Parameter *EPCLengthMin* und *EPCLengthMax* kann ein Filter definiert werden, der Datenträger beim Erfassen ausschließt, wenn deren EPC-Länge nicht innerhalb des vorgegebenen Filterbereichs liegt.

Der Parameter *EPCLengthMin (default)* legt die minimale EPC-Länge in Byte fest, die nach dem Einschalten oder nach einem Neustart der Auswerteeinheit eingestellt wird.

Einstellbare Werte:

Länge [Bit]	Zulässige Werte	Werks-einstellung	Bedeutung
8	0...62	0 (0 Byte)	EPC Mindestlänge für Filter (default)

EPCLengthMin

Parameter-ID: 100F_{hex}
 UHF-Manager: –
 OPC UA: Methoden SetFilter/GetFilter
 Webserver: –

Über die Parameter *EPCLengthMin* und *EPCLengthMax* kann ein Filter definiert werden, der Datenträger beim Erfassen ausschließt, wenn deren EPC-Länge nicht innerhalb des vorgegebenen Filterbereichs liegt.

Der Parameter *EPCLengthMin* legt die minimale EPC-Länge in Byte fest und überschreibt den Parameter *EPCLengthMin (default)* bis die aktuelle TCP-Session beendet oder die Auswerteeinheit neu gestartet wird.

Einstellbare Werte:

Länge [Bit]	Zulässige Werte	Werks-einstellung	Bedeutung
8	0...62	0 (0 Byte)	EPC Mindestlänge für Filter (temporär)

EPCLengthMax (default)

Parameter-ID: 002C_{hex}
 UHF-Manager: –
 OPC UA: Methoden SetFilter/GetFilter
 Webserver: –

Über die Parameter *EPCLengthMin* und *EPCLengthMax* kann ein Filter definiert werden, der Datenträger beim Erfassen ausschließt, wenn deren EPC-Länge nicht innerhalb des vorgegebenen Filterbereichs liegt.

Der Parameter *EPCLengthMax (default)* legt die maximale EPC-Länge in Byte fest, die nach dem Einschalten oder nach einem Neustart der Auswerteeinheit eingestellt wird.

Einstellbare Werte:

Länge [Bit]	Zulässige Werte	Werks-einstellung	Bedeutung
8	0...62	62 (62 Byte)	EPC-Mindestlänge für Filter (default)

EPCLengthMax

Parameter-ID: 1010_{hex}
 UHF-Manager: –
 OPC UA: Methoden SetFilter/GetFilter
 Webserver: –

Über die Parameter *EPCLengthMin* und *EPCLengthMax* kann ein Filter definiert werden, der Datenträger beim Erfassen ausschließt, wenn deren EPC-Länge nicht innerhalb des vorgegebenen Filterbereichs liegt.

Der Parameter *EPCLengthMax* legt die maximale EPC-Länge in Byte fest und überschreibt den Parameter *EPCLengthMax (default)* bis die aktuelle TCP-Session beendet oder die Auswerteeinheit neu gestartet wird.

Einstellbare Werte:

Länge [Bit]	Zulässige Werte	Werks-einstellung	Bedeutung
8	0...62	62 (62 Byte)	EPC-Mindestlänge für Filter (temporär)

EPCFilter (default)

Parameter-ID: 002D_{hex}
 UHF-Manager: Menü: Geräte Einstellungen > Parameter... > Filter
 OPC UA: Methoden SetFilter/GetFilter
 Webserver: Menü: Konfiguration > RFID > Filteroptionen

Über den Parameter *EPCFilter (default)* kann ein konkreter Datenfilter angelegt werden, der Datenträger beim Erfassen direkt nach einer vorgegebenen Filtermaske aussortiert und nur die Datenträger meldet, die dieser Filtermaske entsprechen. Der Default-Filter wird nach dem Einschalten bzw. nach dem Neustart der Auswerteeinheit angewendet.

Die Filtermaske wird in der folgenden Form definiert:

Filtermaske = Adresse [1 Wort] + Länge [1 Wort] + Filterdaten [max. 62 Byte]

Adress- und Längenangaben müssen in Bits angegeben werden. So können Masken auch inmitten von Byte beginnen und enden.

Der Wertebereich jeweils beträgt 0...496 Bits.

Die Summe beider Werte darf 496 nicht überschreiten.

Die 16-Bit-Werte werden als 2 Byte in der Reihenfolge Low – High angegeben.

Das Feld *FILTERDATEN* muss mindestens so viele Byte beinhalten, dass damit die Anzahl Bits im Feld Länge übertragen werden können. Die Bits sind linksbündig auszurichten und am Ende auf eine ganze Bytelänge mit Null-Bits aufgefüllt werden.

Beispiel:

Es sollen nur Datenträger gemeldet werden, deren EPC ab Byte-Adresse 02_{hex} die Daten E2 00 01 02 03_{hex} (Länge 5 Byte) beinhaltet.

Byte-Adresse 0002_{hex} = Bitadresse 0010_{hex}

Byte-Länge 0005_{hex} = Bitlänge 0028_{hex}

Bitadresse [2 Byte]	Bitlänge [2 Byte]	Filterdaten (HEX) [5 Byte]
10 _{hex} 00 _{hex}	28 _{hex} 00 _{hex}	E2 00 01 02 03

Einstellbare Werte:

Länge [Byte]	Zulässige Werte	Werks-einstellung	Bedeutung
4...66	Adresse [2 Byte] Länge [2 Byte] Daten [62 Byte]	Adresse: 0000 _{hex} Länge: 0000 _{hex} Daten: 00 _{hex} ...	Filtern von Datenträgern nach EPC-Daten

7

Inbetriebnahme und Betrieb (Fortsetzung)

EPCFilter

Parameter-ID: 1011_{hex}
 UHF-Manager: –
 OPC UA: Methoden *SetFilter/GetFilter*
 Webserver: –

Über den Parameter *EPCFilter* kann ein konkreter Datenfilter angelegt werden, der Datenträger beim Erfassen direkt nach einer vorgegebenen Filtermaske aussortiert und nur die Datenträger meldet, die dieser Filtermaske entsprechen. Der Parameter *EPCFilter* überschreibt den Parameter *EPCFilter (default)* und ist gültig, bis die aktuelle TCP-Session beendet oder die Auswerteeinheit neu gestartet wird.

Die Filtermaske wird in der folgenden Form definiert:

Filtermaske = Adresse [1 Wort] + Länge [1 Wort] + Filterdaten [max. 62 Byte]

Die Adress- und Längenangaben müssen in Bits angegeben werden. So können Masken auch inmitten von Byte beginnen und enden.

Der Wertebereich jeweils beträgt 0...496 Bits.

Die Summe beider Werte darf 496 nicht überschreiten.

Die 16-Bit-Werte werden als 2 Byte in der Reihenfolge Low – High angegeben.

Das Feld *FILTERDATEN* muss mindestens so viele Byte beinhalten, dass damit die Anzahl Bits im Feld Länge übertragen werden können. Die Bits sind linksbündig auszurichten und am Ende auf eine ganze Bytelänge mit Null-Bits aufgefüllt werden.

Beispiel:

Es sollen nur Datenträger gemeldet werden, deren EPC ab Byte-Adresse 02_{hex} die Daten E2 00 01 02 03_{hex} (Länge 5 Byte) beinhaltet.

Byte-Adresse 0002_{hex} = Bitadresse 0010_{hex}

Byte-Länge 0005_{hex} = Bitlänge 0028_{hex}

Bitadresse [2 Byte]	Bitlänge [2 Byte]	Filterdaten (HEX) [5 Byte]
10 _{hex} 00 _{hex}	28 _{hex} 00 _{hex}	E2 00 01 02 03

Einstellbare Werte:

Länge [Byte]	Zulässige Werte	Werks- einstellung	Bedeutung
4...66	Adresse [2 Byte] Länge [2 Byte] Daten [62 Byte]	Adresse: 0000 _{hex} Länge: 0000 _{hex} Daten: 00 _{hex} ...	Filtern von Datenträgern nach EPC- Daten

TIDFilter (default)

Parameter-ID: 002E_{hex}
 UHF-Manager: Menü: *Geräte Einstellungen > Parameter... > Filter*
 OPC UA: Methoden *SetFilter/GetFilter*
 Webserver: Menü: *Konfiguration > RFID > Filteroptionen*

Über den Parameter *TIDFilter (default)* kann ein konkreter Datenfilter angelegt werden, der Datenträger beim Erfassen direkt nach einer vorgegebenen Filtermaske aussortiert und nur die Datenträger meldet, die dieser Filtermaske entsprechen. Der Default-Filter wird nach dem Einschalten bzw. nach dem Neustart der Auswerteeinheit angewendet.

Die Filtermaske wird in der folgenden Form definiert:

Filtermaske = Adresse [1 Wort] + Länge [1 Wort] + Filterdaten [max. 62 Byte]

Die Adress- und Längenangaben müssen in Bits angegeben werden. So können Masken auch inmitten von Byte beginnen und enden.

Der Wertebereich jeweils beträgt 0...496 Bits.

Die Summe beider Werte darf 496 nicht überschreiten.

Die 16-Bit-Werte werden als 2 Byte in der Reihenfolge Low – High angegeben.

Das Feld *FILTERDATEN* muss mindestens so viele Byte beinhalten, dass damit die Anzahl Bits im Feld Länge übertragen werden können. Die Bits sind linksbündig auszurichten und am Ende auf eine ganze Bytelänge mit Null-Bits aufgefüllt werden.

Beispiel:

Es sollen nur Datenträger gemeldet werden, deren TID ab Byte-Adresse 02_{hex} die Daten E2 00 01 02 03_{hex} (Länge 5 Byte) beinhaltet.

Byte-Adresse 0002_{hex} = Bitadresse 0010_{hex}

Byte-Länge 0005_{hex} = Bitlänge 0028_{hex}

Bitadresse [2 Byte]	Bitlänge [2 Byte]	Filterdaten (HEX) [5 Byte]
10 _{hex} 00 _{hex}	28 _{hex} 00 _{hex}	E2 00 01 02 03

Einstellbare Werte:

Länge [Byte]	Zulässige Werte	Werks- einstellung	Bedeutung
4...66	Adresse [2 Byte] Länge [2 Byte] Daten [62 Byte]	Adresse: 0000 _{hex} Länge: 0000 _{hex} Daten: 00 _{hex} ...	Filtern von Datenträgern nach EPC- Daten

TIDFilter

Parameter-ID: 1012_{hex}
 UHF-Manager: –
 OPC UA: Methoden *SetFilter/GetFilter*
 Webserver: –

Über den Parameter *TIDFilter* kann ein konkreter Datenfilter angelegt werden, der Datenträger beim Erfassen direkt nach einer vorgegebenen Filtermaske aussortiert und nur die Datenträger meldet, die dieser Filtermaske entsprechen. Der Parameter *TIDFilter* überschreibt den Parameter *TIDFilter (default)* und ist gültig, bis die aktuelle TCP-Session beendet oder die Auswerteeinheit neu gestartet wird. Die Filtermaske wird in der folgenden Form definiert:

Filtermaske = Adresse [1 Wort] + Länge [1 Wort] + Filterdaten [max. 62 Byte]

Die Adress- und Längenangaben müssen in Bits angegeben werden. So können Masken auch inmitten von Byte beginnen und enden.

Der Wertebereich jeweils beträgt 0...496 Bits.

Die Summe beider Werte darf 496 nicht überschreiten.

Die 16-Bit-Werte werden als 2 Byte in der Reihenfolge Low – High angegeben.

Das Feld *FILTERDATEN* muss mindestens so viele Byte beinhalten, dass damit die Anzahl Bits im Feld Länge übertragen werden können. Die Bits sind linksbündig auszurichten und am Ende auf eine ganze Bytelänge mit Null-Bits aufgefüllt werden.

Beispiel:

Es sollen nur Datenträger gemeldet werden, deren TID ab Byte-Adresse 02_{hex} die Daten E2 00 01 02 03_{hex} (Länge 5 Byte) beinhaltet.

Byte-Adresse 0002_{hex} = Bitadresse 0010_{hex}

Byte-Länge 0005_{hex} = Bitlänge 0028_{hex}

Bitadresse [2 Byte]	Bitlänge [2 Byte]	Filterdaten (HEX) [5 Byte]
10 _{hex} 00 _{hex}	28 _{hex} 00 _{hex}	E2 00 01 02 03

Einstellbare Werte:

Länge [Byte]	Zulässige Werte	Werks- einstellung	Bedeutung
4...66	Adresse [2 Byte] Länge [2 Byte] Daten [62 Byte]	Adresse: 0000 _{hex} Länge: 0000 _{hex} Daten: 00 _{hex} ...	Filtern von Datenträgern nach <i>TID</i> -Daten

RSSI-Filter

Beim Erfassen von Datenträgern kann die Auswerteeinheit intern Messungen vornehmen, die eine Aussage darüber erlauben, mit welcher Signalstärke der Datenträger empfangen wurde. Über die ermittelte Signalstärke, dem RSSI-Wert, kann ein Filter definiert werden, der beim Erfassen von Datenträgern nur die Datenträger meldet, deren RSSI innerhalb eines vorgegebenen Bereichs liegt.

Vereinfacht kann gesagt werden, dass ein Datenträger, der sich nahe der Antenne befindet, im ungestörten Umfeld zu einem höheren RSSI führt als ein Datenträger, der weiter entfernt ist. So könnten z. B. weiter entfernte Datenträger, die nicht erfasst werden sollen, ausgeblendet werden.

Über die Parameter *RSSIMinFilter* und *RSSIMaxFilter* kann der gewünschte RSSI-Bereich vorgegeben werden. Der gesamte RSSI-Bereich umfasst Werte von –128 bis +127. Wenn das Minimum auf 128 und das Maximum auf +127 gesetzt wird, passieren alle erfassten Datenträger den Filter.

RSSIMinFilter (default)

Parameter-ID: 002F_{hex}
 UHF-Manager: Menü: *Geräte Einstellungen > Parameter... > Filter*
 OPC UA: Methoden *SetFilter/GetFilter*
 Webserver: Menü: *Konfiguration > RFID > Filteroptionen*

RSSIMinFilter (default) legt fest, welche RSSI-Untergrenze für die Erfassung verwendet werden soll. Der festgelegte Wert wird von der Auswerteeinheit nach dem Einschalten oder nach dem Neustart der Auswerteeinheit verwendet.

Einstellbare Werte:

Länge [Byte]	Zulässige Werte	Werks- einstellung	Bedeutung
1	–128...+127	–128	<i>RSSI</i> -Untergrenze für den <i>RSSI</i> -Filter

7

Inbetriebnahme und Betrieb (Fortsetzung)

RSSIMinFilter

Parameter-ID: 1013_{hex}
 UHF-Manager: –
 OPC UA: Methoden *SetFilter/GetFilter*
 Webserver: –

RSSIMinFilter überschreibt den Parameter *RSSIMinFilter (default)* und legt fest, welche RSSI-Untergrenze für die Erfassung verwendet werden soll. Der Parameter ist gültig, bis die aktuelle TCP-Session beendet oder die Auswerteeinheit neu gestartet wird.

Einstellbare Werte:

Länge [Byte]	Zulässige Werte	Werks-einstellung	Bedeutung
1	–128...+127	–128	RSSI-Untergrenze für den RSSI-Filter

RSSIMaxFilter (default)

Parameter-ID: 0030_{hex}
 UHF-Manager: Menü: *Geräte Einstellungen > Parameter... > Filter*
 OPC UA: Methoden *SetFilter/GetFilter*
 Webserver: Menü: *Konfiguration > RFID > Filteroptionen*

RSSIMaxFilter (default) legt fest, welche RSSI-Obergrenze für die Erfassung verwendet werden soll. Der festgelegte Wert wird von der Auswerteeinheit nach dem Einschalten oder nach dem Neustart der Auswerteeinheit verwendet.

Einstellbare Werte:

Länge [Byte]	Zulässige Werte	Werks-einstellung	Bedeutung
1	–128...+127	+127	RSSI-Obergrenze für den RSSI-Filter

RSSIMaxFilter

Parameter-ID: 1014_{hex}
 UHF-Manager: –
 OPC UA: Methoden *SetFilter/GetFilter*
 Webserver: –

RSSIMaxFilter überschreibt den Parameter *RSSIMaxFilter (default)* und legt fest, welche RSSI-Obergrenze für die Erfassung verwendet werden soll. Der Parameter ist gültig, bis die aktuelle TCP-Session beendet oder die Auswerteeinheit neu gestartet wird.

Einstellbare Werte:

Länge [Byte]	Zulässige Werte	Werks-einstellung	Bedeutung
1	–128...+127	+127	RSSI-Obergrenze für den RSSI-Filter

FormattedTagData

Die Funktion *FormattedTagData* kann verwendet werden, wenn verschiedene Datenbereiche eines Datenträgers erfasst oder bearbeitet werden sollen oder wenn die Daten einer besonderen Formatierung entsprechen sollen. Dafür bietet *FormattedTagData* den Komfort, dass die Auswerteeinheit eigenständig alle Befehle ausführt, die notwendig sind, um die erforderlichen Daten in der gewünschten Formatierung zu erfassen oder zu bearbeiten.

Über die Parameter *Präfix für ReadMultipleTagDataFormatted* und *Suffix für ReadMultipleTagDataFormatted* können Text- oder Byte-Sequenzen definiert werden, die den Daten, die mit *ReadMultipleTagDataFormatted* definiert wurden, voran- bzw. nachgestellt werden. So könnte z. B. eine XML-ähnliche Struktur aufgebaut werden.

Beispiel:

Präfix: #0A#0D<TAGLIST>
Format-String: #A#0D<TAG><EPC>%Ex[0, 12]</EPC></TAG>
Suffix: #0A#0D</TAGLIST>

Die formatierten Daten beim Befehl *ReadTagDataFormatted* und *WriteFormattedTagData* werden ohne Präfix und Suffix in folgendem Format übertragen:

FormattedTagData = *FormatierteDaten(Tag)*

Die formatierten Daten beim Befehl *ReadMultipleTagDataFormatted* werden mit Präfix und Suffix in folgendem Format übertragen:

FormattedTagData = *Präfix* + *FormatierteDaten(1.Tag)* + *FormatierteDaten(2.Tag)* + ... + *Suffix*

In einer XML-Datei abgebildet könnten die Daten wie folgt aussehen:

```
<TAGLIST>
  <TAG><EPC>E20102030405060708090A0B</EPC></TAG>
  <TAG><EPC>E20B0A090807060504030201</EPC></TAG>
</TAGLIST>
```



Die folgenden Parameter zur Funktion *FormattedTagData* sind sessionbezogen und nur solange gültig, bis die aktuelle TCP-Session beendet oder die Auswerteeinheit neu gestartet wird. Zur Einstellung der Default-Parameter, die permanent gespeichert werden, ist ein Zugang der Sicherheitsebene Administrator notwendig (siehe *Parameter für Administratoren* auf Seite 52).

Formatdefinition für ReadTagDataFormatted, ReadMultipleTagDataFormatted und WriteFormattedTagData

Parameter-ID: 1008_{hex}
UHF-Manager: –
OPC UA: Methode
SetTagDataFormat/GetTagDataFormat
Webserver: –

Über diesen Parameter kann festgelegt werden, welches Datenformat für die Funktionen *FormattedTagData* verwendet werden soll. Dazu kann aus verschiedenen Formatelementen ein Format-String erstellt werden, der Art und Formatierung der Daten beschreibt, wobei die Elemente beliebig kombiniert werden können. Im 007-Protokoll können bis 99 Zeichen definiert werden. Mit OPC UA oder mit dem Webinterface können auch längere Zeichenketten (bis 1024 Zeichen) definiert werden, die auch im 007-Protokoll gültig sind.

Adress- und Längfelder:

Feld	Bedeutung
Adresse (Byte-Format)	Adressiert Daten als Byte-Offset (Dezimal: 0...65535).
Adresse (Byte.Bit-Format)	Startadresse: Adressiert Daten als Byte-Offset mit Bit-Offset (Dezimal: 0.0...65535.8)
Länge	Bei Adresse (Byte-Format): Anzahl Byte Bei Adresse (Byte.Bit-Format): Anzahl Bits

Ausgabeelemente:

Element	Bedeutung
#	Ausgabe: Definiert einen Byte-Wert (Hex) z. B. #0D#0A für die ASCII-Zeichenfolge 'Carriage Return' 'Line Feed'
##	Ausgabe: Gibt das ASCII-Zeichen '#' aus
%%	Ausgabe: Gibt das ASCII-Zeichen '%' aus
Text	Ausgabe: Beliebiger Text, der ausgegeben werden soll
%A[Adresse, Länge]	Access: Gibt den angegebenen Bereich des Zugriffspassworts im Hex-Format aus
%E[Adresse, Länge]	EPC: Gibt den angegebenen Bereich des EPC im Hex-Format aus
%P[Adresse, Länge]	PC: Gibt den angegebenen Bereich des Protocol-Control-Word aus dem EPC-Speicher im Hex-Format aus

7

Inbetriebnahme und Betrieb (Fortsetzung)

Element	Bedeutung
%T[Adresse, Länge]	TID: Gibt den angegebenen Bereich der TID im Hex-Format aus
%U[Adresse, Länge]	USER: Gibt den angegebenen Bereich der User-Daten im Hex-Format aus

Datenmodifizierer:

Modifizierer	Bedeutung
%d...	Modifizierer d: Gibt Daten als Dezimalzahl im ASCII-Format aus (ASCII: 0...9)
%x...	Modifizierer x: Gibt Daten als HEX-Byte im ASCII-Format aus (ASCII: 0...9a...f)
%X...	Modifizierer X: Gibt Daten als HEX-Byte im ASCII-Format aus (ASCII: 0...9A...F)

Ausgabe von Statuswerten:

Element	Bedeutung
%S[0, 1]	Gibt den Lesestatus aus 0: OK 1: Lesefehler 2: Signaturfehler
%S[1, 1]	Gibt die EPC-Länge aus (Anzahl Byte 2...62)
%S[2, 1]	Gibt den RSSI aus (–128...+127)
%S[3, 1]	Immer 00 _{hex} , mit S[3.0,n], mit n = 1 bis 8 können bis zu 8 Füllbits 0 im Datenstrom erzeugt werden
%S[4, 1]	Immer FF _{hex} , mit S[4.0,n], mit n = 1 bis 8 können bis zu 8 Füllbits 1 im Datenstrom erzeugt werden

Beispiel:

In diesem Beispiel liegt ein Datenträger vor, der folgende Daten enthält:

EPC (12 Byte): E2 01 02 03 04 05 06 07 08 09 0A 0B_{hex}

TID (8 Byte): C0 11 12 13 14 15 16 17_{hex}

USER (5 Byte): 48 41 4C 4C 4F_{hex}

Format-String	Ausgabe
E[0, 12]	E2 01 02 03 04 05 06 07 08 09 0A 0B _{hex}
EX[0, 12]	„E2 01 02 03 04 05 06 07 08 09 0A 0B“
<EPC>%Ex[0, 6]</EPC>	„<EPC>e2 01 02 03 04 05 </EPC>“
EPC:%E[0, 4] ; USER:%UX[0, 5]	„EPC:“ E2 01 02 03hex „ ; USER:48414C4F“
LSB=%Td[0, 1] -MSB=%Td[7, 1]	„LSB=192-MSB=23“
LSB Half-Byte: = Ed[7.4, 4]	„LSB Half-Byte: = 7“



Über die Webserver-Oberfläche im Bereich Konfiguration > RFID > Formatierte Tagdaten können die Formatelemente und deren Auswirkungen auf einfache Weise getestet werden.

Einstellbare Werte:

Länge [Byte]	Zulässige Werte	Werkseinstellung	Bedeutung
007: 0...99 Web und OPC UA: 0...1024	Format-String	„%Ex[0,12]#0d#0a“ EPC-String mit CR LF	Format-String für <i>FormattedTag-Data</i>



Dieser Parameter ist sessionbezogen und hat Gültigkeit bis die aktuelle TCP-Session beendet oder die Auswerteeinheit neu gestartet wird. Zum Festlegen der permanent gespeicherten Default-Werte ist ein Zugang zur Sicherheitsebene Administrator erforderlich (siehe *Parameter für Administratoren* auf Seite 52).

Präfix für ReadMultipleTagDataFormatted

Parameter-ID: 1009_{hex}
 UHF-Manager: –
 OPC UA: Methode
 SetTagDataFormat/GetTagDataFormat
 Webserver: –

Präfix für ReadMultipleTagDataFormatted legt die Text- oder Byte-Sequenz fest, die den Daten, die mit ReadMultipleTagDataFormatted definiert wurden, vorangestellt werden soll.

Einstellbare Werte:

Länge [Byte]	Zulässige Werte	Werkseinstellung	Bedeutung
007: 0...99 Web und OPC UA: 0...1024	String	„Begin#0d#0a“ Text „Begin“ mit CR LF	Präfix für ReadMultipleTag- DataForm- atted

Suffix für ReadMultipleTagDataFormatted

Parameter-ID: 100A_{hex}
 UHF-Manager: –
 OPC UA: Methode
 SetTagDataFormat/GetTagDataFormat
 Webserver: –

Suffix für ReadMultipleTagDataFormatted legt die Text- oder Byte-Sequenz fest, die den Daten, die mit ReadMultipleTagDataFormatted definiert wurden, nachgestellt werden soll.

Einstellbare Werte:

Länge [Byte]	Zulässige Werte	Werkseinstellung	Bedeutung
007: 0...99 Web und OPC UA: 0...1024	String	„End#0d#0a“ Text „End“ mit CR LF	Suffix für ReadMultipleTag- DataForm- atted

Berechnungsformat für die Signaturerzeugung

Parameter-ID: 100B_{hex}
 UHF-Manager: –
 OPC UA: Methode SetTagSignatureFormat/
 GetTagSignatureFormat
 Webserver: –

Definiert die Datenbereiche des Datenträgers, die in die Berechnung zur Erzeugung und Prüfung der Signatur einbezogen werden (üblicherweise den EPC und den TID, bei Datenträgern mit größerem Speicher eventuell auch einen Teil des User-Daten-Bereichs). Der Bereich, in dem die Signatur selbst abgelegt wird (derzeit die ersten 64 Byte des User-Daten-Bereichs) darf nicht mit einbezogen werden.

Die Angabe muss bei der Signaturerzeugung und der Signaturprüfung exakt identisch sein, sonst kann die Signatur nicht als gültig erkannt werden.

Die Angaben werden in der gleichen Systematik erzeugt wie für die formatierte Ausgabe, wobei die Angabe von Formatmodifizierern (X, x, oder d) nicht sinnvoll ist.

Beispiele:

Es sollen 12 Byte des EPC und 12 Byte des TID einbezogen werden:

Berechnungsformat: „%E[0,12]%T[0,12]“

Es sollen 12 Byte des EPC und 12 Byte des TID und 16 Byte des User-Daten-Bereichs ab Adresse 64 einbezogen werden:

Berechnungsformat: „%E[0,12]%T[0,12]%U[64,16]“

Details zur Signaturerzeugung und Prüfung siehe *Datensicherheit* auf Seite 11.

Einstellbare Werte:

Länge [Byte]	Zulässige Werte	Werkseinstellung	Bedeutung
007: 0...99 Web und OPC UA: 0...1024	String	„%E[0,12]%T[0,8]“ 12 Byte EPC + 8 Byte TID	Berechnungsfor- mat für die Signa- turerzeu- gung

7.3.5 Beschreibung der Parameter für Administratoren

Parameter für Administratoren können von Benutzern der Sicherheitsebene *ADMIN* verändert werden. Dazu ist ein Login der entsprechenden Sicherheitsebene erforderlich. Administratorparameter werden dauerhaft in der Auswerteeinheit gespeichert und behalten ihren Wert, bis sie überschrieben werden.

Die Administratorparameter beschreiben vor allem die Konfiguration der angeschlossenen UHF-Hardware, der System- und Netzwerkeigenschaften sowie Default-Parameter für Sonderfunktionen wie *Automatischer Scan*, *FormattedTagData* und Datenträgersignatur.

Die Netzwerkparameter sind für den Betrieb der Auswerteeinheit innerhalb eines Netzwerks notwendig und müssen zur Netzwerkanbindung parametrisiert werden. Systemparameter, wie z. B. *Uhrzeit* oder *Zeitzone* sind nur für bestimmte Gerätefunktionen notwendig, sollten aber korrekt eingestellt werden, um Fehlfunktionen zu vermeiden.



Parameter zur Konfiguration der UHF-Komponenten werden von der Auswerteeinheit verwendet, um eine korrekte Berechnung der abgestrahlten Sendeleistung durchzuführen. Daher sollten diese Parameter anhand der Datenblätter der verwendeten UHF-Komponenten eingestellt werden!

Folgende Gruppen von Administratoren-Parametern werden beschrieben:

- *UHF-Komponenten* (siehe Seite 73)
- *Netzwerk, System* (siehe Seite 75)
- *FormattedTagData (default)* (siehe Seite 79)

Automatisches Scannen

Parameter-ID: 000F_{hex}
 UHF-Manager: Menü: *Geräte Einstellungen > Parameter... > Basic UHF*
 OPC UA: –
 Webserver: –

Durch den Parameter *Automatisches Scannen* kann festgelegt werden, ob und in welchem zeitlichen Abstand eine Antenne den Erfassungsbereich automatisch überwachen soll. Daten, die dabei erfasst werden, werden in dem Format übertragen, das über die Parameter zur Funktion *ReadMultipleTagDataFormatted* festgelegt wurde, siehe Parameter *Formatdefinition für ReadTagDataFormatted*, *ReadMultipleTagDataFormatted* und *WriteFormattedTagData*.

Automatisches Scannen kann für jede TCP-Session unabhängig parametrisiert werden, wobei jeder Session entweder eine Antenne oder alle aktiven Antennen zugeordnet sind. Die Daten werden auf einem separaten TCP-Port als reine Nutzdaten (ohne Protokoll-Overhead) übertragen. So bleibt die Netzlast auf der Hauptverbindung gering und die Daten können ohne Protokollkenntnisse verarbeitet werden. Lediglich die Formatierung der Daten muss bekannt sein.

Beim Abspeichern dieses Parameters werden die Antennenauswahl und die maximale Anzahl an Datenträgern aus dem letzten *UniversalTagList*-Kommando festgehalten und für die Ausführung des automatischen Scanvorgangs benutzt.

Für *Automatisches Scannen* gilt folgende Belegung der TCP-Ports:

Session	TCP-Session über die parametrisiert wird	TCP-Session auf der Daten übertragen werden
1	10001	10011
2	10002	10012
3	10003	10013
4	10004	10014
5	10005	10015

Der Parameter wird als Zeitwert in vielfachen von 10 ms übergeben, wobei der Wert Null bedeutet, dass *Automatisches Scannen* ausgeschaltet ist.

Zeitintervall = (0...255) × 10 ms
 (0: Aus, 10 ms...2550 ms)

Einstellbare Werte:

Länge [Bit]	Zulässige Werte	Werkeinstellung	Bedeutung
8	0...255	0 (Aus)	Wartezeit zwischen zwei automatischen Erfassungen

AsyncScanDelay

Parameter-ID: 0011_{hex}
 UHF-Manager: Menü: *Geräte Einstellungen > Parameter... > Lesen > Schreiben*
 OPC UA: –
 Webserver: Menü: *Konfiguration > RFID > Filteroptionen*

Durch *AsyncScanDelay* kann die Zykluszeit festgelegt werden, mit der in der Betriebsart *ASYNCHRON ERKENNEN/ERFASSEN* nach neuen Datenträgern im Erfassungsbereich gesucht wird.

Zeitintervall = (0...255) × 10 ms
 (0: Aus, 10 ms...2550 ms)

Einstellbare Werte:

Länge [Bit]	Zulässige Werte	Werks-einstellung	Bedeutung
8	1...255	5 Zykluszeit 50 ms	Zykluszeit beim <i>ASYNCHRONEN</i> <i>ERKENNEN/</i> <i>ERFASSEN</i>

UHF-Komponenten

Durch die Konfiguration der UHF-Komponenten können Antennenports aktiviert bzw. deaktiviert und die angeschlossenen UHF-Komponenten hinsichtlich ihrer physikalischen Eigenschaften beschrieben werden.

Die Beschreibung der physikalischen Eigenschaften erfolgt über die Parameter *Antennengewinn* und *Kabeldämpfung*. Diese Parameter werden von der Auswerteeinheit benötigt, um die abgestrahlte Sendeleistung korrekt berechnen zu können. Die Werte können den Datenblättern der verwendeten UHF-Komponenten entnommen werden.



Die abgestrahlte Sendeleistung unterliegt nationalen Vorschriften und muss deshalb auf den maximal erlaubten Wert begrenzt werden. Durch die korrekte Angabe des Antennengewinns und der Kabeldämpfung kann die Auswerteeinheit das Begrenzen selbständig durchführen und somit die Einhaltung der Vorschriften gewährleisten. Darüberhinaus führt die korrekte Berechnung der abgestrahlten Sendeleistung auch zu reproduzierbaren Ergebnissen, wenn z. B. Antennentyp oder Kabellänge geändert wird.



Bei Verwendung von Balluff Antennen BIS U-3xx und Balluff Antennenkabeln BIS U-5xx können die UHF-Komponenten auf einfache Weise über die Konfigurationssoftware UHF-Manager oder den Webserver parametrierbar werden. Die Balluff Komponenten können über ihre Typenbezeichnung direkt ausgewählt werden. Alle erforderlichen Parameter werden dann automatisch gewählt.

7

Inbetriebnahme und Betrieb (Fortsetzung)

Aktive Antennen

Parameter-ID: 0012_{hex}
 UHF-Manager: Menü: *Geräte Einstellungen > Parameter... > Basic UHF*
 OPC UA: Variable *AntennaActive*
 Webserver: Menü: *Konfiguration > RFID > Basis UHF*

Über den globalen Parameter *Aktive Antennen* kann festgelegt werden, welche der vier Antennen aktiviert bzw. deaktiviert werden sollen. Der Parameter wird dauerhaft gespeichert und behält seinen Wert auch nach einem Neustart der Auswerteeinheit. Die einzelnen Antenne können über eine Bitmaske aktiviert (1) bzw. deaktiviert (0) werden.

Beispiel:

Aktive Antennen	Bit 7...Bit 4	Bit 3	Bit 2	Bit 1	Bit 0	Byte
1 und 3 aktiviert, 2 und 4 deaktiviert	0	0	1	0	1	05 _{hex}

Einstellbare Werte:

Länge [Bit]	Zulässige Werte	Werks-einstellung	Bedeutung
8	Bitmaske 0F _{hex} ...00 _{hex}	0F _{hex} Alle Antennen ein	Bit 0: Antenne 1 Bit 1: Antenne 2 Bit 2: Antenne 3 Bit 3: Antenne 4



Die Auswerteeinheit verfügt über eine Portüberwachung, über die erkannt werden kann, ob an einem aktiven Antennenport eine Antenne angeschlossen ist. Wenn keine Antenne angeschlossen ist oder ein Kabelbruch vorliegt, wird eine Kabelbruchmeldung ausgegeben (siehe Kapitel 7.4 auf Seite 85).

Antennengewinn

Parameter-ID: 0013_{hex}
 UHF-Manager: Menü: *Geräte Einstellungen > Parameter... > Sendeleistung*
 OPC UA: –
 Webserver: Menü: *Konfiguration > RFID > Antennen & Leistung*

Der *Antennengewinn* ist eine physikalische Eigenschaft der Antenne, die beschreibt, wieviel der eingespeisten Sendeleistung in Hauptstrahlrichtung abgestrahlt wird. Der *Antennengewinn* beschreibt damit Wirkungsgrad und Richtwirkung der Antenne. Abhängig vom Hersteller der Antenne wird der *Antennengewinn* im Datenblatt unterschiedlich angegeben.

Einheit	Abkürzung	Bedeutung
dBi	G _i	<i>Antennengewinn</i> (linear) bezogen auf einen isotropen Kugelstrahler
dBiC	G _{iC}	<i>Antennengewinn</i> GC (zirkular) bezogen auf einen isotropen Kugelstrahler
dBd	G _D	<i>Antennengewinn</i> bezogen auf einen Halbwellendipol

Der Parameter *Antennengewinn* wird als Antennengewinn bezogen auf einen Halbwellendipol (GD). Je nach Datenblattangabe kann eine Umrechnung in dBd erforderlich sein:

Datenblattangabe	Umrechnung in G _D
G _i (dB _i)	G _D = G _i – 2,15 dB
G _{iC} (dB _{iC})	G _D = G _i – 5,15 dB

Als Parameterwert wird der Antennengewinn G_D in dB/20 angegeben.

Parameterwert =	$\frac{G_D[\text{dBd}]}{0,05 \text{ dB}}$

Einstellbare Werte:

Länge [Bit]	Zulässige Werte	Werks-einstellung	Bedeutung
8	–400...+400	67 (entspricht 3,35 dBd bzw. 5,5 dBi)	<i>Antennengewinn</i> G _D in dB/20 Schritten



Der Parameter sollte aktualisiert werden, wenn sich der verwendete Antennentyp ändert.

7

Inbetriebnahme und Betrieb (Fortsetzung)

Kabeldämpfung

Parameter-ID: 0014_{hex}
 UHF-Manager: Menü: *Geräte Einstellungen > Parameter... > Sendeleistung*
 OPC UA: –
 Webserver: Menü: *Konfiguration > RFID > Antennen & Leistung*

Die Kabeldämpfung ist eine physikalische Eigenschaft des Antennenkabels, die beschreibt, um welchen Faktor ein Signal entlang des Antennenkabels abgeschwächt wird. Die Kabeldämpfung kann dem Datenblatt des verwendeten Antennenkabels entnommen werden. Üblicherweise wird die Kabeldämpfung bezogen auf 1 m Länge angegeben. Dadurch ergibt sich folgender Zusammenhang:

$$\text{Kabeldämpfung [dB]} = \text{Dämpfung} \left[\frac{[\text{dB}]}{\text{m}} \right] \times \text{Kabellänge [m]}$$

Als Parameterwert wird der Antennengewinn G_D in dB/20 angegeben.

$$\text{Parameterwert} = \frac{\text{Kabeldämpfung [dB]}}{0,05 \text{ dB}}$$

Einstellbare Werte:

Länge [Bit]	Zulässige Werte	Werks-einstellung	Bedeutung
8	0...400	7 (entspricht 0,35 dB)	Kabeldämpfung in dB/20 Schritten

Netzwerk, System

Über die Netzwerk- und Systemparameter können allgemeine Einstellungen vorgenommen werden, die für den Betrieb in einem Netzwerk erforderlich sind und gegebenenfalls Zusatzinformation wie Zeit und Gerätestandort bereitgestellt werden.

Im Auslieferungszustand werden folgende Netzwerkparameter verwendet:

- IP-Adresse (IPv4): 192.168.10.2
- Netmask: 255.255.255.0
- Gateway: 192.168.10.254
- Hostname: BISU6127

IP-Address

Parameter-ID: 0019_{hex}
 UHF-Manager: Menü: *Programm Einstellungen > Schnittstelle... > CP/IP*
 OPC UA: –
 Webserver: Menü: *Konfiguration > Netzwerk*

Über die IP-Adresse (IPv4) kann die Auswerteeinheit innerhalb des Netzwerks identifiziert und angesprochen werden. Jede IP-Adresse kann innerhalb eines Subnetzes nur einmal belegt werden. Die IP-Adresse wird über ein Byte-Array der Länge 4 Byte im HEX- oder Dezimal-Format übergeben.

Beispiel:

IP-Adresse	Parameterwert Dezimal	Parameterwert HEX
192.168.10.2	192 168 10 2	C0 A8 0A 02 _{hex}

Einstellbare Werte:

Länge [Byte]	Zulässige Werte	Werks-einstellung	Bedeutung
4	Gültige IPv4-Adresse MSB...LSB	192 168 10 2	IPv4-Adresse

Die Übernahme der Werte erfolgt erst nach einem Geräte-neustart.

7

Inbetriebnahme und Betrieb (Fortsetzung)

Netmask

Parameter-ID: 001A_{hex}
 UHF-Manager: Menü: *Programm Einstellungen > Schnittstelle... > TCP/IP*
 OPC UA: –
 Webserver: Menü: *Konfiguration > Netzwerk*

Über die *Netzmaske* wird festgelegt, wie die IP-Adresse zu interpretieren ist bzw. welche Teile der IP-Adresse zur Identifikation des Netzwerks verwendet werden und welche zur Identifikation des Geräts.

Beispiel: Mit der Netzmaske 255.255.255.0 werden die ersten 3 Byte (MSB...) zur Adressierung des Netzwerks verwendet und nur das letzte Byte (LSB) zur Adressierung des Geräts. Somit können 254 Teilnehmer adressiert werden (z. B. über die IP-Adressen 10.0.0.1...10.0.0.254) ohne einen Router zu verwenden.

Die *Netzmaske* wird über ein Byte-Array der Länge 4 Byte im HEX- oder Dezimal-Format übergeben.

Beispiel:

Netmask	Parameterwert Dezimal	Parameterwert HEX
255.255.255.0	255 255 255 0	FF FF FF 00 _{hex}

Einstellbare Werte:

Länge [Byte]	Zulässige Werte	Werks- einstellung	Bedeutung
4	Gültige Netzmaske MSB...LSB	255 255 255 0	IPv4-Netz- maske

Die Übernahme der Werte erfolgt erst nach einem Geräte-neustart.

DHCP

Parameter-ID: 001B_{hex}
 UHF-Manager: Menü: *Programm Einstellungen > Schnittstelle... > CP/IP*
 OPC UA: –
 Webserver: Menü: *Konfiguration > Netzwerk*

Über *DHCP* (Dynamic Host Configuration Protocol) kann festgelegt werden, ob die Auswerteeinheit für die Netzwerkkommunikation statische, manuell festgelegte Netzwerkparameter (*IP-Adresse, Netzmaske, Gateway, ...*) verwenden soll, oder ob diese Parameter automatisch vom Netzwerk bezogen werden sollen.



DHCP kann nur in einem Netzwerk verwendet werden, das die dynamische Vergabe von IP-Adressen erlaubt. Dies muss vor dem Aktivieren von DHCP sichergestellt werden, da sonst unter Umständen nicht mehr über das Netzwerk auf die Auswerteeinheit zugegriffen werden kann. Im Notfall kann diese Einstellung über den Service-Port (USB) rückgängig gemacht werden. Dazu ist ein Servicekabel M12-USB erforderlich (siehe Kapitel 10.3 auf Seite 173).

Einstellbare Werte:

Länge [Byte]	Zulässige Werte	Werks- einstellung	Bedeutung
1	0, 1	0 Kein DHCP	0: Kein DHCP 1: DHCP

Die Übernahme des Werts erfolgt erst nach einem Geräte-neustart.

7

Inbetriebnahme und Betrieb (Fortsetzung)

Hostname

Parameter-ID: 001C_{hex}
 UHF-Manager: Menü: *Geräte Einstellungen > Parameter... > Geräteparameter*
 OPC UA: Variable *DeviceName*
 Webserver: Menü: *Konfiguration > Gerät*

Befindet sich im Netzwerk mit der Auswerteeinheit ein DNS-Server, kann die Auswerteeinheit alternativ zur IP-Adresse auch über den *Hostname* (Gerätename) angesprochen werden. Der *Hostname* muss dazu einzigartig sein und darf innerhalb des Subnetzes, in dem sich das Gerät befindet, nur einmal vorkommen.

Einstellbare Werte:

Länge [Byte]	Zulässige Werte	Werks-einstellung	Bedeutung
1...63	String mit maximal 63 Zeichen	„BISU6127“	Gerätename ¹⁾ zur Identifikation im Netzwerk

¹⁾ Es dürfen nur die Zeichen A...Z, a...z, 0...9 und '-' verwendet werden, wobei das '-' nicht am Beginn stehen darf.

Die Übernahme des Werts erfolgt erst nach einem Geräte-neustart.

Gateway

Parameter-ID: 001D_{hex}
 UHF-Manager: Menü: *Programm Einstellungen > Schnittstelle... > TCP/IP*
 OPC UA: –
 Webserver: Menü: *Konfiguration > Netzwerk*

Legt das *Standard Gateway* für die TCP/IP-Verbindung fest. Normalerweise ist dies die IP-Adresse des Routers, der die Verbindung zu anderen Netzwerksegmenten herstellt.

Einstellbare Werte:

Länge [Byte]	Zulässige Werte	Werks-einstellung	Bedeutung
4	0.0.0.0 oder gültige IPv4 Adresse	192.168.10.254	Adresse des <i>Standard Gateways</i>

Die Übernahme der Werte erfolgt erst nach einem Geräte-neustart.

Nameserver

Parameter-ID: 001E_{hex}
 UHF-Manager: –
 OPC UA: –
 Webserver: Menü: *Konfiguration > Netzwerk*

Wenn das Netzwerk über *DNS-Server (Domain Name System)* verfügt, kann über den Parameter *Nameserver* die IP-Adresse des primären (DNS IP1) und des alternativen (DNS IP2, sofern vorhanden) DNS-Servers festgelegt werden.

Einstellbare Werte:

Länge [Byte]	Zulässige Werte	Werks-einstellung	Bedeutung
8	Zweimal 0.0.0.0 oder gültige IP-Adresse	0 0 0 0 0 0 0 0	IP-Adressen der DNS-Server 1 und 2.

7

Inbetriebnahme und Betrieb (Fortsetzung)

Gerätestandort

Parameter-ID: 001F_{hex}
 UHF-Manager: Menü: *Geräte Einstellungen > Parameter... > Geräteparameter*
 OPC UA: –
 Webserver: Menü: *Konfiguration > Gerät*

Der Parameter *Gerätestandort* kann als beliebiger Freitext festgelegt werden und soll dabei helfen, das Gerät innerhalb der Anlage zu lokalisieren, z. B. wenn Wartungsarbeiten anstehen.

Einstellbare Werte:

Länge [Byte]	Zulässige Werte	Werks-einstellung	Bedeutung
0...63	String mit maximal 63 Zeichen	„“	Beliebiger Text, z. B. „2. Etage, Anlage 1“

Zeitzone, DST

Parameter-ID: 0020_{hex}
 UHF-Manager: Menü: *Geräte Einstellungen > Parameter... > Geräteparameter*
 OPC UA: –
 Webserver: Menü: *Konfiguration > Gerät*

Für Zeitfunktionen bzw. Zeitstempel kann über *Zeitzone*, *DST* festgelegt werden, welche *Zeitzone* zugrunde gelegt werden soll und ob ein Offset für Sommerzeit bzw. Winterzeit (*DST*, *Daylight Saving Time*) verwendet werden soll.

Der Parameter wird als Offset zur Weltzeit und einem Beschreibungstext in folgender Form übergeben:

Parameterwert = Zeitzone [1 Byte] + DST [1 Byte] + Text [16 Byte]

Beispiel:

Die Zeit soll als mitteleuropäische Sommerzeit (MESZ) angegeben werden. Dies entspricht der Weltzeit +1 Stunde für Mitteleuropa und Offset +1 Stunde für die Sommerzeit (UTC+2). Als Beschreibungstext soll *MESZ* angehängt werden, um klarzustellen, wie die Zeit zu interpretieren ist, wobei der Beschreibungstext gegebenenfalls auf 16 Byte Länge aufgefüllt wird.

Parameterwert = 01_{hex} 01_{hex} „MESZ“ 00_{hex}...00_{hex}

Einstellbare Werte:

Länge [Byte]	Zulässige Werte	Werks-einstellung	Bedeutung
18	Zone: –23...+23 DST: 0, 1, 2, FF _{hex} (Auto) Text: String mit 16 Zeichen	+1 0 „MEZ“ Mitteleuropäische Winterzeit	Zeitzone, DST und Beschreibungstext



Beim Auslesen des Parameters wird stets der effektive Zeitzonewert zurückgegeben. Im obigen Beispiel also der Wert für 2 Stunden (1 Stunde der Zeitzone und 1 Stunde für Sommerzeit). Die Sommerzeitangabe DST wird stets mit 0 zurückgeliefert.

Eine automatische Umstellung auf Sommer- oder Winterzeit wird vom BIS U-6127-Gerät nicht vorgenommen, da die jeweiligen Regelungen lokal verschieden sein können und eine Internetverbindung oftmals nicht zur Verfügung steht.

NTP-Server

Parameter-ID: 0021_{hex}
 UHF-Manager: Menü: *Geräte Einstellungen > Parameter... > Geräteparameter*
 OPC UA: –
 Webserver: Menü: *Konfiguration > Netzwerk*

Wenn das Netzwerk Zugang zu einem NTP-Server (*Network Time Protocol* oder *Zeitserver*) hat, kann über diesen eine Zeitsynchronisation über das Netzwerk erfolgen. Über den Parameter *NTP-Server* wird definiert, wie dieser Zeitserver zu erreichen ist. Als Parameterwert wird ein String mit maximal 63 Zeichen (Byte) übergeben, der eine URL oder eine IP-Adresse beinhalten kann, z. B. „time.google.com“ oder „192.168.10.1“.

Einstellbare Werte:

Länge [Byte]	Zulässige Werte	Werks-einstellung	Bedeutung
0...63	URL oder gültige IPv4-Adresse als String	„“	URL oder Adresse des NTP-Servers

Uhrzeit

Parameter-ID: 0022_{hex}
 UHF-Manager: Menü: *Geräte Einstellungen > Parameter... > Geräteparameter*
 OPC UA: –
 Webserver: Menü: *Konfiguration > Gerät*

Über den Parameter *Uhrzeit* können *Datum* und *Uhrzeit* manuell festgelegt werden, wenn im Netzwerk kein *NTP-Server* zur Verfügung steht.

Einstellbare Werte:

Länge [Byte]	Zulässige Werte	Werks-einstellung	Bedeutung
14	Datum und Uhrzeit im Format „YYYYMMDD-Dhhmmss“	fortlaufend aktualisiert	Datum und Uhrzeit im Format „YYYYMMDD-Dhhmmss“

FormattedTagData (default)

Im Kapitel *Parameter für Experten* auf Seite 50 ist die Funktion *FormattedTagData* mit den relevanten Parametern beschrieben. Mit einem Login der Sicherheitsebene *EXPERT* können diese Parameter nur temporär bzw. bezogen auf eine TCP-Session geändert werden.

Über die Sicherheitsebene *ADMIN* können auch die Default-Werte definiert werden, die nach dem Einschalten oder einem Neustart der Auswerteeinheit verwendet werden. Im 007-Protokoll können bis 99 Zeichen definiert werden. Mit OPC UA oder mit dem Webinterface können auch längere Zeichenketten (bis 1024 Zeichen) definiert werden, die auch im 007-Protokoll gültig sind.

Formatdefinition für ReadTagDataFormatted, ReadMultipleTagDataFormatted und WriteFormattedTagData (default)

Parameter-ID: 0025_{hex}
 UHF-Manager: Menü: *Geräte Einstellungen > Parameter... > Lesen > Schreiben*
 OPC UA: Methode *SetTagDataFormatted/GetTagDataFormatted*
 Webserver: *Konfiguration > RFID > Formatierte Tagdaten*

Legt das Standarddatenformat für die Funktion *FormattedTagData* fest, das nach dem Einschalten oder einem Neustart der Auswerteeinheit verwendet werden soll.

Einstellbare Werte:

Länge [Byte]	Zulässige Werte	Werkseinstellung	Bedeutung
007: 0...99 Web und OPC UA: 0...1024	Format-String	„%Ex[0,12]#0d#0a“ EPC-String mit CR LF	Format-String für <i>ReadTagDataFormatted</i> , <i>ReadMultipleTagDataFormatted</i> und <i>WriteFormattedTagData</i>

7

Inbetriebnahme und Betrieb (Fortsetzung)

Präfix für ReadMultipleTagDataFormatted (default)

Parameter-ID:	0026 _{hex}
UHF-Manager:	Menü: <i>Geräte Einstellungen > Parameter... > Lesen > Schreiben</i>
OPC UA:	Methode <i>SetTagDataFormatted/GetTagDataFormatted</i>
Webserver:	<i>Konfiguration > RFID > Formatierte Tagdaten</i>

Legt das Standardpräfix für die Funktion *FormattedTagData* fest, das nach dem Einschalten oder einem Neustart der Auswerteeinheit verwendet werden soll.

Einstellbare Werte:

Länge [Byte]	Zulässige Werte	Werkseinstellung	Bedeutung
007: 0...99 Web und OPC UA: 0...1024	String	„Begin#0d#0a“ Text „Begin“ mit <i>CR LF</i>	Präfix für <i>ReadMultipleTagDataFormatted</i>

Suffix für ReadMultipleTagDataFormatted (default)

Parameter-ID:	0027 _{hex}
UHF-Manager:	Menü: <i>Geräte Einstellungen > Parameter... > Lesen > Schreiben</i>
OPC UA:	Methode <i>SetTagDataFormatted/GetTagDataFormatted</i>
Webserver:	<i>Konfiguration > RFID > Formatierte Tagdaten</i>

Legt das Standardsuffix für die Funktion *FormattedTagData* fest, das nach dem Einschalten oder einem Neustart der Auswerteeinheit verwendet werden soll.

Einstellbare Werte:

Länge [Byte]	Zulässige Werte	Werkseinstellung	Bedeutung
007: 0...99 Web und OPC UA: 0...1024	String	„End#0d#0a“ Text „End“ mit <i>CR LF</i>	Suffix für <i>ReadMultipleTagDataFormatted</i>

Berechnungsformat für die Signaturerzeugung (default)

Parameter-ID:	0028 _{hex}
UHF-Manager:	–
OPC UA:	Methode <i>SetTagSignatureFormat/GetTagSignatureFormat</i>
Webserver:	<i>Konfiguration > RFID > UHF erweitert</i>

Definiert die Datenbereiche des Datenträgers, die in die Berechnung zur Erzeugung und Prüfung der Signatur einbezogen werden, üblicherweise den EPC und den TID, bei Datenträgern mit größerem Speicher eventuell auch einen Teil des User-Daten-Bereichs.

Der Bereich, in dem die Signatur selbst abgelegt wird (derzeit die ersten 64 Bytes des User-Daten-Bereichs) darf nicht mit einbezogen werden.

Die Angabe muss bei der Signaturerzeugung und der Signaturprüfung exakt identisch sein, sonst kann die Signatur nicht als gültig erkannt werden.

Die Angaben werden in der gleichen Systematik erzeugt wie für die formatierte Ausgabe, wobei die Angabe von Formatmodifizierern (X, x, oder d) nicht sinnvoll ist.

Beispiele:

Es sollen 12 Bytes des EPC und 12 Bytes des TID einbezogen werden:

Berechnungsformat: „%E[0,12]%T[0,12]“

Es sollen 12 Bytes des EPC und 12 Bytes des TID und 16 Bytes des User-Daten-Bereichs ab Adresse 64 einbezogen werden:

Berechnungsformat: „%E[0,12]%T[0,12]%U[64,16]“

Details zur Signaturerzeugung und Prüfung siehe *Datensicherheit* auf Seite 11.

Einstellbare Werte:

Länge [Byte]	Zulässige Werte	Werkseinstellung	Bedeutung
007: 0...99 Web und OPC UA: 0...1024	String	„%E[0,12]%T[0,8]“ 12 Bytes EPC + 8 Bytes TID	Berechnungsformat für die Signaturerzeugung

7

Inbetriebnahme und Betrieb (Fortsetzung)

SignatureType

Parameter-ID: 002A_{hex}

UHF-Manager: –

OPC UA: Methode *SetTagSignatureFormat/*
GetTagSignatureFormat

Webserver: *Konfiguration > RFID > UHF erweitert*

Schaltet die Erzeugung und Prüfung von Tagsignaturen global aus oder ein und legt den Hash- und Signaturalgorithmus fest.

Derzeit ist ausschließlich der Algorithmus SHA256 + ECDSA512 verfügbar.

Einstellbare Werte:

Länge [Byte]	Zulässige Werte	Werks- einstellung	Bedeutung
1	0 und 1	0 (= aus)	Signature Type 0 = Signaturerzeugung und -prüfung aus 1 = Signaturprüfung ein mit SHA526 + ECDSA512-Algorithmus

7.3.6 Erzeugen eines Schlüssels zum Signieren von Tagdaten

Um Tagdaten signieren oder die Signatur prüfen zu können, muss einmalig ein Schlüsselpaar, bestehend aus einem privaten (priv) und einem öffentlichen (pub) Schlüssel erzeugt werden. Der private Schlüssel ist einzigartig und kann bei Verlust nicht wiederhergestellt werden. Da jeder, der den Schlüssel besitzt, gültige Tagsignaturen erzeugen kann, muss der Schlüssel geheimgehalten werden. Der öffentliche Schlüssel kann hingegen auch von Dritten verwendet werden, um eine Signatur auf Gültigkeit zu prüfen.

Der private Schlüssel wird in alle beteiligten BIS-Geräte eingespielt und dort zum Signieren und zum Prüfen der Signatur verwendet. Alle Tags, die mit dem gleichen privaten Schlüssel (auch in unterschiedlichen Geräten) signiert werden, können untereinander getauscht und immer als gültig anerkannt werden. Tags, die mit einem anderen Schlüssel signiert wurden, werden immer als ungültig angesehen.

Um ein Schlüsselpaar zu erzeugen, wird die freie Software *openssl* benötigt, die es sowohl für Windows als auch Linux-PCs gibt oder es müssen die Funktionen auf der Gerätewebseite zum Erzeugen eines Schlüssels genutzt werden. In letzterem Fall empfehlen wir die Nutzung in einem sicheren Netzwerk und das vorübergehende Ausschalten des Geräts nach dem Speichern des Schlüssels auf einen PC.

Schlüsselpaar erzeugen

1. Die Software *openssl* auf einem PC installieren.
2. In der Kommandozeilenapplikation des PCs folgendes Kommando ausführen, um im aktuellen Verzeichnis eine Datei mit dem Namen *nistp224_key.pem* zu erzeugen:

```
openssl ecparam -name secp224r1  
-genkey -noout -out nistp224_key.pem
```

Den privaten und den öffentlichen Schlüssel der Datei anzeigen lassen

- Folgendes Kommandos eingeben:

```
openssl ec -in nistp224_key.pem -text  
-noout
```

Die Anzeige sieht z. B. wie folgt aus:

```
read EC key  
Private-Key: (224 bit)  
priv:1)  
d4:79:60:0b:2a:15:02:5c:48:34:d7:a8:7d:  
c0:c5:c0:c3:73:8b:f8:33:38:aa:bd:4b:d5:  
d7:a2  
pub:  
04:e6:65:43:e3:1e:9a:3d:fd:0c:98:ee:c4:  
60:f4:c8:4e:01:1c:54:28:85:ab:71:a4:02:  
01:89:92:90:05:33:2e:d3:04:4f:f0:22:b0:  
b1:26:a8:0d:f3:c3:fa:43:e7:93:6c:e9:a2:  
4c:e3:44:13:8b  
ASN1 OID: secp224r1  
NIST CURVE: P-224
```

¹⁾ Die auf *priv*: folgenden Daten (28 Byte) sind der private Schlüssel, der auf die Geräte gespielt werden muss.

Einspielen eines Schlüssels in das Gerät, um Tagdaten zu signieren

Um den Schlüssel im *Secure Element* des BIS U-6127 sicher abzuspeichern, gibt es folgende Voraussetzungen:

- einen privaten Schlüssel
- ein Schlüssel-Update-Ticket (eine längere Zeichenkombination), das bei Balluff erworben werden kann
- einen Internetzugang für den PC

i Jedes Schlüssel-Update-Ticket kann nur einmal verwendet werden. Für jedes Gerät und für jede Änderung eines Schlüssels wird ein neues Schlüssel-Update-Ticket benötigt, das über den Balluff Vertrieb erhältlich ist.

1. Die aktuelle Kontextdatei des Geräts auf den PC, durch Klicken auf der Gerätewebseite *Konfiguration / Sicherheit / Secure Element* auf den Button *HERUNTERLADEN KONTEXT DATEI* herunterladen.

i Für diesen Schritt ist noch keine Internetverbindung nötig, aber es sind Administratorrechte erforderlich.

Secure Element Kontext Datei

Herunterladen Kontext Datei

Bild 7-31: Secure Element Kontext Datei

2. Datei (mit der Dateiergung *.WibuCmRaC*) auf dem PC abspeichern.
3. *Optional*: Die Verbindung zum Gerät trennen.
4. Mit dem Internet verbinden.
5. Mit einem Browser (z. B. Google Chrome) auf die Webseite navigieren, die zusammen mit dem Ticket von Balluff mitgeteilt wurde und sicherstellen, dass eine sichere Verbindung vorliegt (bei Google Chrome wird dies durch das Symbol eines geschlossenen Schlosses angezeigt).
6. Den Ticket-Code eingeben.

i Jedes Ticket ist nur für einen Updatevorgang verwendbar.

7. Nach der Aufforderung, die Kontextdatei des Geräts hochzuladen, die zuvor gespeicherte Datei auswählen und zur Webseite übertragen.

8. Nach der Aufforderung, den privaten Schlüssel (*Secret Data*) einzugeben, die 32 Byte an Daten in hexadezimaler Schreibweise eingeben und vor dem Bestätigen prüfen.

i Akzeptiert werden die Zeichen 0...9 und A...F oder a...f.
Der *Elliptic Curve*-Schlüssel ist lediglich 28 Byte lang. Um auf 32 Byte zu kommen, müssen am Ende insgesamt vier Null-Byte (also acht 0-Zeichen) eingefügt werden.

Beispiel

pem-Datei:

```
priv:
d4:79:60:0b:2a:15:02:5c:48:34:d7:
a8:7d:c0:c5:c0:c3:73:8b:f8:33:38:
aa:bd:4b:d5:d7:a2
```

Einzugebender Schlüssel:

```
d479600b2a15025c4834d7a87dc0c5c0
c3738bf83338aabd4bd5d7a200000000
```

Insgesamt müssen genau 64 Zeichen eingegeben werden (dazu kann auch die Zwischenablage des Computers genutzt werden).

9. Eine Update-Datei (mit der Dateiergung *.WibuCmRaU*) für das Gerät von der Webseite auf den PC herunterladen und abspeichern.
10. Den PC mit dem BIS U-6127-Gerät erneut verbinden (die Internetverbindung wird nicht mehr benötigt).
11. Mit einer Benutzerkennung einloggen, die Administratorrechte für das Gerät besitzt.
12. Die erhaltene Datei (mit der Dateiergung *.WibuCmRaU*) auf der Seite *Konfiguration / Sicherheit / Secure Element* auf das Gerät hochladen: zuerst die Datei auswählen und dann *HOCHLADEN UPDATE DATEI* klicken.

Secure Element Update Datei

*.WibuCmRaU Datei auswählen

Hochladen Update Datei

Bild 7-32: Secure Element Update Datei

i Die Datei kann nur erfolgreich auf dasselbe Gerät gespielt werden, von dem zuvor die *WibuCmRaC*-Datei gespeichert wurde.

⇒ Eine Statusmeldung bestätigt ein erfolgreiches Einspielen.

13. Einen Gerätereueustart durchführen.

Einstellen der zu signierenden Daten

Neben dem Schlüssel muss auch die Einstellung der Daten, die signiert werden sollen, für alle beteiligten Geräte gleich sein. Üblicherweise wird der EPC und die TID des Datenträgers in die Signatur einbezogen.

Bei Tags mit 12 Byte EPC und 12 Byte TID (einschließlich 64-Bit-Seriennummer) lautet die gängige Definition:
%E[0,12]%T[0,12].

Bei Tags mit 12 Byte EPC und 8 Byte TID (einschl. 32-Bit-Seriennummer) lautet die gängige Definition:
%E[0,12]%T[0,8].

Die erzeugte Signatur kann grundsätzlich auch mit Hilfe des öffentlichen Schlüssels und einer geeigneten SW-Applikation geprüft werden. Beim BIS U-6127 ist es derzeit erforderlich, den privaten Schlüssel in das *Secure Element* einzuspielen.



Die Definition kann nachträglich nicht geändert werden, ohne dass alle bisher erzeugten Signaturen als ungültig erkannt werden.

Die Einstellung erfolgt auf der Gerätewebseite *Konfiguration / RFID / UHF Erweitert* im Feld *SIGNATUR BERECHNUNGSFORMAT*.

Tag Signatur	
Tag Signatur	SHA256+ECDSA512
Signatur Berechnungsformat	%E[0,12]%T[0,8]

Bild 7-33: Tag Signatur



Die Signatur wird bei allen Schreibbefehlen, die das universelle Ausgabeformat verwenden, erzeugt, sowohl mit dem 007-Protokoll als auch mit OPC UA.

Andere Schreibbefehle, die lediglich einzelne Speicherbänke beschreiben können, erzeugen keine geänderte Signatur und können eine vorhandene Signatur überschreiben oder ungültig werden lassen.

Einschalten der Signaturerzeugung und -prüfung

Die Nutzung der Tagdaten-Signatur wird schließlich durch Wählen des Signaturalgorithmus auf der Gerätewebseite *Konfiguration / RFID / UHF Erweitert* im Feld *TAG SIGNATUR* aus- und eingeschaltet. Die möglichen Werte sind *Off* oder *SHA256+ECDSA512*.



Die Signatur wird bei allen Lesebefehlen, die das universelle Ausgabeformat verwenden überprüft – sowohl mit 007-Protokoll als auch mit OPC UA.

Das Prüfergebnis kann in die Ausgabe übernommen werden, indem das Statusbyte im Formatstring angegeben wird (z. B. als %SX[0,1] oder %Sd[0,1]).

Ein Wert von 0 zeigt eine erfolgreiche Prüfung an. Der Wert 2 bedeutet, dass die Signatur nicht zu den übrigen Tagdaten passt.

7.4 Systemdiagnose

Die Auswerteeinheit BIS U-6127 bietet umfangreiche Funktionen, um den Betriebszustand des Geräts anzuzeigen und mögliche Probleme zu erkennen und abzustellen.

LED-Anzeige

Die wichtigste Anzeige ist die LED *Power/Status*. An ihr lässt sich der grundsätzliche Gerätezustand erkennen:

Anzeige Power/ Status-LED	Bedeutung	Empfohlenes Vorgehen
Aus	Keine Spannungsversorgung oder Gerät defekt	Gerät mit Spannung versorgen.
Orange (beim Einschalten)	Spannungsversorgung in Ordnung, Linux-System noch nicht geladen	Warten, bis System bootet (max. 30 Sekunden).
Orange (während des Betriebs) ¹⁾	Mindestens eine Applikation ist nicht bereit oder hat einen Warnstatus	Anwendungsstatus und Logbuch auf der Gerätewebseite prüfen (siehe unten).
Grün blinkend (nach Einschalten)	Linux-System geladen, Anwendungen und UHF-Reader werden gestartet	Warten, bis System bootet (max. 30 Sekunden).
Grün ¹⁾	System vollständig einsatzbereit	–
Rot ¹⁾	Eine oder mehrere Applikationen hat/haben einen Fehlerstatus	Anwendungsstatus und Logbuch auf der Gerätewebseite prüfen (siehe <i>Anwendungsstatus und Log</i> auf Seite 86).

¹⁾ Dieser LED-Zustand wird auch auf der Gerätewebseite *HOME* angezeigt.

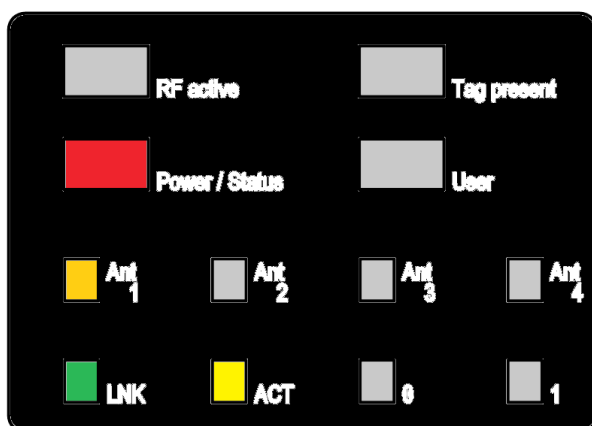


Bild 7-34: LED-Anzeige

Anwendungsstatus und Log

Auf der Gerätewebseite im Tab *LOGBUCH* gibt es drei Abschnitte, die detaillierte Informationen zum Gerätestatus liefern (siehe Bild 7-35).

Wenn die Power/Status-LED signalisiert, dass eine Warnung oder ein Fehler vorliegt, können hier Einzelheiten abgerufen werden, einerseits zu jeder Applikation im Gerät in der Sektion *ANWENDUNGSSTATUS*, andererseits auch als Zeitprotokoll in der Sektion *GERÄT LOGBUCH*. Die verfügbaren Informationen können bei der Fehlersuche hilfreich sein.

BIS U-6127

Home
 Einloggen
 Sprache
 RFID
 Konfiguration
 Logbuch
 Info

Logbuch

Gerät Information

Product Name:	BIS U-6127-081-104-06-ST36	HW Version:	1.0
Serial Number:	DE17040100000001	SW Version:	0.1.11
MAC Address:	50-2d-f4-0d-f4-33	SW Build:	20
IP Address:	192.168.0.236	Contact:	Balluff GmbH

Anwendungsstatus

Status	Anwendung	Info	Zeitstempel
OK	DeviceServer		2020-09-15 14:02:48
OK	OpcUa_U6127_App		2020-09-15 14:02:51
OK	ParameterServer		2020-09-15 14:02:54
OK	Uhf_007_App.P10001		2020-09-15 14:02:56
OK	Uhf_007_App.P10002		2020-09-15 14:02:59
OK	Uhf_007_App.P10003		2020-09-15 14:03:02
OK	Uhf_007_App.P10004		2020-09-15 14:03:04
OK	Uhf_007_App.P10005		2020-09-15 14:02:40
OK	Uhf_007_App.PttyGS0		2020-09-15 14:02:43
OK	Uhf_KBRPReader		2020-09-15 14:02:46

Gerät Logbuch

Logbuch herunterladen

Nr.	Severity	Zeitstempel	Origin	Info
330	INFO	[com.balluff.diagnosis] [34292213696ms] INFO : 2020-09-15 10:18:06	ParameterServer	AppInfo: Application registered successfully. com.balluff.OpcUa_U6127_App
329	WARNING	[com.balluff.diagnosis] [34292213445ms] INFO : 2020-09-15 10:18:06	OpcUa_U6127_App	reported warning state

Bild 7-35: Logbuch

Gelegentliche Fehlersituationen

Die folgenden Fehlersituationen können gelegentlich auftreten:

Fehler	LED-Anzeige Power/Status	Fehlerursachen und -behebung
Fehlermeldung <i>Kabelbruch</i> , Uhf_KBRPReader meldet im Logbuch: <i>Cable break at antenna #</i>	Rot	Antennenanschluss parametrieren, ohne dass eine Antenne angeschlossen wurde oder die Verbindung zur Antenne ist unterbrochen. ► Antennenverbindung und Einstellungen prüfen.
Uhf_KBRPReader meldet im Logbuch: <i>Cannot connect to reader</i>	Rot	Strombegrenzung der Spannungsversorgung zu niedrig, um UHF-Funktionen ordnungsgemäß betreiben zu können. ► Stromversorgung mit höherem Strom bereitstellen, bei wiederholtem Auftreten Service kontaktieren.
Gerät kann über 007 mit TCP nicht erreicht werden (<i>Connection Timed out</i> oder <i>Connection refused</i> beim Client)	Grün	Falsche 007-Portnummer verwendet. ► Korrekte Portnummer verwenden. 007-Protokoll deaktiviert. ► 007 über Webinterface aktivieren. Auf dem angesprochenen Port ist bereits eine Verbindung aktiv. ► Alte Verbindung trennen. Keine IP-Adresse über DHCP erhalten oder falsche IP-Adresse eingestellt. ► Über UHF-Manager am USB-Anschluss prüfen und ggf. ändern.
Fataler Fehler einer Anwendung	Rot	Vielfältige Ursachen möglich. ► Gerät neu starten, bei wiederholtem Auftreten Service kontaktieren.
Gerät startet regelmäßig neu, viele <i>startup</i> -Einträge in kurzer Zeit im Logbuch	Orange	Strombegrenzung der Spannungsversorgung zu niedrig, um UHF-Funktionen ordnungsgemäß betreiben zu können. ► Stromversorgung mit höherem Strom bereitstellen, bei wiederholtem Auftreten Service kontaktieren.
OpcUa_U6127_App läuft nicht (fataler Fehler), keine OPC-UA-Verbindung möglich	Rot	Datum/Uhrzeit ist falsch. ► Datum/Uhrzeit und Zeitzone korrekt setzen Zertifikat nicht vorhanden, ungültig oder mit falschen Datumseintrag ► Datum/Uhrzeit und Zeitzone korrekt setzen, neues Zertifikat erstellen, Gerätereustart

7

Inbetriebnahme und Betrieb (Fortsetzung)

7.5 Betrieb

Beim Betreiben der Auswerteeinheit müssen folgende Gefahren beachtet und vermieden werden:



VORSICHT

Ultrahochfrequente elektromagnetische Wellen

Die Antennen des BIS U-Identifikationssystems senden ultrahochfrequente elektromagnetische Wellen aus. Um Gesundheitsgefährdungen auszuschließen, müssen zusätzliche Maßnahmen getroffen werden.

- ▶ Darauf achten, dass sich Personen nicht über einen längeren Zeitraum im Nahbereich der Antennen aufhalten.
- ▶ Bereiche, die explizit nicht erfasst werden sollen, durch geeignete Maßnahmen abschirmen.

ACHTUNG

Überschreiten der maximalen Stromaufnahme

Bei Überschreiten der maximalen Stromaufnahme kann es zu Schäden an der Auswerteeinheit und an angeschlossenen Systemkomponenten kommen.

- ▶ Beim Betrieb darauf achten, dass der Gesamtstrom, der über den Anschluss Power geführt wird, 3 A nicht übersteigt.
- ▶ Der Spannungsausgang (L+) am IO-Link-Port sowie digitale Ausgänge (E/A) werden über den Anschluss Power versorgt. Die Summe der Teilströme dieser Pins, darf einen maximalen Strom von 2 A nicht übersteigen.

Zur Kommunikation der Auswerteeinheit mit dem steuernden System kann das Balluff 007-Protokoll gewählt werden, das über eine Ethernet TCP/IP-Verbindung übertragen wird. Das Protokoll ist Byte-orientiert und verwendet wenig Overhead, da die vollständige, fehlerfreie und sequenzgerechte Datenübertragung durch den Ethernet-Übertragungskanal sichergestellt wird.

i Das Vorgehen zum Erstellen bzw. Öffnen einer TCP/IP-Socket-Verbindung ist abhängig vom verwendeten System (PC, Steuerung etc.) und der eingesetzten Programmiersprache (als Orientierungshilfe siehe Kapitel 7, Details siehe Dokumentation des steuernden Systems bzw. der gewählten Programmiersprache).

8.1 Protokollablauf

Das Protokoll basiert auf synchronen Befehlen, die nach dem Prinzip *Anfrage – Antwort* aufgebaut sind. Demnach erhält die Steuerung auf jede korrekte Anfrage eine entsprechende Antwort, die Daten oder eine Statusmeldung beinhalten kann. Dabei muss der Ablauf, wie er in diesem Kapitel beschrieben wird, eingehalten werden. Davon abweichende Eingaben werden von der Auswerteeinheit nicht beachtet bzw. nicht quittiert. Nach vollständiger Abarbeitung oder Abbruch eines Befehls kehrt die Auswerteeinheit automatisch in den Grundzustand zurück.

i Einzige Ausnahme, die vom verwendeten Prinzip *Anfrage – Antwort* abweicht, ist die asynchrone Meldung *Tag kommt* bzw. *Tag geht*, die ohne vorherige Anfrage an die Steuerung gesendet wird. Diese Funktion muss durch den Parameter *AsyncOperation* aktiviert werden (siehe *AsyncOperation* in Kapitel 7.3 auf Seite 55).

Einstufige Befehle werden nach dem Prinzip *GRUNDZUSTAND – ANFRAGE – ANTWORT – GRUNDZUSTAND* ausgeführt:

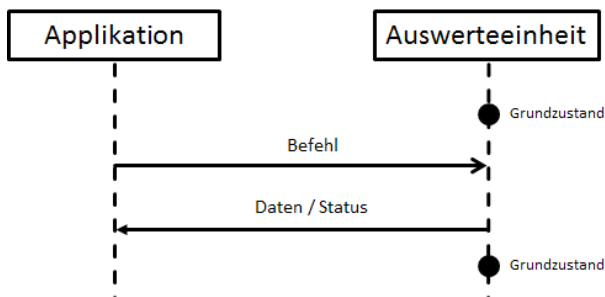


Bild 8-1: Einstufige Befehle

Mehrstufige Befehle werden nach dem Prinzip *GRUNDZUSTAND – ANFRAGE – ANTWORT – QUIITTUNG/DATEN – ANTWORT – ... – GRUNDZUSTAND* ausgeführt:

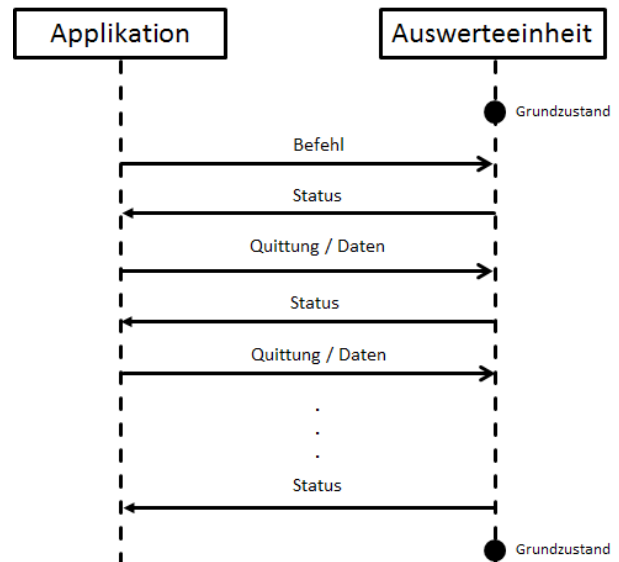


Bild 8-2: Mehrstufige Befehle

Mehrstufige Befehle können von der Steuerung durch den Befehl *Abbruch* (Befehlskennung 'Q') nach jeder empfangenen Antwort abgebrochen werden. Die Auswerteeinheit geht dann zurück in den Grundzustand und wartet auf eine Eingabe.

8.5 Befehlsübersicht

Allgemeine Befehle

Funktion	Befehlskennung		Beschreibung
	ASCII	HEX	
Abbruch	'Q'	51 _{hex}	Abbruch asynchroner Befehlen.
System Reboot	'q'	71 _{hex}	Systemneustart
Netzwerkparameter lesen	'm'	6D _{hex}	Ethernet-Netzwerkparameter auslesen.
Netzwerkparameter ändern	'j'	6A _{hex}	Ethernet-Netzwerkparameter festlegen.
Sendeleistung lesen	'o'	6F _{hex}	Sendeleistung der angegebenen Antenne auslesen.
Sendeleistung ändern	'p'	70 _{hex}	Sendeleistung der angegebenen Antenne festlegen.
Geräteparameter lesen	'G'	47 _{hex}	Geräteparameter auslesen.
Geräteparameter ändern	'E'	45 _{hex}	Geräteparameter festlegen.
Version lesen	'V'	56 _{hex}	Informationen zur Auswerteeinheit auslesen. – BIS U-Typbezeichnung – Hardware-Version/Firmware-Version/Seriennummer – IO-Link-FW-Version

Datenträger erfassen

Funktion	Befehlskennung		Beschreibung
	ASCII	HEX	
Anzahl Datenträger	'N'	4E _{hex}	Abfragen der Anzahl von Tags, die sich im Erfassungsbereich der angegebenen Antenne befinden.
Datenträger erfassen	'M'	4D _{hex}	Erfasst die Datenträger, die sich im Erfassungsbereich der angegebenen Antenne befinden und gibt eine Liste der angeforderten Daten zurück (EPC oder TID).
Datenträger erfassen, erweitert	','	2C _{hex}	Erfasst die Datenträger, die sich im Erfassungsbereich der angegebenen Antenne befinden und gibt eine Liste der angeforderten Daten (EPC oder TID) sowie Zusatzinformationen zurück.

Asynchrone Meldungen Tag geht/Tag kommt

Funktion	Befehlskennung		Beschreibung
	ASCII	HEX	
Datenträger kommt, Event	<DLE> '+'	102B _{hex}	Meldet einen Tag bei Eintreten in den Erfassungsbereich als <i>kommt</i> .
Datenträger geht, Event	<DLE> '-'	102D _{hex}	Meldet einen Tag bei Verlassen des Erfassungsbereichs als <i>geht</i> .

Datenträger bearbeiten

Funktion	Befehlskennung		Beschreibung
	ASCII	HEX	
Datenträger auswählen (Select)	'z'	7A _{hex}	Selektiert einen angegebenen Datenträger innerhalb einer Datenträgerpopulation
Datenträger abwählen (Unselect)	'n'	6E _{hex}	Hebt die Auswahl des zuletzt angegebenen Datenträgers auf, siehe Befehl <i>Select</i>
Datenträger lesen	'L'	4C _{hex}	User-Daten von einem Datenträger lesen Anzahl Byte: 0...1024 Byte
Datenträger lesen, erweitert	'H'	48 _{hex}	Ausgewählte Daten von einem Datenträger lesen. Anzahl Byte: > 1024 Byte
Datenträger lesen, EPC	'O'	4F _{hex}	EPC-Daten von einem Datenträger lesen.
Datenträger lesen, TID	'y'	79 _{hex}	TID-Daten von einem Datenträger lesen.
Datenträger lesen, Bulk	'l'	49 _{hex}	Erfasst die Datenträger, die sich im Erfassungsbereich der angegebenen Antenne befinden und gibt eine Liste der User-Daten zurück.
Datenträger lesen, Bulk erweitert	'>'	3E _{hex}	Erfasst die Datenträger, die sich im Erfassungsbereich der angegebenen Antenne befinden und gibt eine Liste der angeforderten Daten zurück.
Datenträger schreiben	'P'	50 _{hex}	User-Daten auf einen Datenträger schreiben. Anzahl Byte: 0...1024 Byte
Datenträger schreiben, Konstanter Wert	'C'	43 _{hex}	Konstante User-Daten auf einen Datenträger schreiben.

Funktion	Befehlskennung		Beschreibung
	ASCII	HEX	
Datenträger schreiben, EPC	'v'	76 _{hex}	EPC-Daten auf einen Datenträger schreiben und Längeninformation des EPC ggf. anpassen.
Datenträger schreiben, erweitert	'F'	46 _{hex}	Ausgewählte Daten auf einen Datenträger schreiben. Anzahl Byte: > 1024 Byte
Datenträger schreiben, Bulk	'w'	77 _{hex}	Schreiben von User-Daten auf die Datenträger, die sich im Erfassungsbereich der angegebenen Antenne befinden.
Datenträger schreiben, Bulk erweitert	'<'	3C _{hex}	Schreiben von ausgewählten Daten auf die Datenträger, die sich im Erfassungsbereich der angegebenen Antenne befinden und Rückmeldung der erfolgreich beschriebenen Datenträger.
Kill	'k'	6B _{hex}	Deaktiviert einen selektierten Datenträger dauerhaft (irreversibel).
Lock	'l'	6C _{hex}	Sperrern von Speicherbereichen eines selektierten Datenträgers.

Universal Datenträger (Formatierte Tagdaten)

Funktion	Befehlskennung		Beschreibung
	ASCII	HEX	
Datenträger erfassen, universal	'-' 'L'	2D4C _{hex}	Erfasst die Datenträger, die sich im Erfassungsbereich der angegebenen Antenne befinden und gibt eine Liste mit individuell parametrierbaren Daten zurück.
Datenträger lesen, universal	'-' 'R'	2D52 _{hex}	Individuell parametrierbare Daten von einem Datenträger lesen.
Datenträger schreiben, universal	'-' 'W'	2D57 _{hex}	Individuell parametrierbare Daten auf einen Datenträger schreiben.

IO-Link

Funktion	Befehlskennung		Beschreibung
	ASCII	HEX	
Azyklische Bedarfsdaten, lesen	'i'	69 _{hex}	Bedarfs-/Parameterdaten vom IO-Link Device empfangen.
Azyklische Bedarfsdaten, schreiben	'e'	65 _{hex}	Bedarfs-/Parameterdaten zum IO-Link Device senden.
Digitale Ausgangsports, setzen/rücksetzen	'/'	2F _{hex}	Setzen/Rücksetzen von Pin 2 bzw. Pin 4, wenn diese als digitaler Ausgang verwendet werden.
Digitale Eingangsports, lesen	'*'	2A _{hex}	Abfragen der Zustände von Pin 2 bzw. Pin 4, wenn diese als digitale Eingänge betrieben werden.
Zyklische Prozessdaten, lesen	'Y'	59 _{hex}	Zyklische IO-Link Prozessdaten lesen.
Zyklische Prozessdaten, schreiben	'X'	58 _{hex}	Zyklische IO-Link Prozessdaten schreiben.
IO-Link Master Konfiguration, lesen	'#'	23 _{hex}	Auslesen der IO-Link Master Konfiguration.
IO-Link Master Konfiguration, schreiben	'g'	67 _{hex}	Festlegen der IO-Link Master Konfiguration.

8.6 Statuscodes

Status-code	Hex	Funktionsbeschreibung
'0'	30 _{hex}	OK/Erfolgreich
'1'	31 _{hex}	Kein Datenträger im Erfassungsbereich der Antenne.
'2'	32 _{hex}	Lesen des Datenträgers nicht möglich.
'3'	33 _{hex}	Datenträger wurde während des Lesens aus dem Erfassungsbereich der Antenne entfernt.
'4'	34 _{hex}	Schreiben auf den Datenträger ist nicht möglich.
'5'	35 _{hex}	Datenträger wurde während des Schreibens aus dem Erfassungsbereich der Antenne entfernt.
'6'	36 _{hex}	Das Gerät hat ein Hardwareproblem erkannt.
'7'	37 _{hex}	Gesendete Daten entsprechen nicht dem 007-Protokoll.
'8'	38 _{hex}	BCC der empfangenen Daten stimmt nicht mit dem übertragenen BCC überein.
'9'	39 _{hex}	Kabelbruch an einem aktiven Antennenport oder keine Antenne angeschlossen.
'A'	41 _{hex}	Es befindet sich mehr als 1 Datenträger im Erfassungsbereich der Antenne(n) (nur bei Single-Tag-Operationen).
'D'	44 _{hex}	Interner Gerätefehler
'E'	45 _{hex}	CRC oder Signatur des Datenträgers fehlerhaft.
'F'	46 _{hex}	Der gewählte Speicherbereich wird von dem Datenträger nicht unterstützt.
'N'	4E _{hex}	Die angewählte Antenne ist nicht aktiv.
'P'	50 _{hex}	Das Kommando wurde auf dem falschen Ethernet-Port ausgeführt.
'S'	53 _{hex}	Der Befehl oder Parameter wird von der Auswerteeinheit nicht unterstützt.
'X'	58 _{hex}	Zugriff verweigert. Das momentane Benutzerlevel erlaubt diese Aktion nicht.
'Y'	59 _{hex}	Das Gerät ist im Moment in einem Zustand, der die Ausführung des Befehls nicht ermöglicht.
'a'	61 _{hex}	Diese Funktion wird vom Datenträger nicht unterstützt
'b'	62 _{hex}	Falscher oder ungültiger Lizenzschlüssel

Status-code	Hex	Funktionsbeschreibung
'c'	63 _{hex}	Es wurden ungültige Parameterwerte geschrieben.
'd'	64 _{hex}	Die Kommunikation zwischen Auswerteeinheit und Datenträger ist gestört.
'f'	66 _{hex}	Für diese Operation wird ein Passwort benötigt.
'g'	67 _{hex}	Ungültiges Passwort
'h'	68 _{hex}	Der gewählte Speicherbereich ist gesperrt.
'i'	69 _{hex}	Ein angegebener Parameter liegt außerhalb des gültigen Wertebereichs.
'j'	6A _{hex}	Befehl wird vom Datenträger nicht unterstützt/kein oder falscher Datenträger selektiert.

8.7 Allgemeine Befehle

Befehlskennung 'Q': Abbruch

Abbrechen von mehrstufigen oder asynchronen Befehlen. Ein Abbruch ist nach Empfang jeder Antwort möglich. Die Auswerteeinheit geht nach Abbruch in den Grundzustand und wartet auf eine Eingabe.

Byte	Länge	Befehlselement	Wertebereich
00	1	Befehlskennung (ASCII)	'Q'
01	1	BCC	00 _{hex} ...FF _{hex}

Statusmeldung:

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<ACK> oder <NAK>
01	1	Statuscode	Siehe Tabelle <i>Statuscodes</i> auf Seite 94

Befehlskennung 'q': System Reboot

Veranlasst die Auswerteeinheit das System herunterzufahren und neu zu starten.

Nach dem Neustart geht die Auswerteeinheit in den Grundzustand und wartet auf eine Eingabe.

Byte	Länge	Befehlselement	Wertebereich
00	1	Befehlskennung (ASCII)	'q'
01	1	Reserviert	'0'
02	1	BCC	00 _{hex} ...FF _{hex}

Statusmeldung:

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<ACK> oder <NAK>
01	1	Statuscode	Siehe Tabelle <i>Statuscodes</i> auf Seite 94
02	1	BCC	00 _{hex} ...FF _{hex}

Die Ausführung dieses Befehls erfordert eine vorherige Anmeldung mit einem Benutzer mit Admin-Berechtigung.

Befehlskennung 'm': Netzwerkparameter lesen

Auslesen der Ethernet-Netzwerkparameter. Die Parameter werden im ASCII-hex-Zahlenformat übertragen.

Beispiel:

IP-Adresse: 192.168.68.101 „C0A84465“
Subnetzmaske: 255.255.255.0 „FFFFFF00“

Byte	Länge	Befehlselement	Wertebereich
00	1	Befehlskennung (ASCII)	'm'
01	1	BCC	00 _{hex} ...FF _{hex}

Statusmeldung:

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<ACK> oder <NAK>
01	1	Statuscode	Siehe Tabelle <i>Statuscodes</i> auf Seite 94

Bei positiver Statusmeldung werden mit <STX> Daten angefordert.

Byte	Länge	Befehlselement	Wertebereich
00	1	Steuerbefehl	<STX>

Bei erfolgreicher Befehlsausführung folgen Daten.

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<ACK>
01...08	8	IP-Adresse (ASCII hex)	„00000000“... „FFFFFFF“
09...16	8	Subnetzmaske (ASCII hex)	„00000000“... „FFFFFFF“
17...24	8	Gateway-Adresse (ASCII hex)	„00000000“... „FFFFFFF“
25	1	IP Konfiguration (ASCII)	'0': Static '1': DHCP
26	1	BCC	00 _{hex} ...FF _{hex}

Können die Daten nicht bereitgestellt werden, folgt eine negative Statusmeldung.

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<NAK>
01	1	Statuscode	Siehe Tabelle <i>Statuscodes</i> auf Seite 94

Befehlskennung 'j': Netzwerkparameter ändern

Festlegen der Ethernet-Netzwerkparameter. Die Parameter werden im ASCII-hex-Zahlenformat übertragen.

IP-Adresse: 192.168.68.101 „C0A84465“
 Subnetzmaske: 255.255.255.0 „FFFFFFF0“

Byte	Länge	Befehlselement	Wertebereich
00	1	Befehlskennung (ASCII)	'j'
01...08	8	IP-Adresse (ASCII hex)	„00000000“... „FFFFFFF0“
09...16	8	Subnetzmaske (ASCII hex)	„00000000“... „FFFFFFF0“
17...24	8	Gateway-Adresse (ASCII hex)	„00000000“... „FFFFFFF0“
25	1	IP Konfiguration (ASCII)	'0': Static '1': DHCP
26	1	BCC	00 _{hex} ...FF _{hex}

Statusmeldung:

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<ACK> oder <NAK>
01	1	Statuscode	Siehe Tabelle <i>Statuscodes</i> auf Seite 94

Bei positiver Statusmeldung wird mit <STX> ein System Reboot veranlasst, um die neuen Netzwerkparameter zu übernehmen.

Byte	Länge	Befehlselement	Wertebereich
00	1	Steuerbefehl	<STX>

Die Ausführung dieses Befehls erfordert eine vorherige Anmeldung mit einem Benutzer mit Admin-Berechtigung.

Befehlskennung 'o': Sendeleistung lesen

Auslesen der aktuell eingestellten Sendeleistung (ERP/ EIRP) als 1/4-dBm-Wert.

Beispiel:

Beim Auslesen der Sendeleistung werden folgende Werte zurückgegeben (5C_{hex}):

- Sendeleistung High Byte: '5'
- Sendeleistung Low Byte: 'c'

$$5C_{\text{hex}} = 92$$

$$92 \times \frac{1}{4} \text{ dBm} = 23 \text{ dBm}$$

Somit ist eine Sendeleistung von 23 dBm eingestellt.

Byte	Länge	Befehlselement	Wertebereich
00	1	Befehlskennung (ASCII)	'o'
01	1	Antennennummer (ASCII)	'1'...'4': Einzelantenne
02	1	BCC	00 _{hex} ...FF _{hex}

Statusmeldung

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<ACK> oder <NAK>
01	1	Statuscode	Siehe Tabelle <i>Statuscodes</i> auf Seite 94

Bei positiver Statusmeldung werden mit <STX> Daten angefordert.

Byte	Länge	Befehlselement	Wertebereich
00	1	Steuerbefehl	<STX>

Bei erfolgreicher Befehlsausführung folgen Daten.

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<ACK>
01...02	2	Sendeleistung (ASCII hex)	„00“...„FF“
03	1	BCC	00 _{hex} ...FF _{hex}

Können die Daten nicht bereitgestellt werden, folgt eine negative Statusmeldung.

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<NAK>
01	1	Statuscode	Siehe Tabelle <i>Statuscodes</i> auf Seite 94

Befehlskennung 'p': Sendeleistung ändern

Einstellen der Sendeleistung (ERP/EIRP) als 1/4-dBm-Wert. Die Sendeleistung beeinflusst die maximale Reichweite des Erfassungsbereichs der Antenne.

Beispiel:

Einstellen einer Sendeleistung von 23 dBm (200 mW):

$$\frac{23 \text{ dBm}}{1/4 \text{ dBm}} = 92$$

$$92 = 5C_{\text{hex}}$$

$$92 = 5C_{\text{hex}}$$

Dazu müssen folgende Werte übertragen werden:

- Sendeleistung 1. Zeichen: '5'
- Sendeleistung 2. Zeichen: 'C'

i Die maximal zulässige Sendeleistung ist abhängig von der verwendeten Antenne und von den im jeweiligen Land gültigen Funkvorschriften. Detailinformationen siehe Kapitel 5 auf Seite 18 und dem Datenblatt der verwendeten Antenne.

Byte	Länge	Befehlselement	Wertebereich
00	1	Befehlskennung	'p'
01	1	Antennennummer (ASCII)	'0': Alle Antennen '1'...'4': Einzelantenne
02...03	2	Sendeleistung (ASCII hex)	„00“...„FF“
04	1	BCC	00 _{hex} ...FF _{hex}

Statusmeldung:

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<ACK> oder <NAK>
01	1	Statuscode	Siehe Tabelle <i>Statuscodes</i> auf Seite 94

Bei positiver Statusmeldung wird mit <STX> die neue Sendeleistung übernommen.

Byte	Länge	Befehlselement	Wertebereich
00	1	Steuerbefehl	<STX>

Statusmeldung:

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<ACK> oder <NAK>
01	1	Statuscode	Siehe Tabelle <i>Statuscodes</i> auf Seite 94

Befehlskennung 'G': Geräteparameter lesen

Auslesen von allgemeinen und antennenbezogenen Parameterdaten. Für eine detaillierte Parameterbeschreibung siehe Kapitel 7.3 auf Seite 49.

Byte	Länge	Befehlselement	Wertebereich
00	1	Befehlskennung (ASCII)	'G'
01	1	Antennennummer (ASCII)	'1': Antenne 1 '2': Antenne 2 '3': Antenne 3 '4': Antenne 4
02...05	4	Parameternummer (ASCII hex)	„0000“...„FFFF“
06	1	BCC	00 _{hex} ...FF _{hex}

Die positive Statusmeldung enthält die angeforderten Parameterdaten.

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<ACK>
01	1	Reserviert (ASCII)	'0'
02	1	Antennennummer (ASCII)	'0': Allgemein '1': Antenne 1 '2': Antenne 2 '3': Antenne 3 '4': Antenne 4
03...04	1	Anzahl Byte (ASCII)	„00“...„99“
05...08	2	Parameternummer (ASCII hex)	„0000“...„FFFF“
09	4	Daten	00 _{hex} ...FF _{hex}
...	...	...	00 _{hex} ...FF _{hex}
Letztes Byte	1	BCC	00 _{hex} ...FF _{hex}

Können die Daten nicht bereitgestellt werden, folgt eine negative Statusmeldung.

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<NAK>
01	1	Statuscode	Siehe Tabelle <i>Statuscodes</i> auf Seite 94
02	1	BCC	00 _{hex} ...FF _{hex}

Befehlskennung 'E': Geräteparameter ändern

Schreiben von allgemeinen und antennenbezogenen Parametern. Antennenbezogene Parameter können für jede Antenne individuell festgelegt werden. Für eine detaillierte Parameterbeschreibung siehe Kapitel 7.3 auf Seite 49.

Byte	Länge	Befehlselement	Wertebereich
00	1	Befehlskennung (ASCII)	'E'
01	1	Antennennummer (ASCII)	'0': Alle Antennen/ Allgemein '1': Antenne 1 '2': Antenne 2 '3': Antenne 3 '4': Antenne 4
02...03	2	Anzahl Byte (ASCII)	„00“...„99“
04...07	4	Parameternummer (ASCII hex)	„0000“...„FFFF“
08	1	Daten	00 _{hex} ...FF _{hex}
...	...	...	00 _{hex} ...FF _{hex}
Letztes Byte	1	BCC	00 _{hex} ...FF _{hex}

Statusmeldung:

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<NAK>
01	1	Statuscode	Siehe Tabelle Statuscodes auf Seite 94
02	1	BCC	00 _{hex} ...FF _{hex}

Befehlskennung 'V': Version lesen

Liest den Firmware Versionsstring der verwendeten Auswerteeinheit aus.

Byte	Länge	Befehlselement	Wertebereich
00	1	Befehlskennung (ASCII)	'V'
01	1	BCC	00 _{hex} ...FF _{hex}

Bei erfolgreicher Befehlsausführung folgen Daten.

Byte	Länge	Befehlselement	Wertebereich
00	Variabel	Versionsstring	ASCII-String mit variabler Länge
Letztes Byte	1	BCC	00 _{hex} ...FF _{hex}

Können die Daten nicht bereitgestellt werden, folgt eine negative Statusmeldung.

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<NAK>
01	1	Statuscode	Siehe Tabelle Statuscodes auf Seite 94
02	1	BCC	00 _{hex} ...FF _{hex}

8.8 Datenträger erfassen

Befehlskennung 'N': Anzahl Datenträger

Erfasst die Datenträger, die sich im Erfassungsbereich der angegebenen Antenne befinden und gibt die Anzahl der erkannten Datenträger zurück. Mit der Datenträgerauswahl können wahlweise alle oder nur selektierte Datenträger erfasst werden (siehe Befehlskennung 'z': Datenträger auswählen (Select) auf Seite 105).

Byte	Länge	Befehlselement	Wertebereich
00	1	Befehlskennung (ASCII)	'N'
01	1	Antennennummer (ASCII)	'0': Alle aktiven Antennen '1'...'4': Einzelantenne
02	1	Datenträgerauswahl	'A': All 'S': Selected
03	1	BCC	00 _{hex} ...FF _{hex}

Statusmeldung

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<ACK> oder <NAK>
01	1	Statuscode	Siehe Tabelle Statuscodes auf Seite 94

Bei positiver Statusmeldung werden mit <STX> Daten angefordert.

Byte	Länge	Befehlselement	Wertebereich
00	1	Steuerbefehl	<STX>

Bei erfolgreicher Befehlsausführung folgen Daten.

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<ACK>
01	1	Antennennummer (ASCII)	'1'...'4'
02...04	3	Anzahl gefundener Datenträger (ASCII)	„000“...„999“
05	1	BCC	00 _{hex} ...FF _{hex}

Können die Daten nicht bereitgestellt werden, folgt eine negative Statusmeldung.

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<NAK>
01	1	Statuscode	Siehe Tabelle Statuscodes auf Seite 94

Befehlskennung 'M': Datenträger erfassen

Erfasst die Datenträger (max. 255), die sich im Erfassungsbereich der angegebenen Antenne befinden und gibt die unter Datentyp angegebenen Daten zurück. Mit der Datenträgerauswahl können wahlweise alle oder nur selektierte Datenträger erfasst werden (siehe *Befehlskennung 'z': Datenträger auswählen (Select)* auf Seite 105).

Byte	Länge	Befehlselement	Wertebereich
00	1	Befehlskennung (ASCII)	'M'
01	1	Antennennummer (ASCII)	'0': Alle aktiven Antennen '1'...'4': Einzelantenne
02	1	Datentyp: EPC oder TID (ASCII)	'E': EPC 'T': TID
03...05	3	Max. Anzahl Datenträger (ASCII)	„000“...„255“
06	1	Datenträgerauswahl (ASCII)	'0': All '1': Selected
07	1	BCC	00 _{hex} ...FF _{hex}

Die positive Statusmeldung enthält Zusatzinformationen und wird wie folgt übertragen.

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<ACK>
01	1	Antennennummer (ASCII)	'1'...'4'
02	1	Datentyp EPC oder TID (ASCII)	'E': EPC 'T': TID
03...05	3	Anzahl gefundener Datenträger (ASCII)	„000“...„255“
06...07	2	Anzahl Byte für die ID je Datenträger (ASCII)	„64“
08	1	BCC	00 _{hex} ...FF _{hex}

Können die Daten nicht bereitgestellt werden, folgt eine negative Statusmeldung.

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<NAK>
01	1	Statuscode	Siehe Tabelle <i>Statuscodes</i> auf Seite 94

Bei positiver Statusmeldung werden mit <STX> Daten angefordert.

Byte	Länge	Befehlselement	Wertebereich
00	1	Steuerbefehl	<STX>

Anschließend folgen die angeforderten Daten, die bei größerem Datenaufkommen in mehrere Pakete aufgeteilt werden. Jedes Paket enthält die Gesamtzahl der Pakete und die aktuelle Paketnummer. Über den Steuerbefehl <STX> können die Pakete iterativ abgeholt werden.

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<ACK>
01	1	Antennennummer (ASCII)	'1'...'4'
02...04	3	Gesamtzahl der Pakete (ASCII)	„001“...„999“
05...07	3	Paketnummer (ASCII)	„000000“...„999999“
08...13	6	Anzahl Byte im Datenblock (ASCII)	„000000“...„999999“
14	Anzahl	Datenblock	Siehe Beschreibung <i>Datenblock</i> auf Seite 100
Letztes Byte	1	BCC	00 _{hex} ...FF _{hex}

Datenblock

Der Datenblock besteht aus einem oder mehreren Frames mit einer Länge von je 66 Byte. Jeder Frame enthält die angeforderten Daten (EPC oder TID) sowie die Antennennummer der Antenne, die den jeweiligen Datenträger erfasst hat.

Byte	Länge	Befehlselement	Wertebereich
00	1	Antennennummer	01 _{hex} ...04 _{hex}
01	1	Reserviert	00 _{hex}
02...65	64	EPC/TID	Siehe Beschreibung <i>EPC/TID</i> auf Seite 101
66	1	Antennennummer	01 _{hex} ...04 _{hex}
67	1	Reserviert	00 _{hex}
68...131	64	EPC/TID	Siehe Beschreibung <i>EPC/TID</i> auf Seite 101
...	...	...	...

Befehlskennung ',': Datenträger erfassen, erweitert

Erfasst die Datenträger (max. 999), die sich im Erfassungsbereich der angegebenen Antenne befinden und gibt die unter *Datentyp* angegebenen Daten sowie Zusatzinformationen zurück. Mit der *Datenträgerauswahl* können wahlweise alle oder nur selektierte Datenträger erfasst werden (siehe *Befehlskennung 'z': Datenträger auswählen (Select)* auf Seite 105).

Zusatzinformationen:

Feld	Beschreibung
Protocol Control Word (PC)	Definiert in Standard: EPC™ Radio-Frequency Identity Protocols Generation-2 UHF RFID
Extended Protocol Control (XPC 1)	Definiert in Standard: EPC™ Radio-Frequency Identity Protocols Generation-2 UHF RFID
Extended Protocol Control (XPC 2)	Definiert in Standard: EPC™ Radio-Frequency Identity Protocols Generation-2 UHF RFID
Receive Signal Strength Indicator (RSSI)	Received Signal Strength Indicator (RSSI) erlaubt Rückschlüsse über die Signalqualität, mit der der Datenträger empfangen wurde. Er ist u. a. vom Tagtyp und von der Entfernung des erfassten Tags von der Antenne abhängig. Der vorzeichenbehaftete Wert liegt im Bereich -128...+127, höhere Werte bedeuten einen höheren Signalpegel. Im 007-Protokoll wird der Wert als 3 ASCII-Ziffern im Bereich '000'...'255' übertragen. Um in den tatsächlichen Wertebereich zu gelangen, ist folgende Rechnung notwendig: Werte von '000'...'127': Unverändert als Zahl 0...127 interpretieren. Werte von '128'...'255': Durch Subtrahieren von 256 in den Bereich -128...-1 umwandeln.
Zeitstempel	Enthält die Zeit, wann der Datenträger detektiert wurde in der Zeitzone UTC (Universal Time Coordinate) Format: hhmmssnnn hh = Stunden, mm = Minuten, ss = Sekunden, nnn = Millisekunden



Die Felder PC, XPC1 und XPC2 sind nur für Experten Anwendungen. Detailinformationen sind dem UHF-RFID Standard *EPC™ Radio-Frequency Identity Protocols Generation-2 UHF RFID* zu entnehmen.

Byte	Länge	Befehlselement	Wertebereich
00	1	Befehlskennung (ASCII)	','
01	1	Antennennummer (ASCII) (0 = alle aktiven Antennen)	'0'...'4'
02	1	Datentyp: EPC oder TID (ASCII)	'E': EPC 'T': TID
03...05	3	Max. Anzahl Datenträger (ASCII)	'000'...'999'
06	1	Datenträgerauswahl (ASCII)	'0': All '1': Selected
07	1	BCC	00 _{hex} ...FF _{hex}

Die positive Statusmeldung enthält Zusatzinformationen und wird wie folgt übertragen.

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<ACK>
01	1	Antennennummer (ASCII)	'1'...'4'
02	1	Datentyp EPC oder TID (ASCII)	'E': EPC 'T': TID
03...05	3	Anzahl gefundener Datenträger (ASCII)	'000'...'999'
06...07	2	Anzahl Byte Pro Datenträger (ASCII)	'64'
08	1	BCC	00 _{hex} ...FF _{hex}

Können die Daten nicht bereitgestellt werden, folgt eine negative Statusmeldung.

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<NAK>
01	1	Statuscode	Siehe Tabelle <i>Statuscodes</i> auf Seite 94

Bei positiver Statusmeldung werden mit <STX> Daten angefordert.

Byte	Länge	Befehlselement	Wertebereich
00	1	Steuerbefehl	<STX>

Byte	Daten (Hex)	Beschreibung
66	30 00	PC-Wort (EPC-Länge 12 Byte)
68	00 00	XPC_w1
70	00 00	XPC_w2
72	32 32 34	RSSI (ASCII) „224“ = -32
75	31 34 33 32 32 36 34 35 30	Zeitstempel (ASCII) 14:32:26.450
84	04	Tag an Antenne 3 erfasst
85	33	Höchster RSSI an Antenne '3'
86	3E	EPC hat eine Länge von 62 Byte
87	00	Reserviert
88...149	62, 00, 60, 00, 00, 00, 00, 55, 00, 00, 00, 00, 50, 00, 00, 00, 00, 45, 00, 00, 00, 00, 40, 00, 00, 00, 00, 35, 00, 00, 00, 00, 30, 00, 00, 00, 00, 25, 00, 00, 00, 00, 20, 00, 00, 00, 00, 15, 00, 00, 00, 00, 10, 00, 00, 00, 00, 05, 00, 00, 00, 01	EPC: 01, 00, 00, 00, 05, 00, 00, 00, 00, 10, 00, 00, 00, 00, 15, 00, 00, 00, 00, 20, 00, 00, 00, 00, 25, 00, 00, 00, 00, 30, 00, 00, 00, 00, 35, 00, 00, 00, 00, 40, 00, 00, 00, 00, 45, 00, 00, 00, 00, 50, 00, 00, 00, 00, 55, 00, 00, 00, 00, 60, 00, 62
150	F8 00	PC-Wort (EPC-Länge 62 Byte)
152	00 00	XPC_w1
154	00 00	XPC_w2
156	32 32 36	RSSI (ASCII) „226“ = -30
159	31 34 33 32 32 36 34 37 35	Zeitstempel (ASCII) 14:32:26.475

8.9 Datenträger erfassen, asynchron

Befehlskennung <DLE>: asynchrone Tag kommt/Tag geht Meldung

Über die asynchronen Meldungen *TAG KOMMT/TAG GEHT* kann überwacht werden, welche Datenträger sich im Erfassungsbereich der Antennen befinden bzw. welche diesen verlassen.

Die asynchrone Meldung *TAG KOMMT* meldet einen Datenträger einmalig als anwesend, sobald dieser in den Erfassungsbereich einer Antenne gelangt und die Bedingungen der Filterfunktionen erfüllt sind.

Die asynchrone Meldung *TAG GEHT* meldet einen bereits erkannten Datenträger einmalig als abwesend, sobald dieser den Erfassungsbereich einer Antenne verlässt und die Bedingungen der Filterfunktionen erfüllt sind.



Asynchrone Meldungen werden nur gesendet, wenn der asynchrone Modus und das Senden von Meldungen über den Parameter *ASYNCOPE- RATION* (1006_{hex}) aktiviert wurde, siehe Kapitel 7.3 auf Seite 49.



Datenträger mit gleichem EPC werden wie ein einzelner Datenträger behandelt.

Byte	Länge	Befehlselement	Wertebereich
00	1	Asynchrone Meldung	<DLE>
01	1	Meldung „Tag kommt“ oder „Tag geht“	'+' : Tag kommt '-' : Tag geht
02	1	Antennennummer (ASCII)	'0'
03	1	Kennung für EPC-Daten	'E'
04	1	Reserviert	20 _{hex}
05...06	2	Anzahl Byte ID (ASCII)	„64“
07	1	Länge EPC	02 _{hex} ...3E _{hex}
08	1	Reserviert	00 _{hex}
09...70	62	EPC (LSB...MSB)	00 _{hex} ...FF _{hex}
70...73	4	Reserviert	„0000“
74	1	BCC	00 _{hex} ...FF _{hex}

8.10 Datenträger bearbeiten

Befehlskennung 'z': Datenträger auswählen (Select)

Befinden sich mehrere Datenträger im Erfassungsbereich einer Antenne, kann ein einzelner Datenträger zur weiteren Bearbeitung selektiert werden. Dabei wird der gewünschte Datenträger über eine ID maskiert. Welche Daten als ID verwendet werden, kann über das Feld *ID-Typ* festgelegt werden.

Bei einer Selektion nach EPC oder TID ist der ID-Block mit entsprechenden Daten zu füllen. Das Format im ID-Block gleicht dem Format, mit dem das Gerät beim Befehl *Datenträger erfassen* die IDs ausgibt. Die Auswahl Daten der ID gelten immer vom Beginn der ID an. Es kann jedoch eine kürzere Länge im Feld *Anzahl Byte ID* angegeben werden, um ganze ID-Bereiche zu wählen (z. B. nur die ersten 4 Byte der ID müssen übereinstimmen).

Bei einer Selektion nach einem Teil der User-Daten soll der ID-Block mit 00_{hex} gefüllt werden und die Auswahl Daten im Abschnitt *User-Daten* bereitgestellt werden. Hier kann sowohl der Beginn des Auswahlbereichs (Adresse) als auch die Länge (Anzahl Bytes) gewählt werden.

Byte	Länge	Befehlselement	Wertebereich
00	1	Befehlskennung (ASCII)	'z'
01	1	Antennennummer (ASCII)	'0': Alle Antennen '1'...'4': Einzelantenne
02	1	ID-Typ	'E': EPC 'T': TID 'U': USER
03	64	ID-Block	Siehe ID-Block
66	6	Adresse (ASCII)	„000000“... „999999“, bei <i>ID-Typ</i> 'E' oder 'T' immer „000000“ eintragen
71	6	Anzahl Byte (ASCII)	„000000“... „999999“, bei <i>ID-Typ</i> 'E' oder 'T' immer „000000“ eintragen
76	Anzahl Byte	User-Daten, nur bei <i>ID-Typ</i> 'U'	Byte: 00 _{hex} ...FF _{hex}
Letztes Byte	1	BCC	00 _{hex} ...FF _{hex}

ID-Block

Der ID-Block enthält die *ID* sowie ein Längenfeld und wird in folgendem Format übertragen:

Byte	Länge	Befehlselement	Wertebereich
00	1	Anzahl Byte ID	00 _{hex} ...FF _{hex}
01	1	Reserviert	00 _{hex}
02	Anzahl Byte ID	ID (LSB...MSB)	Byte: 00 _{hex} ...FF _{hex}

Statusmeldung:

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<ACK> oder <NAK>
01	1	Statuscode	Siehe Tabelle <i>Statuscodes</i> auf Seite 94

Befehlskennung 'n': Datenträger abwählen (unselect)

Löscht die Datenträgerauswahl, die vorher mit dem Befehl *DATENTRÄGER AUSWÄHLEN (SELECT)* getroffen wurde. Der Befehl hat keine Auswirkungen, wenn sich kein selektierter Datenträger im Erfassungsbereich der angegebenen Antenne befindet.

Byte	Länge	Befehlselement	Wertebereich
00	1	Befehlskennung (ASCII)	'n'
01	1	Antennennummer (ASCII)	'0': Alle Antennen '1'...'4': Einzelantenne
Letztes Byte	1	BCC	00 _{hex} ...FF _{hex}

Statusmeldung

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<ACK> oder <NAK>
01	1	Statuscode	Siehe Tabelle <i>Statuscodes</i> auf Seite 94

Befehlskennung 'L': Datenträger lesen (<1024 Byte)

Auslesen von Daten (<1024 Byte) eines Datenträgers, der sich im Erfassungsbereich der angegebenen Antenne befindet. Über *STARTADRESSE*, *ANZAHL BYTES* und *SPEICHERBANK* wird der zu lesende Speicherbereich vorgegeben. Die angeforderten Daten werden unfragmentiert in einem einzelnen Datenpaket übertragen.

Befinden sich mehrere Datenträger im Erfassungsbereich der angegebenen Antenne, muss der gewünschte Datenträger vor dem Lesen selektiert werden (siehe *Befehlskennung 'z': Datenträger auswählen (Select)* auf Seite 105).

i Für die Speicherbereiche EPC und TID gibt es vereinfachte Befehle, die EPC und TID als gefilterte Information zurückgeben, siehe Befehlskennungen 'O' und 'y'.

i Details zu Verwendung und Organisation der unterschiedlichen Speicherbereiche können dem UHF-RFID Standard *EPC™ Radio-Frequency Identity Protocols Generation-2 UHF RFID* entnommen werden.

Byte	Länge	Befehlselement	Wertebereich
00	1	Befehlskennung (ASCII)	'L'
01...06	6	Startadresse (ASCII)	„000000“... „999999“
07...12	6	Anzahl Byte (ASCII)	„000000“... „999999“
13	1	Antennennummer (ASCII)	'0': Alle aktiven Antennen '1'...'4': Einzelantenne
14	1	Speicherbank (ASCII)	'R': Reserved 'E': EPC 'T': TID 'U': USER
15	1	BCC	00 _{hex} ...FF _{hex}

Statusmeldung

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<ACK> oder <NAK>
01	1	Statuscode	Siehe Tabelle <i>Statuscodes</i> auf Seite 94

Bei positiver Statusmeldung werden mit <STX> Daten angefordert:

Byte	Länge	Befehlselement	Wertebereich
00	1	Steuerbefehl	<STX>

Bei erfolgreicher Befehlsausführung folgen die angeforderten Daten mit der angegebenen Anzahl Byte und zusätzlichem BCC.

Byte	Länge	Befehlselement	Wertebereich
00	1	Daten	00 _{hex} ...FF _{hex}
...	...	...	00 _{hex} ...FF _{hex}
Letztes Byte	1	BCC	00 _{hex} ...FF _{hex}

Können die Daten nicht bereitgestellt werden, folgt eine negative Statusmeldung.

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<NAK>
01	1	Statuscode	Siehe Tabelle <i>Statuscodes</i> auf Seite 94

Befehlskennung 'H': Datenträger lesen, erweitert (>1024 Byte)

Auslesen von Daten (>1024 Byte) eines Datenträgers, der sich im Erfassungsbereich der angegebenen Antenne befindet. Über *STARTADRESSE*, *ANZAHL BYTES* und *SPEICHERBANK* wird der zu lesende Speicherbereich vorgegeben. Abhängig von der Datenmenge werden die Daten fragmentiert in einem oder mehreren Paketen übertragen, die nacheinander von der Auswerteeinheit angefordert werden können.

Befinden sich mehrere Datenträger im Erfassungsbereich der angegebenen Antennen, muss der gewünschte Datenträger vor dem Lesen selektiert werden (siehe *Befehlskennung 'z': Datenträger auswählen (Select)* auf Seite 105).

i Für die Speicherbereiche EPC und TID gibt es vereinfachte Befehle, die EPC und TID als gefilterte Information zurückgeben (siehe *Befehlskennung 'O': Datenträger lesen, EPC* auf Seite 108 und *Befehlskennung 'y': Datenträger lesen, TID* auf Seite 109).

i Details zu Verwendung und Organisation der unterschiedlichen Speicherbereichen können dem UHF-RFID Standard *EPC™ Radio-Frequency Identity Protocols Generation-2 UHF RFID* entnommen werden.

Byte	Länge	Befehlselement	Wertebereich
00	1	Befehlskennung (ASCII)	'H'
01...06	6	Startadresse (ASCII)	„000000“... „999999“
07...12	6	Anzahl Byte (ASCII)	„000000“... „999999“
13	1	Antennennummer (ASCII)	'0': Alle aktiven Antennen '1'...'4': Einzelantenne
14	1	Speicherbank (ASCII)	'R': Reserved 'E': EPC 'T': TID 'U': USER
15	1	BCC	00 _{hex} ...FF _{hex}

Können die Daten nicht bereitgestellt werden, folgt eine negative Statusmeldung.

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<NAK>
01	1	Statuscode	Siehe Tabelle <i>Statuscodes</i> auf Seite 94

Bei erfolgreicher Befehlsausführung folgt eine positive Statusmeldung. Diese enthält das erste Datenpaket und wird in folgendem Format übertragen:

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<ACK> oder <EOT>
01...03	3	Anzahl der Pakete (ASCII)	„000“...„999“
04...06	3	Paketnummer (ASCII)	„000“...„999“
07...12	6	Anzahl Byte (ASCII)	„000000“... „999999“
13...	Anzahl Byte	Daten	Byte: 00 _{hex} ...FF _{hex}
Letztes Byte	1	BCC	00 _{hex} ...FF _{hex}

Sind weitere Pakete vorhanden, dann können diese über <STX> angefordert werden, das letzte übertragene Datenpaket enthält den Status <EOT>.

Byte	Länge	Befehlselement	Wertebereich
00	1	Steuerbefehl	<STX>

Kann eines der Pakete nicht ordnungsgemäß übertragen werden, folgt eine negative Statusmeldung.

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<NAK>
01	1	Statuscode	Siehe Tabelle <i>Statuscodes</i> auf Seite 94

Befehlskennung 'O': Datenträger lesen, EPC

Liest den EPC eines Datenträgers, der sich im Erfassungsbereich der angegebenen Antenne befindet.

Befinden sich mehrere Datenträger im Erfassungsbereich der angegebenen Antenne, muss der gewünschte Datenträger vor dem Lesen selektiert werden (siehe *Befehlskennung 'z': Datenträger auswählen (Select)* auf Seite 105).

Byte	Länge	Befehlselement	Wertebereich
00	1	Befehlskennung (ASCII)	'O'
01	1	Antennennummer (ASCII)	'0': Alle aktiven Antennen '1'...'4': Einzelantenne
02	1	BCC	00 _{hex} ...FF _{hex}

Können die Daten nicht bereitgestellt werden, folgt eine negative Statusmeldung.

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<NAK>
01	1	Statuscode	Siehe Tabelle <i>Statuscodes</i> auf Seite 94

Statusmeldung

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<ACK> oder <NAK>
01	1	Statuscode	Siehe Tabelle <i>Statuscodes</i> auf Seite 94

Bei positiver Statusmeldung werden mit <STX> Daten angefordert.

Byte	Länge	Befehlselement	Wertebereich
00	1	Steuerbefehl	<STX>

Bei erfolgreicher Befehlsausführung folgen die angeforderten Daten.

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<ACK>
01	1	Antennennummer (ASCII) (0 = alle aktiven Antennen)	'0'...'4'
02...03	2	Anzahl Byte (ASCII)	„00“...„99“
04...	Anzahl Byte	EPC-Daten (LSB...MSB ¹⁾)	Byte: 00 _{hex} ...FF _{hex}
Letztes Byte	1	BCC	00 _{hex} ...FF _{hex}

¹⁾ LSB...MSB-Reihenfolge bedeutet eine umgekehrte Reihenfolge gegenüber der Anordnung im Speicher des Datenträgers.

Befehlskennung 'y': Datenträger lesen, TID

Liest die TID eines Datenträgers, der sich im Erfassungsbereich der angegebenen Antenne befindet. Die Länge der gelesenen TID-Daten wird über den Parameter 0004_{hex} festgelegt (siehe *TID-Länge* auf Seite 61).

Befinden sich mehrere Datenträger im Erfassungsbereich der angegebenen Antenne, muss der gewünschte Datenträger vor dem Lesen selektiert werden (siehe *Befehlskennung 'z': Datenträger auswählen (Select)* auf Seite 105).

Byte	Länge	Befehlselement	Wertebereich
00	1	Befehlskennung (ASCII)	'y'
01	1	Antennennummer (ASCII)	'0': Alle aktiven Antennen '1'...'4': Einzelantenne
02	1	BCC	00 _{hex} ...FF _{hex}

Statusmeldung

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<ACK> oder <NAK>
01	1	Statuscode	Siehe Tabelle <i>Statuscodes</i> auf Seite 94

Bei positiver Statusmeldung werden mit <STX> Daten angefordert

Byte	Länge	Befehlselement	Wertebereich
00	1	Steuerbefehl	<STX>

Bei erfolgreicher Befehlsausführung folgen die angeforderten Daten

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<ACK>
01	1	Antennennummer (ASCII) (0 = alle aktiven Antennen)	'0'...'4'
02...03	2	Anzahl Byte (ASCII)	„00“...„99“
04	Anzahl Byte	TID-Daten (LSB...MSB ¹⁾)	Byte: 00 _{hex} ...FF _{hex}
Letztes Byte	1	BCC	00 _{hex} ...FF _{hex}

¹⁾ LSB...MSB-Reihenfolge bedeutet eine umgekehrte Reihenfolge gegenüber der Anordnung im Speicher des Datenträgers.

Können die Daten nicht bereitgestellt werden, folgt eine negative Statusmeldung

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<NAK>
01	1	Statuscode	Siehe Tabelle <i>Statuscodes</i> auf Seite 94

Befehlskennung 'I': Datenträger lesen, Pulk

Auslesen der User-Daten von mehreren Datenträgern, die sich im Erfassungsbereich der angegebenen Antenne befinden. Über die *DATENTRÄGERAUSWAHL* können wahlweise alle Datenträger im Erfassungsbereich ausgelesen werden oder nur eine vorher mit dem Select-Befehl selektierte Untermenge

Über *STARTADRESSE* und *ANZAHL BYTES* wird der zu lesende Speicherbereich festgelegt. Dabei gelten folgende Randbedingungen:

Maximale Datenmenge: 65536 Byte/Datenträger

Maximale Anzahl Datenträger: 255

Zunächst meldet der Befehl nur die Anzahl der Datenträger, die erfasst wurden. Anschließend werden die angeforderten Daten ausgelesen und fragmentiert in einem oder mehreren Paketen übertragen.

Werden erfasste Datenträger vor dem Auslesen aus dem Erfassungsbereich der Antenne entnommen oder können nicht erfolgreich ausgelesen werden, dann werden die Daten durch ein Prüfbyte als ungültig gekennzeichnet.

Byte	Länge	Befehlselement	Wertebereich
00	1	Befehlskennung (ASCII)	'I'
01	1	Antennennummer (ASCII)	"0": Alle aktiven Antennen '1'...'4': Einzelantenne
02...07	6	Startadresse (ASCII)	„000000“... „999999“
08...13	6	Anzahl Byte/Datenträger (ASCII)	„000001“... „065536“
14	1	Datenträgerauswahl	'0': All '1': Selected
15...17	3	Max. Anzahl Datenträger (ASCII)	„000“...„999“
18	1	BCC	00 _{hex} ...FF _{hex}

Kann der Befehl nicht ordnungsgemäß ausgeführt werden, folgt eine negative Statusmeldung.

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<NAK>
01	1	Statuscode	Siehe Tabelle <i>Statuscodes</i> auf Seite 94

Bei erfolgreicher Befehlsausführung folgt eine positive Statusmeldung. Diese enthält die Anzahl der erfassten Datenträger und die Anzahl der Datenbyte, die pro Datenträger übertragen werden.

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<ACK>
01	1	Antennennummer (ASCII) (0 = alle aktiven Antennen)	'0'...'4'
02...04	3	Anzahl gefundener Datenträger (ASCII)	„000“...„999“
05...10	6	Anzahl Byte/Datenträger (ASCII)	„000001“... „065536“
11	1	BCC	00 _{hex} ...FF _{hex}

Die Gesamtzahl der übertragenen Byte ergibt sich nach folgender Formel:

$$\text{Gesamtzahl Byte} = ((\text{Anzahl Byte/Datenträger}) + 1) \times (\text{Anzahl gefundener Datenträger})$$

Bei positiver Statusmeldung werden mit <STX> Daten angefordert.

Byte	Länge	Befehlselement	Wertebereich
00	1	Steuerbefehl	<STX>

Können die Daten nicht bereitgestellt werden, folgt eine negative Statusmeldung.

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<NAK>
01	1	Statuscode	Siehe Tabelle <i>Statuscodes</i> auf Seite 94

Bei erfolgreicher Befehlsausführung folgt eine positive Statusmeldung. Diese enthält das erste Datenpaket und wird in folgendem Format übertragen:

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<ACK> oder <EOT>
01	1	Antennennummer (ASCII) (0 = alle aktiven Antennen)	'0'...'4'
02...04	3	Anzahl der Pakete (ASCII)	„000“...„999“
05...07	3	Paketnummer (ASCII)	„000“...„999“
08...11	3	Datenblock: Anzahl Byte (ASCII)	„000“...„999“
12...	Anzahl Byte	Datenblock	Byte: 00 _{hex} ...FF _{hex}
Letztes Byte	1	BCC	00 _{hex} ...FF _{hex}

Datenblock

Der Datenblock wird mit der angegebenen Anzahl Byte übertragen, die unter *DATENBLOCK: ANZAHL BYTES* angegeben ist. Die Länge der einzelnen Datenfelder (Tag 1...Tag n) entspricht der angeforderten *ANZAHL BYTES/DATENTRÄGER*.

Länge	Befehlselement	Wertebereich
Anzahl Byte/ Datenträger	Daten 1	Byte: 00 _{hex} ...FF _{hex}
1	Prüfbyte 1	00 _{hex} : Gültig FF _{hex} : Ungültig
Anzahl Byte/ Datenträger	Optional: Daten 2	Byte: 00 _{hex} ...FF _{hex}
1	Optional: Prüfbyte 2	00 _{hex} : Gültig FF _{hex} : Ungültig
...	...	...

Sind weitere Pakete vorhanden, können diese über <STX> angefordert werden, das letzte übertragene Datenpaket enthält den Status <EOT>.

Byte	Länge	Befehlselement	Wertebereich
00	1	Steuerbefehl	<STX>

Befehlskennung '>': Datenträger lesen, Pulk erweitert

Auslesen von mehreren Datenträgern, die sich im Erfassungsbereich der angegebenen Antenne befinden. Mit der *DATENTRÄGERAUSWAHL* können wahlweise alle Datenträger im Erfassungsbereich ausgelesen werden oder nur eine vorher mit dem Select-Befehl selektierte Untermenge.

Über *STARTADRESSE*, *ANZAHL BYTES* und *SPEICHERBANK* wird der zu lesende Speicherbereich vorgegeben.

Die angeforderten Daten werden zusammen mit dem EPC des Datenträgers übertragen, um die Daten zuordnen zu können. Abhängig von der Datenmenge werden die Daten fragmentiert in einem oder mehreren Paketen übertragen, die iterativ von der Auswerteeinheit angefordert werden können. Dabei gelten folgende Randbedingungen:

Maximale Datenmenge: 999999 Byte/Datenträger

Maximale Anzahl Datenträger: 999

Zunächst meldet der Befehl nur die Anzahl der Datenträger, die erfasst wurden. Anschließend werden die angeforderten Daten ausgelesen und fragmentiert in einem oder mehreren Paketen übertragen.

Werden erfasste Datenträger vor dem Auslesen aus dem Erfassungsbereich der Antenne entnommen oder können nicht erfolgreich ausgelesen werden, werden die Daten durch ein Prüfbyte als ungültig gekennzeichnet.

Byte	Länge	Befehlselement	Wertebereich
00	1	Befehlskennung (ASCII)	'I'
01	1	Antennennummer (ASCII)	'0': Alle aktiven Antennen '1'...'4': Einzelantenne
02...07	6	Startadresse (ASCII)	„000000“... „999999“
08...13	6	Anzahl Byte/ Datenträger (ASCII)	„000001“... „999999“
14	1	Datenträgerauswahl	'0': All '1': Selected
15...17	3	Max. Anzahl Datenträger (ASCII)	„000“...„999“
18	1	Speicherbank (ASCII)	'R': Reserved 'E': EPC 'T': TID 'U': USER
19	1	BCC	00 _{hex} ...FF _{hex}

Kann der Befehl nicht ordnungsgemäß ausgeführt werden, folgt eine negative Statusmeldung.

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<NAK>
01	1	Statuscode	Siehe Tabelle <i>Statuscodes</i> auf Seite 94

Bei erfolgreicher Befehlsausführung folgt eine positive Statusmeldung. Diese enthält die Anzahl der erfassten Datenträger, die Anzahl der Byte, die für den EPC jedes Datenträgers übertragen werden und die Anzahl der Datenbyte, die pro Datenträger übertragen werden.

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<ACK>
01	1	Antennennummer (ASCII)	'0'...'4'
02...04	3	Anzahl gefundener Datenträger (ASCII)	„000“...„999“
05...06	2	Anzahl Byte je EPC (ASCII)	„64“
07...12	6	Anzahl Byte/ Datenträger (ASCII)	„000000“... „999999“
13	1	BCC	00 _{hex} ...FF _{hex}

Bei positiver Statusmeldung werden mit <STX> Daten angefordert.

Byte	Länge	Befehlselement	Wertebereich
00	1	Steuerbefehl	<STX>

Können die Daten nicht bereitgestellt werden, folgt eine negative Statusmeldung.

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<NAK>
01	1	Statuscode	Siehe Tabelle <i>Statuscodes</i> auf Seite 94

Bei erfolgreicher Befehlsausführung folgt eine positive Statusmeldung. Diese enthält das erste Datenpaket und wird in folgendem Format übertragen:

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<ACK> oder <EOT>
01	1	Antennennummer (ASCII)	'0'...'4'
02...04	3	Anzahl der Pakete (ASCII)	„001“...„999“
05...07	3	Paketnummer (ASCII)	„001“...„999“
08...12	4	Anzahl Byte im folgenden Datenblock (ASCII)	„0000“...„9999“
13...	Anzahl Byte	Datenblock	Byte: 00 _{hex} ...FF _{hex}
Letztes Byte	1	BCC	00 _{hex} ...FF _{hex}

Datenblock

Der Datenblock wird mit der angegebenen Anzahl Byte übertragen, die unter *DATENBLOCK: ANZAHL BYTES* angegeben ist. Die Länge der einzelnen Datenfelder (Tag 1...Tag n) entspricht der angeforderten *ANZAHL BYTES/DATENTRÄGER*.

Länge	Befehlselement	Wertebereich
64	EPC 1 (LSB...MSB)	Byte: 00 _{hex} ...FF _{hex}
Anzahl Byte/ Daten	Daten 1	Byte: 00 _{hex} ...FF _{hex}
1	Prüfbyte 1	00 _{hex} : Gültig FF _{hex} : Ungültig
64	EPC 2 (LSB...MSB)	Byte: 00 _{hex} ...FF _{hex}
Anzahl Byte/ Daten	Daten 2	Byte: 00 _{hex} ...FF _{hex}
1	Prüfbyte 2	00 _{hex} : Gültig FF _{hex} : Ungültig
...	...	...

Sind weitere Pakete vorhanden, können diese über <STX> angefordert werden, das letzte übertragene Datenpaket enthält den Status <EOT>.

Byte	Länge	Befehlselement	Wertebereich
00	1	Steuerbefehl	<STX>

Befehlskennung 'P': Datenträger schreiben
(<1024 Byte)

Schreiben von Daten (<1024 Byte) auf einen Datenträger, der sich im Erfassungsbereich der angegebenen Antenne befindet.

Über *STARTADRESSE* und *ANZAHL BYTES* wird der zu schreibende Speicherbereich vorgegeben. Die Daten werden unfragmentiert in einem einzelnen Datenpaket übertragen. Befinden sich mehrere Datenträger im Erfassungsbereich der angegebenen Antenne, muss der gewünschte Datenträger vor dem Schreiben selektiert werden (siehe *Befehlskennung 'z': Datenträger auswählen (Select)* auf Seite 105).

i Zum Beschreiben von schreibgeschützten Datenträgern ist ein Passwort erforderlich. Schreibbefehle, die mit einem ungültigen Passwort durchgeführt werden, werden mit der Statusmeldung *PASSWORT BENÖTIGT* bzw. *PASSWORT UNGÜLTIG* quittiert.

Das Zugriffspasswort kann über den Parameter 1004_{hex} vorab gesetzt werden (siehe *Speicherbank* auf Seite 54).

Byte	Länge	Befehlselement	Wertebereich
00	1	Befehlskennung (ASCII)	'P'
01	6	Startadresse (ASCII)	„000000“... „999999“
06	6	Anzahl Byte (ASCII)	„000000“... „999999“
11	1	Antennennummer (ASCII)	'0': Alle aktiven Antennen '1'...'4': Einzelantenne
12	1	Speicherbank (ASCII)	'R': Reserved 'E': EPC 'T': TID 'U': USER
13	1	BCC	00 _{hex} ...FF _{hex}

Statusmeldung:

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<ACK> oder <NAK>
01	1	Statuscode	Siehe <i>Statuscodes</i> auf Seite 94

Bei positiver Statusmeldung können mit <STX> Daten übertragen werden.

Byte	Länge	Befehlselement	Wertebereich
00	1	Steuerbefehl	<STX>
01	Anzahl Byte	Daten	Byte: 00 _{hex} ...FF _{hex}
Letztes Byte	1	BCC	00 _{hex} ...FF _{hex}

Statusmeldung:

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<ACK> oder <NAK>
01	1	Statuscode	Siehe <i>Statuscodes</i> auf Seite 94

Befehlskennung 'F': Datenträger schreiben, erweitert (>1024 Byte)

Schreiben von Daten (>1024 Byte) auf einen Datenträger, der sich im Erfassungsbereich der angegebenen Antenne befindet. Über *STARTADRESSE* und *ANZAHL BYTES* und *SPEICHERBANK* wird der zu schreibende Speicherbereich vorgegeben. Abhängig von der Datenmenge werden die Daten fragmentiert in einem oder mehreren Paketen übertragen.

Befinden sich mehrere Datenträger im Erfassungsbereich der angegebenen Antenne, muss der gewünschte Datenträger vor dem Schreiben selektiert werden (siehe *Befehlskennung 'z': Datenträger auswählen (Select)* auf Seite 105).



Zum Beschreiben von schreibgeschützten Datenträgern ist ein Passwort erforderlich. Schreibbefehle, die mit einem ungültigen Passwort durchgeführt werden, werden mit der Statusmeldung *PASSWORT BENÖTIGT* bzw. *PASSWORT UNGÜLTIG* quittiert.

Das Zugriffspasswort kann über den Parameter 1004_{hex} vorab gesetzt werden (siehe *Speicherbank* auf Seite 54).

Byte	Länge	Befehlselement	Wertebereich
00	1	Befehlskennung (ASCII)	'F'
01...06	6	Startadresse (ASCII)	„000000“... „999999“
07...12	1	Anzahl Byte (ASCII)	„000000“... „999999“
13	1	Antennennummer (ASCII)	'0': Alle aktiven Antennen '1'...'4': Einzelantenne
14	1	Speicherbank (ASCII)	'R': Reserved 'E': EPC 'T': TID 'U': USER
15	1	BCC	00 _{hex} ...FF _{hex}

Statusmeldung:

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<ACK> oder <NAK>
01	1	Statuscode	Siehe Tabelle <i>Statuscodes</i> auf Seite 94

Nach jeder positiven Statusmeldung kann ein Datenblock in folgendem Format übertragen werden.

Dies wird wiederholt, bis alle Daten übertragen wurden. Die Anzahl Byte je Paket ist beliebig, darf aber 1024 nicht übersteigen.

Byte	Länge	Befehlselement	Wertebereich
00	1	Steuerbefehl	<STX>
01...06	6	Datenblock: Anzahl Byte (ASCII)	„000000“... „999999“
07	Anzahl Byte	Datenblock	Byte: 00 _{hex} ...FF _{hex}
Letztes Byte	1	BCC	00 _{hex} ...FF _{hex}

Statusmeldung:

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<ACK> oder <NAK>
01	1	Statuscode	Siehe Tabelle <i>Statuscodes</i> auf Seite 94

Befehlskennung 'v': Datenträger schreiben, EPC

Schreiben von EPC-Daten auf einen Datenträger, der sich im Erfassungsbereich der angegebenen Antenne befindet.

Über *ANZAHL BYTES* kann die Größe des EPC-Speicherbereichs festgelegt werden. Wenn notwendig, wird der Datenträger automatisch auf die neue EPC-Speichergröße umkonfiguriert.

Byte	Länge	Befehlselement	Wertebereich
00	1	Befehlskennung (ASCII)	'v'
01	1	Antennennummer (ASCII)	'0': Alle aktiven Antennen '1'...'4': Einzelantenne
02...03	2	Anzahl Byte (ASCII)	„00“ ... „99“
15	1	BCC	00 _{hex} ...FF _{hex}

Statusmeldung:

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<ACK> oder <NAK>
01	1	Statuscode	Siehe Tabelle <i>Statuscodes</i> auf Seite 94

Bei positiver Statusmeldung können mit <STX> Daten übertragen werden.

Byte	Länge	Befehlselement	Wertebereich
00	1	Steuerbefehl	<STX>
01	Anzahl Byte	EPC-Daten (LSB...MSB ¹⁾)	Byte: 00 _{hex} ...FF _{hex}
Letztes Byte	1	BCC	00 _{hex} ...FF _{hex}

¹⁾ LSB...MSB-Reihenfolge bedeutet eine umgekehrte Reihenfolge gegenüber der Anordnung im Speicher des Datenträgers.

Statusmeldung:

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<ACK> oder <NAK>
01	1	Statuscode	Siehe <i>Statuscodes</i> auf Seite 94

Befehlskennung 'w': Datenträger schreiben, Pulk

Schreiben von User-Daten auf mehrere Datenträger, die sich im Erfassungsbereich der angegebenen Antenne befinden. Mit der *DATENTRÄGERAUSWAHL* können wahlweise alle Datenträger im Erfassungsbereich beschrieben werden oder nur eine vorher mit dem Select-Befehl selektierte Untermenge. Es wird die Anzahl der gefundenen und erfolgreich beschriebenen Datenträger zurückgeliefert.

Über *STARTADRESSE* und *ANZAHL BYTES* wird der zu schreibende Speicherbereich vorgegeben. Abhängig von der Datenmenge werden die Daten fragmentiert in einem oder mehreren Paketen übertragen, wobei jedes übertragene Paket mit einer Statusmeldung quittiert wird.

Für die Übertragung gelten folgende Randbedingungen:

- Maximale Datenmenge: 999999 Byte/Datenträger
- Maximale Anzahl Datenträger: 999

Byte	Länge	Befehlselement	Wertebereich
00	1	Befehlskennung (ASCII)	'w'
01	1	Antennennummer (ASCII)	'0': Alle aktiven Antennen '1'...'4': Einzelantenne
02...07	6	Startadresse (ASCII)	„000000“... „999999“
08...13	6	Anzahl Byte (ASCII)	„000000“... „999999“
14	1	Datenträgerauswahl	'0': All '1': Selected
15...17	3	Max. Anzahl Datenträger (ASCII)	„000“...„999“
18	1	BCC	00 _{hex} ...FF _{hex}

Statusmeldung:

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<ACK> oder <NAK>
01	1	Statuscode	Siehe Tabelle <i>Statuscodes</i> auf Seite 94

Bei positiver Statusmeldung kann mit <STX> das erste Datenpaket übertragen werden. Folgen weitere Datenpakete, können diese nach jeder positiven Statusmeldung iterativ übertragen werden.

Byte	Länge	Befehlselement	Wertebereich
00	1	Steuerbefehl	<STX>
01...06	6	Anzahl Byte im folgenden Datenblock (ASCII)	„000000“... „999999“
07	Anzahl Byte	Datenblock	00 _{hex} ...FF _{hex}
Letztes Byte	1	BCC	00 _{hex} ...FF _{hex}

Statusmeldung:

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<ACK> oder <NAK>
01	1	Statuscode	Siehe Tabelle <i>Statuscodes</i> auf Seite 94

Die positive Statusmeldung enthält Zusatzinformationen und wird in nachfolgendem Format übertragen. Das Datenfeld *OPERATION* wird mit Status *PENDING* übertragen, solange weitere Pakete übertragen werden. Das letzte übertragene Paket wird mit dem Status *FINISHED* quittiert.

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<ACK>
01	1	Antennennummer (ASCII)	'0'...'4'
02...04	3	Anzahl gefundene Datenträger	„000“...„999“
05...08	4	Anzahl geschriebener Datenträger	„0000“...„9999“
09	1	Operation	'P': Pending 'F': Finished
Letztes Byte	1	BCC	00 _{hex} ...FF _{hex}

Befehlskennung '<': Datenträger schreiben, Pulk erweitert

Schreiben von Daten auf mehrere Datenträger, die sich im Erfassungsbereich der angegebenen Antenne befinden. Mit der *DATENTRÄGERAUSWAHL* können wahlweise alle Datenträger im Erfassungsbereich beschrieben werden oder nur eine vorher mit dem Select-Befehl selektierte Untermenge. Es wird eine Liste der EPCs aller erfolgreich beschriebenen Datenträger zurückgeliefert.

Über *STARTADRESSE*, *ANZAHL BYTES* und *SPEICHERBANK* wird der zu schreibende Speicherbereich vorgegeben. Abhängig von der Datenmenge werden die Daten fragmentiert in einem oder mehreren Paketen übertragen, wobei jedes übertragene Paket mit einer Statusmeldung quittiert wird.

Für die Übertragung gelten folgende Randbedingungen:

- Maximale Datenmenge: 999999 Byte/Datenträger
- Maximale Anzahl Datenträger: 999

Byte	Länge	Befehlselement	Wertebereich
00	1	Befehlskennung (ASCII)	'w'
01	1	Antennennummer (ASCII)	'0': Alle aktiven Antennen '1'...'4': Einzellantenne
02...07	6	Startadresse (ASCII)	„000000“... „999999“
08...13	6	Anzahl Byte (ASCII)	„000000“... „999999“
14	1	Datenträgerauswahl	'0': All '1': Selected
15...17	3	Max. Anzahl Datenträger (ASCII)	„000“...„999“
18	1	Speicherbank (ASCII)	'R': Reserved 'E': EPC 'T': TID 'U': USER
19	1	BCC	00 _{hex} ...FF _{hex}

Statusmeldung:

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<ACK> oder <NAK>
01	1	Statuscode	Siehe Tabelle <i>Statuscodes</i> auf Seite 94

Bei positiver Statusmeldung kann mit <STX> das erste Datenpaket übertragen werden. Folgen weitere Datenpakete, können diese nach jeder weiteren positiven Statusmeldung übertragen werden.

Byte	Länge	Befehlselement	Wertebereich
00	1	Steuerbefehl	<STX>
01...06	6	Anzahl Byte im folgenden Datenblock (ASCII)	„000000“... „999999“
07	Anzahl Byte	Datenblock	Byte: 00 _{hex} ...FF _{hex}
Letztes Byte	1	BCC	00 _{hex} ...FF _{hex}

Statusmeldung:

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<ACK> oder <NAK>
01	1	Statuscode	Siehe Tabelle <i>Statuscodes</i> auf Seite 94

Die letzte positive Statusmeldung enthält Zusatzinformationen und wird in nachfolgendem Format übertragen. Das Datenfeld *OPERATION* wird mit dem Wert *FINISHED* übertragen.

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<ACK>
01	1	Antennennummer (ASCII)	'0'...'4'
02...04	3	Anzahl erfasster Datenträger	„000“...„999“
05...08	4	Anzahl geschriebener Datenträger	„0000“...„9999“
09...10	2	Anzahl Byte je ID (ASCII)	„64“
11	1	Operation (ASCII)	'F': Finished
Letztes Byte	1	BCC	00 _{hex} ...FF _{hex}

Nach dem letzten übertragenen Paket, d. h. wenn das Feld *OPERATION* in der positiven Statusmeldung *FINISHED* enthält, kann mit <STX> ein abschließender Statusbericht angefordert werden.

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<STX>

Kann der Statusbericht nicht erstellt werden, folgt eine negative Statusmeldung.

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<NAK>
01	1	Statuscode	Siehe Tabelle <i>Statuscodes</i> auf Seite 94

Die positive Statusmeldung wird mit <ACK> oder <EOT> quittiert und enthält Statusinformationen zu den erfolgreich geschriebenen Daten. Wenn mehrere Statuspakete bereitstehen, wird mit <ACK> quittiert, das letzte zu übertragende Paket mit <EOT>.

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<ACK> oder <EOT>
01...03	3	Anzahl der Pakete, die Statusinformationen enthalten	„000“...„999“
04...06	3	Aktuelle Paketnummer	„000“...„999“
07...12	6	Anzahl Byte im Datenblock	„000000“... „999999“
13...	Anzahl Byte	Datenblock	Byte: 00 _{hex} ...FF _{hex}
Letztes Byte	1	BCC	00 _{hex} ...FF _{hex}

Datenblock

Der Datenblock enthält eine Liste der Datenträger (EPCs), die erfolgreich beschrieben wurden.

Byte	Länge	Befehlselement	Wertebereich
00	64	EPC Tag 1	Byte: 00 _{hex} ...FF _{hex}
65	64	EPC Tag 2 (optional)	Byte: 00 _{hex} ...FF _{hex}
...	...	EPC Tag n (optional)	Byte: 00 _{hex} ...FF _{hex}

Mit <STX> können, wenn vorhanden, weitere Statuspakete angefordert werden. Das letzte verfügbare Statuspaket wird mit <EOT> quittiert und enthält die Statusdaten des letzten Pakets.

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<STX>

Befehlskennung 'k': Kill

Deaktiviert einen ausgewählten Datenträger dauerhaft und sperrt diesen für jegliche Benutzung.

Zur Ausführung des *KILL*-Befehls muss zunächst ein *KILL*-Passwort festgelegt und auf den Datenträger geschrieben werden.

Das Passwort hat eine Länge von 4 Byte und wird als String mit 8 Byte im ASCII-hex-Zahlenformat übertragen.

Beispiel für Passwort (MSB...LSB):

- im Hex-Format: 010A8FCC_{hex}
- im ASCII-hex-Format: „010A8FCC“



Ein Kill-Befehl deaktiviert den ausgewählten Datenträger dauerhaft und kann nicht rückgängig gemacht werden!

Details zum Passwortschutz bzw. zum Sperren und Entsperren (*Lock*) von UHF-RFID-Datenträgern können dem Standard *EPC™ Radio-Frequency Identity Protocols Generation-2 UHF RFID* entnommen werden.

Byte	Länge	Befehlselement	Wertebereich
00	1	Befehlskennung (ASCII)	'k'
01	1	Antennennummer (ASCII)	'0': Alle aktiven Antennen '1'...'4': Einzelantenne
02	8	Passwort (ASCII hex) (MSB...LSB)	„00000000“... „FFFFFFFF“
10	1	BCC	00 _{hex} ...FF _{hex}

Statusmeldung:

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<ACK> oder <NAK>
01	1	Statuscode	Siehe <i>Statuscodes</i> auf Seite 94

Bei positiver Statusmeldung kann der *KILL*-Befehl mit <STX> bestätigt werden.

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<STX>

Statusmeldung:

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<ACK> oder <NAK>
01	1	Statuscode	Siehe <i>Statuscodes</i> auf Seite 94

Befehlskennung 'I': Lock

Mit dem **LOCK**-Befehl können Speicherbereiche (RES, EPC, TID, USER) eines UHF-Datenträgers für Schreib- oder Lesezugriffe, sowie für jegliche Zugriffe gesperrt werden. Je nach Sicherheitsstufe können die Speicherbereiche lediglich passwortgeschützt oder komplett gesperrt werden.

Durch die Felder **MASK** und **ACTION** wird spezifiziert, welche Speicherbereiche einen neuen **LOCK**-Status erhalten, und wie dieser aussehen soll. Durch die Verwendung von Bit-Masken kann der **LOCK**-Status mehrerer Speicherbereiche zeitgleich geändert werden.

Vor Ausführung des **LOCK**-Befehls muss der Datenträger selektiert werden und das für den ausgewählten Tag gültige Zugriffspasswort (**ACCESS PW**) in den Parameter 1004_{hex} geschrieben werden (siehe *Speicherbank* auf Seite 54).

- i** Zum Selektieren von Datenträgern (siehe *Befehlskennung 'z': Datenträger auswählen (Select)* auf Seite 105).
- Zum Festlegen eines Zugriffspassworts für einen Datenträger erfolgt durch Schreiben auf die Byteadresse 4...7 der Speicherbank **RESERVED**, siehe *Befehlskennung 'F': Datenträger schreiben, erweitert (>1024 Byte)* auf Seite 114.
- Zum Übertragen des Passworts zum Zugriff auf den Datenträger und Ausführen des **LOCK**-Befehls siehe *Befehlskennung 'E': Geräteparameter ändern* auf Seite 98 (Parameter-Nr: 1002_{hex}).

Mask und Action

MASK: Bit-Maske (16 Bit), über die festgelegt wird, welche Speicherbereiche durch das Feld **ACTION** beeinflusst werden sollen. Der **LOCK**-Status der Speicherbereiche EPC, TID und USER sowie der Bereich, in dem Passwörter gespeichert sind, können unabhängig voneinander gesperrt/entsperrt werden.

- 0: Speicherbereich wird *nicht* durch das Feld **ACTION** beeinflusst
- 1: Speicherbereich wird durch das Feld **ACTION** beeinflusst

ACTION: Bit-Maske (16 Bit), über die der **LOCK**-Status der durch **MASK** angegebenen Speicherbereiche festgelegt wird.

Bit-Nr	15	14	13	12	11	10	9	8
Mask	Nicht verwendet							Kill PW
Action	Nicht verwendet							Status

Bit-Nr	7	6	5	4	3	2	1	0
Mask	Access-Passwort		EPC		TID		USER	
Action	Lock-Status		Lock-Status		Lock-Status		Lock-Status	

Lock-Status der Speicherbereiche EPC, TID, USER

- i** Der Speicherbereich **TID** ist unabhängig vom **LOCK**-Status grundsätzlich schreibgeschützt und kann nur gelesen werden.

Status	Lesen möglich	Schreiben möglich	Status kann verändert werden
00	Ja	Ja	Ja
01	Ja	Ja	Nein
10	Ja	Mit Access-Passwort	Ja
11	Ja	Gesperrt	Nein

Lock-Status für Inhalte des Speicherbereichs Reserved (Access PW/Kill PW)

Status	Lesen möglich	Schreiben möglich	Status kann verändert werden
00	Ja	Ja	Ja
01	Ja	Ja	Nein
10	Mit Access-Passwort	Mit Access-Passwort	Ja
11	Gesperrt	Gesperrt	Nein

Ausführung des Lock-Befehls

Byte	Länge	Befehlselement	Wertebereich
00	1	Befehlskennung (ASCII)	'I'
01	1	Antennennummer (ASCII)	'0': Alle aktiven Antennen '1'...'4': Einzelantenne
02...05	4	Mask (ASCII hex)	„0000“...„03FF“
06...09	4	Action (ASCII hex)	„0000“...„03FF“
10	1	BCC	00 _{hex} ...FF _{hex}

Statusmeldung:

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<ACK> oder <NAK>
01	1	Statuscode	Siehe <i>Statuscodes</i> auf Seite 94

8

007-Protokoll (Fortsetzung)

Bei positiver Statusmeldung kann der Lock-Befehl mit <STX> bestätigt werden.

Byte	Länge	Befehlselement	Wertebereich
00	1	Steuerbefehl	<STX>

Statusmeldung:

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<ACK> oder <NAK>
01	1	Statuscode	Siehe <i>Statuscodes</i> auf Seite 94

8.11 Universeller Datenträgerzugriff (Formatierte Tagdaten)

Über die Funktionen *UNIVERSELLER DATENTRÄGERZUGRIFF (FORMATIERTE TAGDATEN)* können komplexe zusammengesetzte Befehle erzeugt werden, die beim Erfassen, Lesen oder Schreiben von Datenträgern frei definierbare Daten verwenden bzw. zurückgeben. Dabei können unterschiedliche Speicherbereiche sowie die Formatierung der Daten festgelegt werden.

Zum Beispiel kann vorgegeben werden, dass beim Erfassen der Datenträger folgende Daten zurückgegeben werden:

Speicherbereich	Startadresse	Anzahl Byte	Interpretation
EPC	0	12	Hex-Daten
TID	0	8	Hex-Daten
USER	6	4	Hex-Daten als ASCII-String



Für eine Detailbeschreibung zur Anwendung und den verschiedenen Möglichkeiten siehe Kapitel 7.3.3 *Beschreibung der Parameter für Standardbenutzer* auf Seite 69.
 Die Parametrierung der Default-Formate kann über den Webserver oder den UHF-Manager erfolgen (siehe Kapitel 7.2 auf Seite 33 und Kapitel 7.1 auf Seite 29).
 Die Default-Werte der Formatangaben können für jede TCP- und USB-Session separat mit dem Befehl *GERÄTEPARAMETER SCHREIBEN* überschrieben werden.

UNIVERSAL DATENTRÄGER Befehle bieten die Möglichkeit, den Ausgabekanal (TCP-Port) für die angeforderten Daten vorzugeben.

IN-Band: Befehl und Daten werden auf demselben TCP-Port übertragen

OUT-Band: Befehl und Daten werden auf unterschiedlichen TCP-Ports übertragen.

007-Befehlskanal/Session	Ein- und Ausgabe der Daten bei IN-Band	Ein- und Ausgabe der Daten bei OUT-Band
TCP 10001	TCP 10001	TCP 10011
TCP 10001	TCP 10002	TCP 10012
TCP 10001	TCP 10003	TCP 10013
TCP 10001	TCP 10004	TCP 10014
TCP 10001	TCP 10005	TCP 10015
USB-Port	USB-Port	Nicht möglich



Details zu den verfügbaren Port-Modi können Kapitel 6.5 auf Seite 23 entnommen werden.

Über den Ausgabemodus kann festgelegt werden, welche Statusmeldungen auf dem Befehlskanal gesendet werden sollen:

Wert	Bedeutung	Übertragungsschema
'A'	Ack only (nur Status)	Anfrage – Status – Daten
'F'	Full (Status und EOT)	Anfrage – Status – Daten – EOT
'N'	No Status (nur Daten)	Anfrage – Daten

Befehlskennung '-L': Datenträger erfassen, universal

Erfasst die Datenträger (max. 999), die sich im Erfassungsbereich der angegebenen Antenne befinden und gibt die vorher festgelegten formatierten Tagdaten der angegebenen Daten zurück. Über den Ausgabekanal kann festgelegt werden, ob Anfrage und Antwort auf demselben TCP-Port (IN-Band) oder auf verschiedenen TCP-Ports (OUT-Band) übertragen werden.

Byte	Länge	Befehlselement	Wertebereich
00	1	Befehlskennung universal (ASCII)	'-'
01	1	Befehlskennung (ASCII)	'L'
02	1	Antennennummer (ASCII)	'0': Alle aktiven Antennen '1'...'4': Einzelantenne
03...05	3	Max. Anzahl Datenträger (ASCII)	'000'...'999'
06	1	Ausgabekanal	'0': IN-Band '1': OUT-Band
07	1	Ausgabemodus	'A': Ack only 'F': Full Status 'N': No Status
08	1	BCC	00 _{hex} ...FF _{hex}

Statusmeldung (wird nur im Ausgabemodus 'A' und 'F' übertragen):

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<ACK> oder <NAK>
01	1	Statuscode	Siehe Tabelle <i>Statuscodes</i> auf Seite 94

Bei erfolgreicher Befehlsausführung folgen auf dem definierten Datenkanal die formatierten Tagdaten der Datenträger, die sich im Erfassungsbereich der angegebenen Antenne befinden. Die Daten entsprechen der vorgegebenen Formatierung.

Byte	Länge	Befehlselement	Wertebereich
00...	variabel	Präfix + Formatierte Tagdaten(1.Tag) + Formatierte Tagdaten(2.Tag) + ... + Suffix	Alle durch das Format möglichen Werte

Anschließend folgt <EOT> Meldung, die die Anzahl der erfassten Datenträger enthält (wird nur im Ausgabemodus 'F' übertragen)

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<EOT>
01	1	Anzahl Datenträger	'000'...'999'
02	1	BCC	00 _{hex} ...FF _{hex}

Befehlskennung 'R': Datenträger lesen, universal

Lesen von formatierten Tagdaten eines Datenträgers, der sich im Erfassungsbereich der angegebenen Antenne befindet. Über den Ausgabekanal kann festgelegt werden, ob Anfrage und Antwort auf demselben TCP-Port (IN-Band) oder auf verschiedenen TCP-Ports (OUT-Band) übertragen werden.

Befinden sich mehrere Datenträger im Erfassungsbereich der angegebenen Antenne, muss der gewünschte Datenträger vor dem Lesen selektiert werden (siehe *Befehlskennung 'z': Datenträger auswählen (Select)* auf Seite 105).

Byte	Länge	Befehlselement	Wertebereich
00	1	Befehlskennung universal (ASCII)	'_'
01	1	Befehlskennung (ASCII)	'R'
02	1	Antennennummer (ASCII)	'0': Alle aktiven Antennen '1'...'4': Einzelantenne
03...05	3	Reserviert	'000'
06	1	Ausgabekanal	'0': IN-Band '1': OUT-Band
07	1	Ausgabemodus	'A': Ack only 'F': Full Status 'N': No Status
08	1	BCC	00 _{hex} ...FF _{hex}

Statusmeldung (wird nur im Ausgabemodus 'A' und 'F' übertragen):

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<ACK> oder <NAK>
01	1	Statuscode	Siehe Tabelle <i>Statuscodes</i> auf Seite 94

Bei erfolgreicher Befehlsausführung folgen auf dem definierten Datenkanal die angeforderten Daten. Die Daten entsprechen der vorher festgelegten Formatierung.

Byte	Länge	Befehlselement	Wertebereich
00...	variabel	Formatierte Tagdaten des gelesenen Tags	Alle durch das Format möglichen Werte

Anschließend folgt die finale Statusmeldung, die das erfolgreiche Lesen bestätigt oder einen Fehler anzeigt (wird nur im Ausgabemodus 'F' übertragen).

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<ACK> oder <NAK>
01	1	Statuscode	Siehe Tabelle <i>Statuscodes</i> auf Seite 94

Befehlskennung 'W': Datenträger schreiben, universal

Schreiben von formatierten Tagdaten auf einen Datenträger, der sich im Erfassungsbereich der angegebenen Antenne befindet. Über den Ausgabekanal kann festgelegt werden, ob Anfrage und Antwort auf demselben TCP-Port (IN-Band) oder auf verschiedenen TCP-Ports (OUT-Band) übertragen werden.

Befinden sich mehrere Datenträger im Erfassungsbereich der angegebenen Antenne, muss der gewünschte Datenträger vor dem Lesen selektiert werden (siehe *Befehlskennung 'z': Datenträger auswählen (Select)* auf Seite 105).

Byte	Länge	Befehlselement	Wertebereich
00	1	Befehlskennung universal (ASCII)	'-'
01	1	Befehlskennung (ASCII)	'W'
02	1	Antennennummer (ASCII)	'0': Alle aktiven Antennen '1'...'4': Einzelantenne
03...05	3	Reserviert	'000'
06	1	Ausgabekanal	'0': IN-Band '1': OUT-Band
07	1	Ausgabemodus	'A': Ack only 'F': Full Status 'N': No Status
08	1	BCC	00 _{hex} ...FF _{hex}

Statusmeldung (wird nur im Ausgabemodus 'A' und 'F' übertragen):

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<ACK> oder <NAK>
01	1	Statuscode	Siehe Tabelle <i>Statuscodes</i> auf Seite 94

Nach der positiven Statusmeldung, sofern angefordert, können die formatierten Tagdaten übertragen werden. Die Daten müssen der vorher festgelegten Formatierung entsprechen.

Byte	Länge	Befehlselement	Wertebereich
00	variabel	FormatierteTagdaten, die auf den Tag geschrieben werden sollen	Alle durch das Format möglichen Werte



Die Daten müssen exakt in dem Format übergeben werden, die auch ein formatierter Lesebefehl liefern würde. Auch fester Text in der Formatspezifikation muss mit übertragen werden. Enthält die Formatspezifikation Statuswerte (die nur lesbar sind), können diese mit beliebigen Daten im entsprechenden Format belegt werden.

Anschließend folgt die finale Statusmeldung, die das erfolgreiche Schreiben bestätigt oder einen Fehler anzeigt (wird nur im Ausgabemodus 'F' übertragen).

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<ACK> oder <NAK>
01	1	Statuscode	Siehe Tabelle <i>Statuscodes</i> auf Seite 94

8.12 IO-Link

Über die IO-Link-spezifischen Befehle können Daten über die IO-Link-Schnittstelle ausgetauscht sowie digitale Eingangs-/Ausgangsports bedient werden.

Befehlskennung 'i': Azyklische Bedarfsdaten, lesen

IO-Link Device Bedarfsdaten/Parameter lesen.

Byte	Länge	Befehlselement	Wertebereich
00	1	Befehlskennung (ASCII)	'i'
01...04	4	Index MSB...LSB (ASCII hex)	„0000“...„FFFF“
05...08	4	Sub-Index MSB...LSB (ASCII hex)	„0000“...„FFFF“
09	1	BCC	00 _{hex} ...FF _{hex}

Statusmeldung:

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<ACK> oder <NAK>
01	1	Statuscode	Siehe <i>Statuscodes</i> auf Seite 94

Bei positiver Statusmeldung werden mit <STX> Daten angefordert.

Byte	Länge	Befehlselement	Wertebereich
00	1	Steuerbefehl	<STX>

Kann der Befehl nicht ordnungsgemäß ausgeführt werden, folgt eine negative Statusmeldung.

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<NAK>
01	1	Statuscode	Siehe Tabelle <i>Statuscodes</i> auf Seite 94

Bei erfolgreicher Befehlsausführung folgt eine positive Statusmeldung. Diese enthält ein Längenfeld sowie die angeforderten Daten.

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<ACK>
01...02	2	Anzahl Byte (ASCII)	„00“...„99“
03	Anzahl Byte	Daten	Byte: 00 _{hex} ...FF _{hex}
Letztes Byte	1	BCC	00 _{hex} ...FF _{hex}

Befehlskennung 'e': Azyklische Bedarfsdaten, schreiben

Senden von Bedarfsdaten/Parameterdaten über die IO-Link-Schnittstelle.

Byte	Länge	Befehlselement	Wertebereich
00	1	Befehlskennung (ASCII)	'e'
01...04	4	Index MSB...LSB (ASCII hex)	„0000“...„FFFF“
05...08	4	Sub-Index MSB...LSB (ASCII hex)	„0000“...„FFFF“
09...11	3	Anzahl Byte (ASCII)	„000“...„999“
12	1	BCC	00 _{hex} ...FF _{hex}

Statusmeldung:

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<ACK> oder <NAK>
01	1	Statuscode	Siehe <i>Statuscodes</i> auf Seite 94

Bei positiver Statusmeldung können mit <STX> Daten übertragen werden.

Byte	Länge	Befehlselement	Wertebereich
00	1	Steuerbefehl	<STX>
01	Anzahl Byte	Daten	Byte: 00 _{hex} ...FF _{hex}
Letztes Byte	1	BCC	00 _{hex} ...FF _{hex}

Statusmeldung:

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<ACK> oder <NAK>
01	1	Statuscode	Siehe <i>Statuscodes</i> auf Seite 94

Befehlskennung 'l': Digitale Ausgangsports, setzen/rücksetzen

Setzen bzw. Rücksetzen der digitalen Ausgangsports (IO-Link Pin2/Pin4).



Um die digitalen Ausgangsports nutzen zu können, müssen diese entsprechend über die IO-Link Parameter konfiguriert werden (siehe Befehlskennung 'g': IO-Link-Master-Konfiguration, schreiben auf Seite 129).

Byte	Länge	Befehlselement	Wertebereich
00	1	Befehlskennung (ASCII)	'l'
01	1	IO-Link Pin (ASCII)	'2': Pin 2 '4': Pin 4
02	1	Zustand (ASCII)	'0': Low '1': High
03	1	BCC	00 _{hex} ...FF _{hex}

Statusmeldung:

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<ACK> oder <NAK>
01	1	Statuscode	Siehe <i>Statuscodes</i> auf Seite 94

Bei positiver Statusmeldung können mit <STX> die Einstellungen übernommen werden.

Byte	Länge	Befehlselement	Wertebereich
00	1	Steuerbefehl	<STX>

Statusmeldung:

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<ACK> oder <NAK>
01	1	Statuscode	Siehe <i>Statuscodes</i> auf Seite 94

Befehlskennung **: Digitale Eingangsports, lesen

Zustand der digitalen Eingangsports lesen.



Um die digitalen Eingangsports nutzen zu können, müssen diese entsprechend über die IO-Link-Parameter konfiguriert werden (siehe Befehlskennung 'g': IO-Link-Master-Konfiguration, schreiben auf Seite 129).

Byte	Länge	Befehlselement	Wertebereich
00	1	Befehlskennung (ASCII)	'**'
01	1	IO-Link-Pin (ASCII)	'2': Pin 2 '4': Pin 4
03	1	BCC	00 _{hex} ...FF _{hex}

Statusmeldung:

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<ACK> oder <NAK>
01	1	Statuscode	Siehe Statuscodes auf Seite 94

Bei positiver Statusmeldung kann mit <STX> der Zustand des gewählten Eingangsports abgefragt werden.

Byte	Länge	Befehlselement	Wertebereich
00	1	Steuerbefehl	<STX>

Kann der Befehl nicht ordnungsgemäß ausgeführt werden, folgt eine negative Statusmeldung.

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<NAK>
01	1	Statuscode	Siehe Tabelle Statuscodes auf Seite 94

Bei erfolgreicher Befehlsausführung folgt eine positive Statusmeldung. Diese enthält den Zustand des abgefragten Eingangsports.

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<ACK>
01	1	Zustand	'0': Low '1': High
02	1	BCC	00 _{hex} ...FF _{hex}

Befehlskennung '#': IO-Link Master Konfiguration, lesen

Lesen der aktuell verwendeten IO-Link Master-Konfiguration.

Byte	Länge	Befehlselement	Wertebereich
00	1	Befehlskennung (ASCII)	'#'
01	1	BCC	00 _{hex} ...FF _{hex}

Statusmeldung:

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<ACK> oder <NAK>
01	1	Statuscode	Siehe <i>Statuscodes</i> auf Seite 94

Bei positiver Statusmeldung können mit <STX> die Parameterdaten angefordert werden.

Byte	Länge	Befehlselement	Wertebereich
00	1	Steuerbefehl	<STX>

Kann der Befehl nicht ordnungsgemäß ausgeführt werden, folgt eine negative Statusmeldung.

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<NAK>
01	1	Statuscode	Siehe Tabelle <i>Statuscodes</i> auf Seite 94

Bei erfolgreicher Befehlsausführung folgt eine positive Statusmeldung. Diese enthält die IO-Link-Parameterdaten in folgendem Format:

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<ACK>
01	1	Cycle Time Base (ASCII)	'0': 0,1 ms '1': 0,4 ms '2': 1,6 ms
02...03	2	Cycle Time (ASCII)	'00'...'63'
04	1	Modus IO-Link Pin4 (ASCII)	'0': Eingang NO '1': Eingang NC '2': Reserviert '3': Ausgang '4': IO-Link Daten '5': Eingang NO – SIO '6': Eingang NC – SIO
05	1	Modus IO-Link Pin2 (ASCII)	'0': Eingang NO '1': Eingang NC '2': Reserviert '3': Ausgang
06	1	Safe State (ASCII)	'0'...'2'
07	1	Validierung (ASCII)	'0': Keine Validierung '1': Kompatibel '2': Identisch
08	1	Parameter Server (ASCII)	'0': Deaktiviert '1': Löschen '2': Aktiviert
09	1	Parameter Upload (ASCII)	'0': Deaktiviert '1': Aktiviert
10	1	Parameter Download (ASCII)	'0': Deaktiviert '1': Aktiviert
11...14	4	Vendor ID (ASCII hex)	„0000“...„FFFF“
15...20	6	Device ID (ASCII hex)	„000000“...„FFFFFF“
21...22	2	Output Length (ASCII)	„00“...„32“
23...24	2	Input Length (ASCII)	„00“...„32“
25...40	16	Serial Number (ASCII)	ASCII-String
41	1	BCC	00 _{hex} ...FF _{hex}

Befehlskennung 'g': IO-Link-Master-Konfiguration, schreiben

Schreiben der IO-Link-Master-Konfiguration.

Byte	Länge	Befehlselement	Wertebereich
00	1	Befehlskennung (ASCII)	'g'
01	1	Cycle Time Base (ASCII)	'0': 0,1 ms '1': 0,4 ms '2': 1,6 ms
02...03	2	Cycle Time (ASCII)	'00'...'63'
04	1	Modus IO-Link Pin4 (ASCII)	'0': Eingang NO '1': Eingang NC '2': Reserviert '3': Ausgang '4': IO-Link Daten '5': Eingang NO – SIO '6': Eingang NC – SIO
05	1	Modus IO-Link Pin2 (ASCII)	'0': Eingang NO '1': Eingang NC '2': Reserviert '3': Ausgang
06	1	Safe State (ASCII)	'0'...'2'
07	1	Validierung (ASCII)	'0': Keine Validierung '1': Kompatibel '2': Identisch
08	1	Parameter Server (ASCII)	'0': Deaktiviert '1': Löschen '2': Aktiviert
09	1	Parameter Upload (ASCII)	'0': Deaktiviert '1': Aktiviert
10	1	Parameter Download (ASCII)	'0': Deaktiviert '1': Aktiviert
11...14	4	Vendor ID (ASCII hex)	„0000“...„FFFF“
15...20	6	Device ID (ASCII hex)	„000000“...„FFFFFF“
21...22	2	Output Length (ASCII)	„00“...„32“
23...24	2	Input Length (ASCII)	„00“...„32“
25...40	16	Serial Number (ASCII)	ASCII-String
41	1	BCC	00 _{hex} ...FF _{hex}

Statusmeldung:

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<ACK> oder <NAK>
01	1	Statuscode	Siehe <i>Statuscodes</i> auf Seite 94

Bei positiver Statusmeldung können mit <STX> die Parameterdaten übernommen werden.

Byte	Länge	Befehlselement	Wertebereich
00	1	Steuerbefehl	<STX>

Statusmeldung:

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<ACK> oder <NAK>
01	1	Statuscode	Siehe Tabelle <i>Statuscodes</i> auf Seite 94

Befehlskennung 'Y': Zyklische Prozessdaten, lesen

Lesen von Prozessdaten über die IO-Link-Schnittstelle.



Um Daten über die IO-Link-Schnittstelle empfangen zu können, muss der IO-Link-Port (Pin 4) als Datenport (C/Q) konfiguriert sein (siehe Befehlskennung 'g': IO-Link-Master-Konfiguration, schreiben auf Seite 129).

Byte	Länge	Befehlselement	Wertebereich
00	1	Befehlskennung (ASCII)	'Y'
01...03	3	Startadresse (ASCII)	„000“...„999“
04...06	3	Anzahl Byte (ASCII)	„000“...„999“
07	1	BCC	00 _{hex} ...FF _{hex}

Statusmeldung:

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<ACK> oder <NAK>
01	1	Statuscode	Siehe <i>Statuscodes</i> auf Seite 94

Bei positiver Statusmeldung werden mit <STX> Daten angefordert.

Byte	Länge	Befehlselement	Wertebereich
00	1	Steuerbefehl	<STX>

Kann der Befehl nicht ordnungsgemäß ausgeführt werden, folgt eine negative Statusmeldung.

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<NAK>
01	1	Statuscode	Siehe Tabelle <i>Statuscodes</i> auf Seite 94

Bei erfolgreicher Befehlsausführung folgt eine positive Statusmeldung. Diese enthält ein Längenfeld sowie die angeforderten Daten.

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<ACK>
01...03	3	Anzahl Byte (ASCII)	„000“...„999“
04	Anzahl Byte	Daten	Byte: 00 _{hex} ...FF _{hex}
Letztes Byte	1	BCC	00 _{hex} ...FF _{hex}

Befehlskennung 'X': Zyklische Prozessdaten, schreiben

Senden von Prozessdaten über die IO-Link-Schnittstelle.



Um Daten über die IO-Link-Schnittstelle senden zu können, muss der IO-Link Port (Pin 4) als Datenport (C/Q) konfiguriert sein (siehe *Befehlskennung 'g': IO-Link-Master-Konfiguration, schreiben* auf Seite 129).

Byte	Länge	Befehlselement	Wertebereich
00	1	Befehlskennung (ASCII)	'X'
01...03	3	Startadresse (ASCII)	„000“...„999“
04...06	3	Anzahl Byte (ASCII)	„000“...„999“
07	1	BCC	00 _{hex} ...FF _{hex}

Statusmeldung:

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<ACK> oder <NAK>
01	1	Statuscode	Siehe <i>Statuscodes</i> auf Seite 94

Bei positiver Statusmeldung können mit <STX> Daten übertragen werden.

Byte	Länge	Befehlselement	Wertebereich
00	1	Steuerbefehl	<STX>
01	Anzahl Byte	Daten	Byte: 00 _{hex} ...FF _{hex}
Letztes Byte	1	BCC	00 _{hex} ...FF _{hex}

Statusmeldung:

Byte	Länge	Befehlselement	Wertebereich
00	1	Status	<ACK> oder <NAK>
01	1	Statuscode	Siehe <i>Statuscodes</i> auf Seite 94

In diesem Kapitel wird der Standard OPC UA (Open Platform Communications Unified Architecture) für das UHF-RFID-Gerät von Balluff beschrieben. OPC UA ist der zentrale Standard in der Umsetzung der Zukunftsstrategie Industrie 4.0 bzw. IIoT (Industrial Internet of Things) und wird zur Vernetzung vorhandener Industrieanlagen genutzt.

9.1 Grundlagen OPC UA

9.1.1 Beschreibung OPC UA

OPC UA beschreibt eine Sammlung von Spezifikationen für die Industrieautomation. Im Vordergrund dieses Standards steht die Kommunikation zwischen industriellen Geräten (M2M). Mit diesem Standard ist es herstellerübergreifend deutlich einfacher, Parameter, Sensordaten, Regelgrößen und Steueranweisungen zu übertragen oder auszutauschen. OPC UA ist eine internetfreundliche, serviceorientierte Architektur (SOA).

Die OPC Foundation und AIM Germany haben den OPC UA Standard *OPC Unified Architecture for AutoID Companion Specification* definiert, in dem die OPC-UA-Schnittstelle für Identifikationsgeräte beschrieben wird.

Die Identifikationsgeräte werden wie folgt unterteilt:

- Texterkennungsgeräte (OCR)
- Optische Lesegeräte (z. B. QR-Code, Barcode)
- RFID-Lesegeräte
- Lokalisierungssysteme (RTLS)

Alle BIS U-Geräte, die OPC UA unterstützen, gehören zur Gattung der RFID-Lesegeräte in der OPC UA Companion Specification (siehe OPC UA AutoID Companion Specification 1.0).

9.1.2 Systemschaubild

Die Spezifikation beschreibt ein Client-Server-Prinzip. Unter einem OPC-UA-Server versteht man ein Gerät, welches Daten und Informationen anbietet und veröffentlicht. Ein Client greift auf diese Daten und Informationen mittels sogenannter Methoden zu. Auf die BIS U-6127-Auswerteeinheit können sich bis zu 50 Clients anmelden und Daten abgreifen (siehe Bild 9-1).

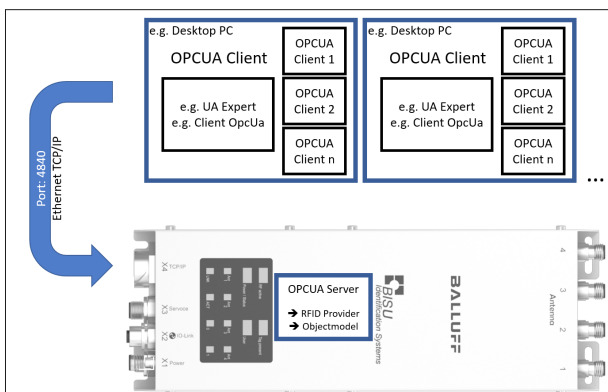


Bild 9-1: Systemschaubild

9.1.3 Sicherheitsmechanismen

Bei der Entstehung des OPC-UA-Standards war die Sicherheitsfrage immer von zentraler Bedeutung. Ältere Industrieanlagen arbeiten meist autark und ohne Anschluss an das Internet. Hier spricht man auch von sogenannten Inselanlagen. Durch die natürliche Isolierung von der Außenwelt (dem Internet) spielte das Thema IT-Sicherheit eine untergeordnete Rolle. Netzwerkangriffe von außerhalb waren praktisch kaum möglich.

Durch die stetig steigende Vernetzung von Anlagen und den Anschluss ans Internet ist es zwingend erforderlich, dass Anlagen gegen Netzwerkangriffe geschützt werden.

OPC UA hat mehrere Sicherheitsmechanismen vorgesehen, um die zu übertragende Daten zu schützen und Prozesse ohne Störung stattfinden lassen zu können:

- *Confidentiality*: Hier werden die Daten auf Transportebene verschlüsselt um diese vor *Mithörern* zu schützen.
- *Integrity*: Dieser Mechanismus stellt sicher, dass die Daten auf dem Weg zum Empfänger nicht verändert werden.
- *Application Authentication*: Hier müssen sich die kommunizierenden Applikationen erst *kennenlernen*. Dies geschieht durch den Austausch von Zertifikaten. Erst wenn Zertifikate ausgetauscht und akzeptiert wurden, werden über die Kommunikationsverbindung Daten übermittelt.
- *User Authorisation*: Um auf das BIS U-6127 vollen Zugriff zu erhalten, muss man sich mit einem Benutzer und einem Passwort anmelden. Durch diesen zusätzlichen Sicherheitsmechanismus wird sichergestellt, dass nur befugte Benutzer auf das Gerät zugreifen können.



Um zu vermeiden, dass ungültige Zertifikate entstehen, beim Erzeugen eines Zertifikats Datum, Uhrzeit sowie Zeitzone korrekt einstellen.

Zertifikate haben eine begrenzte Gültigkeit (die Gültigkeit kann z. B. auf einem Windows-PC angezeigt werden) und müssen nach Ablauf der Gültigkeit ersetzt werden (siehe Abschnitt *OPC/UA* auf Seite 41).

9.2 Sicherheitsmechanismen OPC UA bei BIS U-6127

Beim BIS U-6127 werden die OPC-UA-Sicherheitsgrundeinstellungen im Webserver ausgewählt. Unter *SICHERHEITSEINSTELLUNGEN* (siehe *Sicherheitseinstellungen* auf Seite 40) ist es dem eingeloggten Benutzer möglich, die Sicherheitseinstellungen zu verändern.

OPC/UA Einstellungen

☒ **Unsichere Clientverbindungen zurückweisen** **a**
☒ **Nur vertrauenswürdige Clientzertifikate akzeptieren** **b**
☐ **Secure Element benutzen** **c**

Zertifikatliste

Status	Name	Organisation	Gültig ab	Gültig bis	
Vertrauenswürdig	wibu2048.der	Balluff GmbH	Nov 30 12:15:09 2018 GMT	Nov 30 12:15:09 2023 GMT	🔒 🗑️ d
Zurückgewiesen	UaExpert.der	Balluff GmbH	Oct 16 09:11:06 2018 GMT	Oct 15 09:11:06 2023 GMT	🔒 🗑️ e

Zertifikat erzeugen/download

f
 g

Bild 9-2: Webserver Sicherheitseinstellungen

Im Webserver Reiter OPC UA (siehe Abbildung Bild 9-2) gibt es folgende Sicherheitseinstellungen:

- *UNSICHERE CLIENTVERBINDUNGEN ZURÜCKWEISEN*: Ist dieses Feld aktiviert, werden unsichere OPC-UA-Verbindungen abgelehnt. Somit ist der sichere Zustand aktiviert.
- *NUR VERTRAUENSWÜRDIGE CLIENTZERTIFIKATE AKZEPTIEREN*: Dieses Feld kann vom Benutzer nicht separat bedient werden. Es wird immer synchron zum Feld *UNSICHERE CLIENTVERBINDUNGEN ZURÜCKWEISEN* aktiviert.
- *SECURE ELEMENT BENUTZEN* (verwendet den integrierten Sicherheitsbaustein): Im Gerät BIS U-6127 wird ein dedizierter Sicherheitsbaustein verwendet. Hierauf werden der öffentliche und der private Sicherheitsschlüssel zur Generierung und Authentifizierung von Zertifikaten abgelegt.

Die Felder *UNSICHERE CLIENTVERBINDUNGEN ZURÜCKWEISEN* und *NUR VERTRAUENSWÜRDIGE CLIENTZERTIFIKATE AKZEPTIEREN* sind miteinander gekoppelt und erlauben für OPC UA insgesamt zwei Grundzustände.

1. *Unsicher* (Default): Alle OPC-UA-Verbindungen sind erlaubt.
2. *Sicher*: Im OPC-UA-Client sind nur folgende Sicherheitseinstellungen erlaubt:
 - Security Policy: *BASIC256SHA256*
 - Message Security Mode: *SIGN & ENCRYPT*

Siehe hierzu auch Bild 9-5 auf Seite 135.

Wird eine der drei Sicherheitseinstellungen geändert, muss das Gerät neu gestartet werden, damit die Änderungen wirksam werden.

Nachfolgende Tabelle zeigt eine Übersicht, über die möglichen Sicherheitseinstellungen für OPC UA in der Auswerteeinheit BIS U-6127:

OPC-UA-Einstellung im BIS U-6127		
Unsichere Clientverbindungen zurückweisen	Aus	An
Nur vertrauenswürdige Clientzertifikate akzeptieren	Aus	An
BIS U-6127-Zustand		
	unsicher	sicher
Security Policy des Clients		
None	erlaubt	keine Verbindung möglich
Basic256Sha256	erlaubt	erlaubt
Andere, z. B. AES	nicht erlaubt	keine Verbindung möglich
Message Security Mode des Clients		
None	erlaubt	keine Verbindung möglich
Sign	erlaubt	keine Verbindung möglich
Sign&Encrypt	erlaubt	erlaubt
Zertifikat des Clients		
Neues oder unbekanntes Zertifikat (Nicht in der Zertifikatliste)	erlaubt	keine Verbindung möglich
Zertifikat in der Zertifikatliste im Zustand <i>ZURÜCKGEWIESEN</i>	erlaubt	keine Verbindung möglich
Zertifikat in der Zertifikatliste im Zustand <i>VERTRAUENSWÜRDIG</i>	erlaubt	erlaubt

Möchte man sich mit dem BIS U-6127-Zertifikat zu einem Client verbinden, erscheint die Fehlermeldung *CONNECT ERROR* (siehe Bild 9-3).

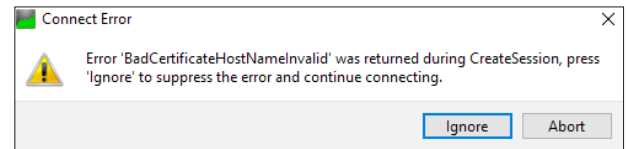


Bild 9-3: Fehlermeldung

Diese Fehlermeldung wird ausgegeben, wenn im Zertifikat entweder keine oder eine falsche IP-Adresse des BIS U-6127 hinterlegt ist. Bei Auslieferung ist noch nicht klar, in welchem IP-Adressraum sich das Gerät befinden wird, daher ist das IP-Adressfeld im Zertifikat leer und nicht beschrieben. Die Meldung kann mit *IGNORE* bestätigt werden.

Wird ein gültiges Zertifikat neu erzeugt (siehe *Sicherheitseinstellungen* auf Seite 40), sollte die Fehlermeldung nicht mehr erscheinen.

9.3 Verbindungsaufbau über OPC UA mit UaExpert

Es gibt mehrere OPC-UA-Clients, um sich auf den OPC-UA-Server der BIS U-6127-Auswerteeinheit zu verbinden. In dieser Betriebsanleitung wird der Verbindungsaufbau mithilfe des UaExperts von Unified Automation exemplarisch dargestellt. Der OPC-UA-Client UaExpert steht kostenlos auf der Homepage von Unified Automation (www.unified-automation.com) zum Download zur Verfügung und muss auf dem PC installiert sein.

Die Verbindung zwischen OPC-UA-Client und OPC-UA-Server (BIS U-6127) kann über eine unsichere (siehe Kapitel 9.3.1) oder sichere Variante (siehe Kapitel 9.3.2 auf Seite 136) hergestellt werden.

9.3.1 Unsicherer Verbindungsaufbau zwischen PC (OPC-UA-Client) und dem BIS U-6127-Gerät (OPC-UA-Server)

PC (OPC-UA-Client) mit dem BIS U-6127-Gerät (OPC-UA-Server) verbinden:

1. Die UaExpert-Anwendung starten.
2. Einen neuen Server hinzufügen.

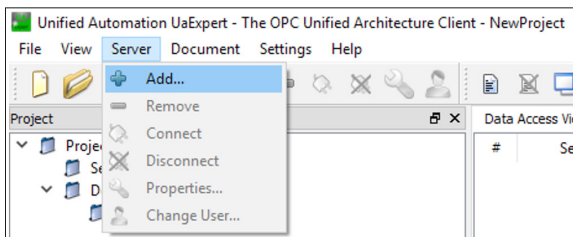


Bild 9-4: Server Dialog

3. Zum Register *ADVANCED* wechseln.
4. *CONFIGURATION NAME* vergeben (z. B. *Balluff BIS-U 6127 RFID Provider*).
5. Folgende *ENDPOINT URL* eintragen:
`opc.tcp://192.168.10.2:4840`

i Die IP-Adresse 192.168.10.2 ist im Auslieferungszustand fest eingestellt. Die IP-Adresse kann über den Webserver, das 007-Protokoll oder den UHF-Manager verändert werden.

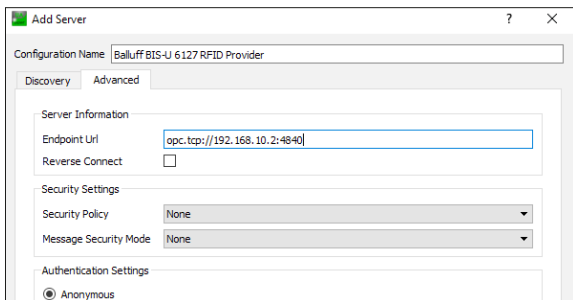


Bild 9-5: OPC-UA-Add-Server

6. Je nach Einstellung im Gerät (Webserver) müssen die Sicherheitseinstellungen *SECURITY POLICY* und *MESSAGE SECURITY MODE* verändert werden (siehe Kapitel 9.2 auf Seite 133). Für den nicht sicheren Verbindungsaufbau in beiden Feldern *NONE* und *NONE* eintragen.

i Sind die *SECURITY POLICY* auf *NONE* und der *MESSAGE SECURITY MODE* auf *NONE* gestellt (siehe Bild 9-5), kann im Auslieferungszustand zwar auf jeden Fall eine Verbindung zwischen Server und Client hergestellt werden, die Verbindung ist aber unsicher (keine Endpunktidentität und keine Verschlüsselung). Wenn ausschließlich sichere Verbindungen verwendet werden sollen, müssen auf Geräteseite unsichere Verbindungen ausgeschlossen werden.

7. Mit Rechtsklick auf den Server und Wählen von *CONNECT* die Verbindung zum Server aufbauen.

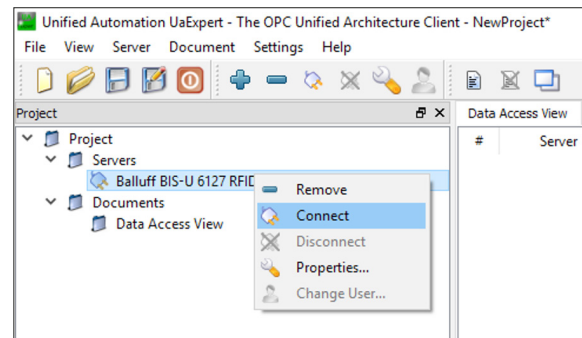


Bild 9-6: Verbindungsaufbau

⇒ Der OPC-UA-Client (PC) ist mit dem OPC-UA-Server (BIS U-6127) verbunden. Dies wird am Server-Icon ebenfalls sichtbar.

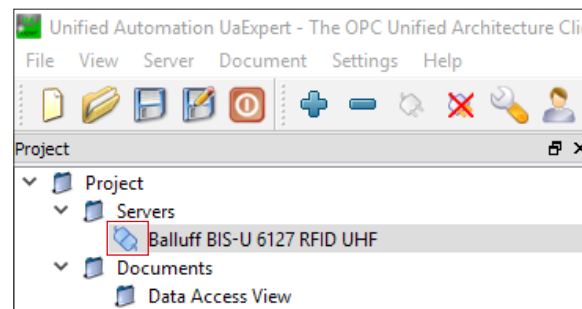


Bild 9-7: Server mit Client verbunden

Zusätzlich wird die komplette Struktur in dem Fenster *ADDRESS SPACE* angezeigt (siehe Bild 9-17).

9.3.2 Sicherer Verbindungsaufbau zwischen PC (OPC-UA-Client) und dem BIS U-6127-Gerät (OPC-UA-Server)

Um einen sicheren Verbindungsaufbau zwischen OPC-UA Client und OPC-UA-Server (BIS U-6127) zu erzwingen, müssen im Webserver des BIS U-6127 Einstellungen vorgenommen werden: Bei den OPC-UA-Einstellungen (siehe Bild 7-19 auf Seite 41) muss das Kontrollkästchen bei *UNSICHERE VERBINDUNGEN ZURÜCKWEISEN* gesetzt werden (automatisch wird zeitgleich das Kontrollkästchen *NUR VERTRAUENSWÜRDIGE CLIENTZERTIFIKATE AKZEPTIEREN* gesetzt).

Falls noch nicht geschehen, oder falls die Netzwerkeinstellungen verändert wurden, muss ein neues Server-Zertifikat erzeugt werden (Kapitel OPC/UA auf Seite 41).

Sicherer Verbindungsaufbau:

1. UaExpert-Anwendung starten.
2. Einen neuen Server hinzufügen.

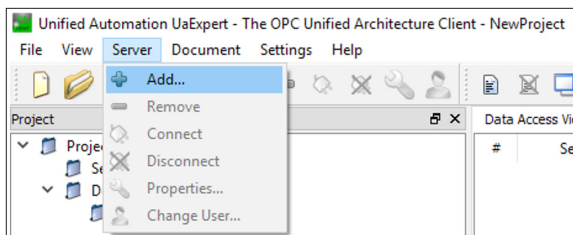


Bild 9-8: Server Dialog

3. Zum Register *ADVANCED* wechseln.
4. *CONFIGURATION NAME* vergeben (z. B. *Balluff BIS-U 6127 RFID Provider*).
5. Folgende *ENDPOINT URL* eintragen: *opc.tcp://<IP-Adresse>:4840*, z.B. *opc.tcp://192.168.3.13:4840*

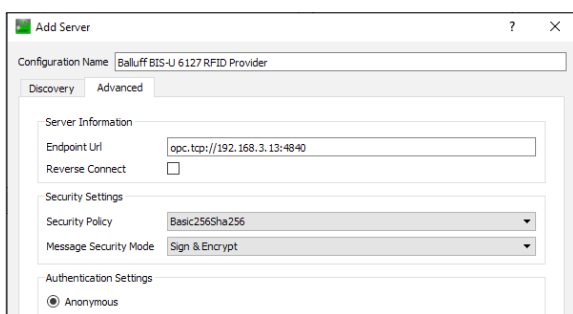


Bild 9-9: Add Server

6. Folgende Sicherheitseinstellungen wählen:
 - *SECURITY POLICY*: Basic256Sha256
 - *MESSAGE SECURITY MODE*: Sign & Encrypt
7. Mit OK bestätigen.

8. Mit Rechtsklick auf den Server und Wählen von *CONNECT* die Verbindung zum Server aufbauen.

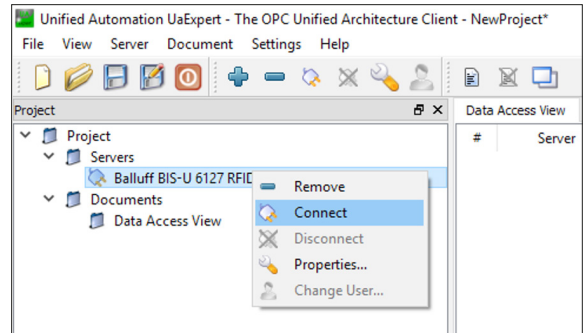


Bild 9-10: Verbindungsaufbau

⇒ Eine Vertrauensabfrage zum Zertifikat des Servers erscheint.

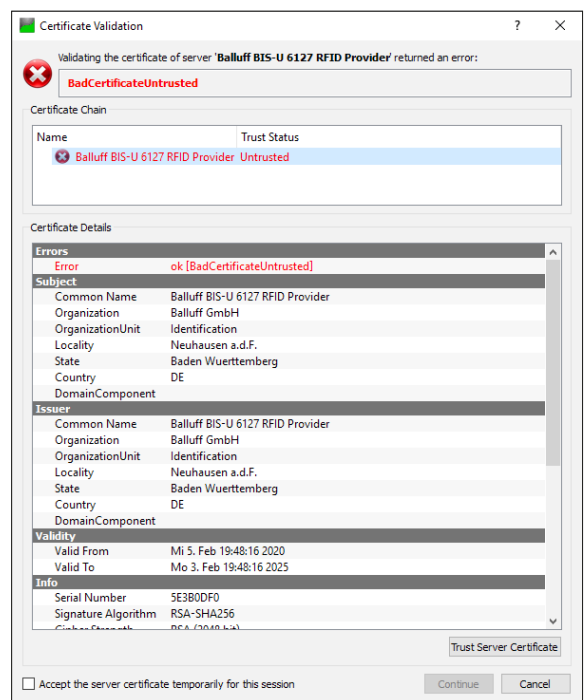


Bild 9-11: Zertifikatsprüfung

9

OPC UA (Fortsetzung)

9. Entsprechen die Daten dem BIS U-6127-Gerät, kann mit *TRUST SERVER CERTIFICATE* eine dauerhafte Vertrauensstellung hergestellt werden.



Ist das Zertifikat abgelaufen (siehe Bild 9-12 unter *VALIDITY*), muss ein neues Zertifikat erstellt und erneut eine Vertrauensstellung hergestellt werden.

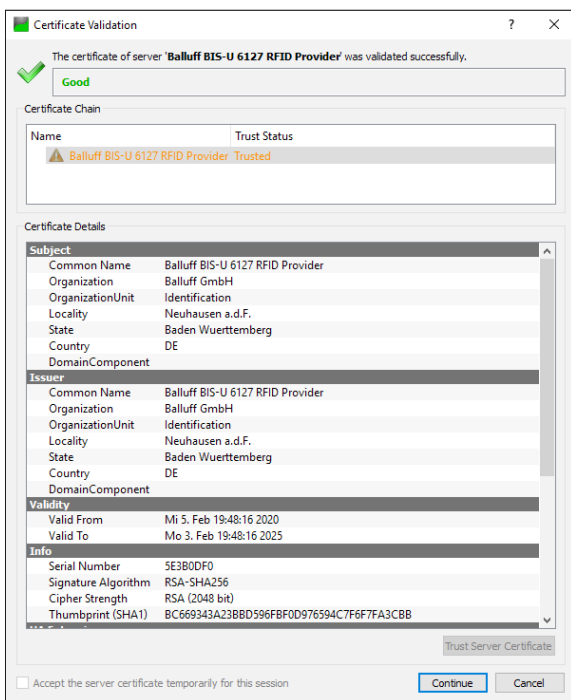


Bild 9-12: Zertifikatsprüfung akzeptiert

- ⇒ Das Zertifikat des BIS U-6127 OPC UA Servers wird von UAExpert akzeptiert.
- ⇒ Der Verbindungswunsch wird trotz akzeptiertem Server-Zertifikat zunächst auch vom BIS U-6127-Gerät abgewiesen (selbst bei erneutem Verbindungsversuch, siehe Schritt 8):

Timestamp	Source	Server	Message
06.10.2020 10:05...	Server Node	Balluff BIS-U 6127 RFID Provider	ApplicationInfo: 'umBISU.balluff.com/BalluffAutoid'
06.10.2020 10:05...	Server Node	Balluff BIS-U 6127 RFID Provider	UserTokenInfo: Anonymous
06.10.2020 10:05...	General		[stack] Opclua_TopConnection_ProcessResponse: Error Message
06.10.2020 10:05...	General		[stack] Opclua_TopConnection_ProcessResponse: Status: 0x01300000
06.10.2020 10:05...	Server Node	Balluff BIS-U 6127 RFID Provider	Error: 'BadSecurityCheckFailed' was returned during OpenSecureChannel
06.10.2020 10:05...	Server Node	Balluff BIS-U 6127 RFID Provider	Connection status of server 'Balluff BIS-U 6127 RFID Provider' changed to 'Disconnected'

Bild 9-13: Log: Verbindungsversuch abgewiesen



Das Clientzertifikat der UA Expert-Anwendung wird auf dem Server (BIS U-6127) noch nicht als sicher eingestuft und daher abgelehnt (für andere Anwendungen gilt das analog).

10. Client-Zertifikat über die Webseite des BIS U-6127 akzeptieren lassen (siehe Kapitel *OPC/UA* auf Seite 41).

⇒ Verbindung zwischen Server und ist jetzt Client möglich.

11. Mit Rechtsklick auf den Server und Wählen von *CONNECT* die Verbindung zum Server aufbauen (siehe Bild 9-10).

12. Die ggf. folgende Fehlermeldung mit *IGNORE* quittieren.

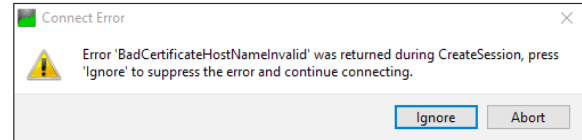


Bild 9-14: Fehlermeldung (Connect Error)

⇒ Die sichere Verbindung zwischen Server und Client ist hergestellt und wird am Server-Icon angezeigt.

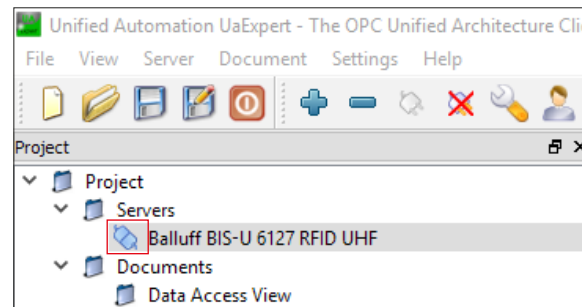


Bild 9-15: Server mit Client verbunden

9.4 Datenmodell Objekt: BIS_U_6127_Rfid_Provider

In diesem Kapitel wird das OPC-UA-Datenmodell beschrieben und dabei speziell auf das OPC-UA-Objekt *BIS_U_6127_Rfid_Provider* eingegangen.

Dieses Objekt ist abgeleitet vom OPC-UA-Objekt *RfidReaderDeviceType*, das wiederum von *AutoldDeviceType* abgeleitet ist. Das Objekt besteht aus Methoden, Variablen und Events:

- Methoden sind vom Client aufrufbare Funktionen, denen Werte übergeben werden können, die eine Aktion ausführen und die anschließend Rückgabewerte zurückliefern können.
- Variablen sind Werte, die aus einem einfachen oder komplexen Datentyp bestehen und die im Allgemeinen vom Client jederzeit gelesen und beschrieben werden können (ggf. gibt es Einschränkungen der Berechtigungen). Variablen in OPC UA sind sessionübergreifend, d. h. ihr Wert wird allen verbundenen Clients gleichermaßen angezeigt.
- Events sind Funktionen, mit denen der OPC-UA-Server (hier die BIS U-6127-Auswerteeinheit) den Clients unaufgefordert Nachrichten zukommen lassen kann, sofern der Client diese Benachrichtigungen aktiviert hat.

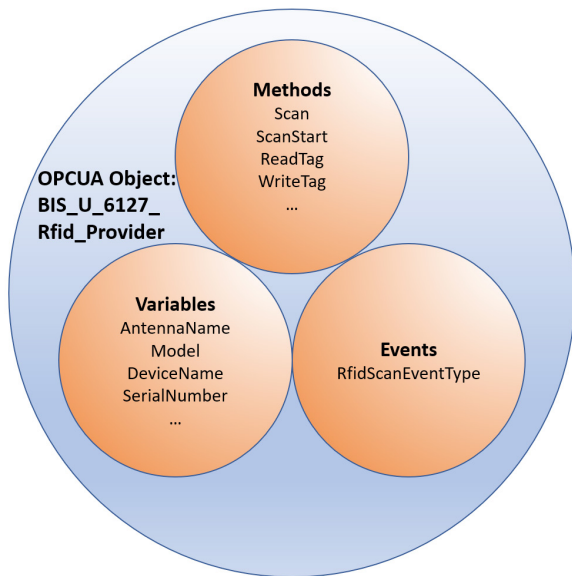


Bild 9-16: Datenmodell Objekt BIS_U_6127_Rfid_Provider

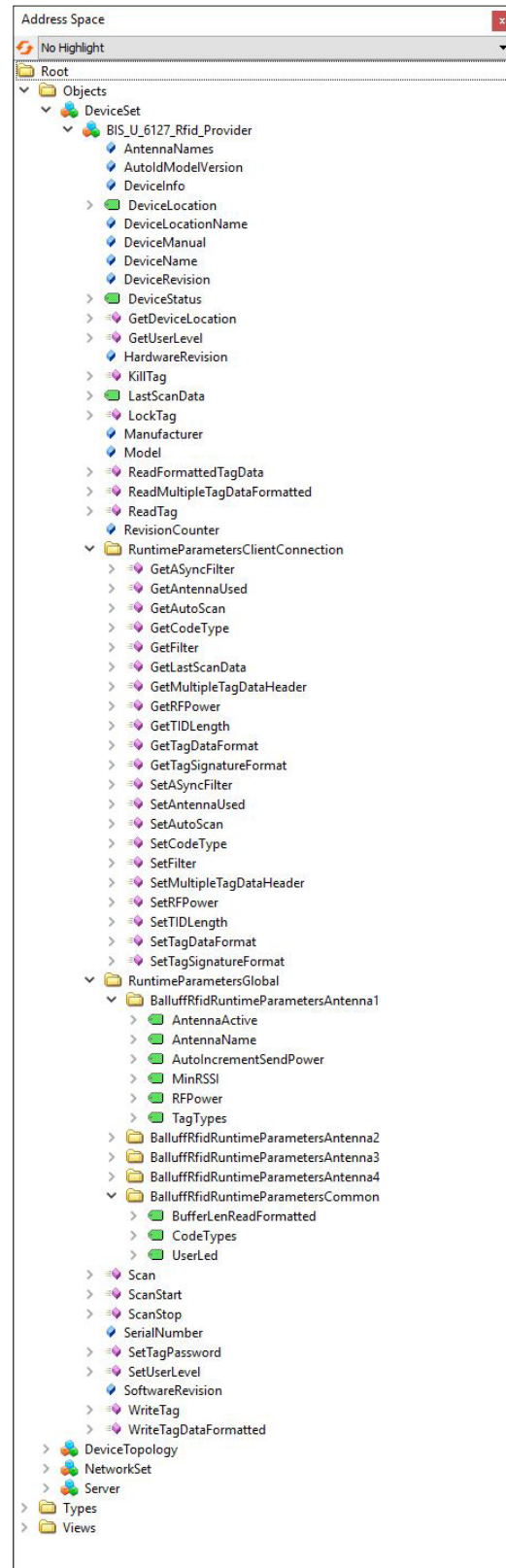


Bild 9-17: Objektstruktur

9.5 Methoden

Das Objekt *BIS_U_6127_Rfid_Provider* enthält mehrere Methoden. Sie können sowohl Aufrufargumente (Input Arguments) als auch Rückgabewerte (Output Arguments) besitzen. In Bild 9-17 auf Seite 138 werden alle Methoden mit einem violetten Symbol gekennzeichnet. Die Methoden, die unter *RUNTIMEPARAMETERSCLIENTCONNECTION* gelistet sind, sind Balluff Erweiterungen. Sie benutzen OPC-UA-Zugriffsfunktionen, um Eigenschaften für die aktuelle Session zu setzen und auszulesen.

Methoden sind nach ihrer Funktion in die drei Unterkapitel aufgeteilt:

- Methoden Geräteeinstellung
- Methoden zum Tag schreiben/lesen
- Methoden für Scan-Einstellungen

Folgende Tabellen liefern eine Übersicht aller Methoden.

Geräteeinstellung

Methoden	Beschreibung	Seite
<i>GetDeviceLocation</i>	Liefert den Gerätestandort	140
<i>SetUserLevel</i>	Wechsel der Benutzeranmeldung	140
<i>GetUserLevel</i>	Liefert aktuellen Benutzer	140

Tag schreiben/lesen

Methoden	Beschreibung	Seite
<i>Scan</i>	Synchroner Scanbetrieb	141
<i>ReadTag</i>	Daten von einem Datenträger lesen	142
<i>WriteTag</i>	Daten auf einen Datenträger schreiben	143
<i>ReadFormatted-TagData</i>	Formatierte Daten von Datenträger lesen	144
<i>WriteTagDataFormatted</i>	Formatierte Daten auf Datenträger schreiben	144
<i>ReadMultipleTag-DataFormatted</i>	Formatierte Daten von mehreren Datenträgern lesen	145
<i>ScanStart</i>	Asynchronen Scanbetrieb starten	146
<i>ScanStop</i>	Asynchronen Scanbetrieb stoppen	146
<i>SetAutoScan</i>	Autonomen Scanbetrieb starten/stoppen	146
<i>GetAutoScan</i>	Liefert Einstellung des autonomen Scanbetriebs	146
<i>GetLastScanData</i>	Liefert zuletzt gescannte Daten	146
<i>LockTag</i>	Sperren von Speicherbereichen eines Datenträgers	147
<i>KillTag</i>	Dauerhaftes Deaktivieren eines Datenträgers	147

Scan-Einstellungen

Methoden	Beschreibung	Seite
<i>SetAntennaUsed</i>	Ein-/Ausschalten von Antennen	148
<i>GetAntennaUsed</i>	Liefert Information über ein- /ausgeschaltete Antennen	148
<i>SetAsynchFilter</i>	Setzen von Filter für den asynchronen Scanbetrieb	148
<i>GetAsynchFilter</i>	Liefert Informationen über asynchronen Filter (Loop-Filter)	149
<i>SetCodeType</i>	Setzt Typ des EPCs	149
<i>GetCodeType</i>	Liefert Typ des EPCs	149
<i>SetFilter</i>	Setzen von Filter für synchronen Scanbetrieb	150
<i>GetFilter</i>	Liefert aktiven Filter für synchronen Scanbetrieb	151
<i>SetMultipleTag-DataHeader</i>	Setzen von Pre- und Suffixe für Tagliste	151
<i>GetMultipleTag-DataHeader</i>	Liefert eingestellte Pre- und Suffixe für Tagliste	152
<i>SetRFPower</i>	Setzen der Antennen-Sendeleistung	152
<i>GetRFPower</i>	Liefert Sendeleistung einer Antenne	152
<i>SetTagDataFormat</i>	Setzen von Formatstring für Daten	153
<i>GetTagDataFormat</i>	Liefert aktuellen Formatstring der Daten	153
<i>SetTagSignature-Format</i>	Ein- /Ausschalten der Signaturerstellung und Signaturüberprüfung	154
<i>GetTagSignature-Format</i>	Liefert Signatureinstellungen	154
<i>SetTagPassword</i>	Schreibt Kennwortinformationen auf einen Tag	155
<i>SetTIDLength</i>	Setzen von der TID Länge	155
<i>GetTIDLength</i>	Liefert eingestellte TID Länge	155

9.5.1 Methoden Geräteeinstellung

GetDeviceLocation

Diese Methode liefert den Gerätestandort zurück.

Aufrufparameter

Name	Datentyp	Beschreibung
LocationType	LocationType (siehe Kapitel 9.7.8) auf- Seite 162)	Gibt den Typ an, in dem der Geräte- standort angegeben werden soll.

Rückgabeparameter

Name	Datentyp	Beschreibung
Location	Location (siehe Kapi- tel 9.7.6 auf Seite 162)	Gibt den Geräte- standort an.

SetUserLevel

Mit dieser Methode kann die Benutzeranmeldung der Session gewechselt werden.
 Eine Anmeldung läuft nach 15 Minuten ohne Nutzung aus.
 Nach spätestens 24 Stunden muss eine neue Anmeldung erfolgen.

Aufrufparameter

Name	Datentyp	Beschreibung
Username	String	Login-Name des neuen Benutzers.
Password	String	Kennwort für den anzumeldenden Nutzer.

Rückgabeparameter

Name	Datentyp	Beschreibung
Status	AutoldOperati- onStatusEnu- meration (siehe Kapitel 9.7.2 auf Seite 161)	Liefert das Ergebnis der Operation.

GetUserLevel

Diese Methode liefert den Login-Namen des aktuellen Benutzers dieser Session.

Rückgabeparameter

Name	Datentyp	Beschreibung
Username	String	Login-Name des Benutzers dieser Session.
Status	AutoldOperati- onStatusEnu- meration (siehe Kapitel 9.7.2 auf Seite 161)	Liefert das Ergebnis der Operation.

9.5.2 Methoden zum Tag schreiben/lesen

Scan

Mit dieser Methode kann der synchrone Scanvorgang (siehe Kapitel 6.5 auf Seite 23) gestartet werden. Durch die Aufrufparameter wird festgelegt, wie lange und wie oft gescannt werden soll.

Die Bedingungen für das Beenden (*SCANSETTINGS*) stehen in Relation zueinander. Sobald eine Bedingung erfüllt ist, wird der Scan-Vorgang gestoppt.

Sowohl die Antennenauswahl (siehe *SetAntennaUsed* auf Seite 148) als auch die aktivierten statischen Filter (siehe *SetFilter* auf Seite 150) der aktuellen Session werden bei dem Scan berücksichtigt.

Aufrufargumente

Name	Datentyp	Beschreibung
Settings	ScanSettings	Einstellungen wie lange oder wie oft der Scan durchgeführt werden soll.

Rückgabewerte

Name	Datentyp	Beschreibung
Result	RfidScanResult[]	Alle erkannten Tags werden mit Informationen wie EPC, Zeitstempel, RSSI-Wert etc. ausgegeben.
Status	AutoldOperationStatusEnumeration (siehe Kapitel 9.7.2 auf Seite 161)	Liefert das Ergebnis der Operation.

Verwendete Strukturen der Aufrufargumente und Rückgabeparameter

ScanSettings (siehe Kapitel 9.7.16 auf Seite 165)

Name	Datentyp	Beschreibung
Duration	Duration	Gibt die Dauer des Scan-Vorgangs an. Der Wert 0 steht für „unendlich lange“.
Cycles	Int32	Gibt die Anzahl an Scan-Durchgängen an. Der Wert 0 steht für „unendlich viele“.

Name	Datentyp	Beschreibung
DataAvailable	Boolean	Wenn dieser Wert auf <i>TRUE</i> gesetzt wird, wird der Scanvorgang beendet, sobald Daten zur Verfügung stehen. Bei <i>FALSE</i> werden nur die Parameter <i>DURATION</i> und <i>CYCLES</i> berücksichtigt.
LocationType	LocationType (siehe Kapitel 9.7.8 auf Seite 162)	Gibt den gewünschten Typ der Standortinformation im Ergebnis an. Es wird nur der Typ <i>LOCATIONNAME</i> unterstützt.

RfidScanResult (siehe Kapitel 9.7.12 auf Seite 163)

Name	Datentyp	Beschreibung
CodeType	CodeTypeDataType (siehe Kapitel 9.7.4 auf Seite 162)	Gibt an, in welchem Format die gescannten Daten unter <i>ScanData</i> ausgegeben werden sollen.
ScanData	ScanData	Daten des erfolgreich gescannten Tags.
Timestamp	UtcTime	Zeitpunkt des Lesens des Tags in der Zeitzone <i>Universal Time Coordinate</i> .
Location	Location	Liefert den Ort zurück, an dem der Tag erkannt wurde.
Sigthings	RfidSighting[] (siehe Kapitel 9.7.13 auf Seite 164)	Informationen zu jeder Lesung des Tags an einer Antenne: 1: Nummer der Antenne 2: RSSI-Wert 3: UtcTime beim Lesen 4: Beim Lesen verwendete Sendeleistung

ReadTag

Mit dieser Methode kann ein bestimmter Speicherbereich eines Tags ausgelesen werden. Welcher Bereich und wie viele Bytes gelesen werden sollen, wird in den Aufrufparametern festgelegt.

Der zu lesende Bereich darf den ausgewählten Speicherbereich nicht überschreiten, sonst kann der Read-Befehl nicht ausgeführt werden und liefert einen Fehler. Die Größe der einzelnen Speicherbereiche ist abhängig vom jeweiligen Tag. Detailinformationen können dem Datenblatt des verwendeten Datenträgers entnommen werden.

Aufrufparameter

Name	Datentyp	Beschreibung
Identifizier	ScanData (siehe Kapitel 9.7.14 auf Seite 164)	EPC des Tags, von dem gelesen werden soll.
CodeType	CodeTypeData-Type (siehe Kapitel 9.7.4 auf Seite 162)	Gibt den Typ für den Parameter <i>Identifizier</i> an.
Region	UInt16	Zu lesender Speicherbereich des Tags. Folgende Werte sind möglich: 0: Reserved bank (Kill- und Access-Passwörter) 1: EPC bank 2: TID bank 3: USER data bank
Offset	UInt32	Gibt die Byteadresse des ersten Byte an, das gelesen werden soll.
Length	ByteString	Gibt die Länge des zu lesenden Bereichs an. Der komplette Bereich (Offset + Length – 1) muss sich innerhalb des ausgewählten Speicherbereichs befinden.
Password	BytesString	Falls der zu lesende Bereich gelockt ist, muss hier das entsprechende 4-Byte-lange Passwort eingetragen werden. Andernfalls muss der Wert „00000000“ eingegeben werden.

Ausgabeparameter

Name	Datentyp	Beschreibung
ResultData	ByteString	Die erfolgreich gelesenen Daten werden als ByteString hier ausgegeben.
Status	AutoidOperationStatusEnumeration (siehe Kapitel 9.7.2 auf Seite 161)	Liefert das Ergebnis der Operation.

WriteTag

Mit dieser Methode können bestimmte Daten auf einen speziellen Speicherbereich eines Tags geschrieben werden. Welche und wie viele Daten gelesen werden sollen, wird über die Aufrufparameter festgelegt. Die zu schreiben- den Daten dürfen nicht zu lang für den angegebenen Speicherbereich sein. Die Größe der einzelnen Speicherbe- reiche ist abhängig vom jeweiligen Tag-Typ. Detailinformati- onen können dem Datenblatt des verwendeten Datenträ- gers entnommen werden.

Aufrufparameter

Name	Datentyp	Beschreibung
Identifizier	ScanData (siehe Kapitel 9.7.14 auf Seite 164)	EPC des Tags, auf den geschrieben werden soll.
CodeType	CodeTypeData- Type (siehe Kapitel 9.7.4 auf Seite 162)	Gibt den Typ für den Parameter <i>Identifiziert</i> an.
Region	UInt16	Zu beschreibender Speicherbereich des Tags. Folgende Werte sind möglich: 0: Reserved bank (Kill- und Access- Passwörter) 1: EPC bank 2: TID bank 3: USER data bank
Offset	UInt32	Gibt die Byte- adresse des ersten Byte an, das geschrieben werden soll.
Data	ByteString	Daten, in Form eines ByteStrings, die auf den Tag geschrie- ben werden sollen. Die Daten dürfen nur so lange sein, dass sie den ausgewähl- ten Speicherbereich nicht überschreiten (Offset beachten).
Password	BytesString	Falls der zu beschreibende Bereich gelockt ist, muss hier das entsprechende 4-Byte-lange Pass- wort eingetragen werden. Andernfalls muss der Wert „00000000“ einge- geben werden.

Ausgabeparameter

Name	Datentyp	Beschreibung
Status	AutoldOperati- onStatusEnu- meration (siehe Kapitel 9.7.2 auf Seite 161)	Liefert das Ergebnis der Operation.

ReadFormattedTagData

Mit dieser Methode können ausgewählte Daten auf einem Tag gelesen und nach Wunsch formatiert ausgegeben werden. Das Ausgabeformat kann über die sessionbezogenen Methoden *SetTagDataFormat()* (siehe Seite 153) und *GETTAGDATAFORMAT()* (siehe Seite 153) eingestellt und ausgelesen werden.

Für eine Detailbeschreibung zur Anwendung und den verschiedenen Möglichkeiten siehe Kapitel 8.11 auf Seite 121, für ein Beispiel zu dieser Methode siehe Seite 167.

Aufrufparameter

Name	Datentyp	Beschreibung
Identifizier	ScanData (siehe Kapitel 9.7.14 auf Seite 164)	EPC des Tags, von dem gelesen werden soll.
CodeType	CodeTypeData-Type (siehe Kapitel 9.7.4 auf Seite 162)	Gibt den Typ für den Parameter <i>IDENTIFIER</i> an.
Password	ByteString	Falls der zu lesende Bereich gelockt ist, muss hier das entsprechende 4 Byte lange Passwort eingetragen werden. Andernfalls muss der Wert „00000000“ eingegeben werden.

Ausgabeparameter

Name	Datentyp	Beschreibung
ReadData	ByteString	Die erfolgreich gelesenen Daten werden als Byte-String hier ausgegeben.
Status	AutoldOperationStatusEnumeration (siehe Kapitel 9.7.2 auf Seite 161)	Liefert das Ergebnis der Operation.

WriteTagDataFormatted

Mit dieser Methode können ausgewählte Daten formatiert auf einem Tag geschrieben werden. Welche Daten geschrieben werden sollen, kann über die Aufrufparameter festgelegt werden. Die Daten müssen in dem Format angegeben werden, das in der aktuellen Session festgelegt ist. Dieses Format kann über die Methoden *SETTAGDATAFORMAT()* (siehe Seite 153) und *GETTAGDATAFORMAT()* (siehe Seite 153) eingestellt und ausgelesen werden.

Aufrufparameter

Name	Datentyp	Beschreibung
Identifizier	ScanData (siehe Kapitel 9.7.14 auf Seite 164)	EPC des Tags, von dem gelesen werden soll.
CodeType	CodeTypeData-Type (siehe Kapitel 9.7.4 auf Seite 162)	Gibt den Typ für den Parameter <i>IDENTIFIER</i> an.
WriteData	ByteString	Die zu schreibenden Daten in Form eines ByteStrings. Wichtig: die Daten müssen im Format der aktuellen Session übergeben werden.
Password	ByteString	Falls der zu beschreibende Bereich gelockt ist, muss hier das entsprechende 4 Byte lange Passwort eingetragen werden. Andernfalls muss der Wert „00000000“ eingegeben werden.

Rückgabeparameter

Name	Datentyp	Beschreibung
Status	AutoldOperationStatusEnumeration (siehe Kapitel 9.7.2 auf Seite 161)	Liefert das Ergebnis der Operation.

ReadMultipleTagDataFormatted

Mit dieser Methode können von mehreren Tags ausgewählt Daten gelesen und formatiert ausgegeben werden. Welche Daten gelesen und wie diese formatiert werden sollen, kann über die Methoden *SetTagDataFormat()* (siehe Seite 153) und *GetTagDataFormat()* (siehe Seite 153) eingestellt und ausgelesen werden.

Des Weiteren kann festgelegt werden, ob und welche Daten den Ausgaben vorangestellt oder angehängt werden sollen. Dies ist über die Methoden *SetMultipleTagDataHeader()* (siehe Seite 151) und *GetMultipleTagDataHeader()* (siehe Seite 152) einstell- und auslesbar.

Aufrufparameter

Name	Datentyp	Beschreibung
Maxtags	UInt32	Gibt die maximale Anzahl Tags an, von denen gelesen werden kann. Die maximale Anzahl ist beschränkt, da der Ausgabeparameter <i>ReadData</i> auf 512000 Byte limitiert ist. Somit darf das Produkt aus <i>Maxtags</i> und der Variablen <i>BufferLenReadFormatted</i> (siehe Seite 159) nicht den Wert 5120000 überschreiten.
Password	ByteString	Falls der zu lesende Bereich gelockt ist, muss hier das entsprechende 4-Byte-lange Passwort eingetragen werden. Es kann nur ein Passwort angegeben werden. Bei Tags mit abweichendem Passwort kann der Lese-Befehl nicht durchgeführt werden.

Rückgabeparameter

Name	Datentyp	Beschreibung
ReadData	ByteString	Die erfolgreich gelesenen Daten werden als Byte-String hier ausgegeben.
ReadTags	UInt32	Gibt die Anzahl der erfolgreich gelesenen Tags an.
Status	AutoIdOperationStatusEnumeration (siehe Kapitel 9.7.2 auf Seite 161)	Liefert das Ergebnis der Operation.

ScanStart

Mit dieser Methode kann der asynchrone Scanvorgang gestartet werden (siehe *Asynchroner Betrieb* auf Seite 24). Dabei werden sowohl die Scan-Settings (Aufrufparameter) als auch die eingestellten Filter (siehe Seite 150) berücksichtigt. Die Unterstützung der Scan-Settings beim Befehl *ScanStart* ist abhängig von der Version der Gerätesoftware. Die Ergebnisse des Scans werden in Form von OPC-UA-Events (*RfidScanEventTyp* auf Seite 165) geliefert und stehen für alle Sessions zur Verfügung. Dieser Betrieb kann durch die Methode *ScanStop* (siehe Seite 146) oder das Beenden der Session gestoppt werden.

Aufrufargumente

Name	Datentyp	Beschreibung
Settings	ScanSettings	Einstellungen wie lange oder wie oft der Scan durchgeführt werden soll.

Ausgabeparameter

Name	Datentyp	Beschreibung
Status	AutoldOperationStatusEnumeration (siehe Kapitel 9.7.2 auf Seite 161)	Liefert das Ergebnis der Operation.

Verwendete Strukturen der Ein- und Ausgabeparameter

ScanSettings (siehe Kapitel 9.7.16 auf Seite 165)

Name	Datentyp	Beschreibung
Duration	Duration	Gibt die Dauer des Scan-Vorgangs in ms an. Der Wert 0 steht für <i>unendlich lange</i> .
Cycles	Int32	Gibt die Anzahl an Scan-Durchgängen an. Der Wert 0 steht für <i>unendlich viele</i> .
DataAvailable	Boolean	Wenn dieser Wert auf <i>TRUE</i> gesetzt wird, wird der Scanvorgang beendet, sobald Daten zur Verfügung stehen. Bei <i>FALSE</i> werden nur die Parameter Duration and Cycles berücksichtigt.
LocationType	LocationType (siehe Kapitel 9.7.8 auf Seite 162)	Gibt den gewünschten Typ der Standortinformation im Ergebnis an.

ScanStop

Mit dieser Methode wird der asynchrone Betrieb gestoppt.

SetAutoScan

Mit dieser Methode kann der autonome Scanbetrieb für die entsprechende Session (siehe *Autonomer Betrieb* auf Seite 27) ein- und ausgeschaltet werden. In diesem Betrieb führt das Gerät zyklische Datenträgererfassungen durch, ohne dass ein Kommando abgesetzt werden muss. Min. Access Level: User
Default Werte: 0: (autonomer Betrieb aus)

Eingabe

Name	Datentyp	Beschreibung
AutoScan	UInt16	0: Ausschalten des autonomen Scanbetriebs 1...65536: Scanintervall in ms

GetAutoScan

Diese Methode liefert die Session-Einstellung des autonomen Scanbetriebs zurück. Der Wert 0 bedeutet, dass der autonome Scan nicht aktiv ist.

Rückgabeparameter

Name	Datentyp	Beschreibung
AutoScan	UInt16	0: autonomer Scanbetrieb ist aus. 1...65536: Scanintervall in ms.
Result	AutoldOperationStatusEnumeration (siehe Kapitel 9.7.2 auf Seite 161)	Liefert das Ergebnis der Operation.

GetLastScanData

Diese Methode liefert den zuletzt erfassten EPC der aktuellen Session. Dabei wird das Ausgabeformat unterstützt, das durch die Methode *SetCodeType()* (siehe Seite 149) eingestellt wurde.

Rückgabeparameter

Name	Datentyp	Beschreibung
LastScanData	ScanData (siehe Kapitel 9.7.14 auf Seite 164)	Zuletzt erfasster EPC dieser Session.
Result	AutoldOperationStatusEnumeration (siehe Kapitel 9.7.2 auf Seite 161)	Liefert das Ergebnis der Operation.

LockTag

Mit dieser Methode kann ein bestimmter Speicherbereich eines Tags für jegliche Zugriffe gesperrt werden. Je nach Auswahl ist diese Einstellung reversibel oder nicht.

Aufrufparameter

Name	Datentyp	Beschreibung
Identifizier	ScanData (siehe Kapitel 9.7.14 auf Seite 164)	EPC des Tags, der gelockt werden soll.
CodeType	CodeTypeData-Type (siehe Kapitel 9.7.4 auf Seite 162)	Gibt den Typ für den Parameter <i>IDENTIFIZIERT</i> an.
Password	ByteString	4 Byte langes Passwort für den Lock-Befehl.
Region	RfidLockRegionEnumeration (siehe Kapitel 9.7.10 auf Seite 163)	Speicherbereich, der gelockt werden soll.
Lock	RfidLockOperationEnumeration (siehe Kapitel 9.7.9 auf Seite 163)	Angabe, wie der Speicherbereich gelockt werden soll.
Offset	UInt32	Wird ignoriert.
Length	UInt32	Wird ignoriert.

Rückgabeparameter

Name	Datentyp	Beschreibung
Status	AutoidOperationStatusEnumeration (siehe Kapitel 9.7.2 auf Seite 161)	Liefert das Ergebnis der Operation.

KillTag

Mit dieser Methode wird ein bestimmter Tag dauerhaft deaktiviert und für jegliche Benutzung gesperrt. Die Deaktivierung kann nicht rückgängig gemacht werden. Zur Ausführung des Kill-Befehls muss zunächst ein Kill-Passwort festgelegt und auf den Datenträger geschrieben werden (Methode *SetTagPassword()*, siehe Seite 155).

Aufrufparameter

Name	Datentyp	Beschreibung
Identifizier	ScanData (siehe Kapitel 9.7.14 auf Seite 164)	EPC des Tags, der deaktiviert werden soll.
CodeType	CodeTypeData-Type (siehe Kapitel 9.7.4 auf Seite 162)	Gibt den Typ für den Parameter <i>IDENTIFIZIERT</i> an.
Password	ByteString	Passwort der Kill-Operation.

Rückgabeparameter

Name	Datentyp	Beschreibung
Status	AutoidOperationStatusEnumeration (siehe Kapitel 9.7.2 auf Seite 161)	Liefert das Ergebnis der Operation.

9.5.3 Methoden für Scan-Einstellungen

SetAntennaUsed

Mit dieser Methode können ein oder mehrere Antennen ausgewählt werden, die in dieser Session aktiv sein sollen.

Min. Access Level: User

Default Werte: Parameter 0012_{hex} (siehe Kapitel 7.3 auf Seite 49)

Eingangsparameter

Name	Datentyp	Beschreibung
AntennaUsed	BalluffAntennaUsed	Auswahl der Antennen, die in dieser Session verwendet werden sollen.

Ausgangsparameter

Name	Datentyp	Beschreibung
Status	AutoldOperationStatusEnumeration (siehe Kapitel 9.7.2 auf Seite 161)	Liefert das Ergebnis der Operation.

GetAntennaUsed

Die Methode liefert die Information, welche Antennen in der aktuellen Session aktiv sind.

Ausgangsparameter

Name	Datentyp	Beschreibung
AntennaUsed	BalluffAntennaUsed	Gibt an, welche Antennen in dieser Session aktiv sind.
Result	AutoldOperationStatusEnumeration (siehe Kapitel 9.7.2 auf Seite 161)	Liefert das Ergebnis der Operation.

SetAsynchFilter

Mit dieser Methode kann das Loop-Filter für die entsprechende Session eingestellt werden. Durch das Filter können Fehlesungen korrigiert und mehrere Scanvorgänge in einer Liste zusammengefasst werden (siehe *Loop Filter* auf Seite 25).

Min. Access Level: Expert

Default Werte: Parameter 0023_{hex}, 0024_{hex} und 0029_{hex} (siehe Kapitel 7.3 auf Seite 49)

Aufrufparameter

Name	Datentyp	Beschreibung
NumberOfReadsToDetectTag	UInt16	Gibt an, wie oft ein Tag erfolgreich gelesen werden muss, bevor er tatsächlich als erfasst gemeldet wird.
NumberOfReadsToRemoveTag	UInt16	Gibt an, wie oft ein Tag nicht mehr erkannt werden muss, bevor er tatsächlich als nicht mehr vorhanden gemeldet wird.
TimeBetweenRemoveAndDetect	UInt16	Die Zeit zwischen <i>Tag nicht mehr erkannt</i> und <i>Tag wieder erfasst</i> . Das bedeutet, diese Zeit muss mindestens verstreichen, bevor ein Tag erneut als erkannt gemeldet werden darf.
UseAsDefault	Boolean	Wenn dieser Wert auf <i>TRUE</i> gesetzt wird, werden die eingestellten Filter als Default-Werte übernommen.

Rückgabeparameter

Name	Datentyp	Beschreibung
Result	AutoldOperationStatusEnumeration (siehe Kapitel 9.7.2 auf Seite 161)	Liefert das Ergebnis der Operation.

GetAsynchFilter

Diese Methode liefert die aktiven Einstellungen des Loop-Filters (siehe *Loop Filter* auf Seite 25).

Rückgabeparameter

Name	Datentyp	Beschreibung
NumberOfReadsToDetectTag	UInt16	Gibt an, wie oft ein Tag erfolgreich gelesen werden muss, bevor er tatsächlich als erfasst gemeldet wird.
NumberOfReadsToRemoveTag	UInt16	Gibt an, wie oft ein Tag nicht mehr erkannt werden muss, bevor er tatsächlich als nicht mehr vorhanden gemeldet wird.
TimeBetween-RemoveAnd-Detect	UInt16	Die Zeit zwischen <i>Tag nicht mehr erkannt</i> und <i>Tag wieder erfasst</i> . Das bedeutet, diese Zeit muss mindestens verstreichen, bevor ein Tag erneut als erkannt gemeldet werden darf.
Result	AutoldOperationStatusEnumeration (siehe Kapitel 9.7.2 auf Seite 161)	Liefert das Ergebnis der Operation.

SetCodeType

Mit dieser Methode kann das Ausgabeformat des EPCs festgelegt werden. Diese Einstellung ist sessionbezogen und wird von folgenden Methoden berücksichtigt:

- *GetLastScanData()* (siehe Seite 146)
- *Scan()* (siehe Seite 141)
- *Events* (siehe Seite 165)

Min. Access Level: User

Default Werte: 0

Aufrufparameter

Name	Datentyp	Beschreibung
CodeType	UInt32	Legt den Typ des Autold Identifiers fest. Mögliche Werte sind: 0,1,2 oder 3. 0: „RAW:BYTES“ 1: „RAW:STRING“ 2: „EPC“ (siehe Kapitel 9.7.15 auf Seite 164) 3: „UID“

Rückgabeparameter

Name	Datentyp	Beschreibung
Result	AutoldOperationStatusEnumeration (siehe Kapitel 9.7.2 auf Seite 161)	Liefert das Ergebnis der Operation.

GetCodeType

Diese Methode liefert das aktuelle Ausgabeformat des EPCs. Diese Einstellung ist sessionbezogen und wird von folgenden Methoden berücksichtigt:

- *GetLastScanData()* (siehe Seite 146)
- *Scan()* (siehe Seite 141)
- *Events* (siehe Seite 165)

Rückgabeparameter

Name	Datentyp	Beschreibung
CodeType	UInt32	Liefert den Typ des EPCs zurück.
Result	AutoldOperationStatusEnumeration (siehe Kapitel 9.7.2 auf Seite 161)	Liefert das Ergebnis der Operation.

SetFilter

Mit dieser Methode kann ein Filter für bestimmte Teile des EPCs und des TIDs festgelegt werden. Des Weiteren können die minimal und maximal zu erreichenden Werte des RSSIs und der EPC-Länge eingestellt werden. Bei dem synchronen Scanbetrieb werden nach der Aktivierung des Filters nur noch die Datenträger angezeigt, deren Daten den Einstellungen des Filters entsprechen. Ein Beispiel zur Anwendung findet man auf Seite 226.

Min. Access Level: Expert

Defaultwert: Der Defaultwert wird über die Geräteparametrierung (siehe Kapitel 7.3 auf Seite 49) eingestellt.

Aufrufparameter

Name	Datentyp	Beschreibung
FilterIndex	UInt16	Index des neu erstellten Filters.
FilterOperation	BalluffFilterOperationEnumeration (siehe Kapitel 9.7.3 auf Seite 162)	Operation, mit der der Filter auf die Daten angewendet werden soll. Zur Zeit wird nur <i>AND</i> unterstützt.
EpcDataFilter	BalluffFilterDataBlock	EPC-Filtereinstellung: ab welcher Adresse, auf wie viele Bits und mit welchen Daten der Filter angewendet werden soll. Diese Filterangaben beziehen sich nur auf die EPCs der Tags.
TidDataFilter	BalluffFilterDataBlock	TID-Filtereinstellung: ab welcher Adresse, auf wie viele Bits und mit welchen Daten der Filter angewendet werden soll. Diese Filterangaben beziehen sich nur auf die TIDs der Tags.
MinRSSI	Int16	Minimaler RSSI-Wert mit dem ein Tag erkannt werden muss. Wertebereich: -128...+127 Default-Wert: -128 (keine Filterung)

Name	Datentyp	Beschreibung
MaxRSSI	Int16	Maximaler RSSI-Wert mit dem ein Tag erkannt werden darf. Wertebereich: -128...+127 Standard: +127 (keine Filterung)
MinEpcLength	UInt16	Minimale EPC-Länge eines Tags in Byte. Wertebereich 0...62 Standard: 0 (keine Filterung)
MaxEpcLength	UInt16	Maximale EPC-Länge eines Tags in Byte. Wertebereich 0...62 Standard: 62 (keine Filterung)
UseAsDefault	Boolean	Wenn dieser Wert auf <i>TRUE</i> gesetzt wird, werden die eingestellten Filter als Default-Werte übernommen. Dazu ist eine vorherige Anmeldung mit Adminrechten notwendig.

Rückgabeparameter

Name	Datentyp	Beschreibung
Result	AutoldOperationStatusEnumeration (siehe Kapitel 9.7.2 auf Seite 161)	Liefert das Ergebnis der Operation.

GetFilter

Diese Methode liefert die Einstellungen für den aktiven Filter zurück. Die Methode ist sessionbezogen.

Aufrufparameter

Name	Datentyp	Beschreibung
Index	UInt16	Index des Filters, dessen Werte ausgegeben werden sollen.

Rückgabeparameter

Name	Datentyp	Beschreibung
EpcDataFilter	BalluffFilterDataBlock	Liefert die Startadresse, die Länge und die Daten des Filters, welcher auf die EPCs angewendet wird.
TidDataFilter	BalluffFilterDataBlock	Liefert die Startadresse, die Länge und die Daten des Filters, welcher auf die TIDs angewendet wird.
MinRSSI	Int16	Minimaler RSSI-Wert mit dem ein Tag erkannt werden muss.
MaxRSSI	Int16	Maximaler RSSI-Wert mit dem ein Tag erkannt werden darf.
MinEpcLength	UInt16	Minimale EPC-Länge eines Tags in Byte.
MaxEpcLength	UInt16	Maximale EPC-Länge eines Tags in Byte.
Result	AutoldOperationStatusEnumeration (siehe Kapitel 9.7.2 auf Seite 161)	Liefert das Ergebnis der Operation.

SetMultipleTagDataHeader

Mit dieser Methode können die Strings, die der Tagliste von *ReadMultipleTagDataFormatted()* (siehe Seite 145) vorangestellt bzw. angehängt werden können, bearbeitet und festgelegt werden (siehe *Präfix für ReadMultipleTagDataFormatted (default)* in Kapitel 7.3 auf Seite 80).

Min. Access Level: Admin

Default Werte: Prefix: Parameter 0026_{hex} (siehe *Präfix für ReadMultipleTagDataFormatted (default)* in Kapitel 7.3 auf Seite 80)

Suffix: Parameter 0027_{hex} (siehe *Suffix für ReadMultipleTagDataFormatted (default)* in Kapitel 7.3 auf Seite 80)

Aufrufparameter

Name	Datentyp	Beschreibung
Prefix	String	String, welcher der Tagliste vorangestellt wird.
Suffix	String	String, welcher der Tagliste angehängt wird.
UseAsDefault	Boolean	Wenn dieser Wert auf <i>TRUE</i> gesetzt wird, werden die eingestellten Strings als Default-Werte übernommen.

Rückgabeparameter

Name	Datentyp	Beschreibung
Result	AutoldOperationStatusEnumeration (siehe Kapitel 9.7.2 auf Seite 161)	Liefert das Ergebnis der Operation.

GetMultipleTagDataHeader

Diese Methode liefert die Strings, die der Tagliste vorangestellt bzw. angehängt werden. Diese Tagliste wird beim Aufruf der Methode *ReadMultipleTagDataFormatted()* (siehe Seite 145) zurückgegeben.

Rückgabeparameter

Name	Datentyp	Beschreibung
Prefix	String	String, welcher der Tagliste vorangestellt wird.
Suffix	String	String, welcher der Tagliste angehängt wird.
Result	AutoldOperationStatusEnumeration (siehe Kapitel 9.7.2 auf Seite 161)	Liefert das Ergebnis der Operation.

SetRFPower

Mit dieser Methode kann die Sendeleistung einer bestimmten Antenne für die aktuelle Session eingestellt werden. Die Einheit der Sendeleistung ist 1/100 dBm. Die eingestellte Leistung beeinflusst die maximale Reichweite des Erfassungsbereichs der Antenne. Die maximal zulässige Sendeleistung ist abhängig von der verwendeten Antenne und den im jeweiligen Land gültigen Funkvorschriften. Detailinformationen können Kapitel 5 auf Seite 18 und dem Datenblatt der verwendeten Antenne entnommen werden.

Min. Access Level: User

Default Werte: Parameter 0008_{hex} (siehe *Sendeleistung beim Lesen (default)* in Kapitel 7.3 auf Seite 58)

Eingangsparameter

Name	Datentyp	Beschreibung
Antenna	BalluffAntenna-Enumeration	Auswahl der Antenne, deren Sendeleistung eingestellt werden soll.
Power	UInt16	Sendeleistung, die eingestellt werden soll in 1/100 dBm.

Ausgangsparameter

Name	Datentyp	Beschreibung
Result	AutoldOperationStatusEnumeration (siehe Kapitel 9.7.2 auf Seite 161)	Liefert das Ergebnis der Operation.

GetRFPower

Die Methode liefert die für diese Session eingestellte Sendeleistung der ausgewählten Antenne in 1/100 dBm zurück.

Eingangsparameter

Name	Datentyp	Beschreibung
Antenna	BalluffAntenna-Enumeration	Auswahl der Antenne, deren Sendeleistung ausgegeben werden soll.

Ausgangsparameter

Name	Datentyp	Beschreibung
Power	UInt16	Sendeleistung für die ausgewählte Antenne in 1/100 dBm.
Result	AutoldOperationStatusEnumeration (siehe Kapitel 9.7.2 auf Seite 161)	Liefert das Ergebnis der Operation.

SetTagDataFormat

Mit dieser Methode kann der Formatstring, mit dem die Daten einzelner Tags bei den Methoden *ReadMultipleTagDataFormatted()* (siehe Seite 145) und *ReadFormattedTagData()* (siehe Seite 144) formatiert werden, festgelegt werden.

Bei der Methode *WriteTagDataFormatted()* (siehe Seite 144) müssen die zu schreibenden Daten dem eingestellten Format entsprechen.

Eine Detailbeschreibung zur Anwendung und den verschiedenen Möglichkeiten ist in Kapitel 8.11 auf Seite 121 zu finden.

Min. Access Level: Admin

Default Werte: Parameter 0025_{hex} (siehe *Formatdefinition für ReadTagDataFormatted, ReadMultipleTagDataFormatted und WriteFormattedTagData (default)* in Kapitel 7.3 auf Seite 79)

Eingangsparameter

Name	Datentyp	Beschreibung
FormatString	String	Format für die zu formatierenden Daten.
UseAsDefault	Boolean	Wenn dieser Wert auf <i>TRUE</i> gesetzt wird, wird das eingestellte Format als Default-Wert übernommen.
Result	AutoldOperationStatusEnumeration (siehe Kapitel 9.7.2 auf Seite 161)	Liefert das Ergebnis der Operation.

GetTagDataFormat

Diese Methode liefert den Formatstring, mit dem die Daten einzelner Tags bei den Methoden *ReadMultipleTagDataFormatted()* (siehe Seite 145) und *ReadFormattedTagData()* (siehe Seite 144) formatiert werden.

Rückgabeparameter

Name	Datentyp	Beschreibung
FormatString	String	Format, in dem die Daten der Tags formatiert werden.
Result	AutoldOperationStatusEnumeration (siehe Kapitel 9.7.2 auf Seite 161)	Liefert das Ergebnis der Operation.

SetTagSignatureFormat

Die Tagdaten können automatisch mit einer Signatur versehen werden. Je nach Wunsch können unterschiedliche Tagdaten in die Generierung dieser Signatur einbezogen werden. Durch die Signatur kann die Unversehrt- und Echtheit der Daten überprüft werden. Mit dieser Methode kann das Erzeugen und die Überprüfung der Signatur ein- bzw. ausgestellt werden. Ebenso können die Daten, die bei der Signaturerzeugung einbezogen werden sollen, festgelegt werden. Eine Detailbeschreibung zur Anwendung ist in Kapitel 3.7 auf Seite 12 zu finden. Ein Beispiel zu dieser Funktion wird auf Seite 168 erläutert.

Min. Access Level: Admin

Default Werte: Parameter 0028_{hex} (siehe *Berechnungsformat für die Signaturerzeugung (default)* in Kapitel 7.3 auf Seite 80)

Aufrufparameter

Name	Datentyp	Beschreibung
Type	BalluffSignatureTypeEnumeration	0: None 1: Basic256Sha256
FormatString	String	Angabe der Daten, die zur Signaturerzeugung einbezogen werden sollen.
UseAsDefault	Boolean	Wenn dieser Wert auf true gesetzt wird, werden die Signatur-Einstellungen als Default-Werte übernommen.

Rückgabeparameter

Name	Datentyp	Beschreibung
Result	AutoldOperationStatusEnumeration (siehe Kapitel 9.7.2 auf Seite 161)	Liefert das Ergebnis der Operation.

GetTagSignatureFormat

Diese Methode liefert die aktuelle Signatureinstellung zurück. Falls die Signaturgenerierung aktiv ist, werden auch die Tagdaten angegeben, die zur Erstellung der Signatur hinzugezogen werden.

Rückgabeparameter

Name	Datentyp	Beschreibung
Type	BalluffSignatureTypeEnumeration	0: None 1: Basic256Sha256
FormatString	String	Daten, die zur Signaturerstellung hinzugezogen werden.
Result	AutoldOperationStatusEnumeration (siehe Kapitel 9.7.2 auf Seite 161)	Liefert das Ergebnis der Operation.

SetTagPassword

Mit dieser Methode können das *Access*- und das *Kill*-Passwort des Datenträgers beschrieben werden. Die Passwörter haben eine Länge von jeweils 4 Byte (MSB first).

Für den Kill-Befehl (S.197) ist es notwendig, dass zuvor ein von 0 verschiedenes Kill-Passwort auf dem Tag geschrieben wurde.

Aufrufparameter

Name	Datentyp	Beschreibung
Identifizier	ScanData (siehe Kapitel 9.7.14 auf Seite 164)	EPC des Tags.
CodeType	CodeTypeData-Type (siehe Kapitel 9.7.4 auf Seite 162)	Gibt den Typ für den Parameter <i>Identifizier</i> an.
PasswordType	RfidPassword-TypeEnumeration (siehe Kapitel 9.7.11 auf Seite 163)	Gibt an, welches Passwort geändert werden soll. Die Werte <i>Read</i> und <i>Write</i> werden bei UHF-Geräten wie dem BIS U.6127 nicht unterstützt, da sie in der Spezifikation UHF EPC Gen2 V1 nicht definiert sind.
AccessPass-word	ByteString	Das aktuelle 4 Byte lange Accesspass-word des Tags.
NewPassword	ByteString	Das neue 4 Byte lange Passwort.

Rückgabeparameter

Name	Datentyp	Beschreibung
Status	AutoldOperati-onStatusEnu-meration (siehe Kapitel 9.7.2 auf Seite 161)	Liefert das Ergebnis der Operation.

SetTIDLength

Mit dieser Methode kann die zu nutzende Länge des TID-Speicherbereichs für alle Datenträger einer bestimmten Antenne eingestellt werden. Die Methode ist session-bezogen.

Min. Access Level: Expert

Default Werte: Parameter 0004_{HEX} (siehe Kapitel 7.3 auf Seite 49)

Eingangsparameter

Name	Datentyp	Beschreibung
Antenna	BalluffAntenna-Enumeration	Antenne, bei der die TID-Länge für alle Tags gelten soll.
TIDLength	Byte	Gewünschte TID-Länge in 2-Byte-Worten, die eingestellt werden soll. Maximal erlaubte Länge: 31 Worte (62 Byte)

Ausgangsparameter

Name	Datentyp	Beschreibung
Result	AutoldOperati-onStatusEnu-meration (siehe Kapitel 9.7.2 auf Seite 161)	Liefert das Ergebnis der Operation.

GetTIDLength

Diese Methode liefert die ausgewählte Länge des TID-Speicherbereichs für alle Tags einer bestimmten Antenne zurück. Die Methode ist sessionbezogen

Eingangsparameter

Name	Datentyp	Beschreibung
Antenna	BalluffAntenna-Enumeration	Antenne, für die die eingestellte TID-Länge zurückgegeben werden soll.

Ausgangsparameter

Name	Datentyp	Beschreibung
TIDLength	Byte	Länge des TID-Speicherbereichs in 2-Byte-Worten.
Result	AutoldOperati-onStatusEnu-meration (siehe Kapitel 9.7.2 auf Seite 161)	Liefert das Ergebnis der Operation.

9.6 Variablen und Konstanten

9.6.1 Geräteinformation /-einstellungen

AntennaName

Datentyp	AntennaNameIdPair (siehe Seite 161)
Default-Wert	Je nach Antenne „Antenna_1“, „Antenna_2“, „Antenna_3“ oder „Antenna_4“
Zugriffsrechte	Lesen: User Schreiben: Admin
007-Parameter	–
Parent	Balluff Erweiterung : AutoldDeviceType/RuntimeParameters
Pfad	Root/DeviceSet/BIS_U_6127_Rfid_Provider/RuntimeParametersGlobal/BalluffRfidRuntimeParametersAntenna[1..4]

Liefert die ID und den Namen der entsprechenden Antenne. Die Daten entsprechen den Werten des ebenfalls globalen Arrays *AntennaNames* (siehe *AntennaNames* auf Seite 156).

AntennaNames

Datentyp	AntennaNameIdPair[4]
Default-Wert	1, „Antenna_1“, 2, „Antenna_2“, 3, „Antenna_3“, 4, „Antenna_4“
Zugriffsrechte	Lesen: User Schreiben: Admin
007-Parameter	–
Parent	RfidReaderDeviceType
Pfad	Root/DeviceSet/BIS_U_6127_Rfid_Provider/

Ein Array mit vier Einträgen des Typs *AntennaNameIdPair* (siehe Seite 161). Ein Eintrag enthält jeweils den Namen und die ID einer Antenne. Die Werte spiegeln sich in den Variablen *AntennaName* der einzelnen Antennen wider.

Datentyp	String
Default-Wert	1.00
Zugriffsrechte	Lesen: User Schreiben: –
007-Parameter	–
Parent	AutoldDeviceType
Pfad	Root/DeviceSet/BIS_U_6127_Rfid_Provider/

Diese Variable liefert die Version der OPC UA Autold Spec. Die Version der verwendeten Spezifikation ist 1.00.

DeviceInfo

Datentyp	String
Default-Wert	„“
Zugriffsrechte	Lesen: User Schreiben: –
007-Parameter	–
Parent	AutoldDeviceType
Pfad	Root/DeviceSet/BIS_U_6127_Rfid_Provider/

Diese Variable ist aktuell ohne Bedeutung.

DeviceLocation

Datentyp	Location (siehe Seite 162)
Default-Wert	„“
Zugriffsrechte	Lesen: User Schreiben: Admin
007-Parameter	001f _{hex}
Parent	AutoldDeviceType
Pfad	Root/DeviceSet/BIS_U_6127_Rfid_Provider/

Diese Variable setzt oder liefert den Gerätestandort. Es wird nur der Typ *NAME* unterstützt. Dieser Wert entspricht der Variablen *DeviceLocationName* (siehe Seite 156) und dem Rückgabewert der Methode *GetDeviceLocation()* (siehe Seite 140).

DeviceLocationName

Datentyp	String
Default-Wert	„“
Zugriffsrechte	Lesen: User Schreiben: Admin
007-Parameter	001f _{hex}
Parent	AutoldDeviceType
Pfad	Root/DeviceSet/BIS_U_6127_Rfid_Provider/

Diese Variable setzt oder liefert den Gerätestandort. Der Wert entspricht dem Feld *NAME* in *DeviceLocation* (siehe Seite 156) und dem Rückgabewert der *METHODE GetDeviceLocation()* (siehe Seite 140).

DeviceManual

Datentyp	String
Default-Wert	www.balluff.com
Zugriffsrechte	Lesen: User Schreiben: –
007-Parameter	–
Parent	AutoldDeviceType
Pfad	Root/DeviceSet/BIS_U_6127_Rfid_Provider/

Diese Variable liefert den Link der Balluff Homepage.

DeviceStatus

Datentyp	DeviceStatusEnumeration (siehe Seite 162)
Default-Wert	0: Idle
Zugriffsrechte	Lesen: User Schreiben: –
007-Parameter	–
Parent	AutoldDeviceType
Pfad	Root/DeviceSet/BIS_U_6127_Rfid_Provider/

Der *DeviceStatus* liefert den aktuellen Zustand des Geräts. In der Regel ist dieser *Idle*. Wird durch eine OPC-UA-Session der synchrone Scanbetrieb mit *ScanStart()* aktiviert, wechselt der Status auf *Scanning*.

DeviceRevision

Datentyp	String
Default-Wert	–
Zugriffsrechte	Lesen: User Schreiben: –
007-Parameter	–
Parent	AutoldDeviceType
Pfad	Root/DeviceSet/BIS_U_6127_Rfid_Provider/

Diese Variable liefert sowohl die Hardware- als auch die Software-Version des Geräts. Die Werte entsprechen den Werten *HardwareRevision* (siehe Seite 157) und *SoftwareRevision* (siehe Seite 158).

HardwareRevision

Datentyp	String
Default-Wert	–
Zugriffsrechte	Lesen: User Schreiben: –
007-Parameter	800e _{hex}
Parent	AutoldDeviceType
Pfad	Root/DeviceSet/BIS_U_6127_Rfid_Provider/

Diese Variable gibt die Hardware-Revision in Form eines Strings an. Sie entspricht außerdem dem Hardware-Teil der Variablen *DeviceRevision* (siehe Seite 157).

Manufacturer

Datentyp	String
Default-Wert	Balluff GmbH
Zugriffsrechte	Lesen: User Schreiben: –
007-Parameter	–
Parent	AutoldDeviceType
Pfad	Root/DeviceSet/BIS_U_6127_Rfid_Provider/

Diese Variable liefert den Namen des Geräteherstellers.

Model

Datentyp	String
Default-Wert	BIS U-6127-081-104-06-ST36
Zugriffsrechte	Lesen: User Schreiben: –
007-Parameter	800f _{hex}
Parent	AutoldDeviceType
Pfad	Root/DeviceSet/BIS_U_6127_Rfid_Provider/

Diese Variable liefert den Namen des Gerätemodells.

SerialNumber

Datentyp	String
Default-Wert	–
Zugriffsrechte	Lesen: User Schreiben: –
007-Parameter	8001 _{hex}
Parent	AutoldDeviceType
Pfad	Root/DeviceSet/BIS_U_6127_Rfid_Provider/

Diese Variable gibt die Seriennummer des Geräts an.

SoftwareRevision

Datentyp	String
Default-Wert	–
Zugriffsrechte	Lesen: User Schreiben: –
007-Parameter	–
Parent	AutoldDeviceType
Pfad	Root/DeviceSet/BIS_U_6127_Rfid_ Provider/

Diese Variable gibt die Softwareversion in Form eines Strings an. Sie entspricht dem Software-Teil der Variablen *DeviceRevision* (siehe Seite 157).

RevisionCounter

Die Variable hat zur Zeit keine Bedeutung und liefert immer den Wert 0.

9.6.2 Scan-Einstellungen

AntennaActive

Datentyp	Boolean
Default-Wert	007-Parameter 0012 _{hex}
Zugriffsrechte	Lesen: User Schreiben: Admin
007-Parameter	00012 _{hex}
Parent	Balluff Erweiterung : AutoldDevice- Type/RuntimeParameters
Pfad	Root/DeviceSet/BIS_U_6127_Rfid_ Provider/RuntimeParametersGlobal/ BalluffRfidRuntimeParametersAn- tenna[1..4]

Mit dieser Variablen kann die entsprechende Antenne global, d. h. für alle Anwendungen aktiviert oder deaktiviert werden. Diese Einstellung entspricht dem Parameter 0012_{hex} (siehe Kapitel 7.3 auf Seite 49). Es ist eine Admin-Berechtigung notwendig.

AutoIncrementSendPower

Datentyp	Byte
Default-Wert	–
Zugriffsrechte	Lesen: User Schreiben: User
007-Parameter	0009 _{hex}
Parent	Balluff Erweiterung : AutoldDevice- Type/RuntimeParameters
Pfad	Root/DeviceSet/BIS_U_6127_Rfid_ Provider/RuntimeParametersGlobal/ BalluffRfidRuntimeParametersAn- tenna[1..4]

Diese Variable gibt die automatische Erhöhung der Schreibleistung für alle Anwendungen der ausgewählten Antenne an.

BufferLenReadFormatted

Datentyp	UInt32
Default-Wert	500
Zugriffsrechte	Lesen: User Schreiben: User
007-Parameter	–
Parent	Balluff Erweiterung: AutoldDeviceType/ RuntimeParameters
Pfad	Root/DeviceSet/BIS_U_6127_Rfid_ Provider/RuntimeParametersGlobal/ BalluffRfidRuntimeParametersCom- mon

Diese Variable legt fest, wie groß (in Byte) der Ausgabepuffer je Datenträger für die Methoden *ReadFormattedTagData()* (siehe Seite 144) und *ReadMultipleTagDataFormatted()* (siehe Seite 145) ist.

CodeTypes

Datentyp	UInt32[]
Default-Wert	0
Zugriffsrechte	Lesen: User Schreiben: Admin
007-Parameter	–
Parent	AutoldDeviceType/RuntimeParameters
Pfad	Root/DeviceSet/BIS_U_6127_Rfid_ Provider/RuntimeParametersGlobal/ BalluffRfidRuntimeParametersCom- mon

Diese Variable gibt an, welche Formate für den EPC unterstützt werden und dient zur Auswahl des gewünschten Formats. Folgende Formate werden unterstützt:

RAW:BYTES	EPC binär
RAW:STRING	EPC ASCII
EPC	EPC-Struktur (siehe Kapitel 9.7.15 auf Seite 164)
UID	AutoID Identifier gemäß ISO/IEC 18000-3 Mode 3, ISO/IEC 18000-63 und GS1 EPCglo- bal™

LastScanData

Datentyp	ByteString
Default-Wert	„“
Zugriffsrechte	Lesen: User Schreiben: –
007-Parameter	–
Parent	AutoldDeviceType
Pfad	Root/DeviceSet/BIS_U_6127_Rfid_Provider/

Diese Variable liefert die Daten des zuletzt erfassten Datenträgers. Sie wird von allen OPC UA Sessions gemeinsam genutzt.

MinRSSI

Datentyp	Int32
Default-Wert	–128 (Parameter 002f _{hex})
Zugriffsrechte	Lesen: User Schreiben: User
007-Parameter	–
Parent	AutoldDeviceType/RuntimeParameters
Pfad	Root/DeviceSet/BIS_U_6127_Rfid_Provider/RuntimeParametersGlobal/BalluffRfidRuntimeParametersAntenna[1..4]

Jeder Tag an der entsprechenden Antenne muss mit mindestens diesem RSSI-Wert erfasst werden, um als erkannt gemeldet zu werden. In OPC UA spiegelt sich dieser Wert in den Filtern wider (siehe *SetFilter* auf Seite 150).

Der RSSI (Received Signal Strength Indicator) ist ein Wert, der die Signalqualität einer empfangenen Datenträgerantwort widerspiegelt. Auf die Entfernung des Datenträgers zur Antenne lassen sich nur bedingt Rückschlüsse ziehen.

RFPower

Datentyp	SByte
Default-Wert	0
Zugriffsrechte	Lesen: User Schreiben: Admin
007-Parameter	0x0008 / 4
Parent	AutoldDeviceType/RuntimeParameters
Pfad	Root/DeviceSet/BIS_U_6127_Rfid_Provider/RuntimeParametersGlobal/BalluffRfidRuntimeParametersAntenna[1..4]

Dieser Wert gibt die Sendeleistung der entsprechenden Antenne in dBm an. Hier sind nur ganzzahlige Werte möglich. Über das Webinterface oder den UHF-Manager können auch feinere Einstellungen vorgenommen werden. Die Sendeleistung beeinflusst die maximale Reichweite des Erfassungsbereichs der Antenne.

TagTypes

Datentyp	UInt32[]
Default-Wert	„EPC Class 1 Gen2 V1“, „ISO 18000-63“
Zugriffsrechte	Lesen: User Schreiben: –
007-Parameter	–
Parent	AutoldDeviceType/RuntimeParameters
Pfad	Root/DeviceSet/BIS_U_6127_Rfid_Provider/RuntimeParametersGlobal/BalluffRfidRuntimeParametersAntenna[1..4]

Dieses Array liefert die vom System unterstützten Tag-Typen.

UserLed

Datentyp	BalluffUserLedEnumeration
Default-Wert	0 = off
Zugriffsrechte	Lesen: User Schreiben: User
007-Parameter	–
Parent	Balluff Erweiterung: AutoldDeviceType/RuntimeParameters
Pfad	Root/DeviceSet/BIS_U_6127_Rfid_Provider/RuntimeParametersGlobal/BalluffRfidRuntimeParametersCommon

Über diese Variable kann die LED des Geräts gesteuert werden. Folgende Werte sind möglich:

- 0: Led off
- 1: Led leuchtet rot
- 2: Led leuchtet gelb
- 3: Led leuchtet grün

9.7 Datentypen

In den folgenden Unterkapiteln werde vor allem die Datentypen Struktur, Enumeration und Union verwendet. Mit Hilfe einer Struktur können mehrere Elemente beliebiger Datentypen zu einem Datenobjekt zusammengefasst werden. Dabei können sowohl die Struktur als Ganzes als auch die einzelnen Elemente angesprochen werden. Bei einer Union werden ebenfalls mehrere Elemente zusammengefasst, allerdings darf von diesen immer nur eines verwendet werden. Da alle Elemente den gleichen Speicherplatz verwenden können, richtet sich die Größe des Speicherplatzes nach dem Bedarf des größten Union-Elements.

Bei einer Enumeration handelt es sich um einen Aufzählungstypen. Jedes Element wird durch einen eindeutigen Namen angegeben und automatisch mit einer Nummer versehen. Das erste Element bekommt in der Regel die Nummer 0. Beispielsweise kann eine Variable des Enumeration-Typs *Farbe* die Werte rot, grün oder blau annehmen.

9.7.1 AntennaNameIdPair

Dieser Datentyp ist eine Struktur, die einer RFID-Antennen-ID einen lesbaren Namen zuordnet. Sie wird bei den Variablen *AntennaNames* (siehe Seite 156) und *AntennaName* (siehe Seite 156) verwendet.

Wert	Datentyp	Beschreibung
AntennaNameIdPair	Struktur	
AntennaId	Int32	ID der Antenne
AntennaName	String	Name der Antenne

9.7.2 AutoldOperationStatusEnumeration

Dieser Datentyp ist ein Enum, das den Status der RIFD-Kommandos widerspiegelt. Folgende Werte sind definiert.

Code	Bedeutung
SUCCESS	Operation war erfolgreich.
MISC_ERROR_TOTAL	Die Operation konnte nicht ausgeführt werden.
MISC_ERROR_PARTIAL	Die Operation wurde nur teilweise ausgeführt.
PERMISSION_ERROR	Die Benutzerrechte sind nicht ausreichend.
PASSWORD_ERROR	Tag-Passwort ist falsch.
REGION_NOT_FOUND_ERROR	Der Speicherbereich steht beim angesprochenen Tag nicht zur Verfügung.
OP_NOT_POSSIBLE_ERROR	Die Operation wird vom angesprochenen Tag nicht unterstützt.
OUT_OF_RANGE_ERROR	Der angegebene Speicherbereich ist nicht zulässig.
NO_IDENTIFIER	Die Operation kann nicht ausgeführt werden, da kein Tag in Reichweite ist.
MULTIPLE_IDENTIFIER	Der Befehl kann nur mit einem Tag arbeiten, es wurden jedoch mehrere selektiert oder gefunden.
READ_ERROR	Beim Lesen des Tags ist ein Fehler aufgetreten.
CODE_NOT_SUPPORTED	Das Codeformat ist nicht korrekt oder der Wert ist ungültig.
WRITE_ERROR	Beim Schreiben des Tags ist ein Fehler aufgetreten.
NOT_SUPPORTED_BY_DEVICE	Kommando oder Parameter werden nicht vom Gerät unterstützt.
NOT_SUPPORTED_BY_TAG	Kommando oder Parameter werden nicht vom Tag unterstützt.
DEVICE_NOT_READY	Das Gerät ist (noch) nicht einsatzbereit, Kabelbruch oder keine Antenne angeschlossen
INVALID_CONFIGURATION	Die Geräteeinstellung ist fehlerhaft, z. B. keine Antenne aktiv
RF_COMMUNICATION_ERROR	Kommunikationsfehler zwischen dem Gerät und dem Tag
DEVICE_FAULT	Wird zurzeit noch nicht verwendet.
TAG_HAS_LOW_BATTERY	–

9.7.3 BalluffFilterOperationEnumeration

Dieser Datentyp ist ein Enum, das angibt, mit welcher Operation der statische Filter auf die Daten angewandt werden soll. Zurzeit wird allerdings nur die Operation *AND* unterstützt. Folgende Werte sind definiert:

Wert	Beschreibung
0 (AND)	Erster Filter bzw. die neuen Filterdaten werden mit den vorhandenen Filtern mit UND verknüpft. Derzeit ist nur ein Filter möglich.
1 (OR)	Wird in der aktuellen Version noch nicht unterstützt.
2 (NAND)	Wird in der aktuellen Version noch nicht unterstützt.
3 (NOR)	Wird in der aktuellen Version noch nicht unterstützt.

9.7.4 CodeTypeDataType

Dieser Datentyp ist ein String, der angibt, wie der erfasste Datenträger abgespeichert werden soll. Folgende Strings bzw. Typen werden unterstützt:

Wert	Beschreibung
„RAW:BYTES“	EPC binary
„RAW:STRING“	EPC ascii
„EPC“	EPC-Struktur (siehe Kapitel 9.7.15 auf Seite 164)
„UID“	AutoID Identifier gemäß ISO/IEC 18000-3 Mode 3, ISO/IEC 18000-63 und GS1 EPCglobal™

9.7.5 DeviceStatusEnumeration

Dieser Datentyp ist ein Enum, das den Zustand des Geräts liefert.

Wert	Beschreibung
0	Idle: Normalzustand
1	Error: Gerätefehler
2	Scanning: Start des asynchronen Scanbetriebs (siehe Kapitel <i>ScanStart</i> auf Seite 146)
3	Busy

9.7.6 Location

Die Union *Location* bietet die Möglichkeit, eine Ortsangabe in verschiedenen Formaten zu speichern. Es wird derzeit nur das Feld *NAME* vom Typ *LocationName* (Gerätestandort als String) unterstützt.

Die Auswahl, welches Feld mit Daten gefüllt ist, erfolgt i. d. R. über eine separate Enumeration-Variable vom Typ *LocationTypeEnumeration* (siehe Seite 162).

Name	Datentyp	Beschreibung
Location	Union	
NMEA	NmeaCoordinateString	Wird nicht unterstützt.
Local	LocalCoordinate	Wird nicht unterstützt.
WGS84	WGS84Coordinate	Wird nicht unterstützt.
Name	LocationName	Gerätestandort als String (<i>LocationName</i> siehe Seite 162).

9.7.7 LocationName

Dieser Datentyp ist ein String, der den Gerätestandort widerspiegelt.

9.7.8 LocationTypeEnumeration

Dieses Enum liefert die Auswahl für den Datentyp der Union *Location* (siehe Seite 162). Diese wird zum Beispiel bei der Methode *GetDeviceLocation()* (siehe Seite 140) verwendet.

Wert	Beschreibung
NMEA_0	Wird zur Zeit nicht unterstützt.
LOCAL_2	Wird zur Zeit nicht unterstützt.
WGS84_4	Wird zur Zeit nicht unterstützt
NAME_5	String, der den Gerätestandort anzeigt.

9.7.9 RfidLockOperationEnumeration

Dieser Datentyp definiert die Aktion, die im Lock-Kommando ausgeführt werden soll. Die folgenden Werte sind definiert und erlaubt. Wie genau sich die jeweilige Aktion auswirkt, ist abhängig von dem ausgewählten Speicherbereich des Tags.

Eine genauere Beschreibung findet man in den Standards nach EPCglobal™ Class1 Generation2 und OPC UA AutoID Companion Specification 1.0.

Wert	Beschreibung	
	Passwörter	Memory bank
Lock_0	Schreib- und Lesebefehle auf das Passwort sind nur mit gültigem Access-Passwort möglich.	Es kann ohne Passwort gelesen, aber nur mit gültigem Access-Passwort geschrieben werden.
Unlock_1	Schreib- und Lesebefehle auf das Passwort sind ohne die Kenntnis des Access-Passworts möglich.	Es kann sowohl die Schreib- als auch die Lese-Operation ohne Passwort ausgeführt werden.
Permanent-Lock_2	Schreib- und Lesebefehle auf das Passwort sind überhaupt nicht mehr möglich. Die Operation ist nicht reversibel.	Es kann ohne Passwort gelesen, aber nur mit gültigem Access-Passwort geschrieben werden. Die Operation ist nicht reversibel.
PermanentUnlock_3	Schreib- und Lesebefehle auf das Passwort sind möglich, allerdings kann der Bereich nicht mehr gelockt werden.	Es kann sowohl die Schreib- als auch die Leseoperation ohne Passwort ausgeführt werden. Allerdings kann der Bereich nicht mehr gelockt werden.

9.7.10 RfidLockRegionEnumeration

Dieser Datentyp definiert den Speicherbereich, der mit der Methode *LockTag()* (siehe Seite 147) gelockt werden soll. Folgende Werte sind definiert:

Wert	Beschreibung
Kill_0	Kill-Passwort
Access_1	Access-Passwort
EPC_2	UID/EPC bank (bank 01)
TID_3	TID bank (bank 10)
User_4	User memory bank (bank 11)

9.7.11 RfidPasswordTypeEnumeration

Dieser Datentyp legt fest, welches Passwort geändert werden soll (Methode: *SetTagPassword()* siehe Kapitel *SetTagPassword* auf Seite 155). Folgende Werte sind definiert:

Wert	Beschreibung
Access_0	Access-Passwort
Kill_1	Kill-Passwort
Read_2	Read-Passwort
Write_3	Write-Passwort

Die Werte Read_2 und Write_2 sind zwar definiert, aber nicht erlaubt. Sie sind im Standard nach EPCglobal™ Class-1 Gen-2 V1 nicht umgesetzt.

9.7.12 RfidScanResult

Diese Struktur liefert die Daten eines erfassten Tags und zusätzliche Informationen im Array vom Typ *Sigthings*. Sie ist wie folgt aufgebaut.

Name	Datentyp	Beschreibung
RfidScanResult	Struktur	
CodeType	CodeTypeData-Type (siehe Seite 162)	Gibt an, in welchem Format die gescannten Daten unter ScanData ausgegeben werden sollen.
ScanData	ScanData	Daten des erfolgreich gescannten Tags.
Timestamp	UtcTime	UtcTime beim Lesen.
Location	Location	Liefert den Ort zurück, an dem der Tag erkannt wurde.
Sightings	RfidSighting[] (siehe Seite 164)	Informationen zu jeder Lesung des Tags an einer Antenne: 1: Nummer der Antenne 2: RSSI-Wert 3: UtcTime beim Lesen 4: Beim Lesen verwendete Sendeleistung

9.7.13 RfidSighting

Diese Struktur liefert zusätzliche Informationen von der Erfassung eines Tags an einer bestimmten Antenne. Die Struktur ist wie folgt aufgebaut.

Name	Datentyp	Beschreibung
RfidSighting	Struktur	
Antennald	Int32	Gibt die ID der Antenne an, an welcher der Tag erfasst wurde.
Strength	Int32	Gibt den RSSI-Wert an, mit dem der Tag erkannt wurde.
Timestamp	UtcTime	Zeitstempel
CurrentPower-Level	Int32	Liefert die eingestellte Sendeleistung der Antenne.

9.7.14 ScanData

Diese Union bietet die Möglichkeit, die gescannten EPCs in verschiedenen Datenformaten abzuspeichern. Die Auswahl des Datenformats erfolgt indirekt über eine separate Enumeration-Variable des Typen *CodeTypeDataType* (siehe Seite 162), die das Format und die Bedeutung definiert.

Name	Datentyp	Beschreibung
ScanData	Union	
ByteString	ByteString	Erfasste Daten im RAW Format.
String	String	Erfasste Daten als String.
Epc	ScanDataEpc (siehe Seite 164)	Erfasste Daten in der <i>ScanDataEpc</i> -Struktur
Custom	BaseDataTyype	Herstellerspezifische Datenstruktur.

9.7.15 ScanDataEpc

Dieser Datentyp ist eine Struktur, die die Möglichkeit bietet, die Inhalte der EPC-Bank strukturiert darzustellen. Sie wird als eine Darstellung der Union *ScanData* verwendet und kommt somit bei Scanergebnissen zum Einsatz. Zu diesem Datentyp gehört der *CodeTypeDataType* EPC (siehe Seite 162).

Die Struktur setzt sich wie folgt zusammen:

Name	Datentyp	Beschreibung
ScanDataEpc	Struktur	
PC	UInt16	Protocol Control Informationen gemäß ISO/IEC 18000-3 Mode 3, ISO/IEC 18000-63 und GS1 EPCglobal™
UId	ByteString	AutoID Identifier gemäß ISO/IEC 18000-3 Mode 3, ISO/IEC 18000-63 und GS1 EPCglobal™
XPC_W1	UInt16	Extended protocol control word 1 gemäß ISO/IEC 18000-3 Mode 3, ISO/IEC 18000-63 und GS1 EPCglobal™
XPC_W2	UInt16	Extended protocol control word 2 gemäß ISO/IEC 18000-3 Mode 3, ISO/IEC 18000-63 und GS1 EPCglobal™

9.7.16 ScanSettings

Diese Struktur legt die Einstellungen für die Methoden *Scan()* (siehe Seite 141) und *ScanStart()* (siehe Seite 146) fest. Anhand von drei Parametern kann angegeben werden, wie lange der Scan andauern soll. Die drei Bedingungen *DURATION*, *CYCLES* und *DATAAVAILABLE* stehen in Relation zueinander. Sobald eine Bedingung erfüllt ist, wird die Scan-Operation beendet.

Die Struktur setzt sich wie folgt zusammen:

Name	Datentyp	Beschreibung
ScanSetting	Struktur	
Duration	Duration	Gibt die Dauer des Scan-Vorgangs in Millisekunden an. Der Wert 0 steht für <i>unendlich lange</i> .
Cycles	Int32	Gibt die Anzahl an Scan-Durchgängen an. Der Wert 0 steht für <i>unendlich viele</i> .
DataAvailable	Boolean	Wenn dieser Wert auf <i>TRUE</i> gesetzt wird, wird der Scanvorgang beendet, sobald Daten zur Verfügung stehen. Bei <i>FALSE</i> werden nur die Parameter <i>Duration</i> und <i>Cycles</i> berücksichtigt.
LocationType	LocationType (siehe Kapitel 9.7.8 auf Seite 162)	Gibt den gewünschten Typ der Standortinformation im Ergebnis an. Es wird nur der Typ <i>LocationName</i> unterstützt.

9.8 Events

In diesem System werden Events vom Typ *RfidScanEventTyp* verwendet. Sie kommen zum Einsatz, sobald aus einer beliebigen OPC-UA-Session der asynchrone Scan-Betrieb (siehe Seite 146) gestartet wird. Für jeden erfassten Tag wird ein Event *RfidScanEventTyp* generiert. Dieses Event liefert sowohl Informationen über die Erfassung als auch über den Tag selbst.

Alle Sessions, die sich bei dem Event angemeldet haben, bekommen dieses auch geliefert.

Für einen nicht mehr erkannten Tag wird kein Event generiert, da dies nicht in der AutoID Spec. definiert ist.

Das Event *RfidScanEventTyp*, das vom generischen *AutoIdScanEventTyp* abgeleitet ist, enthält folgende Datenfelder:

RfidScanEventTyp

Name	Datentyp	Beschreibung
ScanResult	RfidScanResult[]	Alle erkannten Tags werden mit Informationen wie EPC, Zeitstempel, RSSI-Wert etc. ausgegeben.
DeviceName	String	String mit dem Gerätenamen

Verwendete Datentypen

RfidScanResult

Name	Datentyp	Beschreibung
CodeType	CodeTypeData (siehe Seite 162)	Gibt an, in welchem Format die gescannten Daten unter <i>ScanData</i> ausgegeben werden sollen.
ScanData	ScanData	Daten des erfolgreich gescannten Tags.
Timestamp	UtcTime	UtcTime beim Lesen.
Location	Location	Liefert den Ort zurück, an dem der Tag erkannt wurde.
Sightings	RfidSighting[] (siehe Seite 164)	Informationen zu jeder Lesung des Tags an einer Antenne: 1: Nummer der Antenne 2: RSSI-Wert 3: UtcTime beim Lesen 4: Beim Lesen verwendete Sendeleistung

9.9 Beispiele

In den folgenden Unterkapiteln werden verschiedene Beispiele gezeigt. In den Beispielen wird UaExpert als Client verwendet, der auf dem PC installiert sein muss (Download unter www.unified-automation.com).

9.9.1 Verbindungsaufbau

Siehe Kapitel 9.3 *Verbindungsaufbau über OPC UA mit UaExpert* auf Seite 135.

9.9.2 Lesen und Schreiben von Variablen

Sobald die Auswerteeinheit BIS U-6127 mit dem Client UaExpert verbunden ist, werden die Objekte im Window *ADDRESS SPACE* angezeigt.

Um Variablen (werden im *ADDRESS SPACE* mit einem Icon dargestellt) auszulesen, gibt es zwei Möglichkeiten:

- ▶ Die gewünschte Variable im Fenster *ADDRESS SPACE* anklicken (in Bild 9-18 wurde beispielhaft die Variable *DEVICENAME* angeklickt).
 - ⇒ Im Fenster *ATTRIBUTES* werden daraufhin alle Informationen zu der Variablen angezeigt. Wie in der Abbildung zu sehen ist, kann man unter *VALUE – VALUE* (blau markiert) den aktuellen Wert der Variablen sehen. In diesem Fall wäre das *BISU-6127*.

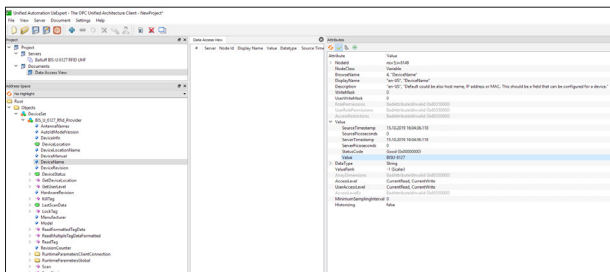


Bild 9-18: Darstellung einer Variablen im *Attributes*-Fenster

- ▶ Per Drop and Drag die gewünschte Variable in das Fenster *DATA ACCESS VIEW* schieben.
 - ⇒ Sobald die Variable sich in diesem Fenster befindet, werden weitere Informationen angezeigt (siehe Bild 9-19). In der Spalte *VALUE* findet man den aktuellen Wert der Variablen.

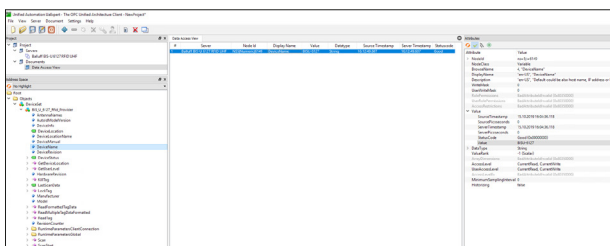


Bild 9-19: Darstellung einer Variablen im *DATA ACCESS VIEW*

9.9.3 Methodenaufrufe

Die Methoden werden im *ADDRESS SPACE*-Fenster mit violetten Icons dargestellt. Mit Rechtsklick auf eine Methode öffnet sich ein kleines Fenster. In der folgenden Abbildung sieht man diesen Vorgang am Beispiel der *GetRFPower*-Methode.

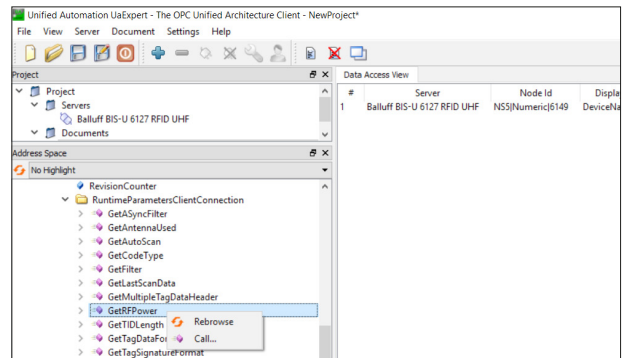


Bild 9-20: Rechtsklick auf Methode

Methoden ausführen

1. Methode *CALL* im Kontextmenü klicken.
 - ⇒ Es öffnet sich erneut ein Fenster, in dem die Aufrufargumente und die Rückgabeparameter der entsprechenden Methode zu sehen sind (*GetRFPower*), siehe Bild 9-21).

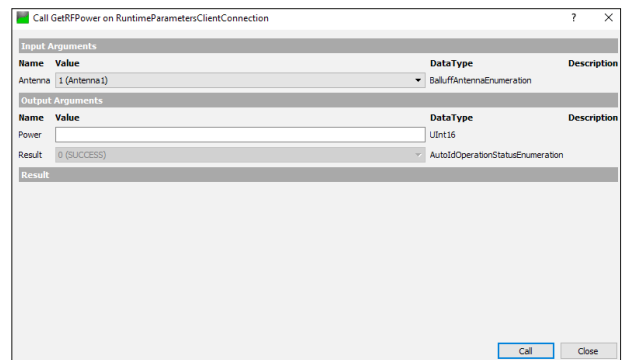


Bild 9-21: Methoden Aufruf *GetRFPower()*

2. Eingabeparameter eingeben und mit *CALL* bestätigen.
 - ⇒ Die Methode wird ausgeführt und das Ergebnis erscheint in den Rückgabeparametern (aktuelles Beispiel, siehe Bild 9-22).

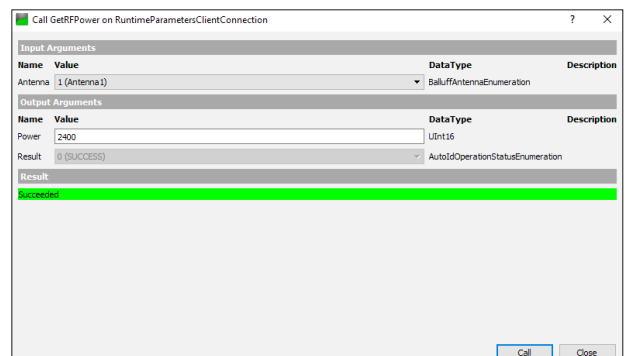


Bild 9-22: Ergebnis Methode *GetRFPower()*

Über die Methode `ReadFormattedTagData()` können gelesene Daten eines Tags nach Wunsch formatiert werden. Das Format kann über die Methode `SetTagDataFormat()` festgelegt werden. In diesem Beispiel ist das Format `%E[0,12]%S[0,3]`.



Zur Ausführung der Methode *ReadFormattedTagData* sind die Aufrufparameter *Identifier*, *CodeType* und *Password* notwendig.



In diesem Beispiel soll der Tag mit dem EPC „080908080808080808080808“ gelesen werden. Der verwendete CodeType ist *RAW:BYTES*, und es ist kein Passwort für die Lese-Operation notwendig. Die Eingaben sehen daher aus wie folgt:



" data-bbox="111 102 886 352"/>

Insgesamt wurden Daten mit einer Länge von 15 Byte gelesen. Dies entspricht der Einstellung des Formatstrings. Diese Information wird über die Angabe *LENGTH* im Parameter *READDATA* ausgegeben. Die gelesenen Daten werden im Anschluss hinter *CONTENT=* angegeben.

Die Anwendung ist im Detail in Kapitel 8.11 auf Seite 121 beschrieben.

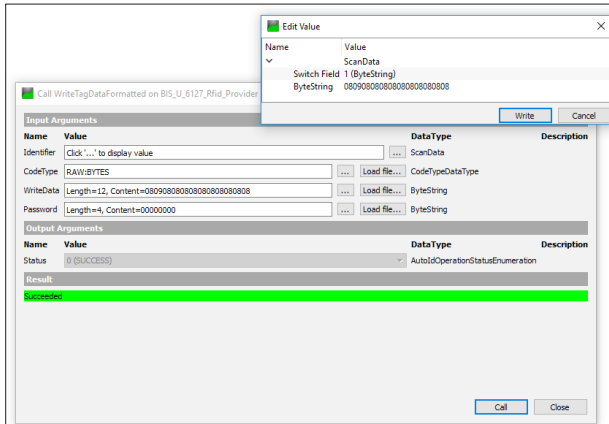


Bild 9-32: Methode WriteTagDataFormatted()

Die Signatur wird bei allen Lesebefehlen überprüft, die das universelle Ausgabeformat verwenden. Das Prüfergebnis kann in die Ausgabe übernommen werden, indem das Statusbyte im Formatstring mit angegeben wird. Der Wert 0 steht für eine erfolgreiche Prüfung, der Wert 2 bedeutet, dass die Signatur nicht zu den übrigen Tagdaten passt.

Bild 9-33 zeigt, dass die Signaturüberprüfung erfolgreich war.

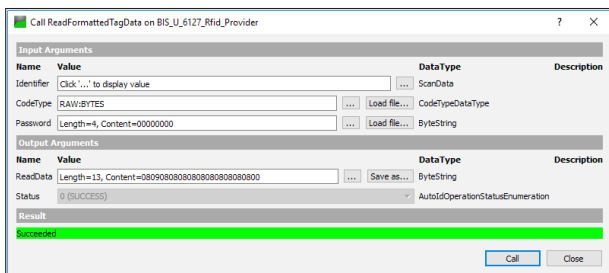


Bild 9-33: Erfolgreiche Signaturüberprüfung

Die Signatur wird auf dem User-Bereich gespeichert. Überschreibt man diesen Bereich mit der Methode *Write-Tag()*, muss im nächsten Lesebefehl die Signaturüberprüfung fehlschlagen. Bild 9-34 zeigt die Ausgabe mit einer fehlgeschlagenen Signaturüberprüfung.

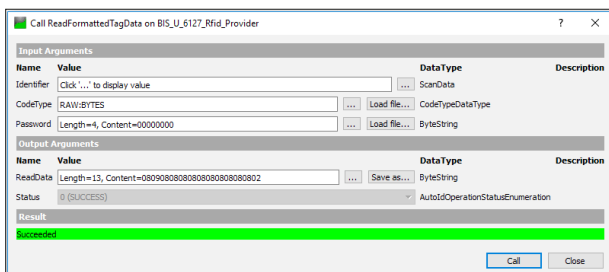


Bild 9-34: Fehlgeschlagene Signaturüberprüfung

9.9.7 Umgang mit statischen Filtern

Das Filter für den synchronen Scanbetrieb kann über die Methode *SetFilter()* eingestellt werden.

Um die Auswirkungen des Filters zu sehen, wurde zuerst ein Scan ohne Filter durchgeführt. Wie in Bild 9-35 zu sehen ist, wurden drei Tags mit folgenden EPCs erfasst:

- 08090808080808080808080808080808
- 3005FB63AC1F3681EC880468
- E21000161504007625901010

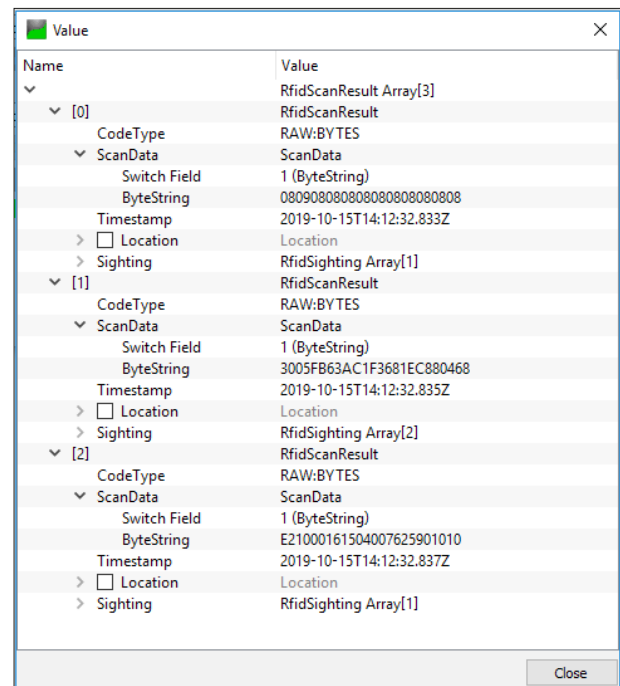


Bild 9-35: Erfassung Tags

Für das erste Beispiel wurden die Einstellungen, die in Bild 9-36 zu sehen sind, für das Filter festgelegt.

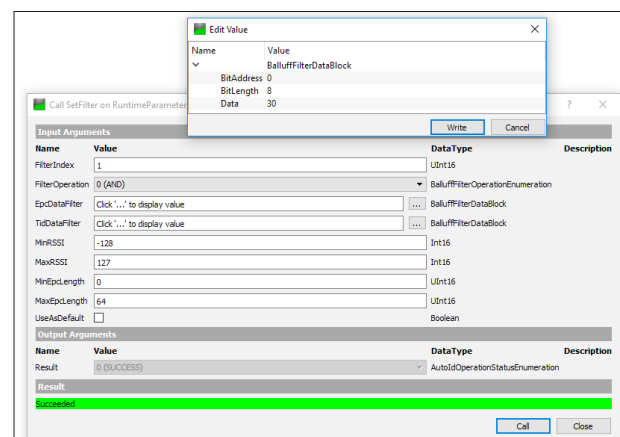


Bild 9-36: Filtereinstellungen

Das bedeutet, es dürfen nur Tags gelistet werden, deren EPC mit „30“ beginnt. Der RSSI-Wert und die EPC-Länge dürfen einen beliebigen gültigen Wert annehmen.

9

OPC UA (Fortsetzung)

Führt man nun die Scan-Methode aus, erhält man folgendes Ergebnis (Bild 9-37).

Name	Value
▼ [0]	RfidScanResult
CodeType	RAW:BYTES
▼ ScanData	ScanData
Switch Field	1 (ByteString)
ByteString	3005FB63AC1F3681EC880468
Timestamp	2019-10-15T15:25:50.550Z
Location	0 (Null)
Switch Field	0 (Null)
▼ Sighting	RfidSighting Array[2]
> [0]	RfidSighting
> [1]	RfidSighting

Bild 9-37: Ergebnis Scan-Methode

Wie erwartet wird nur noch der Tag erkannt, dessen EPC mit „30“ beginnt. Alle anderen Tags werden nicht gelistet.

Da die Adresse und die Länge des Filters in Bits angegeben werden, kann man auch *halbe* Byte filtern.

Das nächste Beispiel zeigt diese Anwendung. In dem Fall sollen die EPCs nach dem Bit-Adressbereich 76...82 selektiert werden.

- 08090808080808080808080808080808
- 3005FB63AC1F3681EC880468
- E21000161504007625901010.

Der Bereich soll den Wert 8080 haben.

Name	Value	DataType	Description
Index	1	UInt16	

Name	Value	DataType	Description
EpcDataFilter	Click ... to display value	BalluffFilterDataBlock	
TidDataFilter	Click ... to display value	BalluffFilterDataBlock	
MinRSSI	-128	Int16	
MaxRSSI	127	Int16	
MinEpcLength	0	UInt16	
MaxEpcLength	64	UInt16	
Result	0 (SUCCESS)	AutoIdOperationStatusEnumeration	

Result: 0 (SUCCESS) AutoIdOperationStatusEnumeration

Call Close

Bild 9-38: Filter 8080

Führt man nach der Anwendung des Filters die Scan-Methode aus, bekommt man nur noch die Tags, deren EPC dem Filter entspricht.

Name	Value
▼ [0]	RfidScanResult
CodeType	RAW:BYTES
▼ ScanData	ScanData
Switch Field	1 (ByteString)
ByteString	08090808080808080808080808080808
Timestamp	2019-10-15T16:31:10.131Z
Location	0 (Null)
Switch Field	0 (Null)
▼ Sighting	RfidSighting Array[1]
> [0]	RfidSighting

Bild 9-39: Ergebnis Filter

9.9.8 Umgang mit Events

In diesem Beispiel wird Schritt für Schritt erklärt, wie man mit dem UaExpert das Event, das durch den asynchronen Betrieb generiert wird, empfangen kann.

1. Das Fenster *EVENT VIEW* unter *DOCUMENTS* – *ADD* hinzufügen.

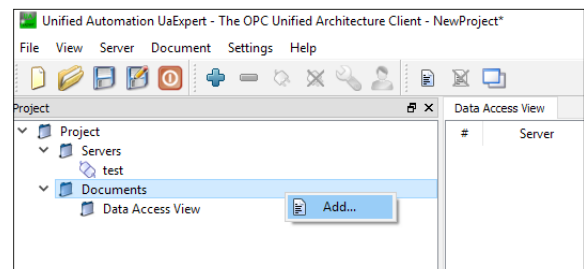


Bild 9-40: Add Documents

2. Das Server-Objekt per Drag and Drop zur Konfiguration hinzufügen, um sich für die gewünschten Events anmelden zu können.

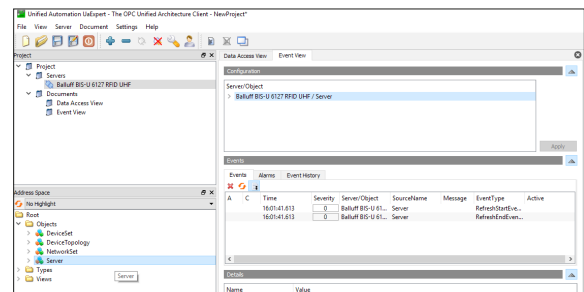


Bild 9-41: Server-Objekt hinzufügen

9

OPC UA (Fortsetzung)

- Um zu dem gewünschten Event zu gelangen, muss das Objekt *BALLUFF BIS-U 6127 RFID UHF /SERVER* aufgeklappt werden. Das Event *RFIDSCANEVENTTYPE* unter *SIMPLEEVENTS - AUTOLDSCANEVENTTYPE* auswählen und die Einstellung mit *APPLY* (rechts unten im Event View) übernehmen.

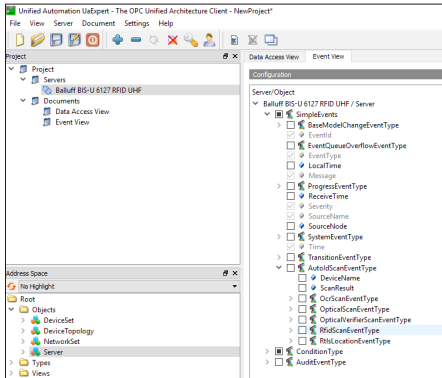


Bild 9-42: Event View

Sobald mit der Methode *ScanStart()* (siehe Seite 146) der asynchrone Betrieb gestartet wird, wird für jeden erfassten Datenträger ein Event generiert. Diese werden im Fenster *EVENTS* unter dem Reiter *EVENT* angezeigt. An dem *EVENT-TYPE* erkennt man, dass es sich um ein *RFIDSCANEVENTTYPE* (siehe Seite 165) handelt. Um weitere Informationen zu dem Event zu erhalten, muss man nur auf das Event klicken. Im Fenster *DETAILS* werden daraufhin alle Daten angezeigt.

Informationen zu den genauen Daten findet man unter dem Kapitel *Events* (siehe Seite 165).

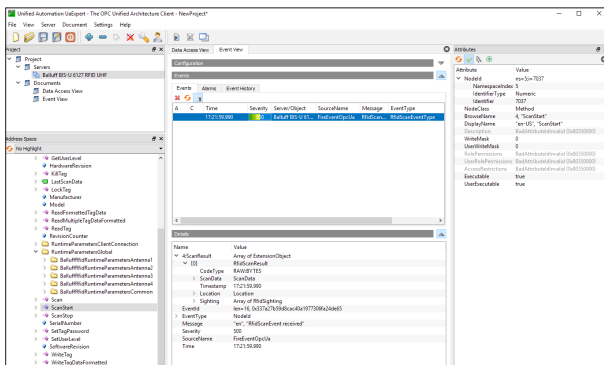


Bild 9-43: Event Details

9.9.9 Global Session Mechanismus

In OPC UA gibt es sowohl sessionbezogene als auch globale Variablen. Die globalen Variablen gelten für alle aktiven und neuen Sessions. Ein Beispiel hierfür ist die Variable *LASTSCANDATA*. Sie wird von allen Sessions verwendet.

In Bild 9-44 und Bild 9-45 sind die Clients abgebildet. Beide Werte der Variablen *LASTSCANDATA* sind wie erwartet identisch.

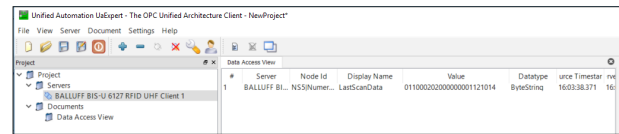


Bild 9-44: UaExpert Client 1

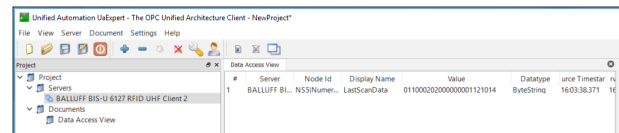


Bild 9-45: UaExpert Client 2

Führt man bei Client 1 die *Scan-Methode* aus, wird nur der EPC *08090808080808080808* erkannt und die Variable *LASTSCANDATA* wird auf diesen Wert gesetzt. Da alle Sessions diese Variable verwenden, ändert sich der Wert bei beiden Clients (siehe Bild 9-46 und Bild 9-47).

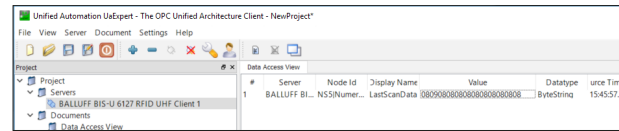


Bild 9-46: Client 1: Variable LastScanData

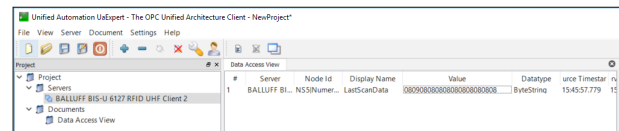


Bild 9-47: Client 2: Variable LastScanData

Möchte man aber den letzten erfassten Tag der einzelnen Session wissen, muss man die Methode *GetLastScanData()* verwenden. Diese ist sessionbezogen und liefert den gewünschten Wert. Im Falle dieses Beispiels liefert die Methode für den Client daher den Wert *08090808080808080808* (siehe Bild 9-48) und für den Client 2 *01100020200000001121014* (siehe Bild 9-49).

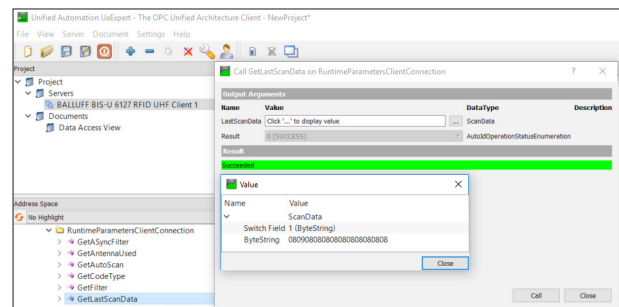


Bild 9-48: Client 1: Methode GetLastScanData

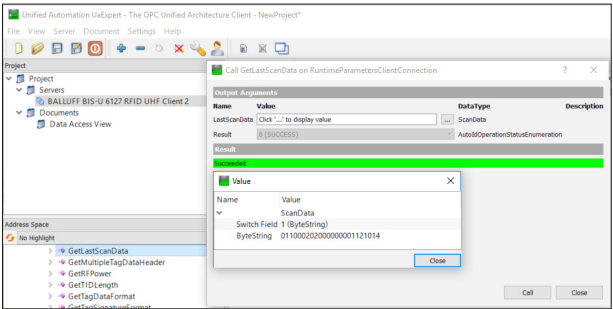


Bild 9-49: Client 2: Methode GetLastScanData

10 Zubehör

Zubehör ist nicht im Lieferumfang enthalten und deshalb getrennt zu bestellen.



Empfohlenes Zubehör finden Sie unter www.balluff.com auf der Produktseite.

Im Folgenden werden einige Komponenten für den Anschluss und den Betrieb des Geräts aufgeführt.

10.1 UHF-Antennen

Typ	Bestellcode
UHF Long Range Antenne (866...868 MHz)	BIS01AW
UHF Long Range Antenne (902...928 MHz)	BIS01AY
UHF Mid Range Antenne (866...868 MHz)	BIS00P0
UHF Mid Range Antenne (902...928 MHz)	BIS00TY
UHF M30 Short Range Antenne (866...868 MHz)	BIS01CP
UHF M30 Short Range Antenne (902...928 MHz)	BIS01CL

10.2 Antennenkabel

Typ	Bestellcode
Koaxialkabel 1 m	BAM01HL
Koaxialkabel 2 m	BAM01HM
Koaxialkabel 3 m	BAM01YR
Koaxialkabel 5 m	BAM01HN
Koaxialkabel 10 m	BAM01HP

(weitere Kabellängen auf Anfrage)

10.3 Anschlusskabel

Typ	Bestellcode
Anschlussleitung Spannungsversorgung, M12, 2 m	BCC032F
Anschlussleitung Service/USB, M12, 2 m	BCC0KNT
Anschlussleitung Service/USB, M12, 3 m	BCC0J56
Anschlussleitung IO-Link, M12, 2 m	BCC039M
Anschlussleitung Ethernet, RJ45, 2 m	BCC0E24

(weitere Kabellängen auf Anfrage)

10.4 Spannungsversorgung/Netzteil

Typ	Bestellcode
Standard-Netzteil 24 VDC, 5 A	BAE0112
IO-Link-Netzteil 24 VDC, 5 A	BAE00T4

10.5 Mechanisches Zubehör

Typ	Bestellcode
Befestigungsplatten	BAM01KN

BIS U-6127-081-1_4-06-ST36

User's Guide



www.balluff.com

1	Notes to the user	6
1.1	About this guide	6
1.2	Symbols and conventions	6
1.3	Scope of delivery	6
1.4	Abbreviations	6
2	Safety	7
2.1	Intended use	7
2.2	Reasonably foreseeable misuse	7
2.3	Explanation of the warnings	7
2.4	General safety notes	7
2.5	Approvals and designations	8
2.6	Disposal	8
3	Product description	9
3.1	General information about the processor unit	9
3.2	Product features	9
3.3	System Overview	9
3.4	Device overview	10
3.5	Custom applications and extensions	10
3.6	Data security	11
3.7	Sign tag data	12
3.8	Display elements	12
3.9	Ethernet TCP/IP	13
3.10	OPC UA	13
3.11	IO-Link master	13
3.12	UHF data carriers (not included in scope of delivery)	14
4	Installation	15
4.1	Selection of the installation location	15
4.2	Mounting the processor unit	15
4.3	Pin assignments	16
4.4	Mounting of the UHF antennas (not included in scope of delivery)	17
4.5	Mounting of the UHF data carriers (not included in scope of delivery)	17
5	Technical data	18
5.1	Dimensions	18
5.2	Mechanical data	18
5.3	Electric data	18
5.4	Ambient conditions	19
5.5	Connectors ANT1...ANT4	19
5.6	IO-Link connection	19
5.7	Ethernet TCP/IP connection	19
5.8	Service connection (USB)	19
5.9	Data carrier	19
5.10	Display elements at a glance	19
5.11	Time and date	20
6	Application planning	21
6.1	General operating conditions	21
6.2	Antenna configurations	21
6.3	Data carrier selection	21
6.4	UHF properties in practice	22
6.5	Operating modes	23

7	Startup and operation	29
7.1	UHF Manager configuration software	29
7.1.1	Install and start configuration software	29
7.1.2	User interface	29
7.1.3	Interface settings	30
7.1.4	Detect data carriers	31
7.1.5	Read/write data carrier	32
7.1.6	Parameter setting	32
7.2	Web server	33
7.2.1	Home	33
7.2.2	Log in/Log out	33
7.2.3	Language settings	34
7.2.4	RFID	35
7.2.5	Configuration	36
7.2.6	Logbook	48
7.2.7	Legal and general information	48
7.3	Parameter configuration	49
7.3.1	Preliminary considerations for parameterization	49
7.3.2	Parameter overview	50
7.3.3	Description of parameters for standard users	53
7.3.4	Description of parameters for experts	56
7.3.5	Description of parameters for administrators	72
7.3.6	Generating a key for signing tag data	82
7.4	System diagnostics	85
7.5	Operation	88
8	007 protocol	89
8.1	Protocol sequence	89
8.2	Control characters	90
8.3	Block Check Character (BCC)	90
8.4	EPC/TID data format	90
8.5	Command overview	91
8.6	Status codes	94
8.7	General commands	95
8.8	Detect data carriers	99
8.9	Detect data carriers, asynchronous	104
8.10	Edit data carrier	105
8.11	Universal data carrier access (Formatted tag data)	121
8.12	IO-Link	125

9	OPC UA	132
9.1	Basics of OPC UA	132
9.1.1	Description of OPC UA	132
9.1.2	System diagram	132
9.1.3	Security mechanisms	132
9.2	OPC UA security mechanisms on BIS U-6127	133
9.3	Connection established via OPC UA with UaExpert	135
9.3.1	Unsecure connection setup between PC (OPC-UA client) and the BIS U-6127 device (OPC-UA server)	135
9.3.2	Secure connection setup between PC (OPC-UA client) and the BIS U-6127 device (OPC-UA server)	136
9.4	Data model object: BIS_U_6127_Rfid_Provider	138
9.5	Methods	139
9.5.1	Device setting methods	140
9.5.2	Write/read methods for tag	141
9.5.3	Methods for scan settings	148
9.6	Variables and constants	156
9.6.1	Device information/settings	156
9.6.2	Scan settings	159
9.7	Data types	161
9.7.1	AntennaNameIdPair	161
9.7.2	AutoldOperationStatusEnumeration	161
9.7.3	BalluffFilterOperationEnumeration	162
9.7.4	CodeTypeDataType	162
9.7.5	DeviceStatusEnumeration	162
9.7.6	Location	162
9.7.7	LocationName	162
9.7.8	LocationTypeEnumeration	162
9.7.9	RfidLockOperationEnumeration	163
9.7.10	RfidLockRegionEnumeration	163
9.7.11	RfidPasswordTypeEnumeration	163
9.7.12	RfidScanResult	163
9.7.13	RfidSighting	164
9.7.14	ScanData	164
9.7.15	ScanDataEpc	164
9.7.16	ScanSettings	165
9.8	Events	165
9.9	Examples	166
9.9.1	Connection setup	166
9.9.2	Reading and writing variables	166
9.9.3	Method calls	166
9.9.4	Read formatted Tag Data	167
9.9.5	Read Multiple Tag Data Formatted	168
9.9.6	Write Tag Data with Signature	168
9.9.7	Dealing with static filters	169
9.9.8	Dealing with events	170
9.9.9	Global Session Mechanism	171
10	Accessories	173
10.1	UHF antennas	173
10.2	Antenna Cable	173
10.3	Connection cable	173
10.4	Power supply/power supply unit	173
10.5	Mechanical accessories	173

1

Notes to the user

1.1 About this guide

This manual describes the BIS U-6127-081-1_4-06-ST36 UHF RFID processor unit and its handling for safe operation.

The guide is intended for qualified technical personnel. Read this guide before installing and operating the processor unit.

1.2 Symbols and conventions

Individual action **instructions** are indicated by a preceding triangle.

- Instruction 1
- ⇒ Action result.

Action sequences are numbered consecutively:

1. Instruction 1
2. Instruction 2

Numbers unless otherwise indicated are decimals (e.g. 23). Hexadecimal numbers are shown with the additional indicator hex (e.g. 00_{hex}).

Characters sent in **ASCII Code** are shown in inverted commas, e.g. 'L'.

Control characters to be sent are set in angle brackets (e.g. <ACK>).

Buttons or selectable menu entries are described in italic and small caps, e.g. *SAVE*.

Menu commands are joined with a greater-than sign, e.g. "Settings > Options" stands for the menu command "Options" from the "Settings" menu.



Note, tip

This symbol indicates general notes.

1.3 Scope of delivery

- BIS U-6127 processor unit
- 5 x caps
- Safety notes – Information sheet on conformity and approval



For corresponding technical documents as well as additional information on available software and accessories, see **www.balluff.com**.

1.4 Abbreviations

BCC	Block Check Character
BIS	Balluff Identification System
CRC	Cyclic Redundancy Check
DC	Direct current
I/O-Port	Digital input or output port
EEPROM	Electrical Erasable and Programmable ROM
EIRP	Equivalent Isotropically Radiated Power
EMC	Electromagnetic compatibility
EPC™	Electronic Product Code
ERP	Effective Radiated Power
FCC	Federal Communications Commission
FE	Function ground
IC	Industry Canada
IP	Internet Protocol
ISO	International Organization for Standardization
kB	Kilobyte
LAN	Local Area Network
MAC-ID	Media Access Control Identifier
MB	Megabyte
OPC UA	Open Platform Communications Unified Architecture
PC	Personal Computer
RFID	Radio Frequency Identification
RFU	Reserved for Future Use
RSSI	Receive Signal Strength Indicator
PLC	Programmable Logic Controller
Tag	Data carrier with antenna/transponder
TCP	Transmission Control Protocol
TID	Tag identifier
UID	Unique Identifier
UHF	Ultra-high frequency
USB	Universal Serial BUS

2

Safety

2.1 Intended use

The BIS U-6127-... UHF processor unit, together with a maximum of 4 connectable UHF antennas, forms the BIS U identification system.

The processor unit provides network functions for connection to a higher-level Ethernet TCP/IP network and is intended for contactless detection and processing of UHF RFID data carriers in an industrial environment. The processor unit may only be used for this purpose.

The BIS U UHF RFID processor unit may only be operated within the approved countries (see information sheet on conformity and approval) and in compliance with the nationally applicable legal regulations.

Flawless function in accordance with the specifications in the technical data is ensured only when using original Balluff accessories. Use of any other components will void the warranty.

In the event of damage resulting from unauthorized intervention or improper use, installation or handling contrary to the provisions of this user's guide, any warranty, guarantee and liability claims against the manufacturer are rendered void.

2.2 Reasonably foreseeable misuse

The products are not intended for the following applications and areas and must not be used there:

- In safety-oriented applications in which personal safety depends on the device function
- In explosive atmospheres
- In food applications

2.3 Explanation of the warnings

Always observe the warnings in these instructions and the measures described to avoid hazards.

The warnings used here contain various signal words and are structured as follows:

SIGNAL WORD
Type and source of the hazard Consequences if not complied with ► Measures to avoid hazards

The individual signal words mean:

NOTICE Identifies a hazard that could damage or destroy the product .
 CAUTION The general warning symbol together with the signal word CAUTION indicates a hazard which can lead to slight or moderate injuries .

2.4 General safety notes

Installation and **startup** may only be performed by qualified personnel with basic electrical knowledge.

Qualified personnel are persons whose technical training, knowledge and experience as well as knowledge of the relevant regulations allow them to assess the work assigned to them, recognize possible hazards and take appropriate safety measures.

The **operator** is responsible for ensuring that local safety regulations are observed.

In particular, the operator must take steps to ensure that a defect in the device will not result in hazards to persons or equipment.

If defects and unresolvable faults occur in the device, take it out of service and secure against unauthorized use.

The product must not be opened, modified or changed. In case of defects and unrepairable malfunctions of the product, it must be taken out of operation and secured against unauthorized use.

The antennas of the identification system BIS U transmit ultra-high frequency electromagnetic waves. IEC 62369 stipulates that personnel must not remain within close range of the UHF antenna for long periods (several hours).

The processor unit and connected accessories may only be supplied with limited power, according to UL 61010-1 Third Edition, Sub. Clauses 9.4 or LPS according to UL 60950-1 or Class 2 according to UL 1310 or UL 1585.

If the maximum current consumption is exceeded, the processor unit and connected system components may be damaged. During operation, it must be ensured that the total current carried via the Power connection does not exceed 3 A.

The voltage output (L+) on the IO-Link port and digital outputs (I/O) are supplied via the Power connection. The sum of the partial currents of these pins must not exceed a maximum current of 2 A.

2

Safety (continued)

2.5 Approvals and designations



See attached information sheet on conformity and approval.



Additional information on directives, approvals and standards can be found at **www.balluff.com** on the product page.

2.6 Disposal

- Observe the national regulations for disposal.



Additional information can be found at **www.balluff.com** on the product page.

3.1 General information about the processor unit

The BIS U-6127 processor unit together with a maximum of four connectable UHF antennas of the BIS U-3... series and UHF RFID data carriers of the BIS U-1... series form the BIS U identification system from Balluff.

Depending on the country variant used (see information sheet on conformity and approval), the antennas transmit signals in a frequency range of 865 MHz...930 MHz and communicate wirelessly with data carriers located in the detection range of the antennas. Four antennas allow data carriers to be detected and processed in different areas as required. If, for example, all antennas are aligned to the same detection range (gate application), this can be enlarged and the detection reliability (depending on the operating mode) increased.

Via the Gigabit Ethernet TCP/IP interface, the processor unit can be integrated into a local network (LAN) and controlled by a higher-level system. A web server is available for configuration.

The BIS U-6127 supports the OPC UA protocol for RFID readers via the TCP/IP interface. This standard primarily supports the automated exchange of information between industrial devices (M2M) (see chapter 9 on page 132).

An IO-Link master interface is available as an additional interface, which enables direct integration of IO-Link components and the input and output of switching signals.

The USB service interface provides service access directly at the installation site without physically disconnecting the processor unit from the network.

Function indicators on the device surface provide information about the function and status of the device at all times.

3.2 Product features

- Robust metal housing with IP65 protection class
- Operation of up to 4 antennas with direct selection and multiplex operation
- RFID UHF operating frequencies: 865 MHz...930 MHz (country-specific)
- Transmitting power adjustable in the range 7 dBm...30 dBm (5 mW...1 W)
- Read/write distance up to 6 meters (typ.)
- Supported data carrier types according to ISO 18000-63 and EPCglobal™ Class1 Generation2
- Ethernet TCP/IP (1000BASE-T, 100BASE-TX, 10BASE-T) according to IEEE 802.3-2008
- Control via OPC UA protocol according to AIM AutoID Companion Specification 1.0
- Increased data security through access restrictions via user accounts
- Encrypted network connections via OPC UA
- Automatic generation of signatures on data carriers to secure data against manipulation
- Storage of the secret keys in a *Secure Element* chip
- IO-Link master interface, freely configurable as IO-Link and I/O port or 2 I/O ports
- Indicators for function and status
- Configuration and monitoring via web server
- USB interface for service functions

3.3 System Overview

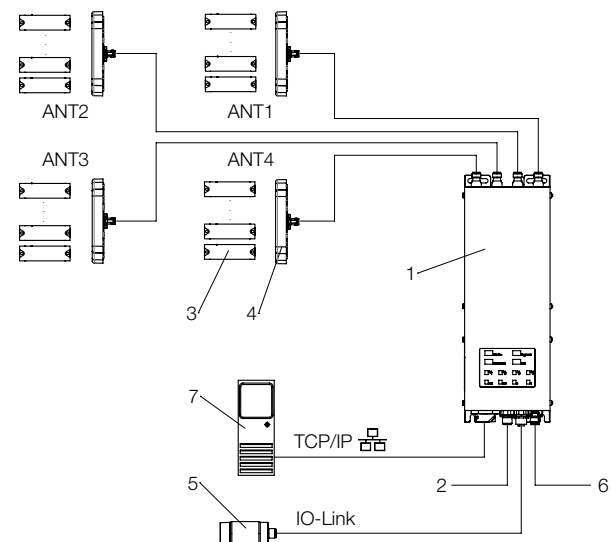


Fig. 3-1: System Overview

1 BIS U-6127	5 IO-Link-Device
2 Service (USB)	6 Power
3 UHF data carrier	7 Ethernet-Host
4 UHF antennas	



To avoid malfunctions, switch off unused antenna ports via the parameterization (see chapter 7.3 on page 49).

3

Product description (continued)

3.4 Device overview

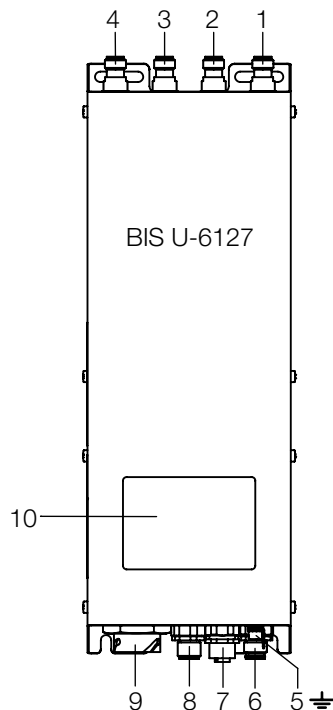


Fig. 3-2: Device overview

1 Antenna port 1	6 X1 Power
2 Antenna port 2	7 X2 IO-Link
3 Antenna port 3	8 X3 Service (USB)
4 Antenna port 4	9 X4 Ethernet TCP/IP
5 FE Functional ground	10 Function displays



To ensure IP65 protection, unused connections must be fitted with sealing caps.

3.5 Custom applications and extensions

The BIS U-6127 processor unit offers many options for adaptation to customer-specific tasks, such as autonomous operation, adjustable data output and input formats and filter functions. In addition, the IO-Link master port enables the actuation of further devices.

Nevertheless, it may be useful to perform further processing steps of data preparation or data-dependent processes in the device, thus saving additional system components, control PCs or similar, and simplifying handling and maintenance.

The Linux-based operating system and the Balluff system architecture of the device also make it possible to integrate customer-specific extensions through additional applications in the device, e.g. to synchronize the scanning process with sensors on the IO-Link port, to actuate displays, to communicate directly with your ERP systems, to implement fully autonomous operation in an application, and much more.

The extension applications can make the most of the advantages and the security concept of the device.



Contact our application specialists for individual consultation and the creation of customized apps.

3.6 Data security

The BIS U-6127 processor unit was also designed to operate in distributed installations and larger networks. As the distribution of networked devices increases, so does the risk of unintentional or intentional modification of the stored or transmitted data.

This applies both to the data on the data carriers used and their transmission to and from the processor unit, and to the data in the processor unit itself and its transmission to the higher-level processing system.

To minimize risks, the device offers some safety features:

- The use of an established Linux-based operating system.
- End-to-end user management provides access protection to device settings at multiple levels. Essential settings (e.g. IP address or antenna configuration), firmware updates or a device restart can only be performed with the *Admin* user role.
- Actuation of the device via OPC UA with optional encryption of the data and two-way endpoint authentication also allows control over extended networks.
- Unused communication protocols and accesses can be blocked.
- Data on standard UHF data carriers can be automatically signed to verify the integrity and authenticity of the data.
- The security-critical private keys for OPC UA and tag signatures can be managed in the memory of the built-in *Secure Element*. From there, they cannot be read even if the device is opened or attacked from the network.

Recommended measures for data security

To ensure the best possible data security, we recommend the following measures:

General

- Assign a different device name to each device on the network.
- Seal off networks connected to the Internet via firewalls, etc.
- Install security updates provided by Balluff.

User accounts

- If possible, the default administrator account *admin_default* should only be used for the initial setup of other user accounts.
- The device-specific password for *admin_default* cannot be changed. Cut off the password printed on the type label and keep it safe!
- Additional accounts can be provided with self-selected passwords (including those with administrator privileges). Secure passwords should contain upper and lower case letters, numbers and special characters and be at least eight characters long.
- Assign user rights and passwords on a person-by-person basis and grant rights only to the extent necessary for the persons' tasks.
- Change passwords that have fallen into unauthorized hands as soon as possible.

For more information on user accounts and associated permissions, see chapter 7.2.5 on page 36.

OPC UA

- Use OPC UA as communication protocol. The BIS U-6127 processor unit implements an extended range of functions of the OPC UA AutoID Companion Specification 1.0.
- For the OPC UA protocol, use the settings *REJECT INSECURE CLIENT CONNECTIONS* and *ACCEPT TRUSTED CLIENT CERTIFICATES ONLY*.
- Block or delete client certificates that are not needed.
- Use the key and certificate management function of the *Secure Element*.
- Assign a different device name to each device on the network.
- Create new device certificates when the network name or IP address changes.
- Also in the OPC UA client, only allow verified device certificates and reject unknown certificates.
- Establish the initial connection and certificate exchange for a new device or device certificate in a secure network environment to ensure that the certificate belongs to the connected device.

007 protocol

- Use the 007 protocol (also used by the UHF Manager as a connection protocol) only in a secure, closed network environment or via USB, as passwords are transmitted unencrypted.
- The 007 protocol can be disabled via the web interface if it is not used.

Web interface

Only operate the web interface for configuring the device in a local network, as the http transmission is not encrypted and entered passwords could be intercepted by third parties.

3

Product description (continued)

3.7 Sign tag data

When data is signed on data carriers, additional data is added to the actual data (TID, EPC, user data) with the help of a secret key and a calculation algorithm, which is later used to verify the authenticity of the data.

A 224-bit secret (private) key and an *elliptic curve* algorithm are used, which offers a high level of security.

When reading the data carriers, the data is accepted as valid only if the following conditions are met:

1. There is a signature.
2. The signature with the correct secret key of the operator was generated.
3. Neither data nor signature were changed afterwards.

UHF data carriers (tags) with at least 64 bytes of memory available in the user area that do not have to be used for application data can use the tag signature. The *FORMATTED READ/WRITE* commands must be used for this. Here, the first 64 bytes of the user area are provided with a signature that usually includes the EPC and the TID of the tag as well as a secret key and can only be generated by devices that have the same secret key.

The key must be generated and programmed into the device by the person setting it up (see chapter 7.3.6 on page 82). The key should be stored securely and protected against unauthorized access. In the device itself, the key is stored securely in the *Secure Element*.

i In order to sign tag data or verify the signature, the customer must import their own private key into the *Secure Element* of the device. To import a key, a special license must be purchased from Balluff Sales: The key update ticket.

3.8 Display elements

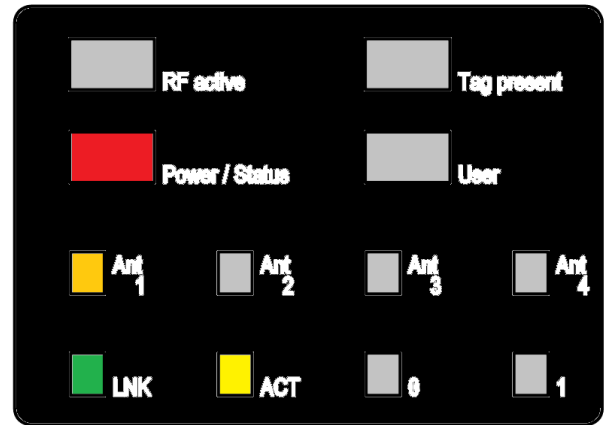


Fig. 3-3: Display elements

BIS U status

LED	Color	Meaning
RF active	Off	Antennas Ant1...Ant4 inactive
	Blue	Active communication via one of the antennas Ant1...Ant4
Tag present	Off	No data carriers in the detection range of Ant1...Ant4
	Yellow (3 s)	Min. 1 data carrier detected in the detection range
Power/status	Off	No supply voltage
	Red	Not ready for operation (see chapter 7.4 on page 85)
	Yellow	When switching on: Supply voltage present During operation: Warning status present (see chapter 7.4 on page 85)
	Green	Operational
	Green flashing (1 s)	Boot mode
User	Off, Red, Yellow, Green	Freely programmable via OPC UA
Ant1 ... Ant4	Off	Antenna port inactive
	Yellow	Antenna port active

3

Product description (continued)

Ethernet TCP/IP status

LED	Color	Meaning
LNK (Link)	Off	No LAN connection
	Green	LAN connection
ACT (Activity)	Off	No data transmission
	Yellow, flashing	Data transfer

IO-Link status

LED	Color	Meaning
0	Off	Status of the input/output is 0
	Yellow	Status of the input/output is 1
	Green	IO-Link communication active
	Green flashing (1 sec)	No IO-Link communication or incorrect IO-Link device
	Green flashing (fast)	IO-Link preoperate during data storage
	Red	IO-Link short circuit/sensor supply short circuit/firmware update
	Red flashing	Validation failed/incorrect configuration of IO-Link data length/self-test after power-on
1	Off	Status of the input/output is 0
	Yellow	Status of the input/output is 1
	Red	Short circuit at output

3.9 Ethernet TCP/IP

The TCP/IP interface complies with the Ethernet standard according to IEEE 802.3-2008 (up to 1 Gigabit) and supports the following transmission modes:

- 1000BASE-T
- 100BASE-TX
- 10BASE-T

The processor unit can be integrated into a local area network (LAN) via the Ethernet interface. A web server provides various functions for startup and parameterization.

i The Ethernet cable should be at least category 5e according to EIA/TIA-568 to ensure data security of the Ethernet transmission. The maximum cable length must not exceed 100 m. For longer cable distances, the use of repeaters is recommended.

3.10 OPC UA

The BIS U-6127 can communicate via the OPC UA data exchange standard. This standard uses the Ethernet interface as the physical basis (see chapter 3.9 on page 13). All physical properties of the Ethernet CP/IP interface also apply to the OPC UA standard.

OPC UA methods allow reading and writing of process data as well as setting and parameterization of a wide variety of UHF parameters.

The advantage of the OPC UA industrial communication standard is that not only special users can operate the interface, but any OPC UA-capable machine can establish communication with the BIS U-6127 based on the data model (machine-to-machine communication).

The OPC UA protocol used here is based on the *Companion Specification for AutoID*, published by AIM Germany and the OPC Foundation.

For a detailed description of the data model with all supported methods see chapter 9 on page 132.

3.11 IO-Link master

IO-Link is defined as a standardized point-to-point connection between sensors/actuators and the I/O module. Via the IO-Link interface, sensors and actuators can transmit further communication data in addition to the binary process signals (e.g. diagnostic signals).

The IO-Link interface is also suitable for connecting an external signal lamp (e.g. a Smart Light – LED signal tower).

Compatibility with standard I/O

- IO-Link sensors/actuators can be connected to existing I/O modules.
- Sensors/actuators that are not IO-Link-capable can be connected to an IO-Link block.
- Standard cables can be used for sensors/actuators

Key technical data

- Serial point-to-point connection
- Communication as an extension to the standard I/O
- Standard I/O connection technology, unshielded, cable length max. 20 m
- Communication by 24 V pulse modulation, standard UART protocol

Standard IO mode

- IO-Link-capable devices are parameterized via the IO-Link interface and then set to SiO mode.
- From this point on, the IO-Link port pin functions as a simple switching input that provides a binary signal.

i Further information on available IO-Link devices and accessories can be found on the Internet at **www.balluff.com**.

3

Product description (continued)

3.12 UHF data carriers (not included in scope of delivery)

The processor unit supports UHF data carriers according to ISO 18000-63 and EPCglobal™ Class1 Generation2.

Important fundamentals on memory banks and their protection status are stated below. More in-depth information on the function of UHF data carriers can be found in the UHF RFID standards mentioned above.

The memory organization of UHF data carriers provides for different memory areas (memory banks) depending on the design:

- Reserved
- EPC
- TID
- USER

i The allocation and the size of the respective memory banks can be found in the data sheet of the data carrier used.

The EPC and USER memory areas (if available) are available to be edited freely.

The TID memory bank is read-only.

The reserved memory area is intended for passwords. An access password and a kill password can be stored in it (see *Lock* and *Kill* commands).

The access password allows reading or writing to memory areas whose protection status requires a password.

The security status for the two passwords in the reserved memory bank can be set individually as follows:

Operation	Unlock	Lock	Unlock Permanent	Lock Permanent
Read	Allowed	Access password	Allowed	Locked
Write	Allowed	Access password	Allowed	Locked
Status reversible	Yes	Yes	No	No

The security status for the EPC, TID and USER memory banks can be set as follows:

Operation	Unlock	Lock	Unlock Permanent	Lock Permanent
Read (EPC, TID, USER)	Allowed	Allowed	Allowed	Allowed
Write (EPC, USER)	Allowed	Access password	Allowed	Locked
Status reversible	Yes	Yes	No	No

i Details on the different memory banks and the *Lock* and *Kill* functions can be found in the UHF RFID standards ISO/IEC 8000-63 and EPCglobal™ Class-1 Generation-2.

4

Installation

4.1 Selection of the installation location

When selecting the installation location, make sure that the surface underneath has sufficient load-bearing capacity and that there is sufficient space for the cable outlets on the plug sides of the processor unit. The permissible bending radius of the cables used should be taken into account.

The device should be mounted as close as possible to the place of use, as the UHF antenna cables are limited in length.

To prevent malfunctions or injuries, the device must be firmly mounted. The mounting location should be as low-vibration, temperature-stable and protected from shocks as possible.



Mounting plates and brackets as well as other mounting accessories can be found at www.balluff.com.

Four slotted holes for M5 screws are provided for mounting the processor unit. These are located at the corners of the housing frame in the area of the front plug panels.

4.2 Mounting the processor unit

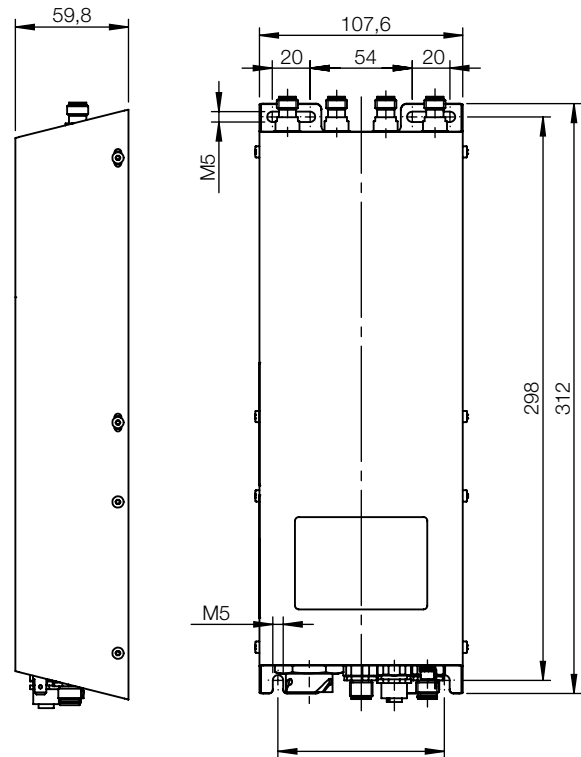


Fig. 4-1: Installation

1. Select a suitable installation position.
2. Fasten processor unit with 4 M5 screws (property class 8.8, lightly oiled, tightening torque $M = 5.2 \text{ Nm}$).

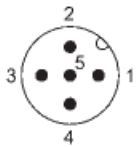
4

Assembly (continued)

4.3 Pin assignments

Power

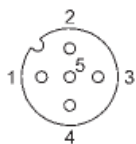
Plug, M12, 5-pin, A-coded



Pin	Description	Function
1	+24V DC	Supply voltage
2	Not used	None
3	GND	Ground
4	Not used	None
5	Not used	None

IO-Link

Socket, M12, 5-pin, A-coded



Pin	Description	Function
1	L+	Supply voltage (output)
2	I/O	Input/Output
3	L-	Ground
4	C/Q, I/O	IO-Link or input/output
5	Not used	None – do not connect!

Service (USB)

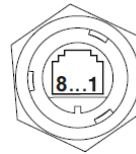
Plug M12, 5-pin, B-coded



Pin	Description	Function
1	+5V	Supply voltage (input)
2	D-	Bidirectional data line -
3	D+	Bidirectional data line +
4	GND	Ground
5	Shield	Cable shielding

Ethernet TCP/IP

Socket, RJ-45, 8-pin



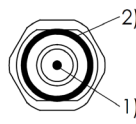
Pin	Description	Function
1	DA+	Bidirectional data A+
2	DA-	Bidirectional data A-
3	DB+	Bidirectional data B+
4	DC+	Bidirectional data C+
5	DC-	Bidirectional data C-
6	DB-	Bidirectional data B-
7	DD+	Bidirectional data D+
8	DD-	Bidirectional data D-



The Ethernet cable should be at least category 5e according to EIA/TIA-568 to ensure data security of the Ethernet transmission. The maximum cable length must not exceed 100 m. For longer cable distances, the use of repeaters is recommended.

Antennas 1...4

Socket, TNC reverse



Pin	Description	Function
1	RF	UHF-Signal
2	GND	Ground



To connect the UHF antennas to the antenna ports of the processor unit, coaxial cables with the plug configuration *Plug TNC Reverse / Plug TNC* are required.

4

Assembly (continued)

4.4 Mounting of the UHF antennas (not included in scope of delivery)

When selecting the installation location, care must be taken to ensure sufficient distance from workplaces where people are permanently present.



CAUTION

Ultra high frequency electromagnetic waves

The antennas of the identification system BIS U transmit ultra-high frequency electromagnetic waves. Additional measures must be taken to prevent health hazards.

- ▶ Determine the mounting position of the antennas in such a way that a safety distance of at least 20 cm between the antennas and workplaces of persons is ensured.
- ▶ Use suitable measures to shield areas that are explicitly not to be covered.

For details on mounting the antennas, see the data sheet of the antenna used.

Align the antennas so that the main beam direction of the antenna is aligned with the location where data carriers are to be detected. The maximum size of the detection range depends on the transmitting power and the aperture angle of the antenna. Larger detection ranges (such as gateways) may only be completely covered by using several antennas.

To ensure the proper functioning of the identification system, the detection range of the antenna and, in particular, the line of sight between the antenna and the data carrier must be free of electromagnetically effective materials (e.g. metal, liquids,...), as these can influence the detection range of the antenna and reduce the maximum range of the RFID system or make it more difficult to detect data carriers.

Areas that are explicitly not to be covered must be shielded by suitable measures.

4.5 Mounting of the UHF data carriers (not included in scope of delivery)

For details on mounting the data carriers, see the data sheet for the data carriers used.

When mounting data carriers, it should be noted that electromagnetically effective materials in the immediate vicinity of the data carrier can reduce the maximum range of the RFID system or make it more difficult to detect data carriers. This applies, for example, when mounting data carriers on metallic surfaces or containers with electromagnetically effective contents (e.g. metal, liquids,...).

Information about whether mounting on metallic surfaces is permissible can be taken from the data sheet of the data carrier. If necessary, suitable spacers must be used.

A high data carrier density also makes identification difficult, e.g. if the data carriers are only a short distance apart or overlap.

5

Technical data

5.1 Dimensions

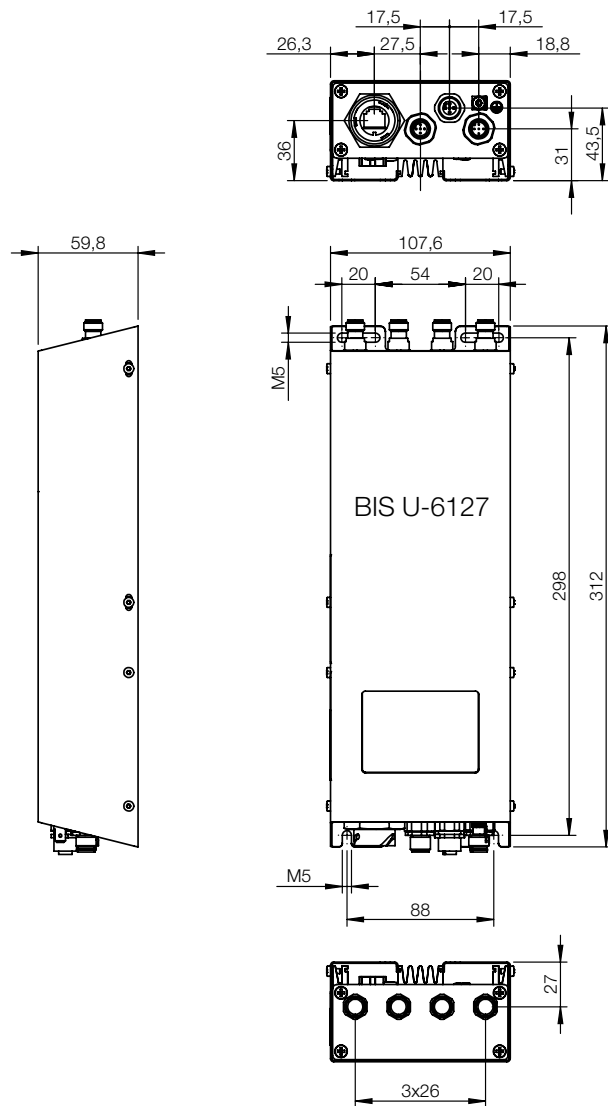


Fig. 5-1: Dimensions (mm)

5.2 Mechanical data

Housing material	Coated steel, anodized aluminum
Dimensions (L x W x H)	312 x 108 x 60 mm
Product weight	Approx. 2050 g
X1 Power	M12 integral plug, 5-pin, A-coded
X2 IO-Link	M12 panel socket, 5-pin, A-coded
X3 Service	Integral plug M12, 5-pin, B-coded
X4 Ethernet TCP/IP	RJ-45 panel socket, 8-pin
1...4 antenna ports	TNC-R integral plug

5.3 Electric data

Power supply VS	+24 V DC $\pm 20\%$ (LPS Class 2)
Residual ripple	5 %
Current consumption without load	1 A
Maximum current consumption	3 A
Interfaces	Ethernet TCP/IP / OPC UA IO-Link master USB (Service)

i The processor unit and connected accessories may only be operated with limited power according to UL 61010-1 Third Edition, Sub. Clauses 9.4 or LPS according to UL 60950-1 or Class 2 according to UL 1310 or UL 1585.

NOTICE

Exceeding the maximum current consumption

If the maximum current consumption is exceeded, the processor unit and connected system components may be damaged.

- During operation, make sure that the total current carried by the Power terminal does not exceed 3 A.
- The voltage output (L+) on the IO-Link port and digital outputs (I/O) are supplied via the Power connection. The sum of the partial currents of these pins, must not exceed a maximum current of 2 A.

5

Technical data (continued)

5.4 Ambient conditions

Operating temperature	–20...+55 °C
Storage temperature	–20...+60 °C
Vibration/shock	EN 60068 part 2-6/27
Degree of protection as per IEC 60529	IP65

5.5 Connectors ANT1...ANT4

Characteristic impedance	50 ohms
Output power max.	1.4 W (31.5 dBm) or 1 W (30 dBm), depending on country variant

5.6 IO-Link connection

IO-Link revision	1.1
Power supply for IO-Link, I/O modules (output)	VS – VD (VD = 0.5...3 V, load-dependent) 1.7 A max. (protected by overcurrent shutoff)
Data rate (IO-Link)	
COM1	4.8 kBit/s
COM2	38.4 kBit/s
COM3	230.4 kBit/s
Pin 2/Pin 4 (I/O mode) Input/Output	VS – VD (VD = 0.5 V...3 V, load dependent) 2 A max.
Pin 4 (IO-Link mode)	C/Q IO-Link data transmission
Cable type	Unshielded, 4-wire ¹⁾
Cable length max.	20 m (in IO-Link mode)

¹⁾ When using IO-Link RFID read/write heads in electromagnetically disturbed environments, the use of shielded cables is recommended.

NOTICE

Exceeding the maximum current consumption

If the maximum current consumption is exceeded, the processor unit and connected system components may be damaged.

- ▶ During operation, make sure that the total current carried by the Power terminal does not exceed 3 A.
- ▶ The voltage output (L+) on the IO-Link port and digital outputs (I/O) are supplied via the Power connection. The sum of the partial currents of these pins, must not exceed a maximum current of 2 A.

5.7 Ethernet TCP/IP connection

Ethernet standards according to IEEE 802.3-2008 (up to 1 Gigabit)	10BASE-T 100BASE-TX 1000BASE-T
Protocol	TCP/IP OPC UA
Data rate max.	10/100/1000 Mbit/s
Cable types	CAT3 (only 10BASE-T) CAT5
Cable length max.	100 m



The use of repeaters is recommended for data transmission over longer distances.

5.8 Service connection (USB)

USB version	2.0
Data rate max.	480 Mbit/s
Cable type	Shielded, 5-wire
Cable length max.	5 m

5.9 Data carrier

ISO	18000-63
EPCglobal™	Class 1 Generation 2
Multi-tagging (maximum number of data carriers)	500

5.10 Display elements at a glance

RF active	Blue
Tag present	Yellow
Power/Status	Red, Yellow, Green
User	Red, Yellow, Green
Antenna 1...Antenna 4	Yellow
Link	Green
Activity	Yellow
IO-Link 0	Red, Yellow, Green
IO-Link 1	Red, Yellow



For a detailed description of the display elements, see chapter 3.8 on page 12.

5

Technical data (continued)

5.11 Time and date

Buffering of time in case of power failure	> 2 days (with fully charged storage capacitor)
Charging time of storage capacitor	8 h
Automatic system time	Network Time Protocol Version 4

6

Application planning

6.1 General operating conditions

The BIS U-6127 can be used in many locations. The IP65 housing and the ambient temperature range of –20...+55 °C make it robust against environmental influences.

For details on mounting and planning the installation location, see chapter 4 on page 15.

6.2 Antenna configurations

Up to four antennas can be connected to the BIS U-6127 device (for mounting of antennas see chapter 4.4 on page 17).

The four antennas can be divided as desired into individual detection ranges and serve these individually, or they can be operated in combination. For example, antenna 1 can monitor a position on a conveyor belt before processing, antenna 2 another position after processing, and antennas 3 and 4 together monitor a gateway.

When aligning the antennas, the application environment must be considered first and foremost. The detection range in which data carriers are located must be precisely defined at the beginning. Then the antennas must be mounted in such a way that the best possible *illumination* of the detection range with the antenna beams is ensured.



If the desired detection range is small and precisely defined (e.g. an area of 30 x 30 x 30 cm), *one* antenna may be sufficient.

If a gate application with varying data carrier positions is to be covered, several antennas are required.

If possible, avoid metallic structures in the detection range or in the immediate vicinity. Metal surfaces shadow the region behind them. Flat metal surfaces can change the beam direction of the radio waves by reflection and lead to cancellation or over-coverage due to superimposition.

The antenna beams may or should overlap in order to avoid *holes* in the detection range. If several antennas are used, it does not matter whether they are arranged next to each other, at an angle or opposite each other. The only focus of the antennas must be on the detection range.

The transmitting power can be used to control the range of the antenna. The ranges also depend on the type of data carrier used. The maximum read ranges are usually significantly greater than the maximum ranges for writing to data carriers. In part, this can be compensated for by specifying a write add-on (targeted increase in power) in the parameter settings.

Another aspect of the antenna configuration is the movement speed of the data carriers. If only the EPC of a data carrier has to be detected and no further data has to be read and written on the tag, then the detection range in the direction of movement can be selected to be smaller, since the process is possible in a shorter time.

If data carriers move relatively quickly through the antenna field and further data must be read or written on the tag, the antennas must be arranged in such a way that the data carriers stay in the antenna field as long as possible, for example, to write the data completely to the data carriers.

The antenna settings can be parameterized in different ways:

- in the UHF Manager
- on the web server of the device
- via the 007 command set
- via the OPC UA commands

For more information, see chapter 7.3 on page 49.

6.3 Data carrier selection

Correctly selected data carriers contribute a great deal to the success of the application. When selecting data carriers, the following factors must be taken into account:

1. Memory size

If only the EPC has to be read for this application, data carriers with a small memory size (user memory) are sufficient. However, if several process data items need to be written to a data carrier, the minimum memory size of a data carrier must be defined.

2. Ambient conditions

The environment of the data carrier plays a decisive role for the function of the entire application. If neither moisture nor mechanical stress is relevant, inexpensive *label* data carriers can be used. If the data carrier comes into contact with moisture, a data carrier with protection class IP67 (or higher) must be used. The main distinction between data carriers, however, is the medium on which the data carrier is mounted. If data carriers have to be mounted on metal, the use of *on-metal tags* must be checked (see chapter 4.5 on page 17).



On-metal tags generally have poorer UHF performance (especially in read/write range) than comparable standard tags.

Every UHF application must be configured in such a way that the data carriers are detected reliably. This applies in particular to the arrangement of the antennas and the position of the data carriers on the goods to be detected.

3. Read/write range

A decisive factor in UHF application planning is the read/write distance, i.e. the distance between the data carrier and the antenna.

6

Application planning (continued)



Since large data carriers can accommodate a larger receiving antenna in their housing and thus extract more electrical energy from the electromagnetic field, their range is also greater than that of small data carriers (with comparable other parameters).

For each application, the selection of the data carrier must be carefully matched to the environmental conditions. The configuration of the overall system should always be designed for maximum process reliability.



Suitable data carriers for a wide range of applications can be found at www.balluff.com.

6.4 UHF properties in practice

Orientation of data carrier to antenna (polarization)

Balluff offers a variety of antennas for the BIS U-6127 device. The antennas offered differ not only in their size, range and frequency band (FCC or ETSI) but also in their polarization.

There are linear-polarized and circular-polarized antennas. With circular-polarized antennas, it does not matter whether the data carrier is aligned horizontally or vertically to the antenna. The data carrier is detected in all orientations.

With linear-polarized antennas, the data carrier must be aligned identically to the antenna – horizontally or vertically (the alignment of the antenna is marked on the antenna housing). An advantage of linear-polarized antennas is more accurate detection. They can be used if the position of the data carriers is precisely defined.

Field strength and distance

In theory, the decrease in electric field strength is inversely proportional to the distance from the antenna ($1/x$). A data carrier requires a typical minimum field strength to be detected. The data carrier can be detected until this minimum field strength is undershot, but it can no longer be detected at greater distances. However, this behavior can only be reliably reproduced in homogeneous laboratory environments.

In practice, the emitted electromagnetic waves of the antenna are reflected by various objects in the room. At different distances from the antenna, local maximums or minimums of the field strength can occur due to superimposition of several waves. The field strength as a function of distance is no longer steadily decreasing.

This has the following effect:

If you move the data carrier away from the antenna, it will no longer be detected after a certain distance. If you move the data carrier a little further away from the antenna, the data carrier can suddenly be detected again. These *holes* in the limit distance are due to the inhomogeneous electromagnetic field. Operation of the UHF system at the limit distance should therefore be avoided.

The following also applies:

Doubling the range requires approximately four times the transmitting power. In the unit of dBm, this means that the transmitting power must be set 6 dBm higher. The reception direction of the wave from the tag to the antenna can also reach its limits, but this cannot be readjusted.

Penetration of electromagnetic wave

One advantage of UHF RFID systems over optical readers is their ability to penetrate opaque materials. The electromagnetic waves of the UHF spectrum penetrate paper and cardboard without significant losses. Likewise, most plastics can be penetrated to read or write to the data carriers behind them.

The penetration of the UHF waves is subject to a natural limit due to the physics involved. If the absorption or reflection of the UHF waves is too great, the corresponding medium cannot be penetrated. This occurs mainly with conductive materials such as steel sheets or aluminum plates. If a data carrier is located behind a steel plate, it cannot be reached by the BIS U-6127 device. This is also referred to as shadowing of a data carrier.

Between total shadowing and free visibility between antenna and data carrier, there are still numerous intermediate stages in which media penetration is limited.

One example of this is ESD containers. Plastic containers that are slightly conductive to prevent electrostatic charging. Data carriers in these containers are only visible to the antenna to a limited extent. Tests must be carried out here in the application planning stage.

A second example of more difficult penetration of electromagnetic waves is moisture. Water is conductive depending on its purity and absorbs UHF waves very strongly due to its polar structure. Other liquids behave differently, the range varying from almost neutral to complete shadowing.

Any application planning process should be approached with this background knowledge in mind, e.g. for applications that are to detect goods that have been exposed to the weather. Wet cardboard boxes can make reading and writing the data carriers inside much more difficult. The transmitting power of the BIS U-6127 should not be set too low for such applications. A certain transmitting power reserve should be allowed for.

To set up the initial transmitting power, the *AutoSetup* function can be used.

SingleTag or MultiTag operation

There are three states that can occur in the detection range in front of the antenna:

- No data carriers
- One data carrier
- Multiple data carriers

The data carriers present in the detection range are detected during an *Inventory* (e.g. *Scan* command), entered in a tag list and, if necessary, transmitted to the application.

If there is only one data carrier in the detection range of the antenna, data can be written to or read from the data carrier immediately. This operating state is called *SingleTag mode*.

If there are several data carriers in the detection range of the antenna, the tag list must be evaluated. Before data can be written to or read from a data carrier, a data carrier must be selected (*Select* command). Data can only be read or written after the data carrier has been selected.

Exceptions are *BulkRead* and *BulkWrite* commands, which perform all these steps for each tag, and *ReadMultipleTagDataFormatted* and *UniversalTagList* commands, respectively.

Typical access times to data carriers (default setting: RX: 160/40 kbps; TX: 40 kbps) are shown in the following table. The times given are examples and vary statistically. They also depend on other settings, in particular the initial *Q-value*.

Number of data carriers	Measured time until an inventory command is processed [ms]
1	109
3	129
7	180
10	219
20	371
31	508
52	891
71	1273
87	1590
100	1879
111	2168
119	2352

Access time to a data carrier



The access time described here refers to the amount of time that elapses during the execution of an inventory command.

The elapsed time until the BIS U-6127 can access data carriers depends primarily on two factors:

1. If a high-speed Miller 2 coding (RX: 320/160 kbps; TX: 80 kbps) is used, the access time is about 29% shorter than with the standard Miller 4 coding (RX: 160/40 kbps; TX: 40 kbps). However, the reliability declines and, in addition, high-speed codings are not permitted in all countries.
2. The number of data carriers in the detection range of the antenna is more important. If there is only one data carrier in front of the antenna, the duration of an *Inventory* command is the shortest. If, for example, there are 10 data carriers in the detection range, the access time can take twice as long.

Bulk application

If several data carriers are to be reliably detected during a scan, the antenna power must be increased compared to reading individual data carriers. This also works if the data carriers are moving at low speed.

With a clever antenna arrangement and the evaluation of multiple scans, it is possible to detect all data carriers in a bulk application.

Using the loop filter (see page 25) can significantly increase the reliability of an application.

6.5 Operating modes

The BIS U-6127 processor unit supports multiple operating modes to establish optimal integration into your control or IT environment:

- Synchronous operation
- Asynchronous operation (with loop filter)
- Synchronous operation with loop filter, *live* or *cumulative* mode
- Autonomous operation

The operating modes refer to the detection of single or multiple data carriers and the readout of data. They differ in how much automatic pre-processing the device is to perform and whether the data read from the data carriers are to be retrieved by the device or provided unprompted.

Writing data to data carriers is always done in synchronous mode.

6

Application planning (continued)

Synchronous operation

This operating mode enables direct control of when and which actions are performed on the air interface with the data carriers. A search for data carriers or a read command is started when a corresponding command is sent via 007 or an OPC UA method is called. The read data are made available to the controlling device immediately after successful processing.

Commands for synchronous operation:

Command	007 protocol	OPC UA
Detect data carriers	<i>GetMultipleTags</i> command <i>GetMultipleTagsExtended</i> command	<i>Scan()</i> method
Read single carrier	<i>Read</i> command <i>ExtendedRead</i> command	<i>ReadTag()</i> method
Detect data carrier and read any data, user-defined output	<i>UniversalTagList</i> command	<i>ReadMultipleTag-DataFormatted()</i> method
Read single data carrier, user defined output	<i>UniversalTagRead</i> command	<i>ReadFormatted-TagData()</i> method

The parameters and return values of the commands and methods can be found in the respective command descriptions.

i If several commands are requested simultaneously via different interfaces, delays may occur in the execution of the command. The device will process these one after the other.

i The functions for searching for UHF data carriers use statistical methods. The processing speed of the commands can therefore not always be calculated exactly for UHF data carriers and may vary from execution to execution.

Asynchronous operation

In this operating mode, the device searches independently for data carriers at adjustable intervals. If new data carriers are found, an *event* is generated, i.e. the controlling device is informed with a message without further action:

- 007: With a spontaneous telegram
- OPC UA: With the triggering of an event

Commands for asynchronous operation:

Command	007 protocol	OPC UA
Start data carrier detection	Set parameter 1006 _{hex} to the value 3 (if only <i>Tag comes</i> messages are desired) or to the value 7 (if both <i>Tag comes</i> and <i>Tag goes</i> should be signaled).	<i>ScanStart()</i> method
End data carrier detection	Set <i>abort</i> command or parameter 1006 _{hex} to the value 0.	<i>ScanStop()</i> method
Notification about new data carriers	<i>Tag comes</i> telegram	<i>RfidScanEvent-Type</i> event
Notification about data carriers no longer found	<i>Tag goes</i> telegram (optional)	not possible
Scan cycle time (pause between 2 scans), global parameter	Parameter 100C _{hex} (value range 1...255 = 10 ms...2.55 s)	Parameter 100C _{hex} (value range 1...255 = 10 ms...2.55 s) via UHF Manager <i>Asynchronous Scan Loop Time</i>

The parameters and return values of the commands and methods can be found in the respective command descriptions.

i In asynchronous mode, the loop filter (see chapter *Loop filter* on page 25) is always in effect with its parameters.

i Asynchronous operation is inactive after a device restart.

6

Application planning (continued)

Loop filter

The loop filter allows stabilization of the list of found data carriers by combining several readings. This way, incorrect readings can be corrected or the results of several searches can be combined in one list.

The loop filter sets the following parameters:

- *Minimum number of successful reads*: How many times a tag must be successfully detected or read in succession for it to be reported as detected/read to the controlling device.

- *Number of non-reads*: How many times a tag must be searched for unsuccessfully in succession before it is reported to the controlling device as no longer present.
- *Waiting time*: The length of time that a tag, after disappearing from the antenna reading field, is ignored before a new detection of the tag can be reported (provided that the condition *Minimum number of successful reads* is met).

Fig. 6-1 illustrates the mode of operation of the filter:

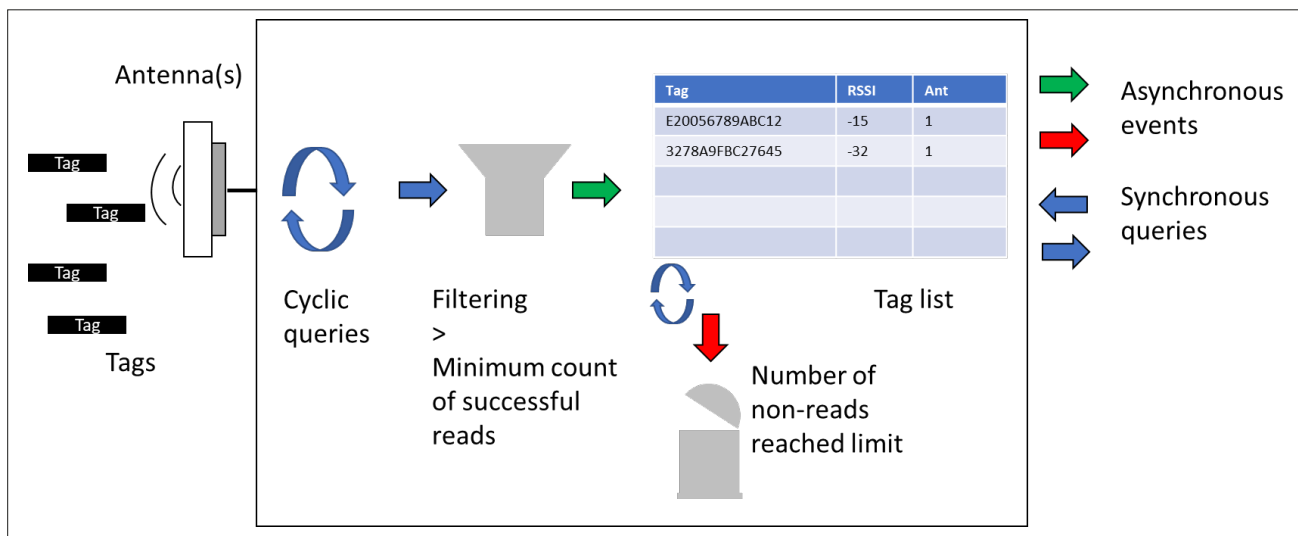


Fig. 6-1: Loop filter mode of operation

The parameters of the loop filter can be set for the current connection as follows:

Parameters	007 protocol	OPC UA
Parameter <i>Minimum number of successful reads</i>	Parameter 100C _{hex} (value range 1...255 scans)	<i>SetASyncFilter()</i> – Method ¹⁾
Parameter <i>Number of non-reads</i>	Parameter 100D _{hex} (value range 1...255 scans)	<i>SetASyncFilter()</i> – Method ¹⁾
Parameter <i>Waiting time</i>	Parameter 100E _{hex} (value range 0...1000 s)	<i>SetASyncFilter()</i> – Method ¹⁾
Scan cycle time (Pause between 2 scans), Global parameter	Parameter 100C _{hex} (value range 1...255 = 10 ms...2.55 s)	Parameter 100C _{hex} (value range 1...255 = 10 ms...2.55 s) via UHF Manager <i>Asynchronous Scan Loop Time</i>

¹⁾ To read out the set parameters, the *GetASyncFilter()* method can be used.

The parameters 0023_{hex}, 0024_{hex} and 0029_{hex} define the respective default values for new connections for both 007 and OPC UA. The defaults can also be set via the UHF Manager.



The loop filter and asynchronous operation currently only support data carrier detection with EPC output. Scanning with output of TID values in combination with the loop filter or in asynchronous detection mode is currently not supported.

6

Application planning (continued)

Loop filter in asynchronous mode

In asynchronous mode, the loop filter is active immediately. An event for a new tag is triggered when the condition *Minimum number of successful reads* is met. An event for a tag that is no longer found is only triggered when the *Number of non-reads* is exceeded.

Loop filter in synchronous mode

In synchronous mode, the loop filter can be used as follows:

- *Live* mode: Scans and filter operation are performed in the background, query of the current data carrier list (after filtering) via the normal synchronous commands. The mode is suitable for continuously repeated queries in short intervals.
- *Cumulative* mode: Scans and filter operation take place in the background, query of all newly found data carriers (including those that have left the antenna read field again in the meantime) via the normal synchronous commands. The mode is suitable for obtaining a complete list of data carriers via triggered or occasional queries (e.g. in a gate application).

In addition to the actual filter function, the combination of the loop filter and synchronous operation has the following advantages:

- The responses to synchronous commands and method calls occur almost without any waiting time, since the actual data carrier search runs independently of this in the background.
- The application on the controlling device can determine when it wants to fetch the results of the data carrier search without the risk of losing results, as they can be collected and cached (accumulated) in the device.

The loop filter can be used in synchronous mode as follows:

Live mode

Command	007 protocol	OPC UA
Start data carrier detection with loop filter, <i>Live</i> mode	Set the parameter 1006 _{hex} to the value 1	<i>ScanStart()</i> method
Read data carrier list <i>Live</i> mode	<i>GetMultipleTags</i> command <i>GetMultipleTagsExtended</i> command	<i>Scan()</i> method
Read data carrier list <i>Live</i> mode and read any data, user-defined output	<i>UniversalTagList</i> command ¹⁾	<i>ReadMultipleTagDataFormatted()</i> method ¹⁾
Output the current number of tags in the data carrier list	<i>GetTagCount</i> command	<i>Scan()</i> method
End data carrier detection with loop filter	<i>Abort</i> command or set parameter 1006 _{hex} to the value 0.	<i>ScanStop()</i> method

¹⁾ The formatted output can only be used if only EPC data and status values are to be output, since data carriers may no longer be in the read field of the antennas at the time of the query and further data may then no longer be available and thus an output is then not carried out.

Cumulative mode

Command	007 protocol	OPC UA
Start data carrier detection with loop filter, <i>cumulative</i> mode	Set the parameter 1006 _{hex} to the value 9	Not possible
Read data carrier list <i>Cumulative</i> mode	<i>GetMultipleTags</i> command <i>GetMultipleTagsExtended</i> command	Not possible
Read data carrier list <i>Cumulative</i> mode and read any data, user-defined output	<i>UniversalTagList</i> command ¹⁾	Not possible
Output the current number of tags in the data carrier list	<i>GetTagCount</i> command	<i>Scan()</i> method
End data carrier detection with loop filter	<i>Abort</i> command or set parameter 1006 _{hex} to the value 0.	<i>ScanStop()</i> method

¹⁾ The formatted output can only be used if only EPC data and status values are to be output, since data carriers may no longer be in the read field of the antennas at the time of the query and further data may then no longer be available and thus an output is then not carried out.

6

Application planning (continued)

Autonomous operation

In autonomous mode, the device performs cyclical data carrier detections without the need to issue a command.

This operating mode is particularly suitable for applications that need to do without an additional controlling system or that are to detect individual data carriers only rarely.

Command	007 protocol	OPC UA
Start autonomous operation	Set the 000F _{hex} parameter to a value between 1 and 255 to set the scan interval in the range 10 ms...2.55 s. This setting and the autonomous operation are retained following a device restart and refer to the TCP channel from which the operation was started.	Call the <i>SetAutoScan()</i> method with a value between 1 and 65535 to set the scan interval in the range 1 ms...65 s. This setting and the autonomous operation are not retained following a device restart.
End autonomous operation	Set parameter 000F _{hex} to the value 0.	Call the <i>SetAutoScan()</i> method with a value of 0.
Receive scan data	<i>USB service interface:</i> No data output <i>Ethernet interface:</i> The data is always output on a separate TCP channel, depending on the 007 TCP channel via which operation was started. The behavior corresponds to a cyclically executed command. <i>Command identifier '-L': Detect data carrier, universal</i> (see page 122) without acknowledges. The parameters for head (antenna) selection and maximum tag number correspond to the last executed <i>UniversalTagList</i> command. If no such command has been executed since the device was started, the following default values apply: Head = 0 (all active antennas) Max. number of tags = Limited only by device	No automatic data output. The <i>LastScanData</i> variable displays the data of a data carrier if at least one was found. The <i>LastScanData</i> variable is shared by all OPC UA sessions. If several sessions are active at the same time, it is recommended to use the method <i>GetLastScanData()</i> , which returns session-related data. If automatic data output under OPC UA is desired, asynchronous operation is recommended.



Autonomous operation with 007 enables the device to cyclically detect data carriers directly after power-on without any further external influence and to report the results automatically to an external system via TCP.

6

Application planning (continued)

Mode	Device auto- matically scans for tags	Usable with			Formatted reading usable	2nd channel possible (007, for- matted)	2nd channel needed
		007 proto- col	OPC UA	Web inter- face			
Synchronous	–	+	+	+	+	+	–
Asynchronous (incl. loop filter)	+	+	+	–	–	–	–
Synchronous + loop filter, Live	+	+	+	–	+ ⁵⁾	+	–
Synchronous + loop filter, cumulative	+	+ ¹⁾	–	–	+ ⁵⁾	+	–
Autonomous operation	+	+ ^{2), 3)}	+ ⁴⁾	–	+	+	+

¹⁾ The cumulative mode can be set via the protocol, but not via the UHF Manager.

²⁾ The UHF Manager can start or stop autonomous operation. However, it cannot display the outputs of autonomous operation, since they take place on a 2nd channel.

³⁾ If a loop filter is required in autonomous operation, it must be reactivated after each device restart and autonomous operation must be reactivated.

⁴⁾ With OPC UA, autonomous operation must be reactivated after each device restart.

⁵⁾ If the loop filter is active, no values from the TID, password or user data area can be output in formatted output. Only data from the EPC bank (EPC, protocol control word) and status values can be output.

7.1 UHF Manager configuration software

The *Balluff UHF Manager* configuration software provides an easy way to start up the RFID system, test basic functions and make parameter settings before installation.

7.1.1 Install and start configuration software



The configuration software is available online at **www.balluff.com**.

Administrator rights may be required to install the software. The software is installed under the preset path (unless it is changed):

C:\Program Files (x86)\Balluff\UHF Manager

1. Start the installation wizard by double-clicking the installation file (UhfManagerSetup_version.msi) and follow the wizard instructions.
2. Double-click on the *Balluff.Uhf.UhfManager.exe* file in the installation directory to start the configuration software.

7.1.2 User interface

After connecting the processor unit via TCP/IP or USB (see chapter 7.1.3 on page 30), the main window is displayed as follows (see Fig. 7-1).

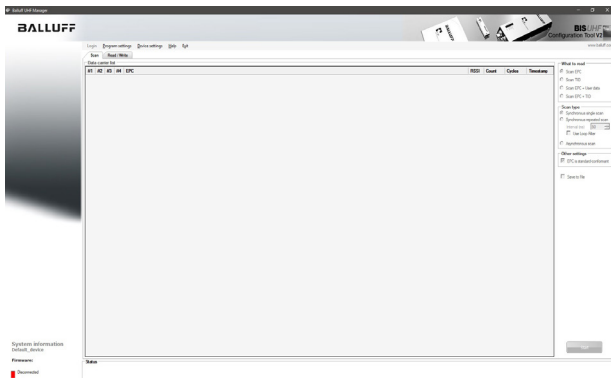


Fig. 7-1: Main window

RFID system information

The left window area displays the RFID system information for a connected BIS processor unit. This shows a schematic representation of the processor unit and provides information about the following:

- Type designation of the connected processor unit
- Firmware version of the processor unit
- Connection status of the interface used
- Currently selected antenna via the radio buttons 1...4 or ALL

Action area

The action area in the center of the window shows the data of the data carriers found in the active field of the antenna and provides the controls necessary to interact with a data carrier.

Status bar

The status bar below the action area shows the result of the last executed action.



Information on the operation of the UHF Manager is provided by the help function. This can be called up via the Help menu or by pressing the F1 key.

Menu

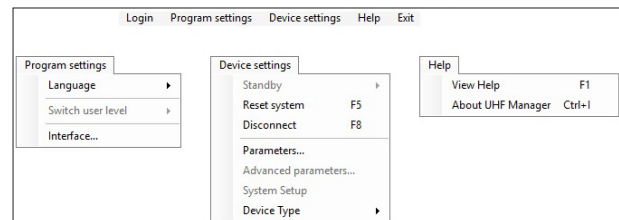


Fig. 7-2: Menu display

Login/Logout

The BIS U-6127 processor unit has password-protected security levels that allow different user groups to make more detailed settings on the device. The *USER/EXPERT/ADMIN* levels can be activated or deactivated via *LOGIN/LOGOUT*. Higher security levels can perform additional settings in the *DEVICE SETTINGS* menu item.

Users are automatically logged out of the system after a period of inactivity of 15 minutes and a new login is required. A new login must be performed after 24 hours at the latest.

Login (on delivery):

Security level	Username	Password
User	w/o	w/o
Admin (default)	admin_default	See type plate on the device



User roles and login data can be managed via user accounts (see *User accounts* on page 11 and *User Management* on page 45).

We recommend creating the following user roles:

Security level	Username	Password
Expert	expert	Freely definable
Administrator	admin	Freely definable

Program settings

- *LANGUAGE*
Switch menu language between German/English.
- *CHANGE USER LEVEL*
This menu item has been replaced by the Login area on the BIS U-6127 and is used only for compatibility with other processor units.
- *INTERFACE...*
Opens the window for the interface settings for RS232 / TCP/IP.

Device settings

- *SLEEP MODE*
Is not available when using the BIS U processor unit.
- *RESET SYSTEM* (F5 key)
Causes the BIS U processor unit to perform a restart. A previous login with administrator rights is required.
- *DISCONNECT/CONNECT* (F8 key)
Opens or closes the last used connection.
- *PARAMETERS...*
Opens the parameter window.
- *ADVANCED PARAMETERS...*
Opens the window for advanced parameters (area is password protected, see menu item *Change user level* on page 30).
- *SYSTEM SETUP*
Area is only accessible to Balluff service staff.
- *DEVICE TYPE*
Shows a list of supported devices and allows manual selection. Depending on the selected device, the user interface changes.

i This function is only intended for offline mode. The *DEVICE TYPE* is selected automatically when the connection is established.

Help

- *VIEW HELP* (F1 key)
Opens the help function for the configuration software
- *VIA UHF MANAGER* (Ctrl + I key)
Opens the window for user information
 - Software version of the configuration software
 - Contact details of Balluff GmbH

Finish

Closes the configuration software.

7.1.3 Interface settings

The *INTERFACE SETTINGS* allow the BIS U processor unit to be connected to a Windows™ PC via a TCP/IP connection. A service port (USB) is also available for maintenance or service functions, which can be connected via a virtual COM port.

TCP/IP connection

Open a TCP/IP connection:

1. Menu: Program settings > Interface...
⇒ The Interface Settings window opens.
2. Select the TCP/IP tab.

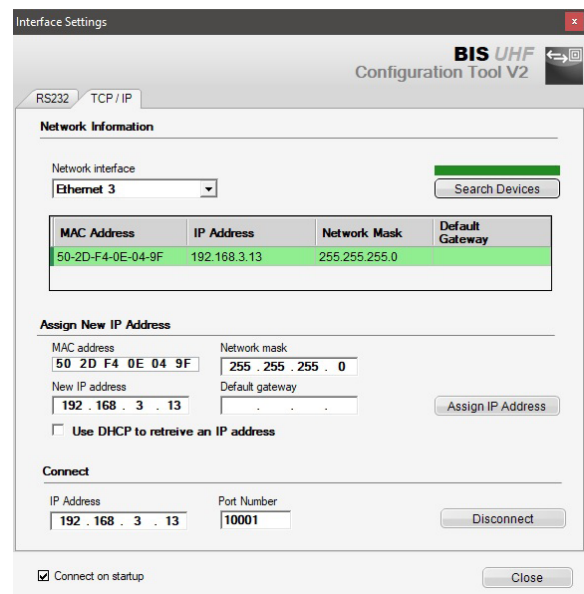


Fig. 7-3: Interface settings

3. Select the network adapter in the *NETWORK INTERFACE* pull-down menu.
4. Click the *BIS SEARCH* button.
⇒ BIS U processor units are searched for and listed in the table.
5. Select BIS U processor unit by clicking on the corresponding line.
6. *CONNECT/DISCONNECT* establishes or disconnects the TCP/IP connection.

In the *ASSIGN NEW IP ADDRESS* area, a new IP address or a new default gateway can be assigned to the device connected via TCP/IP or USB. Via the checkbox *USE DHCP*, the device can be switched to DHCP to automatically obtain an IP address.

i DHCP can only be used in a network that allows the dynamic assignment of IP addresses. This must be ensured before activating DHCP, otherwise it may no longer be possible to access the processor unit via the network. In an emergency, this setting can be reversed via the service port (USB). An M12-USB service cable is required for this (see chapter 10.3 on page 173).

USB connection (virtual COM port)

Open a serial connection via a virtual COM port:

1. Menu: Program settings > Interface...
⇒ The Interface Settings window opens.
2. Select tab RS232.
3. Select port through which the virtual COM port will be connected.
4. The serial connection is established via the *SEARCH* or *CONNECT* button.

i The installation of a driver (download at www.balluff.com) is required for the use of virtual COM ports.
An M12 USB service cable is required to connect the processor unit to the USB port of the PC. For cables and other accessories, see chapter 10.3 on page 173.

7.1.4 Detect data carriers

The *SEARCH TAGS...* button in the *DETECT* tab of the action area can be used to create a data carrier list that lists the data carriers that are within the detection range of the selected antenna.

1. Select the *DETECT* tab in the action area.
2. Select antenna via radio buttons *1...4* or *ALL* in the info area.
3. Click on *SEARCH TAGS...*
⇒ Data carriers in the detection range of the selected antenna are detected and entered in the list.

The data carrier list contains the following information:

- #1...#4: antennas (1...4) that have detected the listed data carrier
- *EPC/TID*: EPC or TID of the data carrier
- *RSSI*: Highest RSSI value measured when the data carrier was detected
- *COUNTER*: Counts how often the data carrier was detected in cyclical operation
- *CYCLES*: Counts the detection intervals in cyclical operation

i Right-click on a data carrier in the list to switch directly to the *READ/WRITE* tab. There, further interactions with the data carrier can be performed.

Data

In the *DATA* selection area, you can select which data (EPC or TID) should be entered in the list when detecting the data carriers.

i The length of the TID data field can be parameterized, see chapter 7.3 on page 49.

Detect

In the *DETECT* selection area, you can define the operating mode with which the data carrier detection is performed.

SYNCHRONOUSLY DETECT ONCE

Via the *SEARCH TAGS...* button, detection of the data carriers is carried out once. The data carrier list is cleared before each operation and filled with the new result.

SYNCHRONOUSLY DETECT REPEATEDLY

The *SEARCH TAGS...* button starts the data carrier detection and repeats it cyclically at the specified interval (ms). In the process, the data carrier list is continuously updated. New data carriers are added to the list. Data carriers that have left the detection range of the antenna are colored red. Cyclical detection continues until it is stopped via the *STOP* button.

The *USE LOOP FILTER* check box can be used to select whether the data carrier detection is to be performed according to certain specifications. These can be defined by various parameters (see chapter 6.5 on page 25).

ASYNCHRONOUSLY DETECT

The *ASYNCHRONOUS DETECTION* mode is started once via the *SEARCH TAGS...* button and runs until it is ended via the *STOP* button. After being started, the data carriers in the detection range of the active antenna are detected and entered in the list (only EPC possible). Data carriers that are newly detected are added to the list. Data carriers that leave the detection range of the antenna are removed from the list so that the list always reflects the current data carrier population.

i The loop filter and the asynchronous detection mode currently only support data carrier detection with EPC output.
Scanning with output of TID values in combination with the loop filter or in asynchronous detection mode is currently not supported.

7.1.5 Read/write data carrier

The *READ/WRITE* tab provides the functions for reading out and writing to data carriers. The desired action can be started via the *READ* and *WRITE* buttons. Before an individual data carrier can be processed, it must be detected in the *DETECT* tab.

Memory area via which the TAG is to be identified

The EPC and TID of the data carrier can be used to select an individual data carrier. An individual data carrier can be selected via the respective drop-down list.



Right-click on a data carrier in the list to switch directly to the *READ/WRITE* tab. There, further interactions with the selected data carrier can be performed.

ACCESS PASSWORD

By selecting the *ACCESS PASSWORD* check box, an input field appears in which an access password can be entered. This function is only intended for data carriers that are secured by an access password.

Which memory area should be processed?

Selection of the memory area to be read or written to. The *EPC*, *TID*, *RESERVED* and *USER DATA* areas are available for selection. Details on the memory areas and their size can be found in the data sheet of the data carriers used.

For the *EPC* and *TID* data, the *START ADDRESS* and *LENGTH* are fixed.

For direct access to the memory banks of *EPC*, *TID*, *RESERVED* as well as the *USER DATA* area, the *START ADDRESS* and *LENGTH* (number of bytes) can be defined via the input fields provided.

Memory area	Read	Write	Start address	Length
<i>EPC</i>	Yes	Yes	Fixed	Parameters
<i>TID</i>	Yes	No	Fixed	Parameters
<i>USER DATA</i>	Yes	Yes	<i>START ADDRESS</i> field	<i>LENGTH</i> field

Data

The data read out is displayed in the *DATA* field. The left area of the data field shows the start addresses of the individual lines. The middle area shows the data in hex format. The right area shows the ASCII representation of the data. Data to be written can be edited directly in the data field by keyboard input (in hex or ASCII format).

Manipulate data

For simple data values, the buttons *INCREMENT*, *DECREMENT*, *CONTINUOUS* and *FIXED VALUE* can be used. In the *START VALUE/VALUE* field, a start value for the *CONTINUOUS* function or a value for the *FIXED VALUE* function can be specified.

Load/save data

Via the buttons *OPEN* or *SAVE*, the hex data of the data field can be exported to a file (*.dat) or imported from a file.

7.1.6 Parameter setting

Depending on the active security level, various settings can be made under *PARAMETERS...* and *ADVANCED PARAMETERS...*

The meaning of the individual parameters and their assignment to the UHF Manager are described in chapter 7.3 on page 49.

The *SEND TO BIS* and *RECEIVE FROM BIS* buttons can be used to transmit the parameters to or read them from the processor unit.

The *SAVE AS...* and *OPEN...* buttons can be used to save the parameter sets in an xml file or to read them in from an xml file. This procedure simplifies the parameterization if several devices are to receive the same parameterization.

The *DEFAULT SETTINGS* button initially only resets the user interface to the values of the delivery state. The *SEND TO BIS* button can be used to transfer the parameters to the processor unit.

7.2 Web server

A browser (e.g. Google Chrome) is required to connect to the web server of the device via TCP/IP. In the address line, enter the IP address of the device preceded by "http://" and followed by "/" (e.g. http://192.168.10.2/).

The BIS U-6127 web server application provides an interface to access the device information. The device settings can be changed and adapted as required.

Fig. 7-4 shows the menu bar of the web server with seven main menus, which are described below.

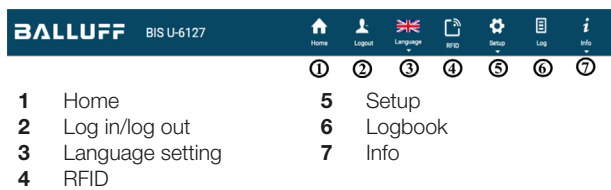


Fig. 7-4: Main menu

7.2.1 Home

Fig. 7-5 shows the home page of the web server application.

The interface is divided into two parts:

- On the left side there is device information (not changeable).
- On the right side the device is illustrated and shows the current state of the LEDs.

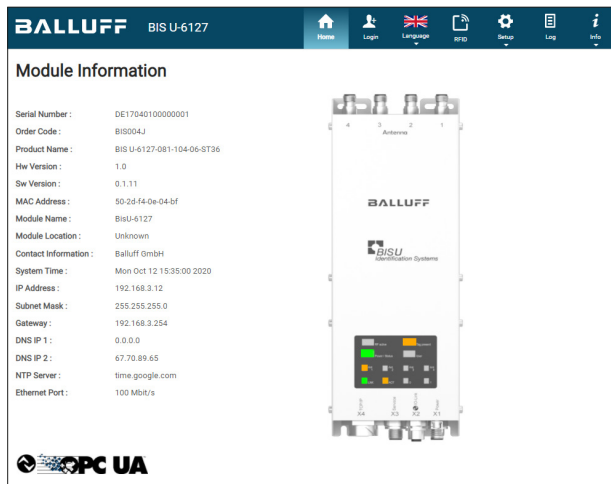


Fig. 7-5: Homepage

7.2.2 Log in/Log out

A majority of the display functions of the device websites also work without logging in. However, the *EXPERT* or *ADMIN* role is required to change many settings. It is then necessary to log in via the menu item *LOG IN*.

Logging in

1. In the *USERNAME* field, enter the name under which you want to log in to the BIS U-6127 device.
2. Under *PASSWORD*, enter the password valid for this user. By clicking on the eye icon next to the dialog box, the characters can be made visible.

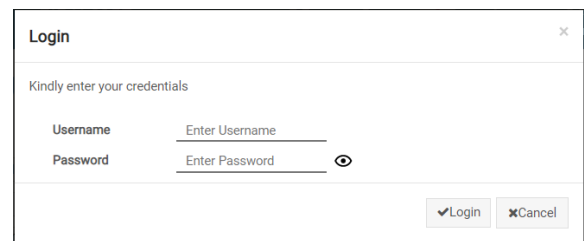


Fig. 7-6: Entry dialog for entering user name and password

Logging out

If the login was successful, the field (2) of the main menu shown in Fig. 7-4 displays the text *LOG OUT*.

Users are automatically logged out of the system after a period of inactivity of 15 minutes and a new login is required. After 24 hours at the latest, you must log in again.

Factory preconfigured users

At the first startup, certain standard user profiles are available on the system ex factory (see the following table).



The default settings should be changed during the first configuration for security reasons!

You can add your own users and provide them with appropriate permissions.

7

Startup and operation (continued)

These users and the corresponding passwords are summarized in the following table:

Name	Standard password	Description
user		Standard user without configuration permission. As a rule, mainly process data and additionally some settings are visible. No configuration is possible however. This is the default user level that each user automatically receives when accessing the BIS U web interface. Login is not required
admin_default	See imprint on the type plate	Administrative user who can configure any aspect of the device. To access this level, it is necessary to log in.

7.2.3 Language settings

There are two language settings for the BIS U-6127 configuration interface: German (default) and English.

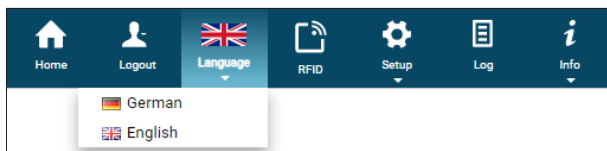


Fig. 7-7: Language settings

The language of the interface can be changed as follows:

- Open the language selection by clicking on the menu item *LANGUAGE* in the main menu and click on the desired language line (see Fig. 7-7).

7.2.4 RFID

Start scan, Read/write

The RFID menu can be called up via the main menu bar (see Fig. 7-4 on page 33).

EPC	Count	RSSI	Antenna
E2 00 90 51 32 05 01 72 22 80 2A F8	0	-29	1 ✓ 3
E2 00 90 51 32 05 01 71 23 90 20 37	0	-35	1 ✓ 3 ✓
E2 00 90 51 32 05 01 72 25 90 10 7F	0	-42	1 ✓ 3
E2 00 90 51 32 05 01 72 24 00 20 3C	0	-32	1 ✓ 3 ✓
E2 00 90 51 32 05 01 71 26 30 0D BB	0	-25	1 ✓ 3
E2 00 90 51 32 05 01 71 26 90 08 B9	0	-60	1 ✓ 3
E2 00 90 51 32 05 01 71 22 70 2A F3	0	-47	1 ✓ 3 ✓
E2 00 90 51 32 05 01 71 27 50 06 87	0	-32	1 ✓ 3
E2 00 90 51 32 05 01 72 26 50 0B 25	0	-43	1 ✓ 3 ✓
E2 00 90 51 32 05 01 71 25 00 16 67	0	-31	1 ✓ 3 ✓
E2 00 90 51 32 05 01 71 21 40 36 5E	0	-26	1 ✓ 3
E2 00 90 51 32 05 01 71 24 40 1C D8	0	-36	1 ✓ 3 ✓
E2 00 90 51 32 05 01 72 27 70 04 91	0	-34	1 ✓ 3 ✓
E2 00 90 51 32 05 01 71 15 40 75 B6	0	-44	1 ✓ 3 ✓

Download Taglist

info: Read Completed

Antenna Status

Antenna 1: On 27 dBm
Antenna 2: Off 27 dBm
Antenna 3: On 27 dBm
Antenna 4: Off 27 dBm

Update Interval: 2 Sec

Start Scan

Tag Parameters

Address: 0
Length: 10
Access Password: 00000000
EPC Bank (selected) User Data TID Bank

EPC Bank: E2 00 90 51 32 05 01 72 22 80 2A F8
User Data: 4F 9E 30 00 E2 00 90 51 32 05
TID Bank:

Write Data Read Data

a Scan list	f Password
b Antenna status	g Memory bank
c Update interval	h EPC of the selected data carrier
d Start address	i Data content at selected address and memory bank
e Length (byte)	

Fig. 7-8: RFID

On this page, tag operations like *START SCAN*, *WRITE DATA* and *READ DATA* can be performed (see Fig. 7-8).

On the right side, the *ANTENNA STATUS* (b) shows the globally active antennas and their powers. These values can be changed for tag scanning on this page. Furthermore, the *UPDATE INTERVAL* (c) shows the duration between two scans. The *ANTENNA STATUS* and the *UPDATE INTERVAL* can be changed to perform the desired scan.

On the left side of the page, the scan list (a) is created in tabular form with EPC, count (how many times the tag was scanned), RSSI and antenna (a selection sign represents each antenna that scanned the tag).

Input parameters for the tag read and tag write operations:

- The start address (d) from which the read/write must begin.
- Length of the bytes to be read (e).
- Password (f) to read/write the tag.
- The memory bank (g) from which data must be read/written.

In addition, *DOWNLOAD TAG LIST* allows you to download the scanned tag list as a comma separated values (CSV) file.

In the upper right corner, information is displayed in red color, e.g. *Read completed successfully*.

7.2.5 Configuration

The configuration is the main menu used to read and change the settings for the device (see Fig. 7-9).

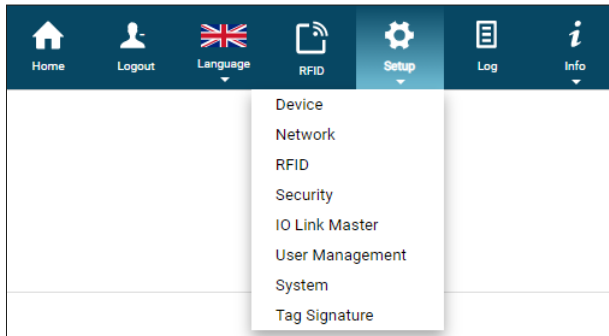


Fig. 7-9: Configuration submenu

In the following sections, each submenu is explained in detail.

General device settings

The general device settings (see Fig. 7-10) are called up in the *CONFIGURATION* menu under *DEVICE* (see Fig. 7-9 on page 36). Settings made here can be carried by the device as meta information.

Fig. 7-10: General device settings

The *MODULE NAME* (a) can be freely selected. A *LOCATION* (b) can also be provided to the device as information.

The time is set in the form shown. The date consists of day and month as a two-digit number, and the year must be entered as a four-digit number. Day, month and year must each be separated by a period and be entered in exactly this sequence. The time is set in hours in 24-hour format and minutes separated by a colon. Under *TIME ZONE NAME* (d) the time zone in which the date was entered is selected. The time difference to UTC (Coordinated Universal Time) must nevertheless be entered manually in the *OFFSET TO UTC* (e) field. The time difference must be given in hours.

To correct time stamps, the desired daylight saving time setting can be entered. An automatic change of daylight saving time does not currently take place to ensure consistent time stamps in industrial processes.

With *SET*, the settings made are transferred to the device, with *REFRESH* they are discarded or updated.

All of the above parameters require an *ADMIN* level to change/update parameters.

Network setting

The settings for the Ethernet interface of the BIS U-6127 (see Fig. 7-11) are called up in the *CONFIGURATION* menu under *NETWORK* (see Fig. 7-9 on page 36).

Fig. 7-11: Network settings

In the delivery state, the static assignment of an IP address is activated (see Fig. 7-11). However, this setting can also be changed to automatic assignment of an IP address via DHCP (a). If static IP address assignment is activated, the *IP ADDRESS* (b) and the *SUBNET MASK* (c) can be set. The newly set IP address can be entered on the type plate of the device by the user. In addition, the settings for the IP addresses of a *GATEWAY* (d) for external network access and the desired primary (e) and secondary (f) DNS name server are also available. If a server with NTP functionality (network time protocol) is to be used for setting the time, this must be entered in the input field (g). Either an IP address or a domain name (e.g. time.google.com) can be entered here.

With *SET* (h) the settings are saved on the device, with *REFRESH* (i) they are discarded or updated.

To activate the settings made on the device, a restart is necessary, which can be triggered with *REBOOT* (j). All of the above parameters require an *ADMIN* level to change/update parameters.

The following settings are used as configuration values in the standard configuration:

Configuration element	Default value
IP assignment	Static
IP address	192.168.10.2
Subnet mask	255.255.255.0
Gateway	0.0.0.0
DNS IP 1	0.0.0.0
DNS IP 2	0.0.0.0
NTP server	

RFID settings

The RFID settings (see Fig. 7-12) are called up in the *CONFIGURATION* menu under *RFID* (see Fig. 7-9 on page 36).

Fig. 7-12: RFID settings

There are five tabs, under each of which different RFID settings can be made:

- Basic UHF
- Antennas & power
- UHF extended
- Filter options
- Formatted tag data

All parameters can be read with any access authorization. However, to change parameter values, certain access rights must be present.

Basic UHF

Fig. 7-13: Basic UHF

i To change the settings, at least the *EXPERT* authorization level is required.

Parameters for general operation:

- (a) *Initial Q-value/expected number of tags* (parameter 0002_{hex}) see page 56
- (b) *TID length* (Parameter 0004_{hex}) in bytes, see page 61
- (c) *Number of read attempts* (Parameter 000A_{hex}) see page 61
- (d) *Activate BlockWrite* (Parameter 000D_{hex}) see page 61
- (e) *Max. write length* (Parameter 000D_{hex}) see page 62
- (f) *Max. read length* (Parameter 000E_{hex}) see page 62
- (g) *Active channels* (Parameter 000B_{hex}) see page 59

7

Startup and operation (continued)

Antennas & power

Antennas and Power									
Enabled	Antenna Type	Gain (dBi)	Cable Type	Loss (dB)	Default Ant Power (ERP)	Default Port Power	Write Add-on		
Ant1 ☒	custom	5.5 dBi	custom	0.35 dB	27 dBm	24 dBm	2 dB	Auto	
Ant2 ☐	custom	5.5 dBi	custom	0.35 dB	27 dBm	24 dBm	2 dB	Auto	
Ant3 ☒	custom	5.5 dBi	custom	0.35 dB	27 dBm	24 dBm	2 dB	Auto	
Ant4 ☐	custom	5.5 dBi	custom	0.35 dB	27 dBm	24 dBm	2 dB	Auto	

Fig. 7-14: Antennas & power

Parameters for antennas & power:



To change settings of the following parameters, the *ADMIN* authorization level is required.

- (a) *Active antennas* (Parameter 0012_{hex}) see page 74
- (b) For *antenna type*, see section *UHF components* on page 73
- (c) *Antenna gain* (Parameter 0013_{hex}) see page 74
- (d) For *cable type* see section *UHF components* on page 73
- (e) *Cable attenuation* (Parameter 0014_{hex}) see page 75



To change settings of the following parameters, at least the *EXPERT* authorization level is required.

- (f) *Transmitting power on read (default)* (Parameter 0008_{hex}) see page 58
- (h) *Automatic increase of transmitting power on write* (Parameter 0009_{hex}) see page 59
- (i) Starts the *Auto-Setup* function for the corresponding antenna (Parameter 1003_{hex}) see page 60

The following parameter is calculated from the other parameters and cannot be changed directly:

- (g) Displays the calculated transmitting power at the antenna jack.

UHF extended

Fig. 7-15: UHF extended

Settings for the air interface:

i To change settings of the following parameters, at least the *EXPERT* authorization level is required.

- (a) *Radio profile* (Parameter 0001_{hex}) see page 56
- (b) *Session (Inventoried Flag)* (Parameter 0005_{hex}) see page 57
- (c) *Pilot tone (long preamble)* (Parameter 0006_{hex}) see page 58
- (d) *Modulation* (Parameter 0007_{hex}) see page 58
- (e) *Initial Q-value/expected number of tags* (Parameter 0002_{hex}) see page 57

Settings for the tag signature:

i To change settings of the following parameters, the *ADMIN* authorization level is required.

- (f) *SignatureType* (Parameter 002A_{hex}) see page 81
- (g) *Calculation format for signature generation (default)* (Parameter 0028_{hex}) see page 80

For information on *Sign tag data*, see chapter 3.7 on page 12.

Filter options

Fig. 7-16: Static filters

Filter options:

i To change settings of the following parameters, at least the *EXPERT* authorization level is required.

- TID bit address (a), TID bit length (b) and TID data (c), see *TIDFilter (default)* (parameter 002E_{hex}) on page 66
- (d) *RSSIMinFilter (default)* (Parameter 002F_{hex}) see page 67
- (e) *RSSIMaxFilter (default)* (Parameter 0030_{hex}) see page 68
- EPC bit address (f), EPC bit length (g) and EPC data (h), see *EPCFilter (default)* (parameter 002D_{hex}) on page 65
- (i) *MinReads or AsyncObserved threshold (default)* (Parameter 0023_{hex}) see page 62
- (j) *MinNoReads or AsyncObserved-Timeout (default)* (Parameter 0024_{hex}) see page 63
- (k) *WaitTime (default)* (Parameter 0029_{hex}) see page 63

i To change settings of the following parameters, the *ADMIN* authorization level is required.

- (l) *AsyncScanDelay* (Parameter 0011_{hex}) see page 73

7

Startup and operation (continued)

Formatted tag data

Formatted Tag Data (f) info : number of Tags Read : 2

Default Tag data format (a)

Prefix for Multiple Tag Read (b)

Suffix for Multiple Tag Read (c)

Set Refresh Test (d)

42 65 67 69 6e 0d 0a 65 32 30 30 39 30 35 31 33 32 30 35 30
 31 37 32 32 37 37 30 30 34 39 31 0d 0a 65 32 30 30 39 30 35
 31 33 32 30 35 30 31 37 31 31 35 34 30 37 35 62 36 0d 0a 45
 6e 64 0d 0a

Begin--e200905132050
 17227700491--e200905
 132050171154075b6--E
 nd--

(e)

Fig. 7-17: Formatted tag data

i To change settings of the following parameters, the *ADMIN* authorization level is required.

Settings for formatted tag data:

- (a) *Format definition for ReadTagDataFormatted, ReadMultipleTagDataFormatted and WriteFormattedTagData (default)* (Parameter 0025_{hex}) see page 79
- (b) *Prefix for ReadMultipleTagDataFormatted (default)* (Parameter 0026_{hex}) see page 80
- (c) *Suffix for ReadMultipleTagDataFormatted (default)* (Parameter 0027_{hex}) see page 80

With *TEST* (d), the defined tag parameters can be checked and displayed in the text field (e) (left: binary, right: ASCII format).

Security settings

The security settings (see Fig. 7-18) are called up in the *CONFIGURATION* menu under *SECURITY* (see Fig. 7-9 on page 36).

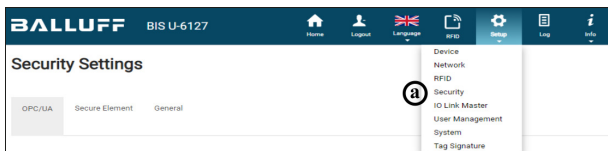


Fig. 7-18: Security settings

There are three tabs, under each of which different security settings can be made:

- OPC/UA
- Secure Element
- General

For more information on *Data security*, see chapter 3.6 on page 11.

OPC/UA

OPC/UA Settings

Refuse Unsecure Client Connections (a) ☒

Accept only Trusted Client Certificates (b) ☐

Use Secure Element (c) ☒

Client Certificate List

Status	Name	Organization	Valid From	Valid To	
Trusted	UaExpert_trusted.der	Balluff GmbH	Oct 2 01:51:33 2020 GMT	Oct 1 01:51:33 2025 GMT	🔒 🗑️ (d)
Rejected	UaExpert_rejected.der	Balluff GmbH	Oct 2 01:51:33 2020 GMT	Oct 1 01:51:33 2025 GMT	🔒 🗑️ (e)

Set Refresh Reboot

Create/Download Certificate

(f) Create Certificate Download (g)

*Please update the date before creating certificate

Fig. 7-19: OPC/UA

OPC/UA settings:

- *REFUSE UNSECURE CLIENT CONNECTIONS* (a) can be used to reject unsecure connections.
- With *ACCEPT ONLY TRUSTED CLIENT CERTIFICATES* (b) only connections with authorized certificate will be allowed and the system is thus protected against unauthorized connection to the OPC/UA server. This setting is coupled with the setting *REFUSE UNSECURE CLIENT CONNECTIONS* (a).
- *USE SECURE ELEMENT* (c) uses the built-in hardware element to store the secret keys, which further increases security.

Certificate list:

The certificate list shows the available certificates on the device. In addition, the certificate details such as status, organization and validity period of the certificate are displayed. The status of the certificate indicates whether the certificate is trusted or rejected by the authorized user or administrator.

With *ADMIN* permission, the list can be changed using buttons (d) and (e). A certificate that is already marked as trusted can be set to the rejected state by clicking the lock icon or deleted from the device by pressing the trash can icon. Similarly, a rejected certificate can be set to the trusted state or deleted from the device.

Generate/download certificate:

- Use *CREATE CERTIFICATE* (f) to create a certificate for the device itself (e.g. after changing the network settings).
- With *DOWNLOAD* (g), a certificate can be downloaded.



To avoid invalid certificates, set the date, time and time zone correctly when generating a certificate.

Certificates have a limited validity (typically several years, the validity can be displayed on a Windows PC, for example) and must be replaced when the validity expires.

For more information on *Data security*, see *OPC UA* in chapter 3.6 on page 11.

7

Startup and operation (continued)

Secure Element

Secure Element

Secure Element Serial Number (a)

Secure Element Licenses (b)

- Found license entry 0:0
- Found license entry 0:50
- Found license entry 0:60
- Found license entry 0:70
- Found license entry 0:1000
- Found license entry 6000573:40401
- Found license entry 6000573:30401

Secure Element Context File

(c)

Secure Element Update File

(d)

(e)

Fig. 7-20: Secure Element

The *SECURE ELEMENT* settings display the details of the security license. It also allows updating the current license.

Secure Element (read-only fields):

- Secure Element serial number (a) represents the unique identification number.
- Secure Element licenses (b) represents the available license.

Secure Element context file:

With *DOWNLOAD CONTEXT FILE* (c), the remote context file (*.WibuCmRaC) can be downloaded.

The file can be used to generate update files for Secure Element licenses.

Secure Element context file:

If current licenses are to be updated or renewed, a ticket must be purchased from Balluff Service for this action. This provides a remote update file (*.WibuCmRaU) from Balluff Service itself or from a specific website. This update file can be uploaded with *CHOOSE A *.WIBUCMRAU FILE* (d), and the updates are applied to the Secure Element with *UPLOAD UPDATE FILE* (e).

For more information on *Data security*, see *OPC UA* in chapter 3.6 on page 11.

7

Startup and operation (continued)

General

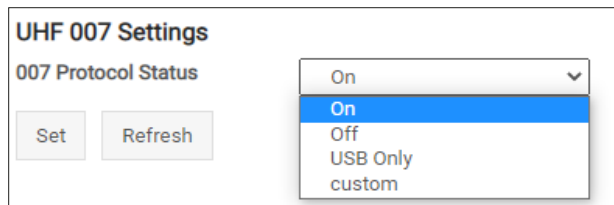


Fig. 7-21: General

On the *GENERAL* page, the ports used by the *UHF 007* communication protocol can be changed. The changes are only applied after a device restart.



007 should only be deactivated for the USB port with caution!

The USB port may be the only way to retrieve and change the IP address of the device once it is lost.

The communication protocol allows connection to the device via five TCP/IP ports and one USB port:

- Port 10001
- Port 10002
- Port 10003
- Port 10004
- Port 10005
- Tty USB port

Four configurations (a) are available:

- *ON* opens all available ports.
- *OFF* closes all available ports.
- *USB ONLY* closes all ports except the USB port.
- *CUSTOM* (read-only) defines the port condition that does not match any of the above three options.

IO-Link settings (web server)

The IO-Link settings (see Fig. 7-22) are called up in the *CONFIGURATION* menu under *IO LINK MASTER* (see Fig. 7-9 on page 36).

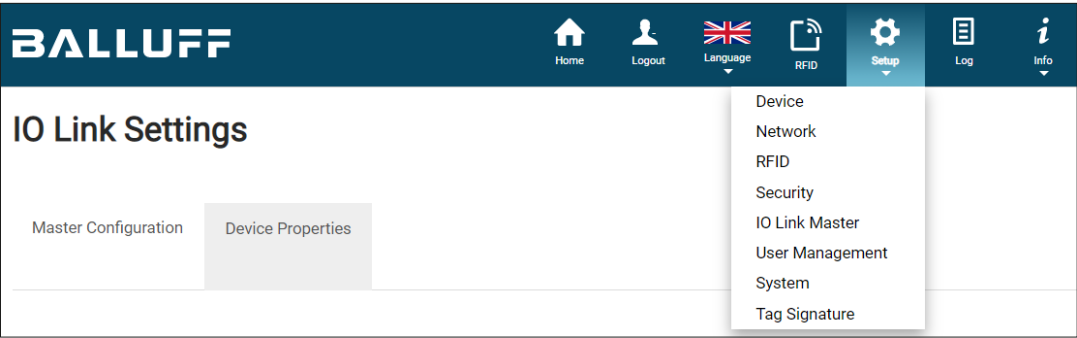


Fig. 7-22: IO-Link settings

There are two tabs, under each of which different settings can be made:

- *MASTER CONFIGURATION*
- *DEVICE PROPERTIES*

All parameters can be read with any access authorization. However, to change parameter values, certain access rights must be present.

Master configuration



To change settings of the following parameters, the *ADMIN* authorization level is required.

Master Parameters	
Vendor ID	0x0378
Device ID	0x000000
Serial Number	
IO-Link Pin 2 Function	Input NC
IO-Link Pin 4 Function	IOL
Safe State	0
Cycle Time Base	0
Cycle Time	0
Parameter Server	Disable
Parameter Download	Disable
Parameter Upload	Disable
Output Length	5
Input Length	0
Validation Mode	No Validation

Fig. 7-23: Master configuration

Device properties



To change settings of the following parameters, the *ADMIN* authorization level is required.

Device Properties	
Process Data	
Inputs	00
Outputs	00 00 00 00 00
Events	
Current Event	no event
Set Output Data Refresh	
Parameters	
Index	1062
Subindex	0
Data	00 50 02 00 64 04 00 64
Set Read Data	

Fig. 7-24: Device properties

With *REFRESH*, the displays of the process data and events can be updated.

Data can be read or written to a specified index and subindex.

User Management

In addition to the standard user profiles, you can create your own users with individual permissions.

The user administration (see Fig. 7-25) is called up in the *CONFIGURATION* menu under *USER ADMINISTRATION* (see Fig. 7-9 on page 36). The configuration page first provides an overview of the available users in the system. By default, only the (invisible) users *ADMIN_DEFAULT* and *USER* are available.

No user data is visible without logging in.

Users who do not have the *ADMIN* role can only see their own data and edit their own password.

Only users who have the *ADMIN* role can see all users, create new users and edit the data and passwords of existing users or delete user accounts.

By deleting and creating a new user, a new password can be set even if the password is unknown.

Available user roles

Role	Description
User	User role with no configuration rights. As a rule, mainly process data and additionally some settings are visible. No configuration is possible however.
Expert	Expert user who is permitted to make some settings.
Admin	Administrative user who can configure any aspect of the device.

User Management

Users List

Users	Roles	
Balluff	☒ Admin ☒ Expert ☒ User	  
Gehard	☐ Admin ☒ Expert ☒ User	  
Superuser	☒ Admin ☒ Expert ☒ User	  
Tom	☐ Admin ☒ Expert ☒ User	  

Add User 

- a** Apply changed user roles
- b** Change password
- c** Deleting users
- d** Creating new users

Fig. 7-25: User list example

System update

The system update (see Fig. 7-26) is called up in the *CONFIGURATION* menu under *SYSTEM* (see Fig. 7-9 on page 36).

System

Software Update

Choose a *.swu file 

Firmware version in the device 0.1.12 

Update  Reboot 

Parameters data Upload

Choose a *.aml file 

Upload 

Parameters data Download

Download 

Fig. 7-26: System

Fig. 7-26 shows the dialog box for the firmware update with the buttons for selecting a firmware file (a), for triggering the update process (c) and for the final device restart (d) that can result from updates.

The firmware update files are signed and only files of this kind can be imported into the system. If a firmware upgrade fails, the device has an emergency system that can be used to import new, signed firmware.



Despite an update, the device initially functions normally and continues to run unchanged (if the update process is taking place or has already been completed). The update only takes effect after a device restart.

After the update has been completed, restart the device with *REBOOT*.

*CHOOSE *.AML FILE* (e) opens a file dialog with which a parameter configuration file saved on the PC can be searched for and selected on the local computer. After a parameter file has been selected, the parameters contained can be imported into the device with *UPLOAD* (f). It is recommended to restart the device afterwards.

With *DOWNLOAD* (g), the current settings of the device can be saved to a local computer.

7

Startup and operation (continued)

Tag signature

Tag signature (see Fig. 7-27) is called up in the *CONFIGURATION* menu under *TAG SIGNATURE* (see Fig. 7-9 on page 36).

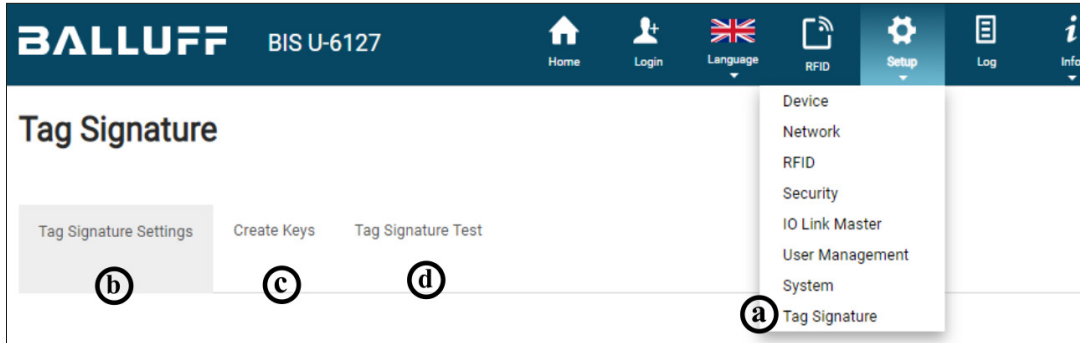


Fig. 7-27: Tag signature

The 3 tabs under *TAG SIGNATURE* contain the functions to configure the tag signature functionality (b), generate a key pair (c) and test the functionality (d) (see chapter 3.6 on page 11).

Tag signature settings

To change the *TAG_SIGNATURE* and *SIGNATURE_CALCULATION_FORMAT* parameters in the *TAG SIGNATURE SETTINGS* tab, administrator rights are required. For information on *Sign tag data*, see chapter 3.7 on page 12.

Private/public key generation

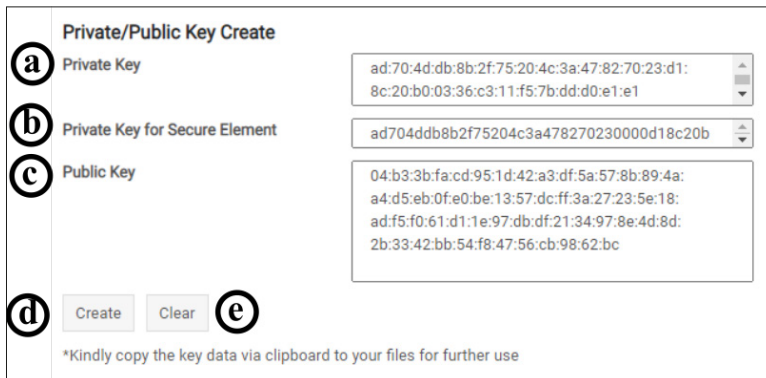


Fig. 7-28: Private/public key generation

With *CREATE* (d), a new random key pair can be generated. The output of the key pair is displayed in text format – *PRIVATE KEY* (a), *PRIVATE KEY FOR SECURE ELEMENT* (b) and *PUBLIC KEY* (c). The values can only be read and copied to the local PC.

The keys are not stored in the device and must be transferred to the *Secure Element* (see section *Generating a key for signing tag data* on page 82).

With *CLEAR* (e), the entire text output can be deleted.

7.2.6 Logbook

General status information can always be viewed under *HOME* (see chapter 7.2.1 on page 33). There you will find compact information about the operating status of the device as well as some settings, such as name and time. The type designation can also be found here.

Device status and function status

The logbook can be called up under *LOG* via the main menu bar (see Fig. 7-4 on page 33). There you will find extended information in case of an error.

- Under the *APPLICATION STATUS* tab, the error status of individual function components can be read out here in detail in order to determine where errors have occurred.
 - Function components with a green check mark have no errors.
 - If a function component is marked with a yellow symbol, then problems have recently occurred in the process.
 - If a function component is marked with a red symbol, it is no longer executable and a serious error has occurred.

Behind the name of the function component, there is also a short description of the status.

- Details about the problem that has occurred can be read out under the *DEVICE LOGBOOK* tab. The diagnostic function for troubleshooting is located here. This information is important should contact be made with our Customer Service Team.

7.2.7 Legal and general information

Further information is available under *INFO* (see Fig. 7-30).



Fig. 7-30: *INFO* menu

GENERAL (a) calls up a short explanation of the meaning of the icons used on the page.

Under *MANUAL* (b), the current manual can be downloaded in all available languages.

LICENSE INFORMATION (c) calls up license texts for the open source components used on the device.

7.3 Parameter configuration

The processor unit can be adapted to the conditions of the application and its ambient conditions via various parameters. The individual parameters and their effects are explained in the following sections.

The following channels can be used to perform parameterization:

- *007 protocol* (see chapter 8 on page 89)
- *UHF Manager configuration software* (see chapter 7.1 on page 29)
- *OPC UA* (see chapter 9 on page 132)
- *Web server* (see chapter 7.2 on page 33)

7.3.1 Preliminary considerations for parameterization



Access to the various parameters is regulated by the authorizations of the user levels *USER/EXPERT/ADMIN*. These can be managed via the web server (see *Data security* on page 11 and *User Management* on page 45).

Transmitting power

In order to set up the processor unit optimally for the application at hand, preliminary considerations regarding parameterization are necessary in addition to the considerations regarding the arrangement of the system components (see chapter 6 on page 21).

The desired read/write distance can be increased or decreased via the transmitting power. In principle, a higher transmitting power also means a higher read/write distance. This applies in particular if there are many data carriers in a confined space or if they are mounted on electromagnetically effective materials (e.g. metal).

However, setting the transmitting power too high can also have disadvantages:

- If several processor units are used simultaneously and their antennas are mounted too close together or even in the detection range of other antennas, interference will occur between the processor units. If spatial separation is not possible, the interference can be reduced by lowering the transmitting power.
- Data carriers mounted further away can be inadvertently detected by an antenna due to high transmitting power.
- A high transmitting power can reduce the receiving sensitivity of the processor unit.



To minimize the influence on the processor unit and its surroundings, the radiated electromagnetic energy should always be minimized in the environment. This means that the transmitting power should not be set higher than is necessary for safe interaction with the desired data carrier population.

In single-tag applications, the Auto-Setup function can be used to set the optimal transmitting power (see *Auto-Setup* on page 60).

Radio parameters and electromagnetically stressed environment

The transmission channel between antenna and data carrier can be adapted via radio parameters. Here, for example, parameters such as data rate and coding can be adapted to the application and the environment. Higher data rates enable faster data exchange between the processor unit and the data carrier, but can make the transmission channel more susceptible to interference from an electromagnetically stressed environment. This can be partially counteracted via the coding.

In principle, we recommend that only experts change the preset radio parameters and only use higher data rates if they are necessary due to the required process speed.

When setting the radio profiles, make sure that the data carriers used support the selected radio profile.

Capture reliability vs. speed

Various parameters can be used to increase the reliability of the identification system (e.g. by repeatedly detecting data carriers) to ensure that only data carriers that are actually located in the desired detection range are detected. Data carriers that have been accidentally detected due to field fluctuations can thus be masked out.

The increase in detection reliability may be at the expense of detection speed, which may be required in dynamic applications. During parameterization, it may then be necessary to find a balance between reliability and speed.

7

Startup and operation (continued)

7.3.2 Parameter overview

The following overview lists the parameters that can be used and provides information about the required security level *STANDARD/EXPERT/ADMIN* as well as the scope and validity period.

Global/Local/Antenna

The scope indicates whether a parameter is valid globally or only for a session or an antenna port.

- GLOBAL:** Parameters are applied to all antennas or sessions. Some parameters are only applied to 007 sessions when the device is restarted.
- SESSION:** Parameters apply only to the current session (TCP connection) and can be set independently for each session.
- ANTENNA:** Parameters refer to one antenna port and can be set independently for each antenna port. These values apply to all sessions.

Persistent/temporary

The validity period defines whether a parameter is stored permanently or only for the current TCP connection (session) or until a restart of the processor unit.

- PERSISTENT:** Parameters are stored permanently and retain their value even after a restart of the processor unit.
- TEMPORARY:** Parameters lose their validity when the current session is ended or the processor unit is restarted.

Reset (Yes/No)

When changing some parameters, a restart of the processor unit is required. The restart must be initiated manually.



Some parameters are marked with the addition *default*. These parameters are persistent and retain their value even after a restart of the processor unit. Depending on the parameter, a higher authorization level may be necessary.

Parameters for standard users

Parameter-ID	Parameters	Global/Session/Antenna	Persistent/temporary	Reset
0003 _{hex}	Max. EPC length (read only)	Global	Persistent	No
1001 _{hex}	Transmitting power on read (current)	Session	Temporary	No
1002 _{hex}	Access password	Session	Temporary	No
1004 _{hex}	Memory bank	Session	Temporary	No
1006 _{hex}	AsyncOperation	Session	Temporary	No
1007 _{hex}	AdminLevel-Login	Session	Temporary	No

Parameters for experts

To set expert parameters, access to the expert security level is required (see *Data security* on page 11 and *User Management* on page 45).

Air interface, radio parameters

Parameter-ID	Parameters	Global/Session/Antenna	Persistent/temporary	Reset
0001 _{hex}	Radio profile	Global	Persistent	No
0002 _{hex}	Initial Q-value/expected number of tags	Global	Persistent	No
0005 _{hex}	Session	Global	Persistent	No
0006 _{hex}	Preamble (pilot tone)	Global	Persistent	No
0007 _{hex}	Modulation (ASK/PR-ASK)	Global	Persistent	No
0008 _{hex}	Transmitting power on read (default), see also session-related parameter 1001 _{hex}	Global	Persistent	No
0009 _{hex}	Automatic increase of transmitting power on write	Global	Persistent	No
000B _{hex}	Active channels (ETSI only)	Global	Persistent	No
1003 _{hex}	Auto-Setup	Session	Persistent	No

7

Startup and operation (continued)

Data, write, read, detect

Parameter-ID	Parameters	Global/Session/Antenna	Persistent/temporary	Reset
0004 _{hex}	TID length	Global	Persistent	No
000A _{hex}	Number of read attempts	Global	Persistent	No
000C _{hex}	BlockWrite when writing	Global	Persistent	No
000D _{hex}	Max. write length	Global	Persistent	No
000E _{hex}	Max. read length	Global	Persistent	No

Loop filter

Parameter-ID	Parameters	Global/Session/Antenna	Persistent/temporary	Reset
0023 _{hex}	MinReads or AsyncObservedThreshold (default)	Global	Persistent	No
100C _{hex}	MinReads or AsyncObservedThreshold	Session	Temporary	No
0024 _{hex}	MinNoReads or AsyncObservedTimeout (default)	Global	Persistent	No
100D _{hex}	MinNoReads or AsyncObservedTimeout	Session	Temporary	No
0029 _{hex}	WaitTime (default)	Global	Persistent	No
100E _{hex}	WaitTime	Session	Temporary	No

Data filter

Parameter-ID	Parameters	Global/Session/Antenna	Persistent/temporary	Reset
002B _{hex}	EPCLength-Min (default)	Global	Persistent	No
100F _{hex}	EPCLength-Min	Session	Temporary	No
002C _{hex}	EPCLength-Max (default)	Global	Persistent	No
1010 _{hex}	EPCLength-Max	Session	Temporary	No
002D _{hex}	EPCFilter (default)	Global	Persistent	No
1011 _{hex}	EPCFilter	Session	Temporary	No
002E _{hex}	TIDFilter (default)	Global	Persistent	No
1012 _{hex}	TIDFilter	Session	Temporary	No

RSSI filter

Parameter-ID	Parameters	Global/Session/Antenna	Persistent/temporary	Reset
002F _{hex}	RSSIMinFilter (default)	Global	Persistent	No
1013 _{hex}	RSSIMinFilter	Session	Temporary	No
0030 _{hex}	RSSIMaxFilter (default)	Global	Persistent	No
1014 _{hex}	RSSIMaxFilter	Session	Temporary	No

FormattedTagData

Parameter-ID	Parameters	Global/Session/Antenna	Persistent/temporary	Reset
1008 _{hex}	Output format for formatted tag data	Session	Temporary	No
1009 _{hex}	Prefix for ReadMultiple-TagDataFormatted	Session	Temporary	No
100A _{hex}	Suffix for ReadMultiple-TagDataFormatted	Session	Temporary	No

7

Startup and operation (continued)

Tag signature

Parameter-ID	Parameters	Global/Session/Antenna	Persistent/temporary	Reset
100B _{hex}	Calculation format for signature generation	Session	Temporary	No

Parameters for administrators

To set the parameters for administrators, access to the *Admin* security level is required (see *Data security* on page 11 and *User Management* on page 45)

Auto functions

Parameter-ID	Parameters	Global/Session/Antenna	Persistent/temporary	Reset
000F _{hex}	Automatic scanning	Session	Persistent	No
0011 _{hex}	AsyncScan-Delay	Global	Persistent	No

Active antennas, equipment (antennas, cables)

Parameter-ID	Parameters	Global/Session/Antenna	Persistent/temporary	Reset
0012 _{hex}	Active antennas	Global	Persistent	No
0013 _{hex}	Antenna gain	Antenna	Persistent	No
0014 _{hex}	Cable attenuation	Antenna	Persistent	No
0015 _{hex}	Antenna polarization	Antenna	Persistent	No
0016 _{hex}	Antenna aperture angle	Antenna	Persistent	No

Network, system

Parameter-ID	Parameters	Global/Session/Antenna	Persistent/temporary	Reset
0019 _{hex}	IP address	Global	Persistent	No
001A _{hex}	Netmask	Global	Persistent	No
001B _{hex}	DHCP	Global	Persistent	No
001C _{hex}	Hostname	Global	Persistent	No
001D _{hex}	Gateway	Global	Persistent	No
001E _{hex}	Name server	Global	Persistent	No
001F _{hex}	Device location	Global	Persistent	No
0020 _{hex}	Time zone	Global	Persistent	No
0021 _{hex}	NTP server	Global	Persistent	No
0022 _{hex}	Time	Global	Persistent	No

Formatted Tag Data (defaults)

Parameter-ID	Parameters	Global/Session/Antenna	Persistent/temporary	Reset
0025 _{hex}	Output format for formatted tag data (default)	Global	Persistent	No
0026 _{hex}	Prefix for ReadMultiple-TagDataFormatted (default)	Global	Persistent	No
0027 _{hex}	Suffix for ReadMultiple-TagDataFormatted (default)	Global	Persistent	No

Tag signature (defaults)

Parameter-ID	Parameters	Global/Session/Antenna	Persistent/temporary	Reset
0028 _{hex}	Calculation format for signature generation (default)	Global	Persistent	No
002A _{hex}	SignatureType	Global	Persistent	No

7.3.3 Description of parameters for standard users

Parameters for standard users can be changed by any user without logging in. These parameters are only temporarily adopted by the processor unit and are only valid for the current session or until the processor unit is restarted.

Max. EPC length (read only)

Parameter-ID: 0003_{hex}

The parameter *Max. EPC length* specifies which maximum number of bytes of the EPC memory area is transferred by the processor unit.

If data carriers are read whose EPC is longer than the set *Max. EPC length*, the read EPC is limited to the set number of bytes.



The parameter *Max. EPC length* is only used for compatibility with other BIS U processor units and cannot be changed. The value is fixed at 496 bits.

Transmitting power on read (current)

Parameter-ID: 1001_{hex}
UHF-Manager: Menu: Device settings > Parameters... > Transmitting power
OPC UA: GetRFPower/SetRFPower
Webserver: Menu: Configuration – RFID – Antennas & power

After switching on or restarting the processor unit, the current transmitting power is taken from the expert parameter *Transmitting power on read (default)*. Depending on the requirements, the transmitting power can be temporarily changed via the parameter *Transmitting power on read (current)*. The setting is retained until it is changed again or the processor unit is restarted.

The set transmitting power is used for read operation. The desired power in quarter dBm is applied as the parameter value.

$$\text{Parameter value} = P(\text{dBm}) \times 4$$

Adjustable power: 7...36 dBm¹⁾ (corresponds to 5...4000 mW)
0 turns off the antenna for this session

¹⁾ The highest possible antenna power depends on the device variant.

Length [bits]	Permissible values	Factory setting	Meaning
8	0, 28...144	108 27 dBm (500 mW)	Current transmitting power in ¼ dBm (ERP or EIRP)



Depending on the device variant, the specifications for the transmitting power are to be understood as ERP values (Equivalent Radiated Power) or EIRP values (Equivalent Isotropically Radiated Power). The respective valid information can be found in the information sheet on conformity and approvals.

7

Startup and operation (continued)

Access password

Parameter-ID: 1002_{hex}
 UHF-Manager: Action area > *READ/WRITE* tab
 OPC UA: Is applied with the respective OPC UA methods for writing and reading
 Webserver: Menu: *RFID* > Action area: *TAG PARAMETERS*

If a password-protected data carrier is to be accessed, the data carrier can be unlocked for further interaction using the *Access password* parameter.

The password must be transferred in *LSB first* format.

If no data carriers with different passwords are in use, it is sufficient to send the parameter once to the processor unit.

The password remains stored in the processor unit until the current session is ended or the processor unit is restarted.

Adjustable values: 4-byte password (Standard 00 00 00 00_{hex})

Length [bits]	Permissible values (hex)	Factory setting (hex)	Meaning
32	00000000... FFFFFFFF	00000000	Access password

Memory bank

Parameter-ID: 0x1004_{hex}
 UHF-Manager: Action area > *READ/WRITE* tab
 OPC UA: Is applied with the respective OPC UA methods for writing and reading
 Webserver: Menu: *RFID* > Action area: *TAG PARAMETERS*

The parameter *Memory bank* can be used to control the memory area of the data carrier on which write/read operations are executed.

Depending on the data carrier used, the memory areas of RFU (Reserved), EPC, TID and USER are available.

If the memory area is changed, the setting is retained until it is changed again or the session is terminated.

Length [bits]	Permissible values	Factory setting	Meaning
8	0, 1, 2 or 3	3 (USER)	Memory bank of data carrier 0: RFU 1: EPC 2: TID 3: USER



Further information on the different storage areas of the data carriers can be found in the EPCglobal™ Class-1 Generation-2 standard for UHF RFID systems (www.epcglobal.de).

AsyncOperation

Parameter-ID: 1006_{hex}
 UHF-Manager: Action area > *DETECT* tab
 (demo only, no cumulative operation)
 OPC UA: Is applied with the respective OPC UA
 methods for writing and reading
 Webserver: –

Various operating modes can be selected for recording a data carrier population. These are described in more detail in chapter 6.5 on page 23.

- **SYNCHRONOUS**
 In synchronous operation, a request must be sent to the processor unit for each detection operation. This then detects the data carriers that are in the detection range of the specified antenna and returns them to the controlling system in the form of a list.
- **ASYNCHRONOUSLY**
 In asynchronous mode, in contrast to synchronous mode, the detection process only has to be started once. This then runs permanently in the background, which keeps the data carrier list up to date. The current list can then be queried via a synchronous request.
- **COMES/GOES messages**
 As an alternative to asynchronous operation with synchronous request, asynchronous messages can also be activated. These then only report changes to the data carrier population. New data carriers are registered via a *COMES* message. Data carriers that leave the detection range are deregistered via a *GOES* message.
- **CUMULATIVE**
 Cumulative, asynchronous operation continuously detects all data carriers in the detection range and adds them to the data carrier list. Only when the list is queried synchronously is it deleted and created again. In this way, all data carriers that have passed through the detection range since the last query can be queried.

The *AsyncOperation* parameter is transferred as a byte, whereby options can be enabled or disabled via the individual bit positions.

Bit positions:

Bit 0 0: *SYNCHRONOUS* 1: *ASYNCHRONOUS*
 Bit 1 0: *COMES* message disabled 1: *COMES* message activated
 Bit 2 0: *GOES* message disabled 1: *GOES* message enabled
 Bit 3 0: *CUMULATE* disabled 1: *CUMULATE* enabled

Length [bits]	Permissible values	Factory setting	Meaning
8	00 _{hex} ...0F _{hex}	00 _{hex} : Synchronous	Synchronous data carrier detection

Examples:

Operation	Bit 3	Bit 2	Bit 1	Bit 0	Byte
<i>SYNCHRONOUS</i>	0	0	0	0	00 _{hex}
<i>ASYNCHRONOUS</i> with synchronous query	0	0	0	1	01 _{hex}
<i>ASYNCHRONOUS</i> with <i>COMES/GOES</i> message	0	1	1	1	07 _{hex}
<i>ASYNCHRONOUS, CUMULATIVE</i>	1	0	0	1	09 _{hex}

AdminLevelLogin

Parameter-ID: 1007_{hex}
 UHF-Manager: Menu: *Login*
 OPC UA:
 Webserver: Menu: *Login*

The *AdminLevelLogin* parameter can be used to switch between the *STANDARD USER/EXPERT/ADMIN* security levels. The *EXPERT* and *ADMIN* security levels are required to edit parameters with a higher security level.

The processor unit is only delivered with a standard admin user. Additional users can be created via the web server (see *Data security* on page 11 and *User Management* on page 45).

When setting the parameter, the user name, a byte with the value 01_{hex} and the user's password must be set. The string does not have to be terminated with a 0 byte.

If the username or password does not match a corresponding entry in the user database, an error status is returned.

When reading the parameter, only the username is returned.

i Users are automatically logged out of the system after a period of inactivity of 15 minutes and a new login is required. After 24 hours at the latest, you must log in again.

Length [bits]	Permissible values	Factory setting	Meaning
Variable	Username + 01 _{hex} + Password	"user"	Login data is transferred as a string

7.3.4 Description of parameters for experts

Parameters for experts can be changed by users of the *EXPERT* and *ADMIN* security levels. This requires a login of the corresponding security levels. Expert parameters are permanently stored in the processor unit and retain their value until they are overwritten.

The following groups of expert parameters are described:

- *Air interface/radio parameters* (see page 56)
- *Write, read* (see page 61)
- *Loop filter* (see page 62)
- *Data filter* (see page 64)
- *RSSI filter* (see page 67)
- *FormattedTagData* (see page 69)

Air interface/radio parameters

The air interface/radio parameters can be used to make settings that affect the radio signal between the data carrier and the processor unit, as well as settings that affect the behavior of data carriers during the detection process.

The following parameters are important for optimal operation of the RFID system and should be set by all users:

- 0002_{hex}: Initial Q-value/expected number of tags
- 0008_{hex}: Transmitting power on read (default)
- 0009_{hex}: Automatic increase of transmitting power on write
- 000B_{hex}: Active channels



Setting further air interface/radio parameters is not necessary in most cases and should only be done by experienced users with the appropriate expertise.

Radio profile

Parameter-ID: 0001_{hex}
 UHF-Manager: Menu: *Device settings > Advanced parameters... > RF settings*
 OPC UA: –
 Webserver: Menu: *Configuration > RFID > UHF extended*

The radio profile defines which connection parameters are used on the air interface between the data carrier and the processor unit:

Tx: Bit rate forward, i.e. from processor unit to data carrier: 40 kBit/s
 Rx: Bit rate backwards, i.e. from data carrier to processor unit: 62.5 kBit/s or 75 kBit/s
 Coding: Coding backwards, i.e. with which coding the data carrier responds.
 Miller-4: Each bit is transmitted as a quadruple bit



Not all profiles are available in every country variant of the device.

The following radio profiles can be set:

Profile no.	Parameter value	Tx [kBit/s]	Rx [kBit/s]	Coding
1	00000902 _{hex}	40	62.5	Miller-4
2	00000B02 _{hex}	40	75	Miller-4

Adjustable values:

Length [bits]	Permissible values	Factory setting	Meaning
32	Parameter values in table	0x00000902 40/62.5/Miller-4	Radio profile

7

Startup and operation (continued)

Initial Q-value/expected number of tags

Parameter-ID: 0x0002_{hex}
 UHF-Manager: Menu:
 Device settings > Parameters... > Basic
 UHF (expected number of tags)
 and
 Devices settings > Advanced
 Parameters... > Air interface (Q-value)
 OPC UA: –
 Webserver: Menu: *Configuration > RFID > UHF*
 extended

The Q-value is used as a key figure for the number of data carriers expected in the detection range of the antenna. The Q-value can be used to optimize the time taken for data carrier detection. In addition, the detection rate can decrease if the Q-value is selected too high.

The set Q-value is only used as a starting value during detection and can be optimized by the processor unit. The following table shows a recommendation for setting the Q-value, depending on the expected number of data carriers:

Expected number of data carriers (approx.)	Recommended Q-value
1	1
2	2
5	3
10	4
25	5
50	6
100	7
200	8
500	9

Adjustable values for the Q-value:

Length [bits]	Permissible values	Factory setting	Meaning
8	1...15	4 (Q-value = 4)	Number of expected data carriers

Setting fields that specify the expected number of tags are always rounded to a number calculated from the Q-value.

Session (Inventoried Flag)

Parameter-ID: 0x0005_{hex}
 UHF-Manager: Menu: *Device Settings > Advanced*
 parameters... > Air interface
 OPC UA: –
 Webserver: Menu: *Configuration > RFID > UHF*
 extended

EPCglobal™ Class-1 Generation-2 data carriers support session flags to indicate whether a data carrier has already been detected. This is done via the status of the session flags (*DETECTED/NOT DETECTED*). In this way, it is possible to control whether and when a data carrier that has already been detected can be detected again. Different rules apply to the 4 sessions (0...3) with regard to the transition from the *Detected* status back to the *UNDETECTED* status.

Adjustable values:

Length [bits]	Permissible values	Factory setting	Meaning
8	0: Session 0 1: Session 1 2: Session 2 3: Session 3	0	Session 0



Changing the session is reserved for experts and is only recommended if the default setting does not provide satisfactory results. Detailed information on the *SESSION* flag can be found in the standard according to EPCglobal™ Class-1 Generation-2.

7

Startup and operation (continued)

Pilot tone (long preamble)

Parameter-ID: 0x0006_{hex}
 UHF-Manager: Menu: *Device settings > Advanced parameters... > RF settings*
 OPC UA: –
 Webserver: Menu: *Configuration > RFID > UHF extended*

Data carriers that respond to queries from the processor unit prefix the data with a preamble that is used by the processor unit for synchronization. In addition, a pilot tone can be transmitted, which can improve synchronization between the data carrier and the processor unit in electromagnetically stressed environments.

Adjustable values:

Length [bits]	Permissible values	Factory setting	Meaning
8	0 or 1	1 (Pilot tone on)	Preamble with or without pilot tone 0: Pilot tone off 1: Pilot tone on

i For reasons of process reliability, it is advisable to leave the pilot tone switched on. In very time-critical applications, switching off the pilot tone may result in a slight time advantage.

Modulation

Parameter-ID: 0x0007_{hex}
 UHF-Manager: Menu: *Device settings > Advanced parameters... > RF settings*
 OPC UA: –
 Webserver: Menu: *Configuration > RFID > UHF extended*

Setting the modulation method used for radio transmission between the processor unit and the data carrier.

i Not all modulation methods are available in every country variant of the device.

Adjustable values:

Length [bits]	Permissible values	Factory setting	Meaning
8	0 or 1	1 (PR-ASK)	Modulation method 0: ASK 1: PR-ASK

i Changing the modulation method is normally not necessary. In electromagnetically stressed environments, the change can be helpful if the default setting does not provide satisfactory results.

Transmitting power on read (default)

Parameter-ID: 0008_{hex}
 UHF-Manager: Menu: *Device settings > Parameters... > Transmitting power*
 OPC UA: Variable *RFPower*
 Webserver: Menu: *Configuration > RFID > Antennas & power*

This parameter is used to specify which transmitting power (in dBm) the processor unit is to set for read operations after switching on or after a restart. The transmitting power is to be understood as radiated power (ERP or EIRP) and is transferred as parameter value in quarter-dBm.

Parameter value = P(dBm) × 4

The following parameters must also be set for correct adjustment of the radiated transmitting power. The required data can be taken from the data sheets of the UHF antenna and the antenna cable used.

- Antenna gain
- Antenna aperture angle
- Antenna polarization
- Cable attenuation

Adjustable power: 7...36 dBm (corresponds to 5 mW...4000 mW)

Length [bits]	Permissible values	Factory setting	Meaning
8	0, 28...144	108 (27 dBm (500 mW))	Standard transmitting power in ¼ dBm (ERP or EIRP)

i The maximum permissible transmitting power (ERP/EIRP) depends on nationally applicable regulations. Information on the maximum permitted transmitting power can be found in the information sheet on conformity and approvals.

i Depending on the device variant, the specifications for transmitting power are to be understood as ERP (Equivalent Radiated Power) or EIRP (Equivalent Isotropically Radiated Power) values. The respective valid information can be found in the information sheet on conformity and approvals.

Automatic increase of transmitting power on write

Parameter-ID: 0009_{hex}
 UHF-Manager: Menu: *Device settings > Parameters... > Transmitting power*
 OPC UA: –
 Webserver: Menu: *Configuration > RFID > Antennas & power*

This parameter can be used to specify whether the same transmitting power is used for write and read operations or whether the transmitting power is increased by an offset value for write operations. Many data carriers require a higher transmitting power for write operations than for read operations.

Write power (dBm) = Read power (dBm) + Offset (dB)

The desired offset power in quarter dB is transferred as the parameter value.

Adjustable offset power: 0...20 dB (corresponds to factor 1...100)

Length [bits]	Permissible values	Factory setting	Meaning
8	0...80	8 (2 dB (~factor 1.6))	Offset power in ¼ dB

The resulting transmitting power is automatically limited to the maximum permissible value.

i The maximum permissible transmitting power (ERP/EIRP) depends on nationally applicable regulations. Information on the maximum permitted transmitting power can be found in the information sheet on conformity and approvals. The device ensures compliance if the correct data of the antennas and cables used have been set.

Active channels

Parameter-ID: 000B_{hex}
 UHF-Manager: Menu: *Device settings > Parameters... > Basic UHF*
 OPC UA: –
 Webserver: Menu: *Configuration > RFID > Basic UHF*

The *Active channels* parameter can be used to define which frequencies or channels are used for communication with the data carrier. The setting is global for all sessions.

i The active channels setting is available only for devices that operate according to the European Union standard or a form derived from it. Further information can be found in the European standard ETSI EN 302 208 or derived national standards.

The following ETSI channels can be used:

ETSI channel	Frequency [MHz]
4	865.7
7	866.3
10	866.9
13	867.5

When using 2...4 channels, these are actuated one after the other via a frequency hopping procedure.

Individual channels can be activated (1) or deactivated (0) via a bit mask.

Example:

Channel assignment	Bit 7...Bit 4	Bit 3	Bit 2	Bit 1	Bit 0	Byte
4 and 10 activated, 7 and 13 deactivated	0	0	1	0	1	05 _{hex}

Adjustable values:

Length [bits]	Permissible values	Factory setting	Meaning
8	Bitmask 0F _{hex} ...00 _{hex}	0F _{hex} All channels on	Bit 0: Channel 4 Bit 1: Channel 7 Bit 2: Channel 10 Bit 3: Channel 13

i

- If only a single channel is active, there may be delays in detection, since a single channel may not be in operation continuously. As of 2 channels or more, this problem no longer exists.
- For static applications, the frequency hopping method can be advantageous, since local field minimums can be masked by the frequency change.
- If several processor units are in operation simultaneously in a confined space, mutual interference may occur if they operate on the same channels. In this case, it is recommended to operate the processor units on different and distant channels, e.g. processor unit 1 on channel 4 and processor unit 2 on channel 13.

7

Startup and operation (continued)

Auto-Setup

Parameter-ID: 1003_{hex}
 UHF-Manager: Menu: *Device settings > Parameters... > Transmitting power*
 OPC UA: –
 Webserver: Menu: *Configuration > RFID > Antennas & power*

When the *Auto-Setup* parameter is set to the value 1, the processor unit starts directly with the Auto-Setup via the specified antenna. During the Auto-Setup, no further commands are accepted by the processor unit, but the value of the parameter can be queried cyclically to detect the end and the result of the Auto-Setup.

The Auto-Setup is used to set the optimal transmitting power in a single tag application. For this purpose, the transmitting power is set so that only the data carrier positioned in front of the antenna is detected and processed.

During Auto-Setup, the RF LED (blue) indicates that the UHF field is on.

To be able to start the Auto-Setup, at least the *EXPERT* user level is required.

Auto-Setup can and must be activated for each antenna individually.

After successful completion, the Auto-Setup modifies both the global parameters 0008_{hex} *Transmitting power for antenna read (default)* and 0009_{hex} *Automatic increase of transmitting power on write* and the session-related parameter 1001_{hex} *Transmitting power for antenna read (current)*.

Adjustable values:

Length [bits]	Permissible values	Factory setting	Meaning
8	1 Automatically falls back to 0, 2, 3 or 4 after completion	0 (Off)	1: Auto-Setup 0: Inactive

The value read back means the following:

- 0: Auto-Setup not yet started or successfully completed. A single tag was able to be reliably read and written to on its own based on the power. All parameters were set.
- 1: Auto-Setup not yet completed.
- 2: Auto-Setup partially successful. Several tags were able to be detected, the transmitting power 0008_{hex} and 1001_{hex} were set to be able to detect and read at least one tag reliably.
- 3: Auto-Setup failed completely. No tag was found or it could not be read. No parameters were changed.
- 4: Auto-Setup partially successful. A single tag was able to be read reliably on its own based on the power, but not written to. The following reasons are possible:
 - Tag does not contain user data.
 - Tags are read-only.
 - The maximum power of the device is not sufficient to write reliably.

The transmitting power 0008_{hex} and 1001_{hex} have been set to reliably detect and read this tag.

7

Startup and operation (continued)

Write, read

The parameters *Write*, *Read* can be used to specify the size of various data fields, whether *BlockWrite* should be used for writing and how often a read command should be repeated in the event of access failure.

TID length

Parameter-ID:	0004 _{hex}
UHF-Manager:	Menu: <i>Device settings > Parameters... > Read-Write</i>
OPC UA:	–
Webserver:	Menu: <i>Configuration > RFID > Basic UHF</i>

The TID length determines how many data words (16 bits) of the TID are transferred from the data carrier to the processor unit. If data carriers are read whose TID is greater than the set TID length, the TID read is limited to the set number of bytes. If data carriers are read whose TID is smaller than the set TID length, the TID is not transmitted to the processor unit.

Adjustable values:

Length [bits]	Permissible values	Factory setting	Meaning
8	1...31 Data words	4 (4 words (8 bytes))	Number of data words (bytes) of the TID

Number of read attempts

Parameter-ID:	000A _{hex}
UHF-Manager:	Menu: <i>Device settings > Parameters... > Basic UHF</i>
OPC UA:	–
Webserver:	Menu: <i>Configuration > RFID > Basic UHF</i>

The *Number of read attempts* parameter is used to specify how often the processor unit attempts to repeat a failed read access to a data carrier before a negative status message is sent to the processor unit.

Adjustable values:

Length [bits]	Permissible values	Factory setting	Meaning
8	0...255	0x05 (5 repetitions)	Number of read attempts or repetitions

Activate BlockWrite

Parameter-ID:	000C _{hex}
UHF-Manager:	Menu: <i>Device settings > Parameters... > Air interface</i>
OPC UA:	–
Webserver:	Menu: <i>Configuration > RFID > Basic UHF</i>

With normal write accesses to a data carrier, the data is written sequentially to the data carrier word by word via several write operations. *Activate BlockWrite* allows several data words (16 bits) to be written to the data carrier with a single write access. The maximum number of data words can be defined via the *Max. write length* parameter.

When using *BlockWrite*, care should be taken to ensure that this command is supported by the data carriers being used.

If the *BlockWrite* command cannot be executed successfully on a data carrier because, for example, the data carrier does not support the command, the write operation is repeated with the ordinary write command.



In time-critical applications, *BlockWrite* can offer a time advantage. However, care must be taken to ensure that all data carriers support this command. Mixed operation of data carriers with and without *BlockWrite* support can lead to higher write/read times.

Adjustable values:

Length [bits]	Permissible values	Factory setting	Meaning
8	0 or 1	0 (<i>BlockWrite</i> off)	0 <i>BlockWrite</i> off 1: <i>BlockWrite</i> on

7

Startup and operation (continued)

Max. write length

Parameter-ID: 000D_{hex}
 UHF-Manager: Menu: *Device settings > Parameters... > Air interface*
 OPC UA: –
 Webserver: Menu: *Configuration > RFID > Basic UHF*

The *Max. write length* defines the maximum number of data words (16 bits) that can be transferred with a *BlockWrite* command.

1 to 255 data words can be transferred, whereby the setting of 0 or 1 corresponds to an ordinary write command.

Adjustable values:

Length [bits]	Permissible values	Factory setting	Meaning
8	1...255	16 (16 words (32 bytes))	Number of data words when writing with <i>BlockWrite</i>

i In a heavily electromagnetically stressed environment, better results may be achieved if fewer data words are transmitted in a command.

Max. read length

Parameter-ID: 000E_{hex}
 UHF-Manager: Menu: *Device settings > Parameters... > Air interface*
 OPC UA: –
 Webserver: Menu: *Configuration > RFID > Basic UHF*

The *Max. read length* defines the maximum number of data words (16 bits) that are transferred from the data carrier to the processor unit with a read command.

Adjustable values

Length [bits]	Permissible values	Factory setting	Meaning
8	1...255	16 (16 words (32 bytes))	Number of data words when reading from the data carrier

i In a heavily electromagnetically stressed environment, better results may be achieved if fewer data words are transmitted in a command.

Loop filter

UHF RFID technology works with electromagnetic waves that are emitted via antennas for communication between the data carrier and the processor unit. These waves are reflected by metallic objects, walls and floors, which can cause undesirable side effects (cancellations or amplifications). For example, data carriers that are further away or data carriers that have already left the reading point may be detected inadvertently.

The *MinReads*, *MinNoReads* and *WaitTime* parameters can be used to define a loop filter which, in the *ASYNCHRONOUS DETECTION* operating mode, specifies the criteria according to which a tag is reported as *COMES (DETECTED)* or as *GOES (ABSENT)* and the time interval after which a tag reported as *GOES* can be re-detected. This can be used to prevent data carriers that have already been detected from being detected again by mistake or to prevent the detection of unwanted data carriers that only respond sporadically.

MinReads or AsyncObserved threshold (default)

Parameter-ID: 0023_{hex}
 UHF-Manager: Menu: *Device settings > Parameters... > Read-Write*
 OPC UA: *SetASyncFilter/GetASyncFilter methods*
 Webserver: Menu: *Configuration > RFID > Filter options*

The *MinReads (default)* parameter defines how often a data carrier must be detected so that it is reported as *COMES*. This value is set after switching on or restarting the processor unit.

If a data carrier is to be detected twice in succession, for example, before it is reported as *COMES*, 2 must be set as the parameter value.

Adjustable values:

Length [bits]	Permissible values	Factory setting	Meaning
8	1...255	1	Required detections to report a data carrier as <i>Comes</i> .

7

Startup and operation (continued)

MinReads or AsyncObserved-Threshold

Parameter-ID: 100C_{hex}
UHF-Manager: –
OPC UA: SetAsyncFilter/GetAsyncFilter methods
Webserver: –

The *MinReads* parameter defines how often a data carrier must be detected so that it is reported as *COMES*. This parameter overwrites the *MinReads (default)* parameter and is valid until the current TCP session is terminated or the processor unit is restarted.

If a data carrier is to be detected twice in succession, for example, before it is reported as *COMES*, 2 must be set as the parameter value.

Adjustable values:

Length [bits]	Permissible values	Factory setting	Meaning
8	1...255	1	Required detections to report a data carrier as <i>COMES</i> .

MinNoReads or AsyncObserved-Timeout (default)

Parameter-ID: 0024_{hex}
UHF-Manager: Menu: *Device settings > Parameters... > Read-Write*
OPC UA: SetAsyncFilter/GetAsyncFilter methods
Webserver: Menu: *Configuration > RFID > Filter options*

The *MinNoReads (default)* parameter specifies how often a data carrier reported as *Comes* must not be detected for it to be reported as *GOES*. This value is set after switching on or restarting the processor unit.

If, for example, a data carrier is only to be reported as *GOES* if it has not been detected twice in succession, 2 must be set as the parameter value.

Adjustable values:

Length [bits]	Permissible values	Factory setting	Meaning
8	1...255	1	Required detection failures to report a data carrier as <i>GOES</i> .

MinNoReads or AsyncObserved-Timeout

Parameter-ID: 100D_{hex}
UHF-Manager: –
OPC UA: SetAsyncFilter/GetAsyncFilter methods
Webserver: –

The *MinNoReads (default)* parameter specifies how often a data carrier reported as *COMES* must not be detected for it to be reported as *GOES*. This parameter overwrites the *MinNoReads (default)* parameter and is valid until the current TCP session is terminated or the processor unit is restarted.

If, for example, a data carrier is only to be reported as *GOES* if it has not been detected twice in succession, 2 must be set as the parameter value.

Adjustable values:

Length [bits]	Permissible values	Factory setting	Meaning
8	1...255	1	Required detection failures to report a data carrier as <i>GOES</i> .

WaitTime (default)

Parameter-ID: 0029_{hex}
UHF-Manager: Menu: *Device settings > Parameters... > Read-Write*
OPC UA: SetAsyncFilter/GetAsyncFilter methods
Webserver: Menu: *Configuration > RFID > Filter options*

The *WaitTime (default)* parameter specifies the time interval after which a data carrier reported as *GOES* can be re-detected. This value is set after switching on or restarting the processor unit.

The 16-bit value is coded in 2 bytes in the order Low – High.

Adjustable values:

Length [bits]	Permissible values	Factory setting	Meaning
16	0...1000	0	Time in seconds during which a data carrier is ignored.

7

Startup and operation (continued)

WaitTime

Parameter-ID: 100E_{hex}
 UHF-Manager: –
 OPC UA: SetASyncFilter/GetASyncFilter methods
 Webserver: –

The *WaitTime* parameter specifies the time interval after which a data carrier reported as *Goes* can be re-detected. This parameter overwrites the *WaitTime (default)* parameter and is valid until the current TCP session is terminated or the processor unit is restarted.

The 16-bit value is coded in 2 bytes in the order Low – High.

Adjustable values:

Length [bits]	Permissible values	Factory setting	Meaning
16	0...1000	0	Time in seconds during which a data carrier is ignored

Data filter

Data filters can be used if only a subset from a data carrier population is to be detected. For this purpose, various criteria can be defined that describe the desired subset. For example, only data carriers whose EPC corresponds to a certain length or whose TID contains a special data sequence can be detected.

EPCLengthMin (default)

Parameter-ID: 002B_{hex}
 UHF-Manager: –
 OPC UA: SetFilter/GetFilter methods
 Webserver: –

The *EPCLengthMin* and *EPCLengthMax* parameters can be used to define a filter that excludes data carriers during detection if their EPC length is not within the specified filter range.

The parameter *EPCLengthMin (default)* defines the minimum EPC length in bytes, which is set after switching on or after a restart of the processor unit.

Adjustable values:

Length [bits]	Permissible values	Factory setting	Meaning
8	0...62	0 (0 byte)	EPC minimum length for filter (default)

EPCLengthMin

Parameter-ID: 100F_{hex}
 UHF-Manager: –
 OPC UA: SetFilter/GetFilter methods
 Webserver: –

The *EPCLengthMin* and *EPCLengthMax* parameters can be used to define a filter that excludes data carriers during detection if their EPC length is not within the specified filter range.

The *EPCLengthMin* parameter sets the minimum EPC length in bytes and overwrites the *EPCLengthMin (default)* parameter until the current TCP session is terminated or the processor unit is restarted.

Adjustable values:

Length [bits]	Permissible values	Factory setting	Meaning
8	0...62	0 (0 byte)	EPC minimum length for filter (temporary)

7

Startup and operation (continued)

EPCLengthMax (default)

Parameter-ID: 002C_{hex}
UHF-Manager: –
OPC UA: SetFilter/GetFilter methods
Webserver: –

The *EPCLengthMin* and *EPCLengthMax* parameters can be used to define a filter that excludes data carriers during detection if their EPC length is not within the specified filter range.

The *EPCLengthMax (default)* parameter defines the maximum EPC length in bytes, which is set after switching on or after a restart of the processor unit.

Adjustable values:

Length [bits]	Permissible values	Factory setting	Meaning
8	0...62	62 (62 bytes)	EPC minimum length for filter (default)

EPCLengthMax

Parameter-ID: 1010_{hex}
UHF-Manager: –
OPC UA: SetFilter/GetFilter methods
Webserver: –

The *EPCLengthMin* and *EPCLengthMax* parameters can be used to define a filter that excludes data carriers during detection if their EPC length is not within the specified filter range.

The *EPCLengthMax* parameter sets the maximum EPC length in bytes and overwrites the *EPCLengthMax (default)* parameter until the current TCP session is terminated or the processor unit is restarted.

Adjustable values:

Length [bits]	Permissible values	Factory setting	Meaning
8	0...62	62 (62 bytes)	EPC minimum length for filter (temporary)

EPCFilter (default)

Parameter-ID: 002D_{hex}
UHF-Manager: Menu: *Device settings* > *Parameters...* > *Filter*
OPC UA: SetFilter/GetFilter methods
Webserver: Menu: *Configuration* > *RFID* > *Filter options*

The *EPCFilter (default)* parameter can be used to create a specific data filter that selects data carriers directly according to a predefined filter mask during detection and reports only those data carriers that match this filter mask. The default filter is applied after switching on or after restarting the processor unit.

The filter mask is defined in the following form:

Filter mask = Address [1 word] + length [1 word] + filter data [max. 62 bytes]

Address and length specifications must be specified in bits. Masks can thus also start and end in the middle of bytes.

The value range in each case is 0...496 bits.

The sum of both values must not exceed 496.

The 16-bit values are specified as 2 bytes in the order Low – High.

The *FILTER DATA* field must contain at least as many bytes that allow the number of bits in the Length field to be transmitted with it. The bits are to be left-aligned and padded at the end to a whole byte length with zero bits.

Example:

Only data carriers whose EPC from byte address 02_{hex} onwards contains the data E2 00 01 02 03_{hex} (length 5 bytes) are to be reported.

Byte address 0002_{hex} = Bit address 0010_{hex}
Byte length 0005_{hex} = Bit length 0028_{hex}

Bit address [2 bytes]	Bit length [2 bytes]	Filter data (HEX) [5 bytes]
10 _{hex} 00 _{hex}	28 _{hex} 00 _{hex}	E2 00 01 02 03

Adjustable values:

Length [byte]	Permissible values	Factory setting	Meaning
4...66	Address [2 bytes] Length [2 bytes] Data [62 bytes]	Address: 0000 _{hex} Length: 0000 _{hex} Data: 00 _{hex} ...	Filtering data carriers by EPC data

EPCFilter

Parameter-ID: 1011_{hex}
 UHF-Manager: –
 OPC UA: *SetFilter/GetFilter methods*
 Webserver: –

The *EPCFilter* parameter can be used to create a specific data filter that selects data carriers directly according to a predefined filter mask when they are detected and reports only those data carriers that match this filter mask. The *EPCFilter* parameter overwrites the *EPCFilter (default)* parameter and is valid until the current TCP session is ended or the processor unit is restarted.

The filter mask is defined in the following form:

Filter mask = Address [1 word] + length [1 word] + filter data [max. 62 bytes]

The address and length specifications must be specified in bits. Masks can thus also start and end in the middle of bytes.

The value range in each case is 0...496 bits.

The sum of both values must not exceed 496.

The 16-bit values are specified as 2 bytes in the order Low – High.

The *FILTER DATA* field must contain at least as many bytes that allow the number of bits in the Length field to be transmitted with it. The bits are to be left-aligned and padded at the end to a whole byte length with zero bits.

Example:

Only data carriers whose EPC from byte address 02_{hex} onwards contains the data E2 00 01 02 03_{hex} (length 5 bytes) are to be reported.

Byte address 0002_{hex} = Bit address 0010_{hex}

Byte length 0005_{hex} = Bit length 0028_{hex}

Bit address [2 bytes]	Bit length [2 bytes]	Filter data (HEX) [5 bytes]
10 _{hex} 00 _{hex}	28 _{hex} 00 _{hex}	E2 00 01 02 03

Adjustable values:

Length [byte]	Permissible values	Factory setting	Meaning
4...66	Address [2 bytes] Length [2 bytes] Data [62 bytes]	Address: 0000 _{hex} Length: 0000 _{hex} Data: 00 _{hex} ...	Filtering data carriers by EPC data

TIDFilter (default)

Parameter-ID: 002E_{hex}
 UHF-Manager: Menu: *Device settings > Parameters... > Filter*
 OPC UA: *SetFilter/GetFilter methods*
 Webserver: Menu: *Configuration > RFID > Filter options*

The *TIDFilter (default)* parameter can be used to create a specific data filter that selects data carriers directly according to a predefined filter mask during detection and reports only those data carriers that match this filter mask. The default filter is applied after switching on or after restarting the processor unit.

The filter mask is defined in the following form:

Filter mask = Address [1 word] + length [1 word] + filter data [max. 62 bytes]

The address and length specifications must be specified in bits. Masks can thus also start and end in the middle of bytes.

The value range in each case is 0...496 bits.

The sum of both values must not exceed 496.

The 16-bit values are specified as 2 bytes in the order Low – High.

The *FILTER DATA* field must contain at least as many bytes that allow the number of bits in the Length field to be transmitted with it. The bits are to be left-aligned and padded at the end to a whole byte length with zero bits.

Example:

Only data carriers whose TID from byte address 02_{hex} onwards contains the data E2 00 01 02 03_{hex} (length 5 bytes) are to be reported.

Byte address 0002_{hex} = Bit address 0010_{hex}

Byte length 0005_{hex} = Bit length 0028_{hex}

Bit address [2 bytes]	Bit length [2 bytes]	Filter data (HEX) [5 bytes]
10 _{hex} 00 _{hex}	28 _{hex} 00 _{hex}	E2 00 01 02 03

Adjustable values:

Length [byte]	Permissible values	Factory setting	Meaning
4...66	Address [2 bytes] Length [2 bytes] Data [62 bytes]	Address: 0000 _{hex} Length: 0000 _{hex} Data: 00 _{hex} ...	Filtering data carriers by <i>EPC</i> data

TIDFilter

Parameter-ID: 1012_{hex}
UHF-Manager: –
OPC UA: *SetFilter/GetFilter methods*
Webserver: –

The *TIDFilter* parameter can be used to create a specific data filter that selects data carriers directly according to a predefined filter mask when they are detected and reports only those data carriers that match this filter mask. The *TIDFilter* parameter overwrites the *TIDFilter (default)* parameter and is valid until the current TCP session is ended or the processor unit is restarted.

The filter mask is defined in the following form:

Filter mask = Address [1 word] + length [1 word] + filter data [max. 62 bytes]

The address and length specifications must be specified in bits. Masks can thus also start and end in the middle of bytes.

The value range in each case is 0...496 bits.

The sum of both values must not exceed 496.

The 16-bit values are specified as 2 bytes in the order Low – High.

The *FILTER DATA* field must contain at least as many bytes that allow the number of bits in the Length field to be transmitted with it. The bits are to be left-aligned and padded at the end to a whole byte length with zero bits.

Example:

Only data carriers whose TID from byte address 02_{hex} onwards contains the data E2 00 01 02 03_{hex} (length 5 bytes) are to be reported.

Byte address 0002_{hex} = Bit address 0010_{hex}

Byte length 0005_{hex} = Bit length 0028_{hex}

Bit address [2 bytes]	Bit length [2 bytes]	Filter data (HEX) [5 bytes]
10 _{hex} 00 _{hex}	28 _{hex} 00 _{hex}	E2 00 01 02 03

Adjustable values:

Length [byte]	Permissible values	Factory setting	Meaning
4...66	Address [2 bytes] Length [2 bytes] Data [62 bytes]	Address: 0000 _{hex} Length: 0000 _{hex} Data: 00 _{hex} ...	Filtering data carriers by <i>TID</i> data

RSSI filter

When data carriers are detected, the processor unit can perform internal measurements that allow a statement to be made about the signal strength with which the data carrier was received. The determined signal strength, the RSSI value, can be used to define a filter that reports only those data carriers whose RSSI lies within a predefined range when data carriers are detected.

In simplified terms, it can be said that a data carrier that is close to the antenna results in a higher RSSI in an undisturbed environment than a data carrier that is further away. This would allow, for example, more distant data carriers that are not to be detected to be masked out.

The *RSSIMinFilter* and *RSSIMaxFilter* parameters can be used to specify the desired RSSI range. The total RSSI range includes values from –128 to +127. If the minimum is set to 128 and the maximum to +127, all detected data carriers pass the filter.

RSSIMinFilter (default)

Parameter-ID: 002F_{hex}
UHF-Manager: Menu: *Device settings > Parameters... > Filter*
OPC UA: *SetFilter/GetFilter methods*
Webserver: Menu: *Configuration > RFID > Filter options*

RSSIMinFilter (default) defines the RSSI lower limit to be used for detection. The defined value is used by the processor unit after switching on or after restarting the processor unit.

Adjustable values:

Length [byte]	Permissible values	Factory setting	Meaning
1	–128...+127	–128	<i>RSSI</i> lower limit for the <i>RSSI</i> filter

7

Startup and operation (continued)

RSSIMinFilter

Parameter-ID: 1013_{hex}
 UHF-Manager: –
 OPC UA: *SetFilter/GetFilter methods*
 Webserver: –

RSSIMinFilter overwrites the *RSSIMinFilter (default)* parameter and defines the RSSI lower limit to be used for detection. The parameter is valid until the current TCP session is terminated or the processor unit is restarted.

Adjustable values:

Length [byte]	Permissible values	Factory setting	Meaning
1	–128...+127	–128	RSSI lower limit for the RSSI filter

RSSIMaxFilter (default)

Parameter-ID: 0030_{hex}
 UHF-Manager: Menu: *Device settings > Parameters... > Filter*
 OPC UA: *SetFilter/GetFilter methods*
 Webserver: Menu: *Configuration > RFID > Filter options*

RSSIMaxFilter (default) specifies the RSSI upper limit to be used for detection. The defined value is used by the processor unit after switching on or after restarting the processor unit.

Adjustable values:

Length [byte]	Permissible values	Factory setting	Meaning
1	–128...+127	+127	RSSI upper limit for the RSSI filter

RSSIMaxFilter

Parameter-ID: 1014_{hex}
 UHF-Manager: –
 OPC UA: *SetFilter/GetFilter methods*
 Webserver: –

RSSIMaxFilter overwrites the *RSSIMaxFilter (default)* parameter and specifies the RSSI upper limit to be used for detection. The parameter is valid until the current TCP session is terminated or the processor unit is restarted.

Adjustable values:

Length [byte]	Permissible values	Factory setting	Meaning
1	–128...+127	+127	RSSI upper limit for the RSSI filter

FormattedTagData

The *FormattedTagData* function can be used if different data areas of a data carrier are to be detected or edited or if the data are to correspond to a special formatting. For this purpose, *FormattedTagData* offers the convenience that the processor unit independently executes all commands that are necessary to detect or edit the required data in the desired formatting.

The parameters *Prefix for ReadMultipleTagDataFormatted* and *Suffix for ReadMultipleTagDataFormatted* can be used to define text or byte sequences that precede or follow the data defined with *ReadMultipleTagDataFormatted*. This would allow, for example, an XML-like structure to be built.

Example:

Prefix: #0A#0D<TAGLIST>
 Format string: #A#0D<TAG><EPC>%Ex[0, 12]</EPC></TAG>
 Suffix: #0A#0D</TAGLIST>

The formatted data with the *ReadTagDataFormatted* and *WriteFormattedTagData* command are transferred without prefix and suffix in the following format:

FormattedTagData = *FormattedData(Tag)*

The formatted data with the *ReadMultipleTagDataFormatted* command is transferred with prefix and suffix in the following format:

FormattedTagData = *Prefix* + *FormattedData(1st Tag)* + *FormattedData(2nd Tag)* + ... + *Suffix*

Mapped to an XML file, the data might look like this:

```
<TAGLIST>
  <TAG><EPC>E20102030405060708090A0B</EPC></TAG>
  <TAG><EPC>E20B0A090807060504030201</EPC></TAG>
</TAGLIST>
```



The following parameters for the *FormattedTagData* function are session-related and are only valid until the current TCP session is ended or the processor unit is restarted. To set the default parameters, which are stored permanently, administrator security level access is required (see *Parameters for administrators* on page 52).

Format definition for ReadTagDataFormatted, ReadMultipleTagDataFormatted and WriteFormattedTagData

Parameter-ID: 1008_{hex}
 UHF-Manager: –
 OPC UA: *SetTagDataFormat/GetTagDataFormat*
 method
 Webserver: –

This parameter can be used to specify which data format is to be used for the *FormattedTagData* functions. For this purpose, a format string can be created from various format elements, which describes the type and formatting of the data, whereby the elements can be combined as desired. In the 007 protocol up to 99 characters can be defined. With OPC UA or with the web interface longer strings (up to 1024 characters) can also be defined, which are also valid in the 007 protocol.

Address and length fields:

Field	Meaning
Address (byte format)	Addresses data as byte offset (decimal: 0...65535).
Address (byte.bit format)	Start address: Addresses data as byte offset with bit offset (decimal: 0.0...65535.8)
Length	For address (byte format): Number of bytes For address (byte.bit format): Number of bits

Output elements:

Element	Meaning
#	Output: Defines a byte value (Hex) e.g. #0D#0A for the ASCII string 'Carriage Return' 'Line Feed'
##	Output: Outputs the ASCII character '#'
%%	Output: Outputs the ASCII character '%'
Text	Output: Any text to be output
%A[address, length]	Access: Outputs the specified range of the access password in hex format
%E[address, length]	EPC: Outputs the specified range of the EPC in hex format
%P[address, length]	PC: Outputs the specified range of the protocol control word from the EPC memory in hex format
%T[address, length]	TID: Outputs the specified range of the TID in hex format
%U[address, length]	USER: Outputs the specified range of user data in hex format

7

Startup and operation (continued)

Data modifier:

Modifier	Meaning
%_d...	Modifier d: Outputs data as decimal number in ASCII format (ASCII: 0...9)
%_x...	Modifier x: Outputs data as HEX byte in ASCII format (ASCII: 0...9a...F)
%_X...	Modifier X: Outputs data as HEX byte in ASCII format (ASCII: 0...9A...F)

Output of status values:

Element	Meaning
%S[0, 1]	Outputs the read status 0: OK 1: Read error 2: Signature error
%S[1, 1]	Outputs the EPC length (number of bytes 2...62)
%S[2, 1]	Outputs the RSSI (-128...+127)
%S[3, 1]	Always 00 _{hex} , with S[3.0,n], with n = 1 to 8 up to 8 fill bits 0 can be generated in the data stream
%S[4, 1]	Always FF _{hex} , with S[4.0,n], with n = 1 to 8 up to 8 fill bits 1 can be generated in the data stream

Example:

In this example, there is a data carrier that contains the following data:

EPC E2 01 02 03 04 05 06 07 08 09 0A 0B_{hex}
(12 bytes):
TID (8 bytes): C0 11 12 13 14 15 16 17_{hex}
USER 48 41 4C 4C 4F_{hex}
(5 bytes):

Format-String	Edition
E[0, 12]	E2 01 02 03 04 05 06 07 08 09 0A 0B _{hex}
EX[0, 12]	"E2 01 02 03 04 05 06 07 08 09 0A 0B"
<EPC>%Ex[0, 6]</EPC>	"<EPC>e2 01 02 03 04 05 </EPC>"
EPC:%E[0, 4]; USER:%UX[0, 5]	"EPC:" E2 01 02 03hex " ; USER:48414C4F"
LSB=%Td[0, 1] -MSB=%Td[7, 1]	"LSB=192-MSB=23"
LSB Half-Byte: = Ed[7.4, 4]	"LSB Half-Byte: = 7"



Via the web server interface in the Configuration > RFID > Formatted Tag Data area, the format elements and their effects can be tested in a simple way.

Adjustable values:

Length [byte]	Permissible values	Factory setting	Meaning
007: 0...99 Web and OPC UA: 0...1024	Format-String	"%Ex[0.12]#0d#0a" EPC string with CR LF	Format string for <i>FormattedTag-Data</i>



This parameter is session-related and is valid until the current TCP session is ended or the processor unit is restarted. To set the permanently stored default values, administrator security level access is required (see *Parameters for administrators* on page 52).

Prefix for ReadMultipleTagDataFormatted

Parameter-ID: 1009_{hex}
 UHF-Manager: –
 OPC UA: SetTagDataFormat/GetTagDataFormat
 method
 Webserver: –

Prefix for ReadMultipleTagDataFormatted specifies the text or byte sequence to be prepended to the data defined with *ReadMultipleTagDataFormatted*.

Adjustable values:

Length [byte]	Permissible values	Factory setting	Meaning
007: 0...99 Web and OPC UA: 0...1024	String	"Begin#0d#0a" Text "Begin" with CR LF	<i>Prefix for ReadMultipleTagDataFormatted</i>

Suffix for ReadMultipleTagDataFormatted

Parameter-ID: 100A_{hex}
 UHF-Manager: –
 OPC UA: SetTagDataFormat/GetTagDataFormat
 method
 Webserver: –

Suffix for ReadMultipleTagDataFormatted specifies the text or byte sequence to be appended to the data defined with *ReadMultipleTagDataFormatted*.

Adjustable values:

Length [byte]	Permissible values	Factory setting	Meaning
007: 0...99 Web and OPC UA: 0...1024	String	"End#0d#0a" Text "End" with CR LF	<i>Suffix for ReadMultipleTagDataFormatted</i>

Calculation format for signature generation

Parameter-ID: 100B_{hex}
 UHF-Manager: –
 OPC UA: SetTagSignatureFormat/GetTagSignatureFormat
 method
 Webserver: –

Defines the data areas of the data carrier that are included in the calculation for generating and verifying the signature (usually the EPC and the TID, possibly also part of the user data area for data carriers with larger memory). The area where the signature itself is stored (currently the first 64 bytes of the user data area) must not be included.

The specification must be exactly the same for signature generation and signature verification, otherwise the signature cannot be recognized as valid.

The specifications are generated using the same system as for the formatted output, although it is not useful to specify format modifiers (X, x, or d).

Examples:

12 bytes of the EPC and 12 bytes of the TID are to be included:

Calculation format: "%E[0.12]%T[0.12]"

12 bytes of the EPC and 12 bytes of the TID and 16 bytes of the user data area starting at address 64 are to be included:

Calculation format: "%E[0.12]%T[0.12]%U[64.16]"

For details on signature generation and verification, see *Data security* on page 11.

Adjustable values:

Length [byte]	Permissible values	Factory setting	Meaning
007: 0...99 Web and OPC UA: 0...1024	String	"%E[0.12]%T[0.8]" 12 byte EPC + 8 byte TID	Calculation format for signature generation

7.3.5 Description of parameters for administrators

Parameters for administrators can be changed by users of the *ADMIN* security level. This requires a login of the corresponding security level. Administrator parameters are permanently stored in the processor unit and retain their value until they are overwritten.

The administrator parameters mainly describe the configuration of the connected UHF hardware, the system and network properties as well as default parameters for special functions such as *Automatic Scan*, *FormattedTagData* and data carrier signature.

The network parameters are necessary for the operation of the processor unit within a network and must be parameterized for the network connection. System parameters, such as *time* or *time zone*, are only necessary for certain device functions, but should be set correctly to avoid malfunctions.

i Parameters for configuring the UHF components are used by the processor unit to perform a correct calculation of the radiated transmitting power. These parameters should therefore be set using the data sheets of the UHF components used!

The following groups of administrator parameters are described:

- *UHF components* (see page 73)
- *Network, system* (see page 75)
- *FormattedTagData (default)* (see page 79)

Automatic scanning

Parameter-ID: 000F_{hex}
 UHF-Manager: Menu: *Device settings > Parameters... > Basic UHF*
 OPC UA: –
 Webserver: –

The *Automatic scan* parameter can be used to specify whether and at what time interval an antenna should automatically monitor the detection range. Data that is detected during this process is transferred in the format that was specified via the parameters for the *ReadMultipleTagDataFormatted* function, see *Format definition for ReadTagDataFormatted*, *ReadMultipleTagDataFormatted* and *WriteFormattedTagData* parameters.

Automatic scanning can be parameterized independently for each TCP session, with either one antenna or all active antennas assigned to each session. The data is transmitted on a separate TCP port as pure user data (without protocol overhead). This keeps the network load on the main connection low and the data can be processed without protocol knowledge. Only the formatting of the data must be known.

When this parameter is saved, the antenna selection and the maximum number of data carriers from the last *UniversalTagList* command are recorded and used to execute the automatic scan.

The following TCP port assignments apply to *Automatic scan*:

Session	TCP session via which parameters are set	TCP session on which data is transferred
1	10001	10011
2	10002	10012
3	10003	10013
4	10004	10014
5	10005	10015

The parameter is transferred as a time value in multiples of 10 ms, where the value zero means that *Automatic scan* is disabled.

Time interval = (0...255) × 10 ms
 (0: Off, 10 ms...2550 ms)

Adjustable values:

Length [bits]	Permissible values	Factory setting	Meaning
8	0...255	0 (Off)	Waiting time between two automatic detections

7

Startup and operation (continued)

AsyncScanDelay

Parameter-ID: 0011_{hex}
 UHF-Manager: Menu: *Device settings > Parameters...*
 > *Read > Write*
 OPC UA: –
 Webserver: Menu: *Configuration > RFID > Filter*
 options

AsyncScanDelay can be used to define the cycle time used to search for new data carriers in the detection range in the *ASYNCHRONOUS DETECTION* operating mode.

Time interval = (0...255) × 10 ms
 (0: Off, 10 ms...2550 ms)

Adjustable values:

Length [bits]	Permissible values	Factory setting	Meaning
8	1...255	5 Cycle time 50 ms	Cycle time for <i>ASYNCHRONOUS DETECTION</i>

UHF components

By configuring the UHF components, antenna ports can be activated or deactivated and the connected UHF components can be described with regard to their physical properties.

The physical properties are described via the *antenna gain* and *cable attenuation* parameters. These parameters are required by the processor unit to correctly calculate the radiated transmitting power. The values can be taken from the data sheets of the UHF components used.



The radiated transmitting power is subject to national regulations and must therefore be limited to the maximum permitted value. By correctly specifying the antenna gain and the cable attenuation, the processor unit can perform the limiting independently and thus ensure compliance with the regulations. Furthermore, the correct calculation of the radiated transmitting power also leads to reproducible results if, for example, the antenna type or cable length is changed.



When using BIS U-3xx antennas from Balluff and BIS U-5xx antenna cables from Balluff, the UHF components can be easily parameterized via the UHF Manager configuration software or the web server. The Balluff components can be selected directly via their type designation. All required parameters are then selected automatically.

7

Startup and operation (continued)

Active antennas

Parameter-ID: 0012_{hex}
 UHF-Manager: Menu: *Device settings > Parameters... > Basic UHF*
 OPC UA: *AntennaActive* variable
 Webserver: Menu: *Configuration > RFID > Basic UHF*

The global parameter *Active antennas* can be used to specify which of the four antennas are to be activated or deactivated. The parameter is stored permanently and retains its value even after a restart of the processor unit. The individual antennas can be activated (1) or deactivated (0) via a bit mask.

Example:

Active antennas	Bit 7...Bit 4	Bit 3	Bit 2	Bit 1	Bit 0	Byte
1 and 3 activated, 2 and 4 deactivated	0	0	1	0	1	05 _{hex}

Adjustable values:

Length [bits]	Permissible values	Factory setting	Meaning
8	Bitmask 0F _{hex} ...00 _{hex}	0F _{hex} All antennas on	Bit 0: Antenna 1 Bit 1: Antenna 2 Bit 2: Antenna 3 Bit 3: Antenna 4

i The processor unit has a port monitoring function which can be used to detect whether an antenna is connected to an active antenna port. If no antenna is connected or if there is a cable break, a cable break message is output (see chapter 7.4 on page 85).

Antenna gain

Parameter-ID: 0013_{hex}
 UHF-Manager: Menu: *Device settings > Parameters... > Transmitting power*
 OPC UA: –
 Webserver: Menu: *Configuration > RFID > Antennas & power*

The *antenna gain* is a physical property of the antenna that describes how much of the supplied transmitting power is radiated in the main beam direction. The *antenna gain* thus describes the efficiency and directionality of the antenna. Depending on the manufacturer of the antenna, the *antenna gain* is specified differently in the data sheet.

Unit	Abbreviation	Meaning
dBi	G _i	<i>Antenna gain</i> (linear) related to an isotropic radiator
dBiC	G _{iC}	<i>Antenna gain</i> GC (circular) related to an isotropic radiator
dBd	G _D	<i>Antenna gain</i> related to a half-wave dipole

The *antenna gain* parameter is defined as antenna gain in relation to a half-wave dipole (GD). Depending on the data sheet specification, a conversion to dBd may be necessary:

Data sheet specification	Conversion to G _D
G _i (dBi)	G _D = G _i – 2.15 dB
G _{iC} (dBiC)	G _D = G _i – 5.15 dB

The parameter value is the antenna gain G_D in dB/20.

Parameter value	G _D [dBd]
=	0.05 dB

Adjustable values:

Length [bits]	Permissible values	Factory setting	Meaning
8	–400...+400	67 (corresponds to 3.35 dBd or 5.5 dBi)	<i>Antenna gain</i> G _D in dB/20 steps

i The parameter should be updated when the type of antenna used changes.

7

Startup and operation (continued)

Cable attenuation

Parameter-ID: 0014_{hex}
 UHF-Manager: Menu: *Device settings > Parameters... > Transmitting power*
 OPC UA: –
 Webserver: Menu: *Configuration > RFID > Antennas & power*

Cable attenuation is a physical property of the antenna cable that describes the factor by which a signal is attenuated along the antenna cable. The cable attenuation can be taken from the data sheet of the antenna cable used. Usually, the cable attenuation is specified in relation to 1 m of length. This results in the following relationship:

$$\text{Cable attenuation [dB]} = \text{Attenuation} \left[\frac{\text{[dB]}}{\text{m}} \right] \times \text{cable length [m]}$$

The parameter value is the antenna gain G_D in dB/20.

$$\text{Parameter value} = \frac{\text{Cable attenuation [dB]}}{0.05 \text{ dB}}$$

Adjustable values:

Length [bits]	Permissible values	Factory setting	Meaning
8	0...400	7 (corresponds to 0.35 dB)	Cable attenuation in dB/20 steps

Network, system

The network and system parameters can be used to make general settings required for operation in a network and, if necessary, to provide additional information such as time and device location.

The following network parameters are used in the delivery state:

- IP address (IPv4): 192.168.10.2
- Netmask: 255.255.255.0
- Gateway: 192.168.10.254
- Hostname: BISU6127

IP address

Parameter-ID: 0019_{hex}
 UHF-Manager: Menu: *Program settings > Interface... > CP/IP*
 OPC UA: –
 Webserver: Menu: *Configuration > Network*

The IP address (IPv4) can be used to identify and address the processor unit within the network. Each IP address can only be assigned once within a subnet. The IP address is transferred via a byte array of length 4 bytes in HEX or decimal format.

Example:

IP address	Parameter value decimal	Parameter value HEX
192.168.10.2	192 168 10 2	C0 A8 0A 02 _{hex}

Adjustable values:

Length [byte]	Permissible values	Factory setting	Meaning
4	Valid IPv4 address MSB...LSB	192 168 10 2	IPv4 address

The values are only accepted after a device restart.

7

Startup and operation (continued)

Netmask

Parameter-ID: 001A_{hex}
 UHF-Manager: Menu: *Program settings > Interface... > TCP/IP*
 OPC UA: –
 Webserver: Menu: *Configuration > Network*

The *netmask* defines how the IP address is to be interpreted or which parts of the IP address are used to identify the network and which are used to identify the device.

Example: With the netmask 255.255.255.0 the first 3 bytes (MSB...) are used for addressing the network and only the last byte (LSB) for addressing the device. 254 subscribers can thus be addressed (e.g. via the IP addresses 10.0.0.1...10.0.0.254) without using a router.

The *netmask* is transferred via a byte array of length 4 bytes in HEX or decimal format.

Example:

Netmask	Parameter value decimal	Parameter value HEX
255.255.255.0	255 255 255 0	FF FF FF 00 _{hex}

Adjustable values:

Length [byte]	Permissible values	Factory setting	Meaning
4	Valid net-mask MSB...LSB	255 255 255 0	IPv4 netmask

The values are only accepted after a device restart.

DHCP

Parameter-ID: 001B_{hex}
 UHF-Manager: Menu: *Program settings > Interface... > CP/IP*
 OPC UA: –
 Webserver: Menu: *Configuration > Network*

DHCP (Dynamic Host Configuration Protocol) can be used to specify whether the processor unit should use static, manually defined network parameters (*IP address, netmask, gateway,...*) for network communication, or whether these parameters should be obtained automatically from the network.

i DHCP can only be used in a network that allows the dynamic assignment of IP addresses. This must be ensured before activating DHCP, otherwise it may no longer be possible to access the processor unit via the network. In an emergency, this setting can be reversed via the service port (USB). An M12-USB service cable is required for this (see chapter 10.3 on page 173).

Adjustable values:

Length [byte]	Permissible values	Factory setting	Meaning
1	0, 1	0 No DHCP	0: No DHCP 1: DHCP

The value is only accepted after a device restart.

7

Startup and operation (continued)

Hostname

Parameter-ID: 001C_{hex}
 UHF-Manager: Menu: *Device settings > Parameters...*
 > *Device parameters*
 OPC UA: *DeviceName* variable
 Webserver: Menu: *Configuration > Device*

If there is a DNS server in the network with the processor unit, the processor unit can also be addressed via the *host name* (device name) as an alternative to the IP address. The *host name* must be unique and may only occur once within the subnet in which the device is located.

Adjustable values:

Length [byte]	Permissible values	Factory setting	Meaning
1...63	String with maximum 63 characters	"BISU6127"	Device name ¹⁾ for identification in the network

¹⁾ Only the characters A...Z, a...z, 0...9 and '-' may be used, whereby the '-' must not be at the beginning.

The value is only accepted after a device restart.

Gateway

Parameter-ID: 001D_{hex}
 UHF-Manager: Menu: *Program settings > Interface... > TCP/IP*
 OPC UA: –
 Webserver: Menu: *Configuration > Network*

Sets the *default gateway* for the TCP/IP connection. Normally, this is the IP address of the router that connects to other network segments.

Adjustable values:

Length [byte]	Permissible values	Factory setting	Meaning
4	0.0.0.0 or valid IPv4 address	192.168.10.254	Address of the <i>default gateway</i>

The values are only accepted after a device restart.

Name server

Parameter-ID: 001E_{hex}
 UHF-Manager: –
 OPC UA: –
 Webserver: Menu: *Configuration > Network*

If the network has *DNS servers* (Domain Name System), the *Nameserver* parameter can be used to specify the IP address of the primary (DNS IP1) and alternate (DNS IP2, if available) DNS servers.

Adjustable values:

Length [byte]	Permissible values	Factory setting	Meaning
8	0.0.0.0 twice or valid IP address	0 0 0 0 0 0 0 0	IP addresses of DNS servers 1 and 2.

7

Startup and operation (continued)

Device location

Parameter-ID: 001F_{hex}
 UHF-Manager: Menu: *Device settings > Parameters...*
 > *Device parameters*
 OPC UA: –
 Webserver: Menu: *Configuration > Device*

The *Device location* parameter can be defined as any free text and is intended to help locate the device within the plant, e.g. when maintenance work is due.

Adjustable values:

Length [byte]	Permissible values	Factory setting	Meaning
0...63	String with maximum 63 characters	“”	Any text, e.g. “2nd floor, plant 1”

Time zone, DST

Parameter-ID: 0020_{hex}
 UHF-Manager: Menu: *Device settings > Parameters...*
 > *Device parameters*
 OPC UA: –
 Webserver: Menu: *Configuration > Device*

For time functions or time stamps, *Time zone, DST* can be used to specify which *time zone* is to be used as the basis and whether an offset for *daylight saving time (DST)* is to be used.

The parameter is transferred as an offset to the universal time and a description text in the following form:

Parameter value = Time zone [1 byte] + DST [1 byte] + text [16 bytes]

Example:

The time is to be specified as Central European Summer Time (CEST). This corresponds to universal time +1 hour for Central Europe and offset +1 hour for Daylight Saving Time (UTC+2). *CEST* is to be appended as description text to clarify how the time is to be interpreted, padding the description text to 16 bytes in length if necessary.

Parameter value = 01_{hex} 01_{hex} “CEST” 00_{hex}...00_{hex}

Adjustable values:

Length [byte]	Permissible values	Factory setting	Meaning
18	Zone: –23...+23 DST: 0, 1, 2, FF _{hex} (Auto) Text: String with 16 characters	+1 0 “CET” Central European Winter Time	Time zone, DST and description text



When reading out the parameter, the effective time zone value is always returned. So in the above example, this is the value for 2 hours (1 hour of the time zone and 1 hour for daylight saving time). The daylight saving time specification DST is always returned with 0.
 An automatic changeover to daylight saving time is not carried out by the BIS U-6127 device, since the respective regulations can be different locally and an Internet connection is often not available.

7

Startup and operation (continued)

NTP server

Parameter-ID: 0021_{hex}
 UHF-Manager: Menu: *Device settings > Parameters... > Device parameters*
 OPC UA: –
 Webserver: Menu: *Configuration > Network*

If the network has access to an NTP server (*Network Time Protocol* or *time server*), time synchronization can be performed via the network using this server. The parameter *NTP server* defines how this time server is to be reached. A string with a maximum of 63 characters (bytes) is transferred as the parameter value, which can contain a URL or an IP address, e.g. "time.google.com" or "192.168.10.1".

Adjustable values:

Length [byte]	Permissible values	Factory setting	Meaning
0...63	URL or valid IPv4 address as string	""	URL or address of the NTP server

Time

Parameter-ID: 0022_{hex}
 UHF-Manager: Menu: *Device settings > Parameters... > Device parameters*
 OPC UA: –
 Webserver: Menu: *Configuration > Device*

The *Time* parameter can be used to set the *date* and *time* manually if no *NTP server* is available on the network.

Adjustable values:

Length [byte]	Permissible values	Factory setting	Meaning
14	Date and time in the format "YYYYMMDD-Dhhmmss"	Continuously updated	Date and time in the format "YYYYMMDD-Dhhmmss"

FormattedTagData (default)

In the chapter *Parameters for experts* on page 50, the *FormattedTagData* function is described with the relevant parameters. With a login of the *EXPERT* security level, these parameters can only be changed temporarily or in relation to a TCP session.

The *ADMIN* security level can also be used to define the default values that are used after the processor unit is switched on or restarted.

In the 007 protocol up to 99 characters can be defined. With OPC UA or with the web interface longer strings (up to 1024 characters) can also be defined, which are also valid in the 007 protocol.

Format definition for ReadTagDataFormatted, ReadMultipleTagDataFormatted and WriteFormattedTagData (default)

Parameter-ID: 0025_{hex}
 UHF-Manager: Menu: *Device settings > Parameters... > Read > Write*
 OPC UA: *SetTagDataFormatted/GetTagDataFormatted* method
 Webserver: *Configuration > RFID > Formatted tag data*

Defines the default data format for the *FormattedTagData* function to be used after switching on or restarting the processor unit.

Adjustable values:

Length [byte]	Permissible values	Factory setting	Meaning
007: 0...99 Web and OPC UA: 0...1024	Format-String	"%Ex[0.12]#0d#0a" EPC string with CR LF	Format string for <i>ReadTagDataFormatted</i> , <i>ReadMultipleTagDataFormatted</i> and <i>WriteFormattedTagData</i>

7

Startup and operation (continued)

Prefix for ReadMultipleTagDataFormatted (default)

Parameter-ID:	0026 _{hex}
UHF-Manager:	Menu: <i>Device settings > Parameters... > Read > Write</i>
OPC UA:	<i>SetTagDataFormatted/GetTagDataFormatted</i> method
Webserver:	<i>Configuration > RFID > Formatted tag data</i>

Defines the default prefix for the *FormattedTagData* function to be used after switching on or restarting the processor unit.

Adjustable values:

Length [byte]	Permissible values	Factory setting	Meaning
007: 0...99 Web and OPC UA: 0...1024	String	"Begin#0d#0a" Text "Begin" with CR LF	Prefix for <i>ReadMultipleTagDataFormatted</i>

Suffix for ReadMultipleTagDataFormatted (default)

Parameter-ID:	0027 _{hex}
UHF-Manager:	Menu: <i>Device settings > Parameters... > Read > Write</i>
OPC UA:	<i>SetTagDataFormatted/GetTagDataFormatted</i> method
Webserver:	<i>Configuration > RFID > Formatted tag data</i>

Defines the default suffix for the *FormattedTagData* function to be used after switching on or restarting the processor unit.

Adjustable values:

Length [byte]	Permissible values	Factory setting	Meaning
007: 0...99 Web and OPC UA: 0...1024	String	"End#0d#0a" Text "End" with CR LF	Suffix for <i>ReadMultipleTagDataFormatted</i>

Calculation format for signature generation (default)

Parameter-ID:	0028 _{hex}
UHF-Manager:	–
OPC UA:	<i>SetTagSignatureFormat/GetTagSignatureFormat</i> method
Webserver:	<i>Configuration > RFID > UHF extended</i>

Defines the data areas of the data carrier that are included in the calculation for generating and verifying the signature, usually the EPC and the TID, possibly also part of the user data area for data carriers with larger memory.

The area where the signature itself is stored (currently the first 64 bytes of the user data area) must not be included.

The specification must be exactly the same for signature generation and signature verification, otherwise the signature cannot be recognized as valid.

The specifications are generated using the same system as for the formatted output, although it is not useful to specify format modifiers (X, x, or d).

Examples:

12 bytes of the EPC and 12 bytes of the TID are to be included:

Calculation format: "%E[0.12]%T[0.12]"

12 bytes of the EPC and 12 bytes of the TID and 16 bytes of the user data area starting at address 64 are to be included:

Calculation format: "%E[0.12]%T[0.12]%U[64.16]"

For details on signature generation and verification, see *Data security* on page 11.

Adjustable values:

Length [byte]	Permissible values	Factory setting	Meaning
007: 0...99 Web and OPC UA: 0...1024	String	"%E[0.12]%T[0.8]" 12 bytes EPC + 8 bytes TID	Calculation format for signature generation

7

Startup and operation (continued)

SignatureType

Parameter-ID: 002A_{hex}

UHF-Manager: –

OPC UA: *SetTagSignatureFormat/GetTagSignatureFormat* method

Webserver: *Configuration > RFID > UHF extended*

Globally turns tag signature generation and verification off or on, and sets the hash and signature algorithm.

Currently, only the SHA256 + ECDSA512 algorithm is available.

Adjustable values:

Length [byte]	Permissible values	Factory setting	Meaning
1	0 and 1	0 (= off)	Signature Type 0 = Signature generation and verification off 1 = Signature verification on with SHA256 + ECDSA512 algorithm

7.3.6 Generating a key for signing tag data

In order to sign tag data or verify the signature, a key pair consisting of a private (priv) and a public (pub) key must be generated once. The private key is unique and cannot be recovered if lost. Since anyone who possesses the key can generate valid tag signatures, the key must be kept secret. The public key, on the other hand, can be used by third parties to check a signature for validity.

The private key is imported into all BIS devices involved and used there for signing and signature verification. All tags signed with the same private key (even in different devices) can be exchanged among themselves and always recognized as valid. Tags signed with a different key are always considered invalid.

To generate a key pair, the free software *openssl* is required, which is available for both Windows and Linux PCs, or the functions on the device website for generating a key must be used. In the latter case, we recommend using it on a secure network and temporarily turning off the device after saving the key to a PC.

Generate key pair

1. Install the *openssl* software on a PC.
2. In the command line application of the PC execute the following command to create a file with the name *nistp224_key.pem*. in the current directory:

```
openssl ecparam -name secp224r1  
-genkey -noout -out nistp224_key.pem
```

Display the private and public key of the file

- Enter the following commands:

```
openssl ec -in nistp224_key.pem -text  
-noout
```

For example, the display looks like this:

```
read EC key  
Private-Key: (224 bit)  
priv:1)  
d4:79:60:0b:2a:15:02:5c:48:34:d7:a8:7d:  
c0:c5:c0:c3:73:8b:f8:33:38:aa:bd:4b:d5:  
d7:a2  
pub:  
04:e6:65:43:e3:1e:9a:3d:fd:0c:98:ee:c4:  
60:f4:c8:4e:01:1c:54:28:85:ab:71:a4:02:  
01:89:92:90:05:33:2e:d3:04:4f:f0:22:b0:  
b1:26:a8:0d:f3:c3:fa:43:e7:93:6c:e9:a2:  
4c:e3:44:13:8b  
ASN1 OID: secp224r1  
NIST CURVE: P-224
```

¹⁾ The data following *priv:* (28 bytes) is the private key that must be loaded on the devices.

Importing a key into the device to sign tag data

To securely store the key in the *Secure Element* of the BIS U-6127, the following are required:

- a private key
- a key update ticket (a long character combination), which can be purchased from Balluff
- Internet access for the PC

i Each key update ticket can only be used once. For each device and for each change of a key, a new key update ticket is required, which can be obtained from Balluff Sales.

1. Download the current context file of the device to the PC by clicking on the *DOWNLOAD CONTEXT FILE* button on the device web page *Configuration / Security / Secure Element*.

i This step does not yet require an Internet connection, but it does require administrator privileges.

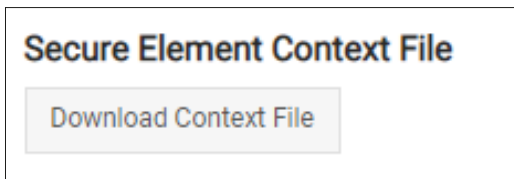


Fig. 7-31: Secure Element context file

2. Save file (with the *.WibuCmRaC* file extension) to the PC.
 3. *Optional:* Disconnect the device.
 4. Connect to the Internet.
 5. Using a browser (e.g. Google Chrome), navigate to the web page that was communicated together with the ticket from Balluff and make sure that there is a secure connection (in Google Chrome, this is indicated by the symbol of a closed padlock).
 6. Enter the ticket code.
- i** Each ticket can only be used for one update process.
7. After the prompt to upload the context file of the device, select the previously saved file and transfer it to the website.

8. After being prompted to enter the private key (*Secret Data*), enter the 32 bytes of data in hexadecimal notation and verify before confirming.

i Accepted characters are 0...9 and A...F or a...f. The *Elliptic Curve* key is only 28 bytes long. To get to 32 bytes, a total of four zero bytes (i.e. eight 0 characters) must be inserted at the end.

Example

pem file:

```
priv:
d4:79:60:0b:2a:15:02:5c:48:34:d7:
a8:7d:c0:c5:c0:c3:73:8b:f8:33:38:
aa:bd:4b:d5:d7:a2
```

Key to be entered:

```
d479600b2a15025c4834d7a87dc0c5c0
c3738bf83338aabd4bd5d7a200000000
```

A total of exactly 64 characters must be entered (the clipboard of the computer can also be used for this purpose).

9. Download an update file (with the *.WibuCmRaU* file extension) for the device from the website to the PC and save it.
10. Reconnect the PC to the BIS U-6127 device (the Internet connection is no longer needed).
11. Log in with a user ID that has administrator rights for the device.
12. Upload the received file (with the *.WibuCmRaU* file extension) to the device on the *Configuration / Security / Secure Element* page: First select the file and then click *UPLOAD UPDATE FILE*.

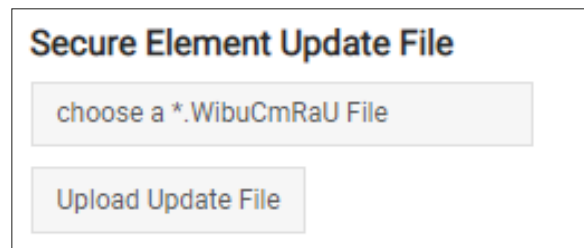


Fig. 7-32: Secure Element update file

i The file can only be successfully loaded on the same device from which the *WibuCmRaC* file was previously saved.

⇒ A status message confirms a successful import.

13. Perform a device restart.

Setting the data to be signed

In addition to the key, the setting of the data to be signed must also be the same for all devices involved. Usually, the EPC and the TID of the data carrier are included in the signature.

For tags with 12 byte EPC and 12 byte TID (including 64 bit serial number) the common definition is: %E[0.12]%T[0.12].

For tags with 12 byte EPC and 8 byte TID (including 32 bit serial number) the common definition is: %E[0.12]%T[0.8].

In principle, the generated signature can also be verified using the public key and a suitable SW application. With the BIS U-6127, it is currently necessary to enter the private key into the *Secure Element*.



The definition cannot be changed subsequently without all signatures created so far being recognized as invalid.

The setting is made on the device web page *Configuration / RFID / UHF Advanced* in the field *SIGNATURE CALCULATION FORMAT*.

Tag Signature	
Tag Signature	SHA256+ECDSA512
Signature Calculation Format	%E[0.12]%T[0.8]

Fig. 7-33: Tag signature



The signature is generated with all write commands that use the universal output format, both with the 007 protocol and with OPC UA. Other write commands, which can only write to individual memory banks, do not create a modified signature and can overwrite or invalidate an existing signature.

Switching on signature generation and verification

The use of the tag data signature is finally switched off and on by selecting the signature algorithm on the device web page *Configuration / RFID / UHF extended* in the *TAG SIGNATURE* field. The possible values are *Off* or *SHA256+ECDSA512*.



The signature is verified for all read commands that use the universal output format – both with 007 protocol and with OPC UA. The check result can be included in the output by specifying the status byte in the format string (e.g. as %SX[0.1] or %Sd[0.1]). A value of 0 indicates a successful check. A value of 2 means that the signature does not match the other tag data.

7

Startup and operation (continued)

7.4 System diagnostics

The BIS U-6127 processor unit offers extensive functions to display the operating status of the device and to detect and remedy possible problems.

LED display

The most important display is the *Power/Status* LED. It indicates the basic device status:

Display of Power/Status LED	Meaning	Recommended procedure
Off	No power supply or device defective	Supply the device with voltage.
Orange (when switched on)	Power supply OK, Linux system not yet loaded	Wait until system boots (max. 30 seconds).
Orange (during operation) ¹⁾	At least one application is not ready or has a warning status	Check application status and logbook on the device website (see below).
Flashing green (after switching on)	Linux system loaded, applications and UHF reader are started	Wait until system boots (max. 30 seconds).
Green ¹⁾	System fully operational	–
Red ¹⁾	One or more applications has/have an error status	Check application status and logbook on the device website (see <i>Application status and log</i> on page 86).

¹⁾ This LED state is also displayed on the device website *HOME*.

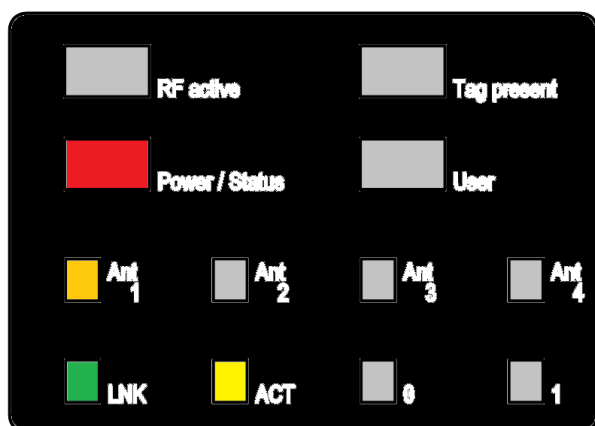


Fig. 7-34: LED display

7

Startup and operation (continued)

Application status and log

On the device website in the *LOGBOOK* tab, there are three sections that provide detailed information about the device status (see Fig. 7-35).

If the Power/Status LED signals that there is a warning or an error, details can be retrieved here, on the one hand for each application in the device in the *APPLICATION STATUS* section, and on the other hand also as a time log in the *LOG* section. The available information can be helpful for troubleshooting.

BIS U-6127

Home
 Login
 Language
 RFID
 Setup
 Log
 Info

Log

Module Information

Product Name:	BIS U-6127-081-104-06-ST36	HW Version:	1.0
Serial Number:	DE17040100000001	SW Version:	0.1.11
MAC Address:	50-2d-f4-0d-f4-33	SW Build:	20
IP Address:	192.168.0.236	Contact:	Balluff GmbH

Application Status

Status	Application	Info	Time Stamp
OK	DeviceServer		2020-09-15 14:02:48
OK	OpcUa_U6127_App		2020-09-15 14:02:51
OK	ParameterServer		2020-09-15 14:02:54
OK	Uhf_007_App.P10001		2020-09-15 14:02:56
OK	Uhf_007_App.P10002		2020-09-15 14:02:59
OK	Uhf_007_App.P10003		2020-09-15 14:03:02
OK	Uhf_007_App.P10004		2020-09-15 14:03:04
OK	Uhf_007_App.P10005		2020-09-15 14:02:40
OK	Uhf_007_App.PttyGS0		2020-09-15 14:02:43
OK	Uhf_KBRPReader		2020-09-15 14:02:46

Log
Download Log

Nr.	Severity	Time Stamp	Origin	Info
330	INFO	[com.balluff.diagnostics] [34292213696ms] INFO : 2020-09-15 10:18:06	ParameterServer	AppInfo: Application registered successfully. com.balluff.OpcUa_U6127_App
329	WARNING	[com.balluff.diagnostics] [34292213445ms] INFO : 2020-09-15 10:18:06	OpcUa_U6127_App	reported warning state

Fig. 7-35: Logbook

7

Startup and operation (continued)

Occasional error situations

The following error situations may occur occasionally:

Error	Power/Status LED display	Error causes and rectification
Error message <i>Cable break</i> , Uhf_KBRPReader reports in logbook: <i>Cable break at antenna #</i>	Red	Antenna connection parameterized without an antenna being connected or the connection to the antenna is interrupted. ► Check antenna connection and settings.
Uhf_KBRPReader reports in logbook: <i>Cannot connect to reader</i>	Red	Power supply current limit too low to operate UHF functions properly. ► Provide power supply with higher current, contact service in case of repeated occurrence.
Device cannot be reached via 007 with TCP (<i>connection timed out or connection refused at the client</i>)	Green	Incorrect 007 port number used. ► Use correct port number. 007 protocol disabled. ► Activate 007 via web interface. A connection is already active on the addressed port. ► Disconnect previous connection. No IP address received via DHCP or incorrect IP address set. ► Check via UHF Manager on USB port and change if necessary.
Fatal error of an application	Red	Multiple causes possible. ► Restart device, contact service in case of repeated occurrence.
Device restarts regularly, many <i>startup</i> entries in short time in logbook	Orange	Power supply current limit too low to operate UHF functions properly. ► Provide power supply with higher current, contact service in case of repeated occurrence.
OpcUa_U6127_App does not run (fatal error), no OPC-UA connection possible	Red	Date/time is incorrect. ► Set date/time and time zone correctly Certificate does not exist, invalid or with incorrect date entry ► Set date/time and time zone correctly, create new certificate, restart device

7

Startup and operation (continued)

7.5 Operation

When operating the processor unit, the following hazards must be observed and avoided:

CAUTION

Ultra high frequency electromagnetic waves

The antennas of the identification system BIS U transmit ultra-high frequency electromagnetic waves. Additional measures must be taken to prevent health hazards.

- ▶ Make sure that people do not stay in the vicinity of the antennas for an extended period of time.
- ▶ Use suitable measures to shield areas that are explicitly not to be covered.

NOTICE

Exceeding the maximum current consumption

If the maximum current consumption is exceeded, the processor unit and connected system components may be damaged.

- ▶ During operation, make sure that the total current carried by the Power terminal does not exceed 3 A.
- ▶ The voltage output (L+) on the IO-Link port and digital outputs (I/O) are supplied via the Power connection. The sum of the partial currents of these pins, must not exceed a maximum current of 2 A.

For communication of the processor unit with the controlling system, the Balluff 007 protocol can be selected, which is transmitted via an Ethernet TCP/IP connection. The protocol is byte-oriented and uses little overhead, since complete, error-free and sequence-correct data transmission is ensured by the Ethernet transmission channel.

i The procedure for creating or opening a TCP/IP socket connection depends on the system used (PC, controller, etc.) and the programming language used (for guidance, see chapter 7, for details, see the documentation of the controlling system or the selected programming language).

8.1 Protocol sequence

The protocol is based on synchronous commands, which are structured according to the *Request – Response* principle. Accordingly, the controller receives a corresponding response to each correct request, which may contain data or a status message. The sequence as described in this chapter must be followed. Inputs that deviate from this are ignored or not acknowledged by the processor unit. After a command has been completely processed or aborted, the processor unit automatically returns to the basic status.

i The only exception, which deviates from the *Request – Response* principle used, is the asynchronous message *Tag comes* or *Tag goes*, which is sent to the controller without a previous request. This function must be activated via the parameter *AsyncOperation* (see *AsyncOperation* in chapter 7.3 on page 55).

Single-stage commands are executed according to the principle *BASIC STATE – REQUEST – RESPONSE – BASIC STATE*:

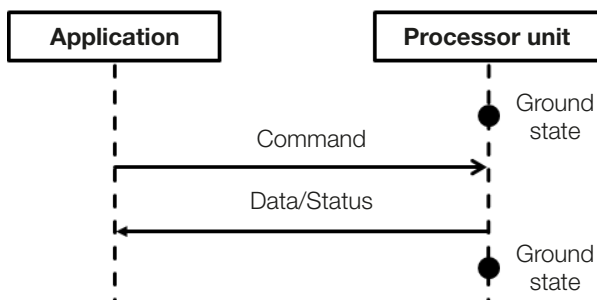


Fig. 8-1: Single-stage commands

Multi-stage commands are executed according to the principle *BASIC STATE – REQUEST – RESPONSE – ACKNOWLEDGMENT/DATA – RESPONSE – ... – BASIC STATE*:

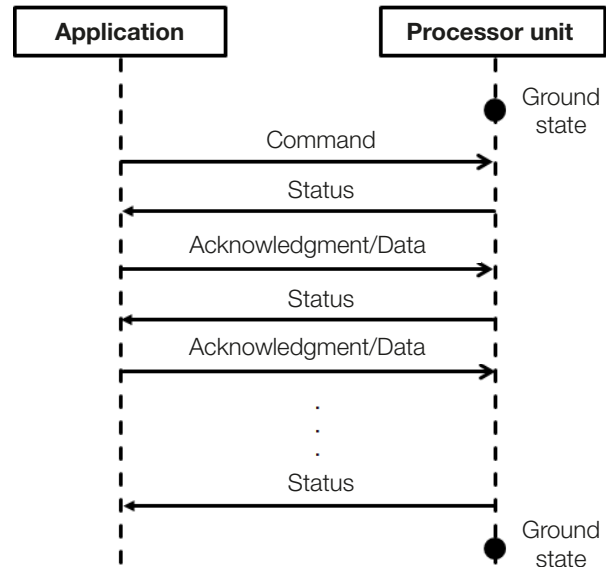


Fig. 8-2: Multi-stage commands

Multi-stage commands can be aborted by the controller using the *Abort* command (command identifier 'Q') after each response received. The processor unit then returns to the basic state and waits for an input.

8.5 Command overview

General commands

Function	Command recognition		Description
	ASCII	HEX	
Abort	'Q'	51 _{hex}	Abort asynchronous commands.
System Reboot	'q'	71 _{hex}	System reboot
Read network parameters	'm'	6D _{hex}	Read Ethernet network parameters.
Change network parameters	'j'	6A _{hex}	Set Ethernet network parameters.
Read transmitting power	'o'	6F _{hex}	Read out transmitting power of specified antenna.
Change transmitting power	'p'	70 _{hex}	Set transmitting power of specified antenna.
Read device parameters	'G'	47 _{hex}	Read out device parameters.
Change device parameters	'E'	45 _{hex}	Set device parameters.
Read version	'V'	56 _{hex}	Read out information on processor unit. – BIS U type designation – Hardware version/firmware version/serial number – IO-Link FW version

Detect data carriers

Function	Command recognition		Description
	ASCII	HEX	
Number of data carriers	'N'	4E _{hex}	Query the number of tags that are within the detection range of the specified antenna.
Detect data carriers	'M'	4D _{hex}	Detects the data carriers that are in the detection range of the specified antenna and returns a list of the requested data (EPC or TID).
Detect data carriers, extended	','	2C _{hex}	Detects the data carriers that are in the detection range of the specified antenna and returns a list of the requested data (EPC or TID) and additional information.

Asynchronous messages, Tag goes/Tag comes

Function	Command recognition		Description
	ASCII	HEX	
Data carrier comes, event	<DLE> '+'	102B _{hex}	Reports a tag as Comes when it enters the detection range.
Data carrier goes, event	<DLE> '-'	102D _{hex}	Reports a tag as Goes when it leaves the detection range.

Edit data carrier

Function	Command recognition		Description
	ASCII	HEX	
Select data carrier (Select)	'z'	7A _{hex}	Selects a specified data carrier within a data carrier population
Deselect data carrier (Unselect)	'n'	6E _{hex}	Deselects the last specified data carrier, see <i>Select</i> command
Read data carrier	'L'	4C _{hex}	Read user data from a data carrier Number of bytes: 0...1024 bytes
Read data carrier, extended	'H'	48 _{hex}	Read selected data from a data carrier. Number of bytes: > 1024 bytes
Read data carrier, EPC	'O'	4F _{hex}	Read EPC data from a data carrier.
Read data carrier, TID	'y'	79 _{hex}	Read TID data from a data carrier.
Read data carrier, bulk	'l'	49 _{hex}	Detects the data carriers that are in the detection range of the specified antenna and returns a list of the user data.
Read data carrier, bulk extended	'>'	3E _{hex}	Detects the data carriers that are in the detection range of the specified antenna and returns a list of the requested data.
Write data carrier	'P'	50 _{hex}	Write user data to a data carrier. Number of bytes: 0...1024 bytes
Write data carrier, constant value	'C'	43 _{hex}	Write constant user data to a data carrier.

Function	Command recognition		Description
	ASCII	HEX	
Write data carrier, EPC	'v'	76 _{hex}	Write EPC data to a data carrier and adjust length information of the EPC if necessary.
Write data carrier, extended	'F'	46 _{hex}	Write selected data to a data carrier. Number of bytes: > 1024 bytes
Write data carrier, bulk	'w'	77 _{hex}	Write user data to the data carriers that are in the detection range of the specified antenna.
Write data carrier, bulk extended	'<'	3C _{hex}	Write selected data to the data carriers that are in the detection range of the specified antenna and feedback of the successfully written data carriers.
Kill	'k'	6B _{hex}	Permanently (irreversibly) deactivates a selected data carrier.
Lock	'l'	6C _{hex}	Lock memory areas of a selected data carrier.

Universal data carrier (formatted tag data)

Function	Command recognition		Description
	ASCII	HEX	
Detect data carrier, universal	'-' 'L'	2D4C _{hex}	Detects the data carriers that are in the detection range of the specified antenna and returns a list with individually parameterizable data.
Read data carrier, universal	'-' 'R'	2D52 _{hex}	Read individually parameterizable data from a data carrier.
Write data carrier, universal	'-' 'W'	2D57 _{hex}	Write individually parameterizable data to a data carrier.

IO-Link

Function	Command recognition		Description
	ASCII	HEX	
Acyclical demand data, read	'i'	69 _{hex}	Receive demand/parameter data from IO-Link device.
Acyclical demand data, write	'e'	65 _{hex}	Send demand/parameter data to IO-Link device.
Digital output ports, set/reset	'/'	2F _{hex}	Set/reset pin 2 or pin 4 if used as digital output.
Digital input ports, read	'**'	2A _{hex}	Query states of pin 2 or pin 4, if these are operated as digital inputs.
Cyclical process data, read	'Y'	59 _{hex}	Read cyclical IO-Link process data.
Cyclical process data, write	'X'	58 _{hex}	Write cyclical IO-Link process data.
IO-Link master configuration, read	'#'	23 _{hex}	Read out the IO-Link master configuration.
IO-Link master configuration, write	'g'	67 _{hex}	Set the IO-Link master configuration.

8.6 Status codes

Status code	Hex	Functional description
'0'	30 _{hex}	OK/Successful
'1'	31 _{hex}	No data carrier in the detection range of the antenna.
'2'	32 _{hex}	Reading of data carrier not possible.
'3'	33 _{hex}	Data carrier was removed from the detection range of the antenna during reading.
'4'	34 _{hex}	Cannot write to the data carrier.
'5'	35 _{hex}	Data carrier was removed from the detection range of the antenna during writing.
'6'	36 _{hex}	The device has detected a hardware problem.
'7'	37 _{hex}	Sent data does not comply with 007 protocol.
'8'	38 _{hex}	BCC of the received data does not match the transmitted BCC.
'9'	39 _{hex}	Cable break on an active antenna port or no antenna connected.
'A'	41 _{hex}	There is more than 1 data carrier in the detection range of the antenna(s) (only for single tag operations).
'D'	44 _{hex}	Internal device error
'E'	45 _{hex}	CRC or signature of the data carrier incorrect.
'F'	46 _{hex}	The selected memory area is not supported by the data carrier.
'N'	4E _{hex}	The selected antenna is not active.
'P'	50 _{hex}	The command was executed on the wrong Ethernet port.
'S'	53 _{hex}	The command or parameter is not supported by the processor unit.
'X'	58 _{hex}	Access denied. The current user level does not allow this action.
'Y'	59 _{hex}	The device is currently in a state that does not allow the command to be executed.
'a'	61 _{hex}	This function is not supported by the data carrier
'b'	62 _{hex}	Incorrect or invalid license key

Status code	Hex	Functional description
'c'	63 _{hex}	Invalid parameter values were written.
'd'	64 _{hex}	Communication between the processor unit and the data carrier is interrupted.
'f'	66 _{hex}	A password is required for this operation.
'g'	67 _{hex}	Invalid password
'h'	68 _{hex}	The selected memory area is locked.
'i'	69 _{hex}	A specified parameter is outside the valid range of values.
'j'	6A _{hex}	Command is not supported by the data carrier/no or incorrect data carrier selected.

8.7 General commands

Command identifier 'Q': Abort

Cancel multi-stage or asynchronous commands. An abort is possible after receiving each response. The processor unit goes to the basic state after abort and waits for an input.

Byte	Length	Command element	Value range
00	1	Command identifier (ASCII)	'Q'
01	1	BCC	00 _{hex} ...FF _{hex}

Status message:

Byte	Length	Command element	Value range
00	1	Status	<ACK> or <NAK>
01	1	Status code	See table <i>Status codes</i> on page 94

Command identifier 'q': System reboot

Causes the processor unit to shut down and restart the system.

After the restart, the processor unit goes into the basic state and waits for an input.

Byte	Length	Command element	Value range
00	1	Command identifier (ASCII)	'q'
01	1	Reserved	'0'
02	1	BCC	00 _{hex} ...FF _{hex}

Status message:

Byte	Length	Command element	Value range
00	1	Status	<ACK> or <NAK>
01	1	Status code	See table <i>Status codes</i> on page 94
02	1	BCC	00 _{hex} ...FF _{hex}

The execution of this command requires prior login with a user with admin privileges.

Command identifier 'm': Read network parameters

Readout of Ethernet network parameters. The parameters are transferred in ASCII-hex number format.

Example:

IP address: 192.168.68.101 "C0A84465"
Subnet mask: 255.255.255.0 "FFFFFF00"

Byte	Length	Command element	Value range
00	1	Command identifier (ASCII)	'm'
01	1	BCC	00 _{hex} ...FF _{hex}

Status message:

Byte	Length	Command element	Value range
00	1	Status	<ACK> or <NAK>
01	1	Status code	See table <i>Status codes</i> on page 94

If the status message is positive, data is requested with <STX>.

Byte	Length	Command element	Value range
00	1	Control command	<STX>

If the command is executed successfully, data follows.

Byte	Length	Command element	Value range
00	1	Status	<ACK>
01...08	8	IP address (ASCII hex)	"00000000"... "FFFFFFF"
09...16	8	Subnet mask (ASCII hex)	"00000000"... "FFFFFFF"
17...24	8	Gateway address (ASCII hex)	"00000000"... "FFFFFFF"
25	1	IP configuration (ASCII)	'0': Static '1': DHCP
26	1	BCC	00 _{hex} ...FF _{hex}

If the data cannot be provided, a negative status message follows.

Byte	Length	Command element	Value range
00	1	Status	<NAK>
01	1	Status code	See table <i>Status codes</i> on page 94

Command identifier 'j': Change network parameters

Set the Ethernet network parameters. The parameters are transferred in ASCII-hex number format.

IP address: 192.168.68.101 "C0A84465"
Subnet mask: 255.255.255.0 "FFFFFF00"

Byte	Length	Command element	Value range
00	1	Command identifier (ASCII)	'j'
01...08	8	IP address (ASCII hex)	"00000000"... "FFFFFFF"
09...16	8	Subnet mask (ASCII hex)	"00000000"... "FFFFFFF"
17...24	8	Gateway address (ASCII hex)	"00000000"... "FFFFFFF"
25	1	IP configuration (ASCII)	'0': Static '1': DHCP
26	1	BCC	00 _{hex} ...FF _{hex}

Status message:

Byte	Length	Command element	Value range
00	1	Status	<ACK> or <NAK>
01	1	Status code	See table <i>Status codes</i> on page 94

If the status message is positive, a system reboot is initiated with <STX> in order to adopt the new network parameters.

Byte	Length	Command element	Value range
00	1	Control command	<STX>

The execution of this command requires prior login with a user with admin privileges.

Command identifier 'o': Read transmitting power

Readout of the currently set transmitting power (ERP/EIRP) as 1/4-dBm value.

Example:

When reading out the transmitting power, the following values are returned (5c_{hex}):

- Transmitting power High byte: '5'
- Transmitting power Low byte: 'c'

$$5C_{\text{hex}} = 92$$

$$92 \times \frac{1}{4} \text{ dBm} = 23 \text{ dBm}$$

A transmitting power of 23 dBm is thus set.

Byte	Length	Command element	Value range
00	1	Command identifier (ASCII)	'o'
01	1	Antenna number (ASCII)	'1'...'4': Single antenna
02	1	BCC	00 _{hex} ...FF _{hex}

Status message

Byte	Length	Command element	Value range
00	1	Status	<ACK> or <NAK>
01	1	Status code	See table <i>Status codes</i> on page 94

If the status message is positive, data is requested with <STX>.

Byte	Length	Command element	Value range
00	1	Control command	<STX>

If the command is executed successfully, data follows.

Byte	Length	Command element	Value range
00	1	Status	<ACK>
01...02	2	Transmitting power (ASCII hex)	"00"... "FF"
03	1	BCC	00 _{hex} ...FF _{hex}

If the data cannot be provided, a negative status message follows.

Byte	Length	Command element	Value range
00	1	Status	<NAK>
01	1	Status code	See table <i>Status codes</i> on page 94

Command identifier 'p': Change transmitting power

Setting the transmitting power (ERP/EIRP) as ¼-dBm value. The transmitting power influences the maximum range of the detection range of the antenna.

Example:

Set a transmitting power of 23 dBm (200 mW):

$$\frac{23 \text{ dBm}}{\frac{1}{4} \text{ dBm}} = 92$$

$$92 = 5C_{\text{hex}}$$

The following values must be transferred for this purpose:

- Transmitting power 1st character: '5'
- Transmitting power 2nd character: 'C'

i The maximum permissible transmitting power depends on the antenna used and on the radio regulations applicable in the respective country. For detailed information, see chapter 5 on page 18 and the data sheet of the antenna used.

Byte	Length	Command element	Value range
00	1	Command recognition	'p'
01	1	Antenna number (ASCII)	'0': All antennas '1'...'4': Single antenna
02...03	2	Transmitting power (ASCII hex)	"00"..."FF"
04	1	BCC	00 _{hex} ...FF _{hex}

Status message:

Byte	Length	Command element	Value range
00	1	Status	<ACK> or <NAK>
01	1	Status code	See table <i>Status codes</i> on page 94

If the status message is positive, the new transmitting power is accepted with <STX>.

Byte	Length	Command element	Value range
00	1	Control command	<STX>

Status message:

Byte	Length	Command element	Value range
00	1	Status	<ACK> or <NAK>
01	1	Status code	See table <i>Status codes</i> on page 94

Command identifier 'G': Read device parameters

Reading out general and antenna-related parameter data. For a detailed parameter description, see chapter 7.3 on page 49.

Byte	Length	Command element	Value range
00	1	Command identifier (ASCII)	'G'
01	1	Antenna number (ASCII)	'1': Antenna 1 '2': Antenna 2 '3': Antenna 3 '4': Antenna 4
02...05	4	Parameter number (ASCII hex)	"0000"..."FFFF"
06	1	BCC	00 _{hex} ...FF _{hex}

The positive status message contains the requested parameter data.

Byte	Length	Command element	Value range
00	1	Status	<ACK>
01	1	Reserved (ASCII)	'0'
02	1	Antenna number (ASCII)	'0': General '1': Antenna 1 '2': Antenna 2 '3': Antenna 3 '4': Antenna 4
03...04	1	Number of bytes (ASCII)	"00"..."99"
05...08	2	Parameter number (ASCII hex)	"0000"..."FFFF"
09	4	Data	00 _{hex} ...FF _{hex}
...	...	...	00 _{hex} ...FF _{hex}
Last byte	1	BCC	00 _{hex} ...FF _{hex}

If the data cannot be provided, a negative status message follows.

Byte	Length	Command element	Value range
00	1	Status	<NAK>
01	1	Status code	See table <i>Status codes</i> on page 94
02	1	BCC	00 _{hex} ...FF _{hex}

Command identifier 'E': Change device parameters

Writing general and antenna-related parameters. Antenna-related parameters can be set individually for each antenna. For a detailed parameter description, see chapter 7.3 on page 49.

Byte	Length	Command element	Value range
00	1	Command identifier (ASCII)	'E'
01	1	Antenna number (ASCII)	'0': All antennas/ General '1': Antenna 1 '2': Antenna 2 '3': Antenna 3 '4': Antenna 4
02...03	2	Number of bytes (ASCII)	"00"... "99"
04...07	4	Parameter number (ASCII hex)	"0000"... "FFFF"
08	1	Data	00 _{hex} ...FF _{hex}
...	...	...	00 _{hex} ...FF _{hex}
Last byte	1	BCC	00 _{hex} ...FF _{hex}

Status message:

Byte	Length	Command element	Value range
00	1	Status	<NAK>
01	1	Status code	See table <i>Status codes</i> on page 94
02	1	BCC	00 _{hex} ...FF _{hex}

Command identifier 'V': Read version

Reads out the firmware version string of the processor unit used.

Byte	Length	Command element	Value range
00	1	Command identifier (ASCII)	'V'
01	1	BCC	00 _{hex} ...FF _{hex}

If the command is executed successfully, data follows.

Byte	Length	Command element	Value range
00	Variable	Version string	ASCII string with variable length
Last byte	1	BCC	00 _{hex} ...FF _{hex}

If the data cannot be provided, a negative status message follows.

Byte	Length	Command element	Value range
00	1	Status	<NAK>
01	1	Status code	See table <i>Status codes</i> on page 94
02	1	BCC	00 _{hex} ...FF _{hex}

8

007 protocol (continued)

8.8 Detect data carriers

Command identifier 'N': Number of data carriers

Detects the data carriers that are within the detection range of the specified antenna and returns the number of detected data carriers. With the data carrier selection, either all or only selected data carriers can be detected (see *Command identifier 'z': Select data carrier (Select)* on page 105).

Byte	Length	Command element	Value range
00	1	Command identifier (ASCII)	'N'
01	1	Antenna number (ASCII)	'0': All active antennas '1'...'4': Single antenna
02	1	Data carrier selection	'A': All 'S': Selected
03	1	BCC	00 _{hex} ...FF _{hex}

Status message

Byte	Length	Command element	Value range
00	1	Status	<ACK> or <NAK>
01	1	Status code	See table <i>Status codes</i> on page 94

If the status message is positive, data is requested with <STX>.

Byte	Length	Command element	Value range
00	1	Control command	<STX>

If the command is executed successfully, data follows.

Byte	Length	Command element	Value range
00	1	Status	<ACK>
01	1	Antenna number (ASCII)	'1'...'4'
02...04	3	Number of data carriers found (ASCII)	"000"... "999"
05	1	BCC	00 _{hex} ...FF _{hex}

If the data cannot be provided, a negative status message follows.

Byte	Length	Command element	Value range
00	1	Status	<NAK>
01	1	Status code	See table <i>Status codes</i> on page 94

Command identifier 'M': Detect data carriers

Detects the data carriers (max. 255) that are located in the detection range of the specified antenna and returns the data specified under data type. With the data carrier selection, either all or only selected data carriers can be detected (see *Command identifier 'z': Select data carrier (Select)* on page 105).

Byte	Length	Command element	Value range
00	1	Command identifier (ASCII)	'M'
01	1	Antenna number (ASCII)	'0': All active antennas '1'...'4': Single antenna
02	1	Data type: EPC or TID (ASCII)	'E': EPC 'T': TID
03...05	3	Max. number of data carriers (ASCII)	"000"... "255"
06	1	Data carrier selection (ASCII)	'0': All '1': Selected
07	1	BCC	00 _{hex} ...FF _{hex}

The positive status message contains additional information and is transmitted as follows.

Byte	Length	Command element	Value range
00	1	Status	<ACK>
01	1	Antenna number (ASCII)	'1'...'4'
02	1	Data type EPC or TID (ASCII)	'E': EPC 'T': TID
03...05	3	Number of data carriers found (ASCII)	"000"... "255"
06...07	2	Number of bytes for the ID per data carrier (ASCII)	"64"
08	1	BCC	00 _{hex} ...FF _{hex}

If the data cannot be provided, a negative status message follows.

Byte	Length	Command element	Value range
00	1	Status	<NAK>
01	1	Status code	See table <i>Status codes</i> on page 94

If the status message is positive, data is requested with <STX>.

Byte	Length	Command element	Value range
00	1	Control command	<STX>

This is followed by the requested data, which is divided into several packets if there is a large amount of data. Each packet contains the total number of packets and the current packet number. Via the control command <STX>, the packets can be fetched iteratively.

Byte	Length	Command element	Value range
00	1	Status	<ACK>
01	1	Antenna number (ASCII)	'1'...'4'
02...04	3	Total number of packets (ASCII)	"001"... "999"
05...07	3	Packet number (ASCII)	"000000"... "999999"
08...13	6	Number of bytes in the data block (ASCII)	"000000"... "999999"
14	Quantity	Data block	See description <i>Data block</i> on page 100
Last byte	1	BCC	00 _{hex} ...FF _{hex}

Data block

The data block consists of one or more frames with a length of 66 bytes each. Each frame contains the requested data (EPC or TID) and the antenna number of the antenna that detected the respective data carrier.

Byte	Length	Command element	Value range
00	1	Antenna number	01 _{hex} ...04 _{hex}
01	1	Reserved	00 _{hex}
02...65	64	EPC/TID	See description <i>EPC/TID</i> on page 101
66	1	Antenna number	01 _{hex} ...04 _{hex}
67	1	Reserved	00 _{hex}
68...131	64	EPC/TID	See description <i>EPC/TID</i> on page 101
...	...	...	...

EPC and TID are always transmitted with a data length of 62 bytes in LSB-first format. If the length is less than 62 bytes, then the EPC/TID field is padded with leading pad bytes (00_{hex}). The actual length of EPC/TID is specified by the length field.

Byte	Length	Command element	Value range
00	1	EPC/TID length	00 _{hex} ...3E _{hex}
01	1	Reserved	00 _{hex}
02...63	62	EPC/TID (LSB...MSB)	00 _{hex} ...FF _{hex}

The EPC data of the data carriers in the detection range of antenna 1 are to be detected. In front of antenna 1 there is a data carrier with an EPC length of 12 bytes and a data carrier with an EPC length of 62 bytes. The transmitted data block looks like this.

Byte	Data (Hex)	Description
00	01	Tag detected at antenna 1
01	00	Reserved
02	0C	EPC has a length of 12 bytes
03	00	Reserved
04...65	00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 00, 12, 11, 10, 09, 08, 07, 06, 05, 04, 03, 02, 01	Pad-Byte + EPC EPC: 01, 02, 03, 04, 05, 06, 07, 08, 09, 10, 11, 12
66	01	Reserved
67	00	Reserved
68	3E	EPC has a length of 62 bytes
69...131	62, 00, 60, 00, 00, 00, 00, 55, 00, 00, 00, 00, 50, 00, 00, 00, 00, 45, 00, 00, 00, 00, 40, 00, 00, 00, 00, 35, 00, 00, 00, 00, 30, 00, 00, 00, 00, 25, 00, 00, 00, 00, 20, 00, 00, 00, 00, 15, 00, 00, 00, 00, 10, 00, 00, 00, 00, 05, 00, 00, 00, 01	EPC: 01, 00, 00, 00, 05, 00, 00, 00, 00, 10, 00, 00, 00, 00, 15, 00, 00, 00, 00, 20, 00, 00, 00, 00, 25, 00, 00, 00, 00, 30, 00, 00, 00, 00, 35, 00, 00, 00, 00, 40, 00, 00, 00, 00, 45, 00, 00, 00, 00, 50, 00, 00, 00, 00, 55, 00, 00, 00, 00, 60, 00, 62

Command identifier 'z': Detect data carriers, extended

Detects the data carriers (max. 999) that are located in the detection range of the specified antenna and returns the data specified under *Data type* as well as additional information. With the *data carrier selection*, either all or only selected data carriers can be detected (see *Command identifier 'z': Select data carrier (Select)* on page 105).

Additional information:

Field	Description
Protocol Control Word (PC)	Defined in standard: EPC™ Radio-Frequency Identity Protocols Generation-2 UHF RFID
Extended Protocol Control (XPC 1)	Defined in standard: EPC™ Radio-Frequency Identity Protocols Generation-2 UHF RFID
Extended Protocol Control (XPC 2)	Defined in standard: EPC™ Radio-Frequency Identity Protocols Generation-2 UHF RFID
Receive Signal Strength Indicator (RSSI)	Received Signal Strength Indicator (RSSI) allows conclusions to be drawn about the signal quality with which the data carrier was received. It depends, among other things, on the tag type and the distance of the detected tag from the antenna. The signed value is in the range -128...+127, higher values mean a higher signal level. In the 007 protocol, the value is transmitted as 3 ASCII digits in the range '000'...'255'. To get to the actual value range, the following calculation is necessary: Values from '000'...'127': Interpret unchanged as number 0...127. Values from '128'...'255': Convert to the range -128...-1 by subtracting 256.
Time stamp	Contains the time when the data carrier was detected in the UTC (Universal Time Coordinate) time zone Format: hhmmssnnn hh = hours, mm = minutes, ss = seconds, nnn = milliseconds



The PC, XPC1 and XPC2 fields are for expert applications only. Detailed information can be found in the UHF RFID standard *EPC™ Radio-Frequency Identity Protocols Generation-2 UHF RFID*.

Byte	Length	Command element	Value range
00	1	Command identifier (ASCII)	'z'
01	1	Antenna number (ASCII) (0 = all active antennas)	'0'...'4'
02	1	Data type: EPC or TID (ASCII)	'E': EPC 'T': TID
03...05	3	Max. number of data carriers (ASCII)	'000'...'999'
06	1	Data carrier selection (ASCII)	'0': All '1': Selected
07	1	BCC	00 _{hex} ...FF _{hex}

The positive status message contains additional information and is transmitted as follows.

Byte	Length	Command element	Value range
00	1	Status	<ACK>
01	1	Antenna number (ASCII)	'1'...'4'
02	1	Data type EPC or TID (ASCII)	'E': EPC 'T': TID
03...05	3	Number of data carriers found (ASCII)	'000'...'999'
06...07	2	Number of bytes per data carrier (ASCII)	'64'
08	1	BCC	00 _{hex} ...FF _{hex}

If the data cannot be provided, a negative status message follows.

Byte	Length	Command element	Value range
00	1	Status	<NAK>
01	1	Status code	See table <i>Status codes</i> on page 94

If the status message is positive, data is requested with <STX>.

Byte	Length	Command element	Value range
00	1	Control command	<STX>

This is followed by the requested data, which is divided into several packets if there is a large amount of data. Each packet contains the total number of packets and the current packet number. Via the control command <STX>, the packets can be fetched iteratively.

Byte	Length	Command element	Value range
00	1	Status	<ACK>
01	1	Antenna number (ASCII)	'1'...'4'
02...04	3	Number of packets (ASCII)	"001"... "999"
05...07	3	Packet number (ASCII)	"001"... "999"
08...13	6	Number of bytes (ASCII)	"000000"... "999999"
14	Quantity	Data block	See description of data block
Last byte	1	BCC	00 _{hex} ...FF _{hex}

Data block

The data block consists of one or more frames, each 66 bytes long. Each frame contains the requested data (EPC or TID) and the antenna number of the antenna that detected the respective data carrier.

Byte	Length	Command element	Value range
00	1	Antennas at which the data carrier was detected (bit-mask)	01 _{hex} ...0F _{hex}
01	1	Antenna at which the highest RSSI value was determined for the data carrier (ASCII)	'1'...'4'
02...65	64	EPC/TID	See description of EPC/TID
66	2	PC	0000 _{hex} ... FFFF _{hex}
68	2	XPC_w1	0000 _{hex} ... FFFF _{hex}
70	2	XPC_w2	0000 _{hex} ... FFFF _{hex}
72	3	RSSI (ASCII)	"000"... "255" ¹⁾
75	9	Time stamp (ASCII)	"000000000"... "235959999"

Byte	Length	Command element	Value range
84	1	Antennas at which the data carrier was detected (bit-mask)	01 _{hex} ...0F _{hex}
85	1	Antenna at which the highest RSSI value was determined for the data carrier (ASCII)	'1'...'4'
86...149	64	EPC/TID	See description of EPC/TID
...	...	...	...

¹⁾ To obtain the RSSI in the usual value range of -128...+127, subtract 256 from the numeric value for values above 127.

EPC/TID

EPC and TID are always transmitted with a data length of 62 bytes in LSB-first format. If the length is less than 62 bytes, then the EPC/TID field is padded with leading pad bytes (00_{hex}). The actual length of EPC/TID is specified by the length field.

Byte	Length	Command element	Value range
00	1	EPC/TID length	00 _{hex} ...3E _{hex}
01	1	Reserved	00 _{hex}
02...63	62	EPC/TID (LSB...MSB)	00 _{hex} ...FF _{hex}

Example:

- The EPC data of the data carriers in the range of antenna 1 and 3 are to be detected.
- In front of antenna 1 there is a data carrier with an EPC length of 12 bytes.
- In front of antenna 3 there is a data carrier with an EPC length of 62 bytes.

The transmitted data block looks like this.

Byte	Data (Hex)	Description
00	01	Tag detected at antenna 1
01	31	Highest RSSI at antenna '1'
02	0C	EPC has a length of 12 bytes
03	00	Reserved

8.10 Edit data carrier

Command identifier 'z': Select data carrier (Select)

If there are several data carriers in the detection range of an antenna, a single data carrier can be selected for further processing. The desired data carrier is masked via an ID. The data which is used as the ID can be defined via the *ID type* field.

When selecting by EPC or TID, the ID block must be filled with the corresponding data. The format in the ID block is the same as the format with which the device outputs the IDs with the *Detect data carriers* command. The selection data for the ID is always valid from the beginning of the ID. However, a shorter length can be specified in the *Number of bytes ID* field to select entire ID ranges (e.g. only the first 4 bytes of the ID must match).

In case of a selection according to a part of the user data, the ID block should be filled with 00_{hex} and the selection data should be provided in the *User data* section. Here, both the start of the selection area (address) and the length (number of bytes) can be selected.

Byte	Length	Command element	Value range
00	1	Command identifier (ASCII)	'z'
01	1	Antenna number (ASCII)	'0': All antennas '1'...'4': Single antenna
02	1	ID type	'E': EPC 'T': TID 'U': USER
03	64	ID-Block	See ID block
66	6	Address (ASCII)	"000000"... "999999", for <i>ID type</i> 'E' or 'T' always enter "000000"
71	6	Number of bytes (ASCII)	"000000"... "999999", for <i>ID type</i> 'E' or 'T' always enter "000000"
76	No. of bytes	User data, only for <i>ID type</i> 'U'	Byte: 00 _{hex} ...FF _{hex}
Last byte	1	BCC	00 _{hex} ...FF _{hex}

ID-Block

The ID block contains the *ID* and a length field and is transferred in the following format:

Byte	Length	Command element	Value range
00	1	Number of bytes ID	00 _{hex} ...FF _{hex}
01	1	Reserved	00 _{hex}
02	Number of bytes ID	ID (LSB...MSB)	Byte: 00 _{hex} ...FF _{hex}

Status message:

Byte	Length	Command element	Value range
00	1	Status	<ACK> or <NAK>
01	1	Status code	See table <i>Status codes</i> on page 94

Command identifier 'n': Deselect data carrier (unselect)

Deletes the data carrier selection previously made with the *SELECT DATA CARRIERS* command. The command has no effect if there is no selected data carrier in the detection range of the specified antenna.

Byte	Length	Command element	Value range
00	1	Command identifier (ASCII)	'n'
01	1	Antenna number (ASCII)	'0': All antennas '1'...'4': Single antenna
Last byte	1	BCC	00 _{hex} ...FF _{hex}

Status message

Byte	Length	Command element	Value range
00	1	Status	<ACK> or <NAK>
01	1	Status code	See table <i>Status codes</i> on page 94

Command identifier 'L': Read data carrier (<1024 bytes)

Read out data (<1024 bytes) from a data carrier that is located in the detection range of the specified antenna. The memory area to be read is specified via *START ADDRESS*, *NUMBER OF BYTES* and *MEMORY BANK*. The requested data are transferred in unfragmented form in a single data packet.

If there are several data carriers in the detection range of the specified antenna, the desired data carrier must be selected before reading (see *Command identifier 'z': Select data carrier (Select)* on page 105).

i For the memory areas EPC and TID, there are simplified commands which return EPC and TID as filtered information, see command identifiers 'O' and 'y'.

i Details on the use and organization of the different memory areas can be found in the UHF RFID standard *EPC™ Radio-Frequency Identity Protocols Generation-2 UHF RFID*.

Byte	Length	Command element	Value range
00	1	Command identifier (ASCII)	'L'
01...06	6	Start address (ASCII)	"000000"... "999999"
07...12	6	Number of bytes (ASCII)	"000000"... "999999"
13	1	Antenna number (ASCII)	'0': All active antennas '1'...'4': Single antenna
14	1	Memory bank (ASCII)	'R': Reserved 'E': EPC 'T': TID 'U': USER
15	1	BCC	00 _{hex} ...FF _{hex}

Status message

Byte	Length	Command element	Value range
00	1	Status	<ACK> or <NAK>
01	1	Status code	See table <i>Status codes</i> on page 94

If the status message is positive, data is requested with <STX>:

Byte	Length	Command element	Value range
00	1	Control command	<STX>

If the command is executed successfully, the requested data follows with the specified number of bytes and additional BCC.

Byte	Length	Command element	Value range
00	1	Data	00 _{hex} ...FF _{hex}
...	...	...	00 _{hex} ...FF _{hex}
Last byte	1	BCC	00 _{hex} ...FF _{hex}

If the data cannot be provided, a negative status message follows.

Byte	Length	Command element	Value range
00	1	Status	<NAK>
01	1	Status code	See table <i>Status codes</i> on page 94

Command identifier 'H': Read data carrier, extended (>1024 bytes)

Read out data (>1024 bytes) from a data carrier that is located in the detection range of the specified antenna. The memory area to be read is specified via *START ADDRESS*, *NUMBER OF BYTES* and *MEMORY BANK*. Depending on the amount of data, the data is transmitted in fragmented form in one or more packets, which can be requested one after the other by the processor unit.

If there are several data carriers in the detection range of the specified antennas, the desired data carrier must be selected before reading (see *Command identifier 'z': Select data carrier (Select)* on page 105).

i For the EPC and TID memory areas there are simplified commands which return EPC and TID as filtered information (see *Command identifier 'O': Read data carrier, EPC* on page 108 and *Command identifier 'y': Read data carrier, TID* on page 109).

i Details on the use and organization of the different memory areas can be found in the UHF RFID standard *EPC™ Radio-Frequency Identity Protocols Generation-2 UHF RFID*.

Byte	Length	Command element	Value range
00	1	Command identifier (ASCII)	'H'
01...06	6	Start address (ASCII)	"000000"... "999999"
07...12	6	Number of bytes (ASCII)	"000000"... "999999"
13	1	Antenna number (ASCII)	'0': All active antennas '1'...'4': Single antenna
14	1	Memory bank (ASCII)	'R': Reserved 'E': EPC 'T': TID 'U': USER
15	1	BCC	00 _{hex} ...FF _{hex}

If the data cannot be provided, a negative status message follows.

Byte	Length	Command element	Value range
00	1	Status	<NAK>
01	1	Status code	See table <i>Status codes</i> on page 94

If the command is executed successfully, a positive status message follows. This contains the first data packet and is transmitted in the following format:

Byte	Length	Command element	Value range
00	1	Status	<ACK> or <EOT>
01...03	3	Number of packets (ASCII)	"000"... "999"
04...06	3	Packet number (ASCII)	"000"... "999"
07...12	6	Number of bytes (ASCII)	"000000"... "999999"
13...	No. of bytes	Data	Byte: 00 _{hex} ...FF _{hex}
Last byte	1	BCC	00 _{hex} ...FF _{hex}

If further packets are available, then they can be requested via <STX>, the last transmitted data packet contains the status <EOT>.

Byte	Length	Command element	Value range
00	1	Control command	<STX>

If one of the packets cannot be transferred properly, a negative status message follows.

Byte	Length	Command element	Value range
00	1	Status	<NAK>
01	1	Status code	See table <i>Status codes</i> on page 94

Command identifier 'O': Read data carrier, EPC

Reads the EPC of a data carrier that is within the detection range of the specified antenna.

If there are several data carriers in the detection range of the specified antenna, the desired data carrier must be selected before reading (see *Command identifier 'z': Select data carrier (Select)* on page 105).

Byte	Length	Command element	Value range
00	1	Command identifier (ASCII)	'O'
01	1	Antenna number (ASCII)	'0': All active antennas '1'...'4': Single antenna
02	1	BCC	00 _{hex} ...FF _{hex}

If the data cannot be provided, a negative status message follows.

Byte	Length	Command element	Value range
00	1	Status	<NAK>
01	1	Status code	See table <i>Status codes</i> on page 94

Status message

Byte	Length	Command element	Value range
00	1	Status	<ACK> or <NAK>
01	1	Status code	See table <i>Status codes</i> on page 94

If the status message is positive, data is requested with <STX>.

Byte	Length	Command element	Value range
00	1	Control command	<STX>

If the command is executed successfully, the requested data will follow.

Byte	Length	Command element	Value range
00	1	Status	<ACK>
01	1	Antenna number (ASCII) (0 = all active antennas)	'0'...'4'
02...03	2	Number of bytes (ASCII)	"00"..."99"
04...	No. of bytes	EPC data (LSB...MSB ¹⁾)	Byte: 00 _{hex} ...FF _{hex}
Last byte	1	BCC	00 _{hex} ...FF _{hex}

¹⁾ LSB...MSB sequence means a reversed sequence compared to the arrangement in the memory of the data carrier.

Command identifier 'y': Read data carrier, TID

Reads the TID of a data carrier that is located in the detection range of the specified antenna. The length of the read TID data is specified via parameter 0004_{hex} (see *TID length* on page 61).

If there are several data carriers in the detection range of the specified antenna, the desired data carrier must be selected before reading (see *Command identifier 'z': Select data carrier (Select)* on page 105).

Byte	Length	Command element	Value range
00	1	Command identifier (ASCII)	'y'
01	1	Antenna number (ASCII)	'0': All active antennas '1'...'4': Single antenna
02	1	BCC	00 _{hex} ...FF _{hex}

Status message

Byte	Length	Command element	Value range
00	1	Status	<ACK> or <NAK>
01	1	Status code	See table <i>Status codes</i> on page 94

If the status message is positive, data is requested with <STX>

Byte	Length	Command element	Value range
00	1	Control command	<STX>

If the command is executed successfully, the requested data follows

Byte	Length	Command element	Value range
00	1	Status	<ACK>
01	1	Antenna number (ASCII) (0 = all active antennas)	'0'...'4'
02...03	2	Number of bytes (ASCII)	"00"..."99"
04	No. of bytes	TID data (LSB...MSB ¹⁾)	Byte: 00 _{hex} ...FF _{hex}
Last byte	1	BCC	00 _{hex} ...FF _{hex}

¹⁾ LSB...MSB sequence means a reversed sequence compared to the arrangement in the memory of the data carrier.

If the data cannot be provided, a negative status message follows

Byte	Length	Command element	Value range
00	1	Status	<NAK>
01	1	Status code	See table <i>Status codes</i> on page 94

Command identifier 'I': Read data carrier, bulk

Read user data from several data carriers located in the detection range of the specified antenna. Via the *DATA CARRIER SELECTION*, all data carriers in the detection range can be read out or only a subset previously selected with the Select command

The memory area to be read is defined via *START ADDRESS* and *NUMBER OF BYTES*. The following boundary conditions apply:

Maximum data quantity: 65536 bytes/data carrier

Maximum number of data carriers: 255

Initially, the command reports only the number of data carriers that have been detected. Then the requested data is read out and transmitted in fragmented form in one or more packets.

If detected data carriers are removed from the detection range of the antenna before they are read out or if they cannot be read out successfully, the data are marked as invalid by a check byte.

Byte	Length	Command element	Value range
00	1	Command identifier (ASCII)	'I'
01	1	Antenna number (ASCII)	'0': All active antennas '1'...'4': Single antenna
02...07	6	Start address (ASCII)	"000000"... "999999"
08...13	6	Number of bytes/ data carrier (ASCII)	"000001"... "065536"
14	1	Data carrier selection	'0': All '1': Selected
15...17	3	Max. number of data carriers (ASCII)	"000"... "999"
18	1	BCC	00 _{hex} ...FF _{hex}

If the command cannot be executed properly, a negative status message follows.

Byte	Length	Command element	Value range
00	1	Status	<NAK>
01	1	Status code	See table <i>Status codes</i> on page 94

If the command is executed successfully, a positive status message follows. This contains the number of detected data carriers and the number of data bytes transferred per data carrier.

Byte	Length	Command element	Value range
00	1	Status	<ACK>
01	1	Antenna number (ASCII) (0 = all active antennas)	'0'...'4'
02...04	3	Number of data carriers found (ASCII)	"000"... "999"
05...10	6	Number of bytes/ data carrier (ASCII)	"000001"... "065536"
11	1	BCC	00 _{hex} ...FF _{hex}

The total number of bytes transferred is calculated according to the following formula:

$$\text{Total number of bytes} = ((\text{Number of bytes/data carrier}) + 1) \times (\text{Number of data carriers found})$$

If the status message is positive, data is requested with <STX>.

Byte	Length	Command element	Value range
00	1	Control command	<STX>

If the data cannot be provided, a negative status message follows.

Byte	Length	Command element	Value range
00	1	Status	<NAK>
01	1	Status code	See table <i>Status codes</i> on page 94

If the command is executed successfully, a positive status message follows. This contains the first data packet and is transmitted in the following format:

Byte	Length	Command element	Value range
00	1	Status	<ACK> or <EOT>
01	1	Antenna number (ASCII) (0 = all active antennas)	'0'...'4'
02...04	3	Number of packets (ASCII)	"000"... "999"
05...07	3	Packet number (ASCII)	"000"... "999"
08...11	3	Data block: Number of bytes (ASCII)	"000"... "999"
12...	No. of bytes	Data block	Byte: 00 _{hex} ...FF _{hex}
Last byte	1	BCC	00 _{hex} ...FF _{hex}

Data block

The data block is transferred with the specified number of bytes, which is given under *DATA BLOCK: NUMBER OF BYTES*. The length of the individual data fields (Tag 1...Tag n) corresponds to the requested *NUMBER OF BYTES/DATA CARRIER*.

Length	Command element	Value range
Number of bytes/data carrier	Data 1	Byte: 00 _{hex} ...FF _{hex}
1	Check byte 1	00 _{hex} : Valid FF _{hex} : Invalid
Number of bytes/data carrier	Optional: Data 2	Byte: 00 _{hex} ...FF _{hex}
1	Optional: Check byte 2	00 _{hex} : Valid FF _{hex} : Invalid
...	...	...

If further packets are available, they can be requested via <STX>, the last transmitted data packet contains the status <EOT>.

Byte	Length	Command element	Value range
00	1	Control command	<STX>

Command identifier '>': Read data carrier, bulk extended

Read out several data carriers that are located in the detection range of the specified antenna. With the *DATA CARRIER SELECTION*, either all data carriers in the detection range can be read out or only a subset previously selected with the Select command.

The memory area to be read is specified via *START ADDRESS*, *NUMBER OF BYTES* and *MEMORY BANK*.

The requested data is transmitted together with the EPC of the data carrier in order to be able to allocate the data. Depending on the amount of data, the data is transmitted in fragmented form in one or more packets, which can be requested iteratively by the processor unit. The following boundary conditions apply:

Maximum amount of data: 999999 bytes/data carrier

Maximum number of data carriers: 999

Initially, the command reports only the number of data carriers that have been detected. Then the requested data is read out and transmitted in fragmented form in one or more packets.

If detected data carriers are removed from the detection range of the antenna before being read out or if they cannot be read out successfully, the data are marked as invalid by a check byte.

Byte	Length	Command element	Value range
00	1	Command identifier (ASCII)	'I'
01	1	Antenna number (ASCII)	'0': All active antennas '1'...'4': Single antenna
02...07	6	Start address (ASCII)	"000000"... "999999"
08...13	6	Number of bytes/data carrier (ASCII)	"000001"... "999999"
14	1	Data carrier selection	'0': All '1': Selected
15...17	3	Max. number of data carriers (ASCII)	"000"... "999"
18	1	Memory bank (ASCII)	'R': Reserved 'E': EPC 'T': TID 'U': USER
19	1	BCC	00 _{hex} ...FF _{hex}

If the command cannot be executed properly, a negative status message follows.

Byte	Length	Command element	Value range
00	1	Status	<NAK>
01	1	Status code	See table <i>Status codes</i> on page 94

If the command is executed successfully, a positive status message follows. This contains the number of data carriers detected, the number of bytes transferred for the EPC of each data carrier, and the number of data bytes transferred per data carrier.

Byte	Length	Command element	Value range
00	1	Status	<ACK>
01	1	Antenna number (ASCII)	'0'...'4'
02...04	3	Number of data carriers found (ASCII)	"000"..."999"
05...06	2	Number of bytes per EPC (ASCII)	"64"
07...12	6	Number of bytes/data carrier (ASCII)	"000000"..."999999"
13	1	BCC	00 _{hex} ...FF _{hex}

If the status message is positive, data is requested with <STX>.

Byte	Length	Command element	Value range
00	1	Control command	<STX>

If the data cannot be provided, a negative status message follows.

Byte	Length	Command element	Value range
00	1	Status	<NAK>
01	1	Status code	See table <i>Status codes</i> on page 94

If the command is executed successfully, a positive status message follows. This contains the first data packet and is transmitted in the following format:

Byte	Length	Command element	Value range
00	1	Status	<ACK> or <EOT>
01	1	Antenna number (ASCII)	'0'...'4'
02...04	3	Number of packets (ASCII)	"001"..."999"
05...07	3	Packet number (ASCII)	"001"..."999"
08...12	4	Number of bytes in the following data block (ASCII)	"0000"..."9999"
13...	No. of bytes	Data block	Byte: 00 _{hex} ...FF _{hex}
Last byte	1	BCC	00 _{hex} ...FF _{hex}

Data block

The data block is transferred with the specified number of bytes, which is given under *DATA BLOCK: NUMBER OF BYTES*. The length of the individual data fields (Tag 1...Tag n) corresponds to the requested *NUMBER OF BYTES/DATA CARRIER*.

Length	Command element	Value range
64	EPC 1 (LSB...MSB)	Byte: 00 _{hex} ...FF _{hex}
Number of bytes/data	Data 1	Byte: 00 _{hex} ...FF _{hex}
1	Check byte 1	00 _{hex} : Valid FF _{hex} : Invalid
64	EPC 2 (LSB...MSB)	Byte: 00 _{hex} ...FF _{hex}
Number of bytes/data	Data 2	Byte: 00 _{hex} ...FF _{hex}
1	Check byte 2	00 _{hex} : Valid FF _{hex} : Invalid
...	...	...

If further packets are available, they can be requested via <STX>, the last transmitted data packet contains the status <EOT>.

Byte	Length	Command element	Value range
00	1	Control command	<STX>

**Command identifier 'P': Write data carrier
(<1024 bytes)**

Write data (<1024 bytes) to a data carrier that is within the detection range of the specified antenna.

The memory area to be written is specified via *START ADDRESS* and *NUMBER OF BYTES*. The data is transferred in unfragmented form in a single data packet.

If there are several data carriers in the detection range of the specified antenna, the desired data carrier must be selected before writing (see *Command identifier 'z': Select data carrier (Select)* on page 105).

i A password is required to write to read-only data carrier.
Write commands executed with an invalid password are acknowledged with the status message *PASSWORD REQUIRED* or *PASSWORD INVALID*.

The access password can be set in advance via parameter 1004_{hex} (see *Memory bank* on page 54).

Byte	Length	Command element	Value range
00	1	Command identifier (ASCII)	'P'
01	6	Start address (ASCII)	"000000"... "999999"
06	6	Number of bytes (ASCII)	"000000"... "999999"
11	1	Antenna number (ASCII)	'0': All active antennas '1'...'4': Single antenna
12	1	Memory bank (ASCII)	'R': Reserved 'E': EPC 'T': TID 'U': USER
13	1	BCC	00 _{hex} ...FF _{hex}

Status message:

Byte	Length	Command element	Value range
00	1	Status	<ACK> or <NAK>
01	1	Status code	See <i>Status codes</i> on page 94

If the status message is positive, data can be transmitted with <STX>.

Byte	Length	Command element	Value range
00	1	Control command	<STX>
01	No. of bytes	Data	Byte: 00 _{hex} ...FF _{hex}
Last byte	1	BCC	00 _{hex} ...FF _{hex}

Status message:

Byte	Length	Command element	Value range
00	1	Status	<ACK> or <NAK>
01	1	Status code	See <i>Status codes</i> on page 94

Command identifier 'F': Write data carrier, extended (>1024 bytes)

Write data (>1024 bytes) to a data carrier that is within the detection range of the specified antenna. The memory area to be written is specified via *START ADDRESS*, *NUMBER OF BYTES* and *MEMORY BANK*. Depending on the amount of data, the data is transmitted in fragmented form in one or more packets.

If there are several data carriers in the detection range of the specified antenna, the desired data carrier must be selected before writing (see *Command identifier 'z': Select data carrier (Select)* on page 105).



A password is required to write to read-only data carrier.
Write commands executed with an invalid password are acknowledged with the status message *PASSWORD REQUIRED* or *PASSWORD INVALID*.

The access password can be set in advance via parameter 1004_{hex} (see *Memory bank* on page 54).

Byte	Length	Command element	Value range
00	1	Command identifier (ASCII)	'F'
01...06	6	Start address (ASCII)	"000000"... "999999"
07...12	1	Number of bytes (ASCII)	"000000"... "999999"
13	1	Antenna number (ASCII)	'0': All active antennas '1'...'4': Single antenna
14	1	Memory bank (ASCII)	'R': Reserved 'E': EPC 'T': TID 'U': USER
15	1	BCC	00 _{hex} ...FF _{hex}

Status message:

Byte	Length	Command element	Value range
00	1	Status	<ACK> or <NAK>
01	1	Status code	See table <i>Status codes</i> on page 94

After each positive status message, a data block can be transferred in the following format.
This is repeated until all data has been transferred.
The number of bytes per packet is arbitrary, but must not exceed 1024.

Byte	Length	Command element	Value range
00	1	Control command	<STX>
01...06	6	Data block: Number of bytes (ASCII)	"000000"... "999999"
07	No. of bytes	Data block	Byte: 00 _{hex} ...FF _{hex}
Last byte	1	BCC	00 _{hex} ...FF _{hex}

Status message:

Byte	Length	Command element	Value range
00	1	Status	<ACK> or <NAK>
01	1	Status code	See table <i>Status codes</i> on page 94

Command identifier 'v': Write data carrier, EPC

Write EPC data to a data carrier located in the detection range of the specified antenna.

The size of the EPC memory area can be defined via *NUMBER OF BYTES*. If necessary, the data carrier is automatically reconfigured to the new EPC memory size.

Byte	Length	Command element	Value range
00	1	Command identifier (ASCII)	'v'
01	1	Antenna number (ASCII)	'0': All active antennas '1'...'4': Single antenna
02...03	2	Number of bytes (ASCII)	"00"..."99"
15	1	BCC	00 _{hex} ...FF _{hex}

Status message:

Byte	Length	Command element	Value range
00	1	Status	<ACK> or <NAK>
01	1	Status code	See table <i>Status codes</i> on page 94

If the status message is positive, data can be transmitted with <STX>.

Byte	Length	Command element	Value range
00	1	Control command	<STX>
01	No. of bytes	EPC data (LSB...MSB ¹⁾)	Byte: 00 _{hex} ...FF _{hex}
Last byte	1	BCC	00 _{hex} ...FF _{hex}

¹⁾ LSB...MSB sequence means a reversed sequence compared to the arrangement in the memory of the data carrier.

Status message:

Byte	Length	Command element	Value range
00	1	Status	<ACK> or <NAK>
01	1	Status code	See <i>Status codes</i> on page 94

Command identifier 'w': Write data carrier, bulk

Write user data to several data carriers that are located in the detection range of the specified antenna. With the *DATA CARRIER SELECTION*, either all data carriers in the detection range can be written to or only a subset previously selected with the Select command. The number of data carriers found and successfully written is returned.

The memory area to be written is specified via *START ADDRESS* and *NUMBER OF BYTES*. Depending on the amount of data, the data is transmitted in fragmented form in one or more packets, with each transmitted packet acknowledged with a status message.

The following boundary conditions apply to the transfer:

- Maximum amount of data: 999999 bytes/data carrier
- Maximum number of data carriers: 999

Byte	Length	Command element	Value range
00	1	Command identifier (ASCII)	'w'
01	1	Antenna number (ASCII)	'0': All active antennas '1'...'4': Single antenna
02...07	6	Start address (ASCII)	"000000"... "999999"
08...13	6	Number of bytes (ASCII)	"000000"... "999999"
14	1	Data carrier selection	'0': All '1': Selected
15...17	3	Max. number of data carriers (ASCII)	"000"... "999"
18	1	BCC	00 _{hex} ...FF _{hex}

Status message:

Byte	Length	Command element	Value range
00	1	Status	<ACK> or <NAK>
01	1	Status code	See table <i>Status codes</i> on page 94

If the status message is positive, the first data packet can be transmitted with <STX>. If further data packets follow, they can be transmitted iteratively after each positive status message.

Byte	Length	Command element	Value range
00	1	Control command	<STX>
01...06	6	Number of bytes in the following data block (ASCII)	"000000"... "999999"
07	No. of bytes	Data block	00 _{hex} ...FF _{hex}
Last byte	1	BCC	00 _{hex} ...FF _{hex}

Status message:

Byte	Length	Command element	Value range
00	1	Status	<ACK> or <NAK>
01	1	Status code	See table <i>Status codes</i> on page 94

The positive status message contains additional information and is transmitted in the following format. The *OPERATION* data field is transmitted with status *PENDING* as long as further packets are being transmitted. The last transmitted packet is acknowledged with the status *FINISHED*.

Byte	Length	Command element	Value range
00	1	Status	<ACK>
01	1	Antenna number (ASCII)	'0'...'4'
02...04	3	Number of data carriers found	"000"... "999"
05...08	4	Number of data carriers written	"0000"... "9999"
09	1	Operation	'P': Pending 'F': Finished
Last byte	1	BCC	00 _{hex} ...FF _{hex}

Command identifier '<': Write data carrier, bulk extended

Write data to several data carriers that are within the detection range of the specified antenna. With the *DATA CARRIER SELECTION*, either all data carriers in the detection range can be written to or only a subset previously selected with the Select command. A list of EPCs of all successfully written data carriers is returned.

The memory area to be written is specified via *START ADDRESS*, *NUMBER OF BYTES* and *MEMORY BANK*. Depending on the amount of data, the data is transmitted in fragmented form in one or more packets, with each transmitted packet acknowledged with a status message.

- The following boundary conditions apply to the transfer:
- Maximum amount of data: 999999 bytes/data carrier
 - Maximum number of data carriers: 999

Byte	Length	Command element	Value range
00	1	Command identifier (ASCII)	'w'
01	1	Antenna number (ASCII)	'0': All active antennas '1'...'4': Single antenna
02...07	6	Start address (ASCII)	"000000"... "999999"
08...13	6	Number of bytes (ASCII)	"000000"... "999999"
14	1	Data carrier selection	'0': All '1': Selected
15...17	3	Max. number of data carriers (ASCII)	"000"... "999"
18	1	Memory bank (ASCII)	'R': Reserved 'E': EPC 'T': TID 'U': USER
19	1	BCC	00 _{hex} ...FF _{hex}

Status message:

Byte	Length	Command element	Value range
00	1	Status	<ACK> or <NAK>
01	1	Status code	See table <i>Status codes</i> on page 94

If the status message is positive, the first data packet can be transmitted with <STX>. If further data packets follow, they can be transmitted after each further positive status message.

Byte	Length	Command element	Value range
00	1	Control command	<STX>
01...06	6	Number of bytes in the following data block (ASCII)	"000000"... "999999"
07	No. of bytes	Data block	Byte: 00 _{hex} ...FF _{hex}
Last byte	1	BCC	00 _{hex} ...FF _{hex}

Status message:

Byte	Length	Command element	Value range
00	1	Status	<ACK> or <NAK>
01	1	Status code	See table <i>Status codes</i> on page 94

The last positive status message contains additional information and is transmitted in the following format. The *OPERATION* data field is transmitted with the value *FINISHED*.

Byte	Length	Command element	Value range
00	1	Status	<ACK>
01	1	Antenna number (ASCII)	'0'...'4'
02...04	3	Number of detected data carriers	"000"... "999"
05...08	4	Number of data carriers written	"0000"... "9999"
09...10	2	Number of bytes per ID (ASCII)	"64"
11	1	Operation (ASCII)	'F': Finished
Last byte	1	BCC	00 _{hex} ...FF _{hex}

After the last transmitted packet, i.e. when the *OPERATION* field contains *FINISHED* in the positive status message, a final status report can be requested with <STX>.

Byte	Length	Command element	Value range
00	1	Status	<STX>

If the status report cannot be generated, a negative status message follows.

Byte	Length	Command element	Value range
00	1	Status	<NAK>
01	1	Status code	See table <i>Status codes</i> on page 94

The positive status message is acknowledged with <ACK> or <EOT> and contains status information about the successfully written data. If several status packets are ready, they are acknowledged with <ACK>, the last packet to be transmitted with <EOT>.

Byte	Length	Command element	Value range
00	1	Status	<ACK> or <EOT>
01...03	3	Number of packets containing status information	"000"... "999"
04...06	3	Current packet number	"000"... "999"
07...12	6	Number of bytes in the data block	"000000"... "999999"
13...	No. of bytes	Data block	Byte: 00 _{hex} ...FF _{hex}
Last byte	1	BCC	00 _{hex} ...FF _{hex}

Data block

The data block contains a list of the data carriers (EPCs) that were successfully written.

Byte	Length	Command element	Value range
00	64	EPC Tag 1	Byte: 00 _{hex} ...FF _{hex}
65	64	EPC Tag 2 (optional)	Byte: 00 _{hex} ...FF _{hex}
...	...	EPC Tag n (optional)	Byte: 00 _{hex} ...FF _{hex}

With <STX>, further status packets can be requested, if available. The last available status packet is acknowledged with <EOT> and contains the status data of the last packet.

Byte	Length	Command element	Value range
00	1	Status	<STX>

Command identifier 'k': Kill

Permanently disables a selected data carrier and locks it to prevent any use.

To execute the *KILL* command, a *KILL* password must first be set and written to the data carrier.

The password has a length of 4 bytes and is transmitted as a string with 8 bytes in ASCII hex number format.

Example of password (MSB...LSB):

- in hex format: 010A8FCC_{hex}
- in ASCII-hex-format: "010A8FCC"



A kill command permanently disables the selected data carrier and cannot be undone!

Details on password protection and locking and unlocking (*Lock*) of UHF RFID data carriers can be found in the *EPC™ Radio-Frequency Identity Protocols Generation-2 UHF RFID* standard.

Byte	Length	Command element	Value range
00	1	Command identifier (ASCII)	'k'
01	1	Antenna number (ASCII)	'0': All active antennas '1'...'4': Single antenna
02	8	Password (ASCII hex) (MSB...LSB)	"00000000"... "FFFFFFF"
10	1	BCC	00 _{hex} ...FF _{hex}

Status message:

Byte	Length	Command element	Value range
00	1	Status	<ACK> or <NAK>
01	1	Status code	See <i>Status codes</i> on page 94

If the status message is positive, the *KILL* command can be confirmed with <STX>.

Byte	Length	Command element	Value range
00	1	Status	<STX>

Status message:

Byte	Length	Command element	Value range
00	1	Status	<ACK> or <NAK>
01	1	Status code	See <i>Status codes</i> on page 94

Command identifier 'I': Lock

The *LOCK* command can be used to lock memory areas (RES, EPC, TID, USER) of a UHF data carrier against write or read accesses, as well as any other accesses. Depending on the security level, the memory areas can only be password-protected or completely locked. The *MASK* and *ACTION* fields are used to specify which memory areas are to receive a new *LOCK* status and what this should look like. By using bit masks, the *LOCK* status of several memory areas can be changed at the same time. Before executing the *LOCK* command, the data carrier must be selected and the access password (*ACCESS PW*) valid for the selected tag must be written to parameter 1004_{hex} (see *Memory bank* on page 54).

i For selecting data carriers (see *Command identifier 'z': Select data carrier (Select)* on page 105).
To set an access password for a data carrier, write to byte address 4...7 of the *RESERVED* memory bank, see *Command identifier 'F': Write data carrier, extended (>1024 bytes)* on page 114.
To transfer the password to access the data carrier and execute the *LOCK* command, see *Command identifier 'E': Change device parameters* on page 98 (parameter no: 1002_{hex}).

Mask and action

MASK: Bit mask (16 bits) used to define which memory areas are to be influenced by the *ACTION* field. The *LOCK* status of the EPC, TID and USER memory areas and the area where passwords are stored can be locked/unlocked independently.

- 0: Memory area is *not* affected by the *ACTION* field
- 1: Memory area is influenced by the *ACTION* field

ACTION: Bit mask (16 bits) used to define the *LOCK* status of the memory areas specified by *MASK*.

Bit no.	15	14	13	12	11	10	9	8
Mask	Not used							Kill PW
Action	Not used							Status

Bit no.	7	6	5	4	3	2	1	0
Mask	Access password		EPC		TID		USER	
Action	Lock-Status		Lock-Status		Lock-Status		Lock-Status	

Lock status of the memory areas EPC, TID, USER

i The *TID* memory area is always write-protected regardless of the lock status and can only be read.

Status	Reading possible	Writing possible	Status can be changed
00	Yes	Yes	Yes
01	Yes	Yes	No
10	Yes	With access password	Yes
11	Yes	Locked	No

Lock status for contents of Reserved memory area (Access PW/Kill PW)

Status	Reading possible	Writing possible	Status can be changed
00	Yes	Yes	Yes
01	Yes	Yes	No
10	With access password	With access password	Yes
11	Locked	Locked	No

Execution of Lock command

Byte	Length	Command element	Value range
00	1	Command identifier (ASCII)	'I'
01	1	Antenna number (ASCII)	'0': All active antennas '1'...'4': Single antenna
02...05	4	Mask (ASCII hex)	"0000"... "03FF"
06...09	4	Action (ASCII hex)	"0000"... "03FF"
10	1	BCC	00 _{hex} ...FF _{hex}

Status message:

Byte	Length	Command element	Value range
00	1	Status	<ACK> or NAK>
01	1	Status code	See <i>Status codes</i> on page 94

8

007 protocol (continued)

If the status message is positive, the Lock command can be confirmed with <STX>.

Byte	Length	Command element	Value range
00	1	Control command	<STX>

Status message:

Byte	Length	Command element	Value range
00	1	Status	<ACK> or <NAK>
01	1	Status code	See <i>Status codes</i> on page 94

8.11 Universal data carrier access (Formatted tag data)

The *UNIVERSAL DATA CARRIER ACCESS (FORMATTED TAG DATA)* functions can be used to create complex compound commands that use or return freely definable data when recording, reading or writing to data carriers. Different memory areas as well as the formatting of the data can be defined.

For example, it is possible to specify that the following data is returned when the data carriers are detected:

Memory area	Start address	No. of bytes	Interpretation
EPC	0	12	Hex data
TID	0	8	Hex data
USER	6	4	Hex data as ASCII string

i For a detailed description of the application and the different possibilities see chapter 7.3.3 *Description of parameters for standard users* on page 69.
The default formats can be parameterized via the web server or the UHF Manager (see chapter 7.2 on page 33 and chapter 7.1 on page 29).
The default values of the format specifications can be overwritten separately for each TCP and USB session with the *WRITE DEVICE PARAMETER* command.

UNIVERSAL DATA CARRIER commands provide the possibility to specify the output channel (TCP port) for the requested data.

IN-Band: Command and data are transmitted on the same TCP port

OUT-Band: Command and data are transmitted on different TCP ports.

007 command channel/session	Input and output of the data at IN band	Input and output of the data at OUT band
TCP 10001	TCP 10001	TCP 10011
TCP 10001	TCP 10002	TCP 10012
TCP 10001	TCP 10003	TCP 10013
TCP 10001	TCP 10004	TCP 10014
TCP 10001	TCP 10005	TCP 10015
USB port	USB port	Not possible

i Details about the available port modes can be seen in chapter 6.5 on page 23.

The output mode can be used to specify which status messages are to be sent on the command channel:

Value	Meaning	Transmission scheme
'A'	Ack only (status only)	Request – Status – Data
'F'	Full (Status and EOT)	Request – Status – Data – EOT
'N'	No status (data only)	Request – Data

Command identifier '-L': Detect data carrier, universal

Detects the tags (max. 999) that are in the detection range of the specified antenna and returns the predefined formatted tag data of the specified data. The output channel can be used to specify whether the request and response are transmitted on the same TCP port (IN band) or on different TCP ports (OUT band).

Byte	Length	Command element	Value range
00	1	Universal command identifier (ASCII)	'L'
01	1	Command identifier (ASCII)	'L'
02	1	Antenna number (ASCII)	'0': All active antennas '1'...'4': Single antenna
03...05	3	Max. number of data carriers (ASCII)	'000'...'999'
06	1	Output channel	'0': IN band '1': OUT band
07	1	Output mode	'A': Ack only 'F': Full status 'N': No status
08	1	BCC	00 _{hex} ...FF _{hex}

Status message (only transmitted in output mode 'A' and 'F'):

Byte	Length	Command element	Value range
00	1	Status	<ACK> or <NAK>
01	1	Status code	See table <i>Status codes</i> on page 94

If the command is executed successfully, the formatted tag data of the data carriers located in the detection range of the specified antenna follow on the defined data channel. The data corresponds to the specified formatting.

Byte	Length	Command element	Value range
00...	Variable	Prefix + FormattedTag-Data(1st tag) + FormattedTag-Data(2nd tag) + ... + Suffix	All values possible through the format

This is followed by the <EOT> message containing the number of detected data carriers (transmitted only in output mode 'F')

Byte	Length	Command element	Value range
00	1	Status	<EOT>
01	1	Number of data carriers	'000'...'999'
02	1	BCC	00 _{hex} ...FF _{hex}

Command identifier ‘-R’: Read data carrier, universal

Read formatted tag data from a data carrier that is within the detection range of the specified antenna. The output channel can be used to specify whether the request and response are transmitted on the same TCP port (IN band) or on different TCP ports (OUT band).

If there are several data carriers in the detection range of the specified antenna, the desired data carrier must be selected before reading (see *Command identifier ‘z’: Select data carrier (Select)* on page 105).

Byte	Length	Command element	Value range
00	1	Universal command identifier (ASCII)	‘-’
01	1	Command identifier (ASCII)	‘R’
02	1	Antenna number (ASCII)	‘0’: All active antennas ‘1’...‘4’: Single antenna
03...05	3	Reserved	‘000’
06	1	Output channel	‘0’: IN band ‘1’: OUT band
07	1	Output mode	‘A’: Ack only ‘F’: Full status ‘N’: No status
08	1	BCC	00 _{hex} ...FF _{hex}

Status message (only transmitted in output mode ‘A’ and ‘F’):

Byte	Length	Command element	Value range
00	1	Status	<ACK> or <NAK>
01	1	Status code	See table <i>Status codes</i> on page 94

If the command is executed successfully, the requested data follow on the defined data channel. The data corresponds to the previously defined formatting.

Byte	Length	Command element	Value range
00...	Variable	Formatted tag data of the read tag	All values possible through the format

This is followed by the final status message, which confirms a successful read or indicates an error (only transmitted in output mode ‘F’).

Byte	Length	Command element	Value range
00	1	Status	<ACK> or <NAK>
01	1	Status code	See table <i>Status codes</i> on page 94

Command identifier '-W': Write data carrier, universal

Write formatted tag data to a data carrier located within the detection range of the specified antenna. The output channel can be used to specify whether the request and response are transmitted on the same TCP port (IN band) or on different TCP ports (OUT band).

If there are several data carriers in the detection range of the specified antenna, the desired data carrier must be selected before reading (see *Command identifier 'z': Select data carrier (Select)* on page 105).

Byte	Length	Command element	Value range
00	1	Universal command identifier (ASCII)	'_'
01	1	Command identifier (ASCII)	'W'
02	1	Antenna number (ASCII)	'0': All active antennas '1'...'4': Single antenna
03...05	3	Reserved	'000'
06	1	Output channel	'0': IN band '1': OUT band
07	1	Output mode	'A': Ack only 'F': Full status 'N': No status
08	1	BCC	00 _{hex} ...FF _{hex}

Status message (only transmitted in output mode 'A' and 'F'):

Byte	Length	Command element	Value range
00	1	Status	<ACK> or <NAK>
01	1	Status code	See table <i>Status codes</i> on page 94

After the positive status message, if requested, the formatted tag data can be transferred. The data must correspond to the previously specified formatting.

Byte	Length	Command element	Value range
00	Variable	FormattedTag data to be written to the tag	All values possible through the format



The data must be transferred exactly in the format that would also be supplied by a formatted read command. Fixed text in the format specification must also be transferred. If the format specification contains status values (which are read-only), these can be assigned any data in the corresponding format.

This is followed by the final status message, which confirms successful writing or indicates an error (only transmitted in output mode 'F').

Byte	Length	Command element	Value range
00	1	Status	<ACK> or <NAK>
01	1	Status code	See table <i>Status codes</i> on page 94

8.12 IO-Link

The IO-Link-specific commands can be used to exchange data via the IO-Link interface and to operate digital input/output ports.

Command identifier 'i': Acyclical demand data, read

Read IO-Link device demand data/parameters.

Byte	Length	Command element	Value range
00	1	Command identifier (ASCII)	'i'
01...04	4	Index MSB...LSB (ASCII hex)	"0000"... "FFFF"
05...08	4	Sub-index MSB...LSB (ASCII hex)	"0000"... "FFFF"
09	1	BCC	00 _{hex} ...FF _{hex}

Status message:

Byte	Length	Command element	Value range
00	1	Status	<ACK> or <NAK>
01	1	Status code	See <i>Status codes</i> on page 94

If the status message is positive, data is requested with <STX>.

Byte	Length	Command element	Value range
00	1	Control command	<STX>

If the command cannot be executed properly, a negative status message follows.

Byte	Length	Command element	Value range
00	1	Status	<NAK>
01	1	Status code	See table <i>Status codes</i> on page 94

If the command is executed successfully, a positive status message follows. This contains a length field and the requested data.

Byte	Length	Command element	Value range
00	1	Status	<ACK>
01...02	2	Number of bytes (ASCII)	"00"... "99"
03	No. of bytes	Data	Byte: 00 _{hex} ...FF _{hex}
Last byte	1	BCC	00 _{hex} ...FF _{hex}

Command identifier 'e': Acyclical demand data, write

Send demand data/parameter data via the IO-Link interface.

Byte	Length	Command element	Value range
00	1	Command identifier (ASCII)	'e'
01...04	4	Index MSB...LSB (ASCII hex)	"0000"... "FFFF"
05...08	4	Sub-index MSB...LSB (ASCII hex)	"0000"... "FFFF"
09...11	3	Number of bytes (ASCII)	"000"... "999"
12	1	BCC	00 _{hex} ...FF _{hex}

Status message:

Byte	Length	Command element	Value range
00	1	Status	<ACK> or <NAK>
01	1	Status code	See <i>Status codes</i> on page 94

If the status message is positive, data can be transmitted with <STX>.

Byte	Length	Command element	Value range
00	1	Control command	<STX>
01	No. of bytes	Data	Byte: 00 _{hex} ...FF _{hex}
Last byte	1	BCC	00 _{hex} ...FF _{hex}

Status message:

Byte	Length	Command element	Value range
00	1	Status	<ACK> or <NAK>
01	1	Status code	See <i>Status codes</i> on page 94

Command identifier 'I': Digital output ports, set/reset

Set or reset the digital output ports (IO-Link Pin2/Pin4).



To be able to use the digital output ports, they must be configured accordingly via the IO-Link parameters (see *Command identifier 'g': IO-Link master configuration, write* on page 129).

Byte	Length	Command element	Value range
00	1	Command identifier (ASCII)	'/'
01	1	IO-Link pin (ASCII)	'2': Pin 2 '4': Pin 4
02	1	Status (ASCII)	'0': Low '1': High
03	1	BCC	00 _{hex} ...FF _{hex}

Status message:

Byte	Length	Command element	Value range
00	1	Status	<ACK> or <NAK>
01	1	Status code	See <i>Status codes</i> on page 94

If the status message is positive, the settings can be accepted with <STX>.

Byte	Length	Command element	Value range
00	1	Control command	<STX>

Status message:

Byte	Length	Command element	Value range
00	1	Status	<ACK> or <NAK>
01	1	Status code	See <i>Status codes</i> on page 94

8

007 protocol (continued)

Command identifier '**': Digital input ports, read

Read status of digital input ports.



To be able to use the digital input ports, they must be configured accordingly via the IO-Link parameters (see *Command identifier 'g': IO-Link master configuration, write* on page 129).

Byte	Length	Command element	Value range
00	1	Command identifier (ASCII)	'**'
01	1	IO-Link pin (ASCII)	'2': Pin 2 '4': Pin 4
03	1	BCC	00 _{hex} ...FF _{hex}

Status message:

Byte	Length	Command element	Value range
00	1	Status	<ACK> or <NAK>
01	1	Status code	See <i>Status codes</i> on page 94

If the status message is positive, the status of the selected input port can be queried with <STX>.

Byte	Length	Command element	Value range
00	1	Control command	<STX>

If the command cannot be executed properly, a negative status message follows.

Byte	Length	Command element	Value range
00	1	Status	<NAK>
01	1	Status code	See table <i>Status codes</i> on page 94

If the command is executed successfully, a positive status message follows. This contains the status of the queried input port.

Byte	Length	Command element	Value range
00	1	Status	<ACK>
01	1	Status	'0': Low '1': High
02	1	BCC	00 _{hex} ...FF _{hex}

Command identifier ‘#’: IO-Link master configuration, read

Read the currently used IO-Link master configuration.

Byte	Length	Command element	Value range
00	1	Command identifier (ASCII)	‘#’
01	1	BCC	00 _{hex} ...FF _{hex}

Status message:

Byte	Length	Command element	Value range
00	1	Status	<ACK> or <NAK>
01	1	Status code	See <i>Status codes</i> on page 94

If the status message is positive, the parameter data can be requested with <STX>.

Byte	Length	Command element	Value range
00	1	Control command	<STX>

If the command cannot be executed properly, a negative status message follows.

Byte	Length	Command element	Value range
00	1	Status	<NAK>
01	1	Status code	See table <i>Status codes</i> on page 94

If the command is executed successfully, a positive status message follows. This contains the IO-Link parameter data in the following format:

Byte	Length	Command element	Value range
00	1	Status	<ACK>
01	1	Cycle Time Base (ASCII)	‘0’: 0.1 ms ‘1’: 0.4 ms ‘2’: 1.6 ms
02...03	2	Cycle Time (ASCII)	‘00’...‘63’
04	1	IO-Link mode Pin4 (ASCII)	‘0’: Input NO ‘1’: Input NC ‘2’: Reserved ‘3’: Output ‘4’: IO-Link data ‘5’: Input NO – SIO ‘6’: Input NC – SIO
05	1	IO-Link mode Pin2 (ASCII)	‘0’: Input NO ‘1’: Input NC ‘2’: Reserved ‘3’: Output
06	1	Safe State (ASCII)	‘0’...‘2’
07	1	Validation (ASCII)	‘0’: No validation ‘1’: Compatible ‘2’: Identical
08	1	Parameter server (ASCII)	‘0’: Disabled ‘1’: Delete ‘2’: Enabled
09	1	Upload parameters (ASCII)	‘0’: Disabled ‘1’: Enabled
10	1	Parameter download (ASCII)	‘0’: Disabled ‘1’: Enabled
11...14	4	Vendor ID (ASCII hex)	“0000”...“FFFF”
15...20	6	Device ID (ASCII hex)	“000000”...“FFFFFF”
21...22	2	Output Length (ASCII)	“00”...“32”
23...24	2	Input Length (ASCII)	“00”...“32”
25...40	16	Serial Number (ASCII)	ASCII-String
41	1	BCC	00 _{hex} ...FF _{hex}

Command identifier 'g': IO-Link master configuration, write

Write the IO-Link master configuration.

Byte	Length	Command element	Value range
00	1	Command identifier (ASCII)	'g'
01	1	Cycle Time Base (ASCII)	'0': 0.1 ms '1': 0.4 ms '2': 1.6 ms
02...03	2	Cycle Time (ASCII)	'00'...'63'
04	1	IO-Link mode Pin4 (ASCII)	'0': Input NO '1': Input NC '2': Reserved '3': Output '4': IO-Link data '5': Input NO – SIO '6': Input NC – SIO
05	1	IO-Link mode Pin2 (ASCII)	'0': Input NO '1': Input NC '2': Reserved '3': Output
06	1	Safe State (ASCII)	'0'...'2'
07	1	Validation (ASCII)	'0': No validation '1': Compatible '2': Identical
08	1	Parameter server (ASCII)	'0': Disabled '1': Delete '2': Enabled
09	1	Upload parameters (ASCII)	'0': Disabled '1': Enabled
10	1	Parameter download (ASCII)	'0': Disabled '1': Enabled
11...14	4	Vendor ID (ASCII hex)	"0000"... "FFFF"
15...20	6	Device ID (ASCII hex)	"000000"... "FFFFFF"
21...22	2	Output Length (ASCII)	"00"... "32"
23...24	2	Input Length (ASCII)	"00"... "32"
25...40	16	Serial Number (ASCII)	ASCII-String
41	1	BCC	00 _{hex} ...FF _{hex}

Status message:

Byte	Length	Command element	Value range
00	1	Status	<ACK> or <NAK>
01	1	Status code	See <i>Status codes</i> on page 94

If the status message is positive, the parameter data can be accepted with <STX>.

Byte	Length	Command element	Value range
00	1	Control command	<STX>

Status message:

Byte	Length	Command element	Value range
00	1	Status	<ACK> or <NAK>
01	1	Status code	See table <i>Status codes</i> on page 94

Command identifier 'Y': Cyclical process data, read

Read process data via the IO-Link interface.



To be able to receive data via the IO-Link interface, the IO-Link port (pin 4) must be configured as a data port (C/Q) (see *Command identifier 'g': IO-Link master configuration, write* on page 129).

Byte	Length	Command element	Value range
00	1	Command identifier (ASCII)	'Y'
01...03	3	Start address (ASCII)	"000"... "999"
04...06	3	Number of bytes (ASCII)	"000"... "999"
07	1	BCC	00 _{hex} ...FF _{hex}

Status message:

Byte	Length	Command element	Value range
00	1	Status	<ACK> or <NAK>
01	1	Status code	See <i>Status codes</i> on page 94

If the status message is positive, data is requested with <STX>.

Byte	Length	Command element	Value range
00	1	Control command	<STX>

If the command cannot be executed properly, a negative status message follows.

Byte	Length	Command element	Value range
00	1	Status	<NAK>
01	1	Status code	See table <i>Status codes</i> on page 94

If the command is executed successfully, a positive status message follows. This contains a length field and the requested data.

Byte	Length	Command element	Value range
00	1	Status	<ACK>
01...03	3	Number of bytes (ASCII)	"000"... "999"
04	No. of bytes	Data	Byte: 00 _{hex} ...FF _{hex}
Last byte	1	BCC	00 _{hex} ...FF _{hex}

8

007 protocol (continued)

Command identifier 'X': Cyclical process data, write

Send process data via the IO-Link interface.



To be able to send data via the IO-Link interface, the IO-Link port (pin 4) must be configured as a data port (C/Q) (see *Command identifier 'g': IO-Link master configuration, write* on page 129).

Byte	Length	Command element	Value range
00	1	Command identifier (ASCII)	'X'
01...03	3	Start address (ASCII)	"000" ... "999"
04...06	3	Number of bytes (ASCII)	"000" ... "999"
07	1	BCC	00 _{hex} ...FF _{hex}

Status message:

Byte	Length	Command element	Value range
00	1	Status	<ACK> or <NAK>
01	1	Status code	See <i>Status codes</i> on page 94

If the status message is positive, data can be transmitted with <STX>.

Byte	Length	Command element	Value range
00	1	Control command	<STX>
01	No. of bytes	Data	Byte: 00 _{hex} ...FF _{hex}
Last byte	1	BCC	00 _{hex} ...FF _{hex}

Status message:

Byte	Length	Command element	Value range
00	1	Status	<ACK> or <NAK>
01	1	Status code	See <i>Status codes</i> on page 94

This chapter describes the OPC UA (Open Platform Communications Unified Architecture) standard for the UHF RFID device from Balluff.
OPC UA is the central standard in the implementation of the future strategy for Industry 4.0 or IIoT (Industrial Internet of Things) and is used to network existing industrial plants.

9.1 Basics of OPC UA

9.1.1 Description of OPC UA

OPC UA describes a collection of specifications for industrial automation. The focus of this standard is on communication between industrial devices (M2M). This standard makes it much easier to transmit or exchange parameters, sensor data, control variables and control instructions across manufacturers. OPC UA is an Internet-friendly, service-oriented architecture (SOA).
The OPC Foundation and AIM Germany have defined the OPC UA standard *OPC Unified Architecture for AutotID Companion Specification*, which describes the OPC UA interface for identification devices.

The identification devices are classified as follows:

- Text recognition devices (OCR)
- Optical readers (e.g. QR code, barcode)
- RFID readers
- Localization systems (RTLS)

All BIS U devices that support OPC UA belong to the genus of RFID readers in the OPC UA Companion Specification (see OPC UA AutotID Companion Specification 1.0).

9.1.2 System diagram

The specification describes a client-server principle. An OPC UA server is a device that offers and publishes data and information. A client accesses this data and information by means of methods. Up to 50 clients can log on to the BIS U-6127 processor unit and access data (see Fig. 9-1).

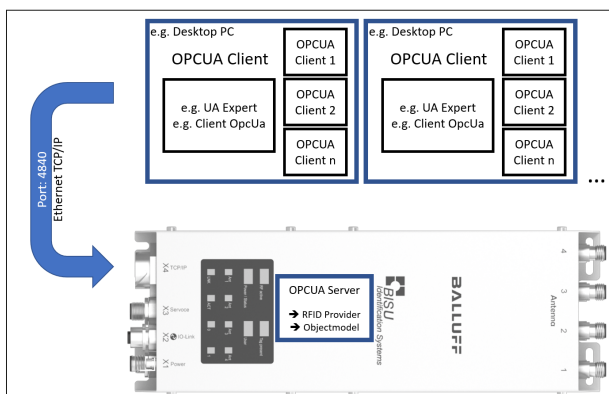


Fig. 9-1: System diagram

9.1.3 Security mechanisms

When the OPC UA standard was created, the issue of security was always of central importance. Older industrial plants usually operate autonomously and without connection to the Internet. These are also referred to as island plants. Due to their natural isolation from the outside world (the Internet), the issue of IT security played a subordinate role. Network attacks from outside were virtually impossible.

Due to the constantly increasing networking of plants and the connection to the Internet, it is imperative that plants are protected against network attacks.

OPC UA has provided several security mechanisms to protect the data to be transmitted and to allow processes to take place without interference:

- *Confidentiality*: Here the data is encrypted at the transport level to protect it from *eavesdroppers*.
- *Integrity*: This mechanism ensures that the data is not modified on its way to the recipient.
- *Application authentication*: Here, the communicating applications must first *authenticate each other*. This is done by exchanging certificates. Only when certificates have been exchanged and accepted can data be transmitted via the communication link.
- *User authorization*: To gain full access to the BIS U-6127, you must log in with a user name and password. This additional security mechanism ensures that only authorized users can access the device.



To avoid invalid certificates, set the date, time and time zone correctly when generating a certificate.

Certificates have a limited validity (the validity can be displayed on a Windows PC, for example) and must be replaced when the validity expires (see section *OPC/UA* on page 41).

9.2 OPC UA security mechanisms on BIS U-6127

On the BIS U-6127, the basic OPC UA security settings are selected in the web server. Under *SECURITY SETTINGS* (see *Security settings* on page 40) it is possible for the logged-in user to change the security settings.

OPC/UA Settings

Refuse Unsecure Client Connections **a** ☒

Accept only Trusted Client Certificates **b** ☐

Use Secure Element **c** ☒

Client Certificate List

Status	Name	Organization	Valid From	Valid To	
Trusted	UaExpert_trusted.der	Balluff GmbH	Oct 2 01:51:33 2020 GMT	Oct 1 01:51:33 2025 GMT	🔒 🗑️ d
Rejected	UaExpert_rejected.der	Balluff GmbH	Oct 2 01:51:33 2020 GMT	Oct 1 01:51:33 2025 GMT	🔒 🗑️ e

Set Refresh Reboot

Create/Download Certificate

f Create Certificate Download **g**

*Please update the date before creating certificate

Fig. 9-2: Web server security settings

In the web server tab OPC UA (see figure Fig. 9-2), there are the following security settings:

- *REFUSE UNSECURE CLIENT CONNECTIONS*: If this field is activated, unsecure OPC UA connections are rejected. The secure state is thus activated.
- *ACCEPT ONLY TRUSTED CLIENT CERTIFICATES*: This field cannot be operated separately by the user. It is always activated synchronously with the *REJECT UNSECURE CLIENT CONNECTIONS* field.
- *USE SECURE ELEMENT* (uses the integrated security module): A dedicated security module is used in the BIS U-6127 device. The public and private security keys for generating and authenticating certificates are stored on this.

The fields *REFUSE UNSECURE CLIENT CONNECTIONS* and *ACCEPT ONLY TRUSTED CLIENT CERTIFICATES* are linked and allow a total of two basic states for OPC UA.

1. *Unsecure* (default): All OPC-UA connections are allowed.
2. *Secure*: Only the following security settings are allowed in the OPC UA client:
 - Security policy: *BASIC256SHA256*
 - Message security mode: *SIGN & ENCRYPT*

See also Fig. 9-5 on page 135.

If any of the three security settings are changed, the device must be restarted for the changes to take effect.

9

OPC UA (continued)

The following table shows an overview of the possible security settings for OPC UA in the BIS U-6127 processor unit:

OPC-UA setting in BIS U-6127		
Reject unsecure client connections	Off	On
Accept trusted client certificates only	Off	On
BIS U-6127 status		
	Unsecure	Secure
Security policy of client		
None	Allowed	No connection possible
Basic256Sha256	Allowed	Allowed
Other, e.g. AES	Not allowed	No connection possible
Message security mode of client		
None	Allowed	No connection possible
Sign	Allowed	No connection possible
Sign&Encrypt	Allowed	Allowed
Client certificate		
New or unknown certificate (not in certificate list)	Allowed	No connection possible
Certificate in certificate list in status <i>REJECTED</i>	Allowed	No connection possible
Certificate in certificate list in status <i>TRUSTED</i>	Allowed	Allowed

If you try to connect to a client with the BIS U-6127 certificate, the error message *CONNECT ERROR* appears (see Fig. 9-3).

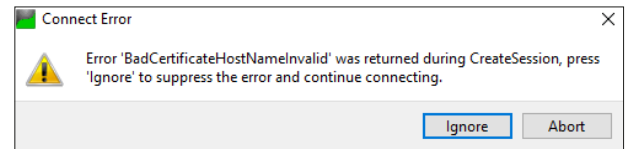


Fig. 9-3: Error message

This error message is output if either no IP address or an incorrect IP address of the BIS U-6127 is stored in the certificate. At the time of delivery, it is not yet clear in which IP address range the device will be located, therefore the IP address field in the certificate is empty and not written to. The message can be confirmed with *IGNORE*. If a new valid certificate is generated (see *Security settings* on page 40), the error message should no longer appear.

9.3 Connection established via OPC UA with UaExpert

There are several OPC-UA clients to connect to the OPC-UA server of the BIS U-6127 processor unit. In this user's guide, the connection setup using the UaExpert from Unified Automation is shown as an example. The OPC-UA client UaExpert is available for download free of charge from the Unified Automation homepage (www.unified-automation.com) and must be installed on the PC.

The connection between OPC-UA client and OPC-UA server (BIS U-6127) can be established via an unsecure (see chapter 9.3.1) or secure variant (see chapter 9.3.2 on page 136).

9.3.1 Unsecure connection setup between PC (OPC-UA client) and the BIS U-6127 device (OPC-UA server)

Connect the PC (OPC-UA client) to the BIS U-6127 device (OPC-UA server):

1. Launch the UaExpert application.
2. Add a new server.

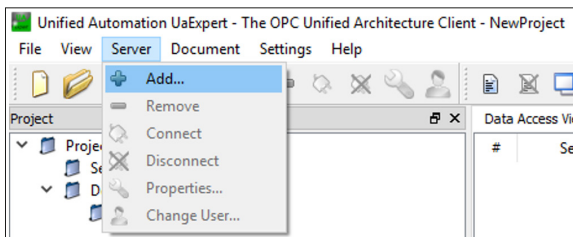


Fig. 9-4: Server Dialog

3. Switch to the *ADVANCED* tab.
4. Assign a *CONFIGURATION NAME* (e.g. *Balluff BIS U-6127 RFID Provider*).
5. Enter the following *ENDPOINT URL*:
`opc.tcp://192.168.10.2:4840`

i The IP address 192.168.10.2 is fixed in the delivery state. The IP address can be changed via the web server, the 007 protocol or the UHF Manager.

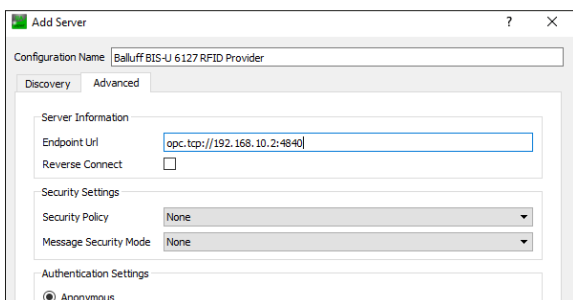


Fig. 9-5: OPC-UA-Add-Server

6. Depending on the settings in the device (web server), the security settings of *SECURITY POLICY* and *MESSAGE SECURITY MODE* must be changed (see chapter 9.2 on page 133). For an unsecure connection, enter *NONE* and *NONE* in both fields.

i If the *SECURITY POLICY* is set to *NONE* and the *MESSAGE SECURITY MODE* is set to *NONE* (see Fig. 9-5), a connection between server and client can be established in any case in the delivery state, but the connection is unsecure (no endpoint identity and no encryption). If only secure connections are to be used, unsecure connections must be blocked on the device side.

7. Right-click on the server and select *CONNECT* to connect to the server.

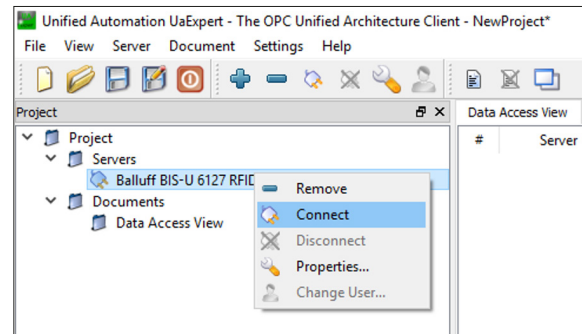


Fig. 9-6: Connection setup

⇒ The OPC-UA client (PC) is connected to the OPC-UA server (BIS U-6127). This is also visible by the server icon.

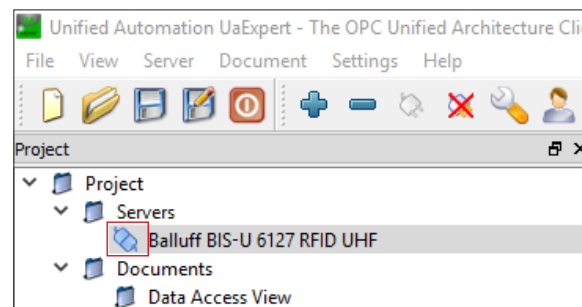


Fig. 9-7: Server connected to client

In addition, the complete structure is displayed in the *ADDRESS SPACE* window (see Fig. 9-17).

9.3.2 Secure connection setup between PC (OPC-UA client) and the BIS U-6127 device (OPC-UA server)

To force a secure connection between OPC-UA client and OPC-UA server (BIS U-6127), settings must be made in the web server of the BIS U-6127: In the OPC/UA settings (see Fig. 7-19 on page 41) the check box *REJECT UNSECURE CONNECTIONS* must be set (the check box *ACCEPT TRUSTED CLIENT CERTIFICATES ONLY* is set automatically at the same time).

If not already done, or if the network settings have been changed, a new server certificate must be generated (chapter *OPC/UA* on page 41).

Secure connection setup:

1. Launch UaExpert application.
2. Add a new server.

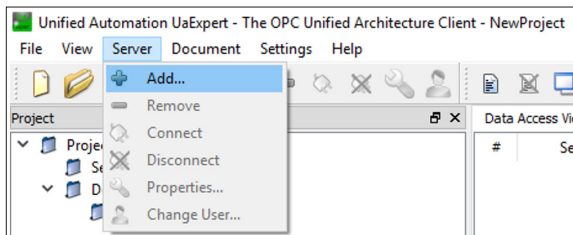


Fig. 9-8: Server Dialog

3. Switch to the *ADVANCED* tab.
4. Assign a *CONFIGURATION NAME* (e.g. *Balluff BIS U-6127 RFID Provider*).
5. Enter the following *ENDPOINT URL*: *opc.tcp://<IP address>:4840*, e.g. *opc.tcp://192.168.3.13:4840*

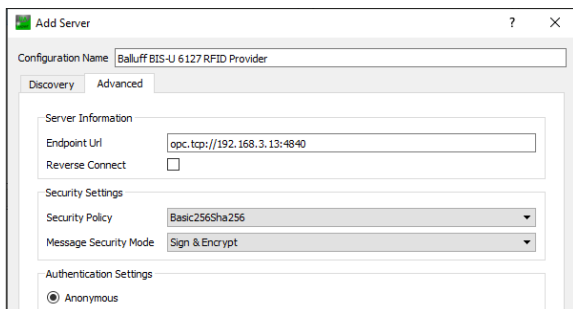


Fig. 9-9: Add Server

6. Select the following security settings:
 - *SECURITY POLICY*: Basic256Sha256
 - *MESSAGE SECURITY MODE*: Sign & Encrypt
7. Confirm with OK.

8. Right-click on the server and select *CONNECT* to connect to the server.

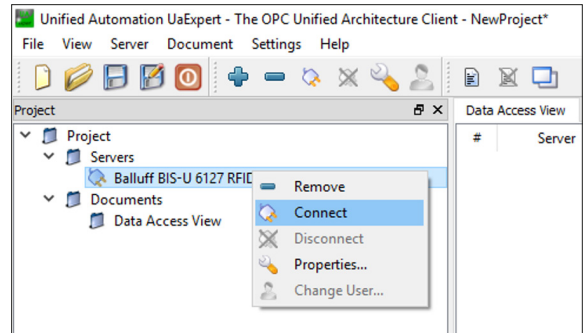


Fig. 9-10: Connection setup

⇒ A trust query about the server's certificate appears.

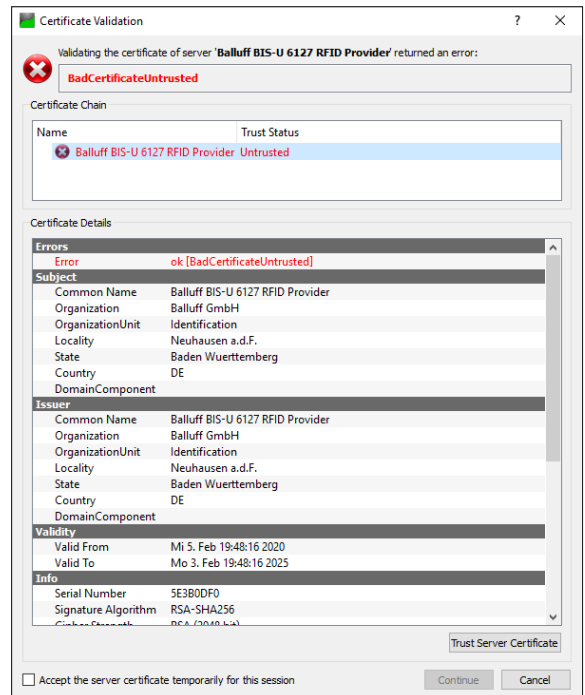


Fig. 9-11: Certificate check

9

OPC UA (continued)

9. If the data corresponds to the BIS U-6127 device, a permanent trust status can be established with *TRUST SERVER CERTIFICATE*.

i If the certificate has expired (see Fig. 9-12 under *VALIDITY*), a new certificate must be created and a trust status established again.

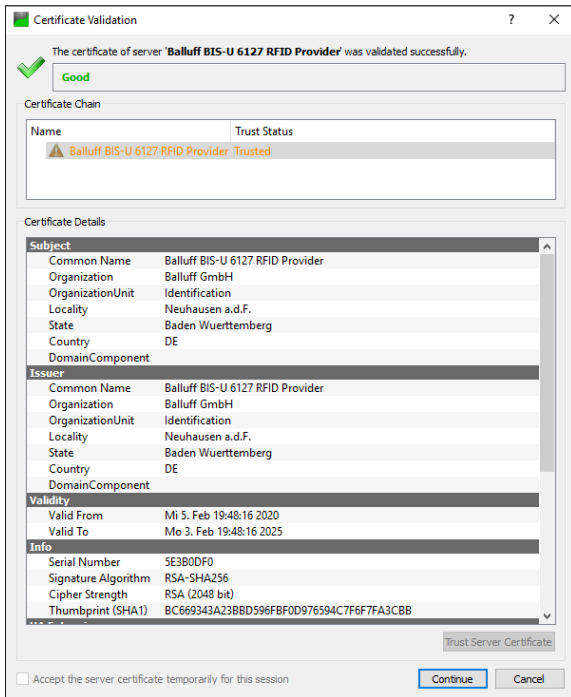


Fig. 9-12: Certificate check accepted

- ⇒ The certificate of the BIS U-6127 OPC UA Server is accepted by UAExpert.
 ⇒ The connection request is initially also rejected by the BIS U-6127 device despite an accepted server certificate (even if a new connection attempt is made, see step 8):

Timestamp	Source	Server	Message
06.10.2020 10:05...	Server Node	Balluff BIS-U 6127 RFID Provider	ApplicationUri: 'urn:Balluff.com:BalluffAutoid'
06.10.2020 10:05...	Server Node	Balluff BIS-U 6127 RFID Provider	Used UserTokenType: Anonymous
06.10.2020 10:05...	General		[EventId] OpClt_TcpConnection_ProcessResponse: Error Message!
06.10.2020 10:05...	General		[EventId] OpClt_TcpConnection_ProcessResponse: Status (0x0130000)
06.10.2020 10:05...	Server Node	Balluff BIS-U 6127 RFID Provider	Error 'BadSecurityCheckedFailed' was returned during OpenSecureChannel
06.10.2020 10:05...	Server Node	Balluff BIS-U 6127 RFID Provider	Connection status of server 'Balluff BIS-U 6127 RFID Provider' changed to 'Disconnected'

Fig. 9-13: Log: Connection attempt rejected

i The client certificate of the UA Expert application is not yet classified as secure on the server (BIS U-6127) and is therefore rejected (this applies also to other applications).

10. Get the client certificate accepted via the BIS U-6127 website (see chapter *OPC/UA* on page 41).
 ⇒ Connection between server and client is now possible.
 11. Right-click on the server and select *CONNECT* to connect to the server (see Fig. 9-10).

12. Acknowledge the following error message with *IGNORE*.

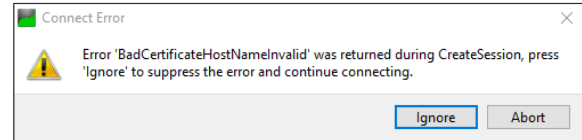


Fig. 9-14: Error message (Connect Error)

- ⇒ The secure connection between server and client is established and displayed by the server icon.

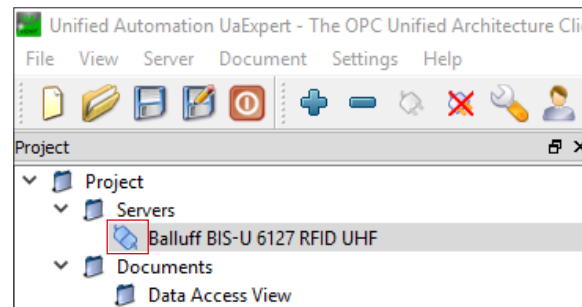


Fig. 9-15: Server connected to client

9.4 Data model object: BIS_U_6127_Rfid_Provider

This chapter describes the OPC-UA data model and deals specifically with the OPC-UA object *BIS_U_6127_Rfid_Provider*.

This object is derived from the OPC-UA object *RfidReaderDeviceType*, which in turn is derived from *AutoldDeviceType*. The object consists of methods, variables and events:

- Methods are client-callable functions to which values can be transferred, which perform an action and then return values.
- Variables are values that consist of a simple or complex data type and that can generally be read and written to by the client at any time (there may be restrictions on permissions). Variables in OPC UA are cross-session, i.e. their value is displayed equally to all connected clients.
- Events are functions with which the OPC-UA server (here the BIS U-6127 processor unit) can send unsolicited messages to the clients, provided that the client has activated these notifications.

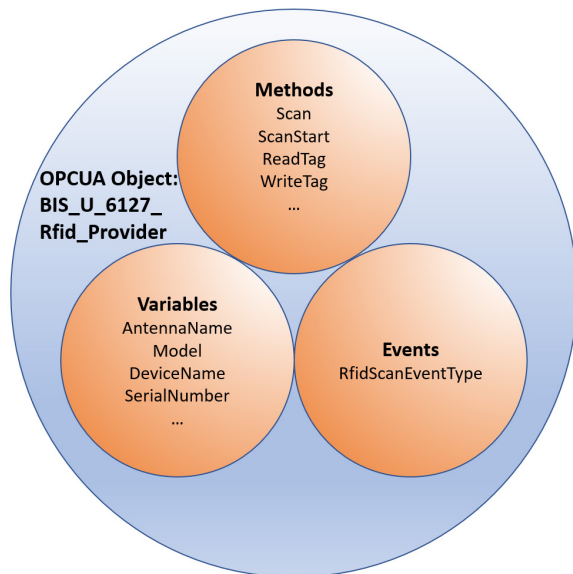


Fig. 9-16: Data model object BIS_U_6127_Rfid_Provider

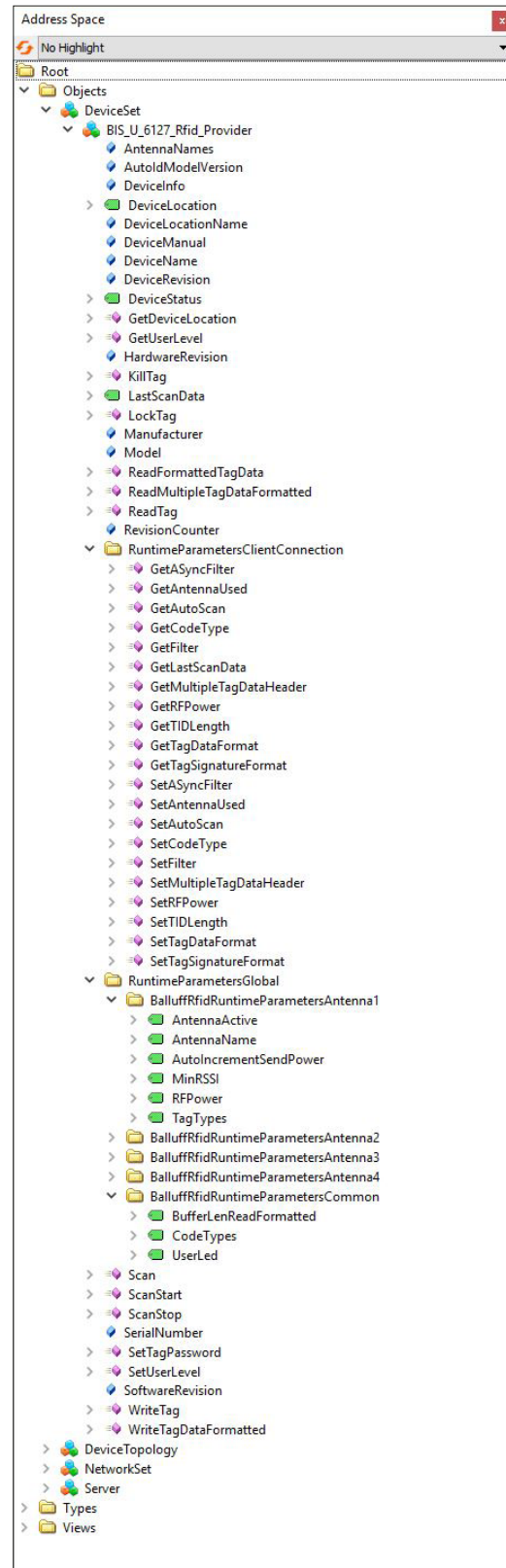


Fig. 9-17: Object structure

9.5 Methods

The *BIS_U_6127_Rfid_Provider* object contains several methods. They can have both call arguments (input arguments) and return values (output arguments). In Fig. 9-17 on page 138, all methods are marked with a violet symbol. The methods listed under *RUNTIMEPARAMETERSCLIENTCONNECTION* are Balluff extensions. They use OPC-UA access functions to set and read properties for the current session.

Methods are divided into the three subchapters according to their function:

- *Device setting methods*
- *Write/read methods for tag*
- *Methods for scan settings*

The following tables provide an overview of all methods.

Device setting

Method	Description	Page
<i>GetDeviceLocation</i>	Supplies the device location	140
<i>SetUserLevel</i>	Change of user login	140
<i>GetUserLevel</i>	Returns current user	140

Write/read tag

Method	Description	Page
<i>Scan</i>	Synchronous scanning mode	141
<i>ReadTag</i>	Read data from a data carrier	142
<i>WriteTag</i>	Write data to a data carrier	143
<i>ReadFormatted-TagData</i>	Read formatted data from data carrier	144
<i>WriteTagDataFormatted</i>	Write formatted data to data carrier	144
<i>ReadMultipleTag-DataFormatted</i>	Read formatted data from multiple data carriers	145
<i>ScanStart</i>	Start asynchronous scanning mode	146
<i>ScanStop</i>	Stop asynchronous scanning mode	146
<i>SetAutoScan</i>	Start/stop autonomous scanning mode	146
<i>GetAutoScan</i>	Returns setting of autonomous scanning mode	146
<i>GetLastScanData</i>	Returns last scanned data	146
<i>LockTag</i>	Lock memory areas of a data carrier	147
<i>KillTag</i>	Permanently deactivate a data carrier	147

Scan settings

Method	Description	Page
<i>SetAntennaUsed</i>	Switch antennas on/off	148
<i>GetAntennaUsed</i>	Provides information about antennas switched on/off	148
<i>SetAsynchFilter</i>	Set filters for asynchronous scanning mode	148
<i>GetAsynchFilter</i>	Provides information about asynchronous filters (loop filters)	149
<i>SetCodeType</i>	Sets type of EPC	149
<i>GetCodeType</i>	Returns type of EPC	149
<i>SetFilter</i>	Set filters for synchronous scanning mode	150
<i>GetFilter</i>	Returns active filter for synchronous scanning mode	151
<i>SetMultipleTag-DataHeader</i>	Set prefixes and suffixes for tag list	151
<i>GetMultipleTag-DataHeader</i>	Returns set prefixes and suffixes for tag list	152
<i>SetRFPower</i>	Set antenna transmitting power	152
<i>GetRFPower</i>	Returns transmitting power of an antenna	152
<i>SetTagDataFormat</i>	Set format string for data	153
<i>GetTagDataFormat</i>	Returns current format string of data	153
<i>SetTagSignature-Format</i>	Enable/disable signature creation and signature verification	154
<i>GetTagSignature-Format</i>	Returns signature settings	154
<i>SetTagPassword</i>	Writes password information on a tag	155
<i>SetTIDLength</i>	Set TID length	155
<i>GetTIDLength</i>	Returns set TID length	155

9.5.1 Device setting methods

GetDeviceLocation

This method returns the device location.

Call parameter

Name	Data Type	Description
LocationType	LocationType (see chapter 9.7.8) on page 162)	Specifies the type in which the device location is to be specified.

Return parameter

Name	Data Type	Description
Location	Location (see chapter 9.7.6 on page 162)	Specifies the device location.

SetUserLevel

This method can be used to change the user login of the session.

A login expires after 15 minutes without use. After 24 hours at the latest, you must log in again.

Call parameter

Name	Data Type	Description
Username	String	Login name of the new user.
Password	String	Password for the user to be logged in.

Return parameter

Name	Data Type	Description
Status	AutoldOperati- onStatusEnum- eration (see chapter 9.7.2 on page 161)	Returns the result of the operation.

GetUserLevel

This method returns the login name of the current user of this session.

Return parameter

Name	Data Type	Description
Username	String	Login name of the user of this session.
Status	AutoldOperati- onStatusEnum- eration (see chapter 9.7.2 on page 161)	Returns the result of the operation.

9.5.2 Write/read methods for tag

Scan

This method can be used to start the synchronous scanning process (see chapter 6.5 on page 23). The call parameters define how long and how often scanning is to be performed.

The conditions for stopping (*SCANSETTINGS*) are related to each other. As soon as a condition is fulfilled, the scanning process is stopped.

Both the antenna selection (see *SetAntennaUsed* on page 148) and the activated static filters (see *SetFilter* on page 150) of the current session are taken into account during the scan.

Call arguments

Name	Data Type	Description
Settings	ScanSettings	Settings for how long or how often the scan should be performed.

Return values

Name	Data Type	Description
Result	RfidScanResult[]	All detected tags are output with information such as EPC, timestamp, RSSI value, etc.
Status	AutoldOperationStatusEnumeration (see chapter 9.7.2 on page 161)	Returns the result of the operation.

Structures used by call arguments and return parameters

ScanSettings (see chapter 9.7.16 on page 165)

Name	Data Type	Description
Duration	Duration	Specifies the duration of the scanning process. The value 0 stands for "infinite length".
Cycles	Int32	Specifies the number of scan passes. The value 0 stands for "infinite number".

Name	Data Type	Description
DataAvailable	Boolean	If this value is set to <i>TRUE</i> , the scan will stop as soon as data is available. With <i>FALSE</i> , only the parameters <i>DURATION</i> and <i>CYCLES</i> are considered.
LocationType	LocationType (see chapter 9.7.8 on page 162)	Specifies the desired type of location information in the result. Only the <i>LOCATION-NAME</i> type is supported.

RfidScanResult (see chapter 9.7.12 on page 163)

Name	Data Type	Description
CodeType	CodeTypeDataType (see chapter 9.7.4 on page 162)	Specifies the format in which the scanned data should be output under Scan-Data.
ScanData	ScanData	Data of the successfully scanned tag.
Timestamp	UtcTime	Time of tag read in <i>Universal Time Coordinate</i> time zone.
Location	Location	Returns the location where the tag was detected.
Sightings	RfidSighting[] (see chapter 9.7.13 on page 164)	Information about each read of the tag on an antenna: 1: Number of the antenna 2: RSSI value 3: UtcTime at read 4: Transmitting power used during read

ReadTag

This method can be used to read a specific memory area of a tag. The area and how many bytes are to be read are specified in the call parameters.

The area to be read must not exceed the selected memory area, otherwise the Read command cannot be executed and returns an error. The size of the individual memory areas depends on the respective tag. Detailed information can be taken from the data sheet of the data carrier used.

Call parameter

Name	Data Type	Description
Identifier	ScanData (see chapter 9.7.14 on page 164)	EPC of the tag to be read from.
CodeType	CodeTypeData- Type (see chapter 9.7.4 on page 162)	Specifies the type for the <i>Identifier</i> parameter.
Region	UInt16	Memory area of the tag to be read. The following values are possible: 0: Reserved bank (kill and access passwords) 1: EPC bank 2: TID bank 3: USER data bank
Offset	UInt32	Specifies the byte address of the first byte to be read.
Length	ByteString	Specifies the length of the area to be read. The complete area (Offset + Length – 1) must be within the selected memory area.
Password	BytesString	If the area to be read is locked, the corresponding 4-byte-long password must be entered here. Otherwise the value "00000000" must be entered.

Output parameter

Name	Data Type	Description
ResultData	ByteString	The successfully read data are output here as a Byte-String.
Status	AutoldOperati- onStatusEnu- meration (see chapter 9.7.2 on page 161)	Returns the result of the operation.

WriteTag

This method can be used to write specific data to a special memory area of a tag. Which and how much data is to be read is specified via the call parameters. The data to be written must not be too long for the specified memory area. The size of the individual memory areas depends on the respective tag type. Detailed information can be taken from the data sheet of the data carrier used.

Call parameter

Name	Data Type	Description
Identifier	ScanData (see chapter 9.7.14 on page 164)	EPC of the tag to be written to.
CodeType	CodeTypeData-Type (see chapter 9.7.4 on page 162)	Specifies the type for the <i>Identifier</i> parameter.
Region	UInt16	Memory area of the tag to be written to. The following values are possible: 0: Reserved bank (kill and access passwords) 1: EPC bank 2: TID bank 3: USER data bank
Offset	UInt32	Specifies the byte address of the first byte to be written.
Data	ByteString	Data, in the form of a ByteString, to be written to the tag. The data may only be so long that they do not exceed the selected memory area (note offset).
Password	ByteString	If the area to be written to is locked, the corresponding 4-byte-long password must be entered here. Otherwise the value "00000000" must be entered.

Output parameter

Name	Data Type	Description
Status	AutoidOperationStatusEnumeration (see chapter 9.7.2 on page 161)	Returns the result of the operation.

ReadFormattedTagData

This method can be used to read selected data on a tag and output it formatted as desired. The output format can be set and read via the session-related methods *SetTagDataFormat()* (see page 153) and *GETTAGDATAFORMAT()* (see page 153). For a detailed description of the application and the different possibilities see chapter 8.11 on page 121, for an example of this method see page 167.

Call parameter

Name	Data Type	Description
Identifier	ScanData (see chapter 9.7.14 on page 164)	EPC of the tag to be read from.
CodeType	CodeTypeData-Type (see chapter 9.7.4 on page 162)	Specifies the type for the <i>IDENTIFIER</i> parameter.
Password	ByteString	If the area to be read is locked, the corresponding 4-byte-long password must be entered here. Otherwise the value "00000000" must be entered.

Output parameter

Name	Data Type	Description
ReadData	ByteString	The successfully read data are output here as a ByteString.
Status	AutoldOperationStatusEnumeration (see chapter 9.7.2 on page 161)	Returns the result of the operation.

WriteTagDataFormatted

With this method, selected data can be written in formatted form on a tag. The data which is to be written can be specified via the call parameters. The data must be specified in the format that is set in the current session. This format can be set and read via the methods *SETTAGDATAFORMAT()* (see page 153) and *GETTAGDATAFORMAT()* (see page 153).

Call parameter

Name	Data Type	Description
Identifier	ScanData (see chapter 9.7.14 on page 164)	EPC of the tag to be read from.
CodeType	CodeTypeData-Type (see chapter 9.7.4 on page 162)	Specifies the type for the <i>IDENTIFIER</i> parameter.
WriteData	ByteString	The data to be written in the form of a ByteString. Important: The data must be transferred in the format of the current session.
Password	ByteString	If the area to be written to is locked, the corresponding 4-byte-long password must be entered here. Otherwise the value "00000000" must be entered.

Return parameter

Name	Data Type	Description
Status	AutoldOperationStatusEnumeration (see chapter 9.7.2 on page 161)	Returns the result of the operation.

ReadMultipleTagDataFormatted

This method can be used to read and output formatted data selected from several tags. The data which is to be read and how it is to be formatted can be set and read via the methods *SetTagDataFormat()* (see page 153) and *GetTagDataFormat()* (see page 153).

Furthermore, it is possible to specify whether and which data should be prepended or appended to the outputs. This can be set and read via the methods *SetMultipleTagDataHeader()* (see page 151) and *GetMultipleTagDataHeader()* (see page 152).

Call parameter

Name	Data Type	Description
Maxtags	UInt32	Specifies the maximum number of tags that can be read from. The maximum number is limited because the <i>Read-Data</i> output parameter is limited to 512000 bytes. The product of <i>Maxtags</i> and the variable <i>BufferLenReadFormatted</i> (see page 159) therefore must not exceed the value 5120000.
Password	ByteString	If the area to be read is locked, the corresponding 4-byte-long password must be entered here. Only one password can be specified. For tags with a different password, the read command cannot be executed.

Return parameter

Name	Data Type	Description
ReadData	ByteString	The successfully read data are output here as a Byte-String.
ReadTags	UInt32	Indicates the number of successfully read tags.
Status	AutoidOperationStatusEnumeration (see chapter 9.7.2 on page 161)	Returns the result of the operation.

ScanStart

This method can be used to start the asynchronous scanning process (see *Asynchronous operation* on page 24). Both the scan settings (call parameters) and the set filters (see page 150) are taken into account. Support for the scan settings with the *ScanStart* command depends on the version of the device software. The results of the scan are delivered in the form of OPC-UA events (*RfidScanEventType* on page 165) and are available for all sessions. This operation can be stopped by the *ScanStop* method (see page 146) or by ending the session.

Call arguments

Name	Data Type	Description
Settings	ScanSettings	Settings for how long or how often the scan should be performed.

Output parameter

Name	Data Type	Description
Status	AutoldOperationStatusEnumeration (see chapter 9.7.2 on page 161)	Returns the result of the operation.

Structures used by input and output parameters

ScanSettings (see chapter 9.7.16 on page 165)

Name	Data Type	Description
Duration	Duration	Specifies the duration of the scan process in ms. The value 0 stands for <i>infinite length</i> .
Cycles	Int32	Specifies the number of scan passes. The value 0 stands for <i>infinite number</i> .
DataAvailable	Boolean	If this value is set to <i>TRUE</i> , the scan will stop as soon as data is available. With <i>FALSE</i> , only the parameters Duration and Cycles are considered.
LocationType	LocationType (see chapter 9.7.8 on page 162)	Specifies the desired type of location information in the result.

ScanStop

This method is used to stop asynchronous operation.

SetAutoScan

This method can be used to switch the autonomous scanning mode on and off for the corresponding session (see *Autonomous operation* on page 27). In this mode, the device performs cyclical data carrier detections without the need to issue a command.

Min. Access Level: User

Default values: 0: (autonomous mode off)

Input

Name	Data Type	Description
AutoScan	UInt16	0: Switch off autonomous scanning mode 1...65536: Scan interval in ms

GetAutoScan

This method returns the session setting of the autonomous scanning mode. The value 0 means that autonomous scanning is not active.

Return parameter

Name	Data Type	Description
AutoScan	UInt16	0: Autonomous scanning mode is off. 1...65536: Scan interval in ms.
Result	AutoldOperationStatusEnumeration (see chapter 9.7.2 on page 161)	Returns the result of the operation.

GetLastScanData

This method returns the last detected EPC of the current session. It supports the output format set by the *SetCodeType()* method (see page 149).

Return parameter

Name	Data Type	Description
LastScanData	ScanData (see chapter 9.7.14 on page 164)	Last detected EPC of this session.
Result	AutoldOperationStatusEnumeration (see chapter 9.7.2 on page 161)	Returns the result of the operation.

LockTag

This method can be used to lock a specific memory area of a tag for any access. Depending on the selection, this setting may or may not be reversible.

Call parameter

Name	Data Type	Description
Identifier	ScanData (see chapter 9.7.14 on page 164)	EPC of the tag to be locked.
CodeType	CodeTypeDataType (see chapter 9.7.4 on page 162)	Specifies the type for the <i>IDENTIFIED</i> parameter.
Password	ByteString	4-byte-long password for the lock command.
Region	RfidLockRegionEnumeration (see chapter 9.7.10 on page 163)	Memory area to be locked.
Lock	RfidLockOperationEnumeration (see chapter 9.7.9 on page 163)	Specification of how the memory area is to be locked.
Offset	UInt32	Is ignored.
Length	UInt32	Is ignored.

Return parameter

Name	Data Type	Description
Status	AutoidOperationStatusEnumeration (see chapter 9.7.2 on page 161)	Returns the result of the operation.

KillTag

This method permanently disables a specific tag and locks it from any use. The deactivation cannot be undone.

To execute the kill command, a kill password must first be set and written to the data carrier (*SetTagPassword()* method, see page 155).

Call parameter

Name	Data Type	Description
Identifier	ScanData (see chapter 9.7.14 on page 164)	EPC of the tag to be disabled.
CodeType	CodeTypeDataType (see chapter 9.7.4 on page 162)	Specifies the type for the <i>IDENTIFIED</i> parameter.
Password	ByteString	Password of the kill operation.

Return parameter

Name	Data Type	Description
Status	AutoidOperationStatusEnumeration (see chapter 9.7.2 on page 161)	Returns the result of the operation.

9.5.3 Methods for scan settings

SetAntennaUsed

This method can be used to select one or more antennas to be active in this session.

Min. Access Level: User

Default values: Parameter 0012_{hex} (see chapter 7.3 on page 49)

Input parameter

Name	Data Type	Description
AntennaUsed	BalluffAntennaUsed	Selection of antennas to be used in this session.

Output parameter

Name	Data Type	Description
Status	AutoldOperationStatusEnumeration (see chapter 9.7.2 on page 161)	Returns the result of the operation.

GetAntennaUsed

The method provides information about which antennas are active in the current session.

Output parameter

Name	Data Type	Description
AntennaUsed	BalluffAntennaUsed	Indicates which antennas are active in this session.
Result	AutoldOperationStatusEnumeration (see chapter 9.7.2 on page 161)	Returns the result of the operation.

SetAsynchFilter

This method can be used to set the loop filter for the corresponding session. The filter can be used to correct false readings and to combine multiple scans into one list (see *Loop filter* on page 25).

Min. Access Level: Expert

Default values: Parameters 0023_{hex}, 0024_{hex} and 0029_{hex} (see chapter 7.3 on page 49)

Call parameter

Name	Data Type	Description
NumberOfReadsToDetectTag	UInt16	Specifies how many times a tag must be successfully read before it is actually reported as detected.
NumberOfReadsToRemoveTag	UInt16	Specifies how many times a tag must be no longer detected before it is actually reported as no longer present.
TimeBetweenRemoveAndDetect	UInt16	The time between <i>tag no longer detected</i> and <i>tag detected again</i> . This means that at least this time must elapse before a tag may be reported as detected again.
UseAsDefault	Boolean	If this value is set to <i>TRUE</i> , the set filters are taken as default values.

Return parameter

Name	Data Type	Description
Result	AutoldOperationStatusEnumeration (see chapter 9.7.2 on page 161)	Returns the result of the operation.

GetAsynchFilter

This method provides the active settings of the loop filter (see *Loop filter* on page 25).

Return parameter

Name	Data Type	Description
NumberOfReadsToDetectTag	UInt16	Specifies how many times a tag must be successfully read before it is actually reported as detected.
NumberOfReadsToRemoveTag	UInt16	Specifies how many times a tag must be no longer detected before it is actually reported as no longer present.
TimeBetween-RemoveAnd-Detect	UInt16	The time between <i>tag no longer detected</i> and <i>tag detected again</i> . This means that at least this time must elapse before a tag may be reported as detected again.
Result	AutoldOperationStatusEnumeration (see chapter 9.7.2 on page 161)	Returns the result of the operation.

SetCodeType

This method can be used to set the output format of the EPC. This setting is session-related and is taken into account by the following methods:

- *GetLastScanData()* (see page 146)
- *Scan()* (see page 141)
- *Events* (see page 165)

Min. Access Level: User

Default values: 0

Call parameter

Name	Data Type	Description
CodeType	UInt32	Sets the type of the Autold identifier. Possible values are: 0, 1, 2 or 3. 0: "RAW:BYTES" 1: "RAW:STRING" 2: "EPC" (see chapter 9.7.15 on page 164) 3: "UID"

Return parameter

Name	Data Type	Description
Result	AutoldOperationStatusEnumeration (see chapter 9.7.2 on page 161)	Returns the result of the operation.

GetCodeType

This method returns the current output format of the EPC. This setting is session-related and is taken into account by the following methods:

- *GetLastScanData()* (see page 146)
- *Scan()* (see page 141)
- *Events* (see page 165)

Return parameter

Name	Data Type	Description
CodeType	UInt32	Returns the type of the EPC.
Result	AutoldOperationStatusEnumeration (see chapter 9.7.2 on page 161)	Returns the result of the operation.

SetFilter

This method can be used to set a filter for certain parts of the EPC and the TID. Furthermore, the minimum and maximum values of the RSSI to be achieved and the EPC length can be set.

In synchronous scanning mode, only the data carriers whose data match the settings of the filter are displayed after the filter is activated. An example of the application can be found on page 226.

Min. Access Level: Expert

Default value: The default value is set via the device parameterization (see chapter 7.3 on page 49).

Call parameter

Name	Data Type	Description
FilterIndex	UInt16	Index of the newly created filter.
FilterOperation	BalluffFilterOperationEnumeration (see chapter 9.7.3 on page 162)	Operation with which the filter is to be applied to the data. Currently only <i>AND</i> is supported.
EpcDataFilter	BalluffFilterDataBlock	EPC filter setting: From which address, on how many bits and with which data the filter should be applied. These filter specifications refer only to the EPCs of the tags.
TidDataFilter	BalluffFilterDataBlock	TID filter setting: From which address, on how many bits and with which data the filter should be applied. These filter specifications refer only to the TIDs of the tags.
MinRSSI	Int16	Minimum RSSI value with which a tag must be detected. Value range: -128...+127 Default value: -128 (no filtering)
MaxRSSI	Int16	Maximum RSSI value with which a tag may be detected. Value range: -128...+127 Default: +127 (no filtering)

Name	Data Type	Description
MinEpcLength	UInt16	Minimum EPC length of a tag in bytes. Value range 0...62 Default: 0 (no filtering)
MaxEpcLength	UInt16	Maximum EPC length of a tag in bytes. Value range 0...62 Default: 62 (no filtering)
UseAsDefault	Boolean	If this value is set to <i>TRUE</i> , the set filters are taken as default values. This requires a prior login with admin rights.

Return parameter

Name	Data Type	Description
Result	AutoldOperationStatusEnumeration (see chapter 9.7.2 on page 161)	Returns the result of the operation.

GetFilter

This method returns the settings for the active filter. The method is session-related.

Call parameter

Name	Data Type	Description
Index	UInt16	Index of the filter whose values are to be output.

Return parameter

Name	Data Type	Description
EpcDataFilter	BalluffFilterDataBlock	Returns the start address, length and data of the filter which is applied to the EPCs.
TidDataFilter	BalluffFilterDataBlock	Returns the start address, length and data of the filter which is applied to the TIDs.
MinRSSI	Int16	Minimum RSSI value with which a tag must be detected.
MaxRSSI	Int16	Maximum RSSI value with which a tag may be detected.
MinEpcLength	UInt16	Minimum EPC length of a tag in bytes.
MaxEpcLength	UInt16	Maximum EPC length of a tag in bytes.
Result	AutoldOperationStatusEnumeration (see chapter 9.7.2 on page 161)	Returns the result of the operation.

SetMultipleTagDataHeader

This method can be used to edit and specify the strings that can be prepended or appended to the tag list of *ReadMultipleTagDataFormatted()* (see page 145) (see *Prefix for ReadMultipleTagDataFormatted (default)* in chapter 7.3 on page 80).

Min. Access Level: Admin

Default values: Prefix: Parameter 0026_{hex} (see *Prefix for ReadMultipleTagDataFormatted (default)* in chapter 7.3 on page 80)

Suffix: Parameter 0027_{hex} (see *Suffix for ReadMultipleTagDataFormatted (default)* in chapter 7.3 on page 80)

Call parameter

Name	Data Type	Description
Prefix	String	String which will be prepended to the tag list.
Suffix	String	String which will be appended to the tag list.
UseAsDefault	Boolean	If this value is set to <i>TRUE</i> , the set strings are taken as default values.

Return parameter

Name	Data Type	Description
Result	AutoldOperationStatusEnumeration (see chapter 9.7.2 on page 161)	Returns the result of the operation.

GetMultipleTagDataHeader

This method returns the strings that will be prepended or appended to the tag list. This tag list is returned when calling the *ReadMultipleTagDataFormatted()* method (see page 145).

Return parameter

Name	Data Type	Description
Prefix	String	String which will be prepended to the tag list.
Suffix	String	String which will be appended to the tag list.
Result	AutoldOperationStatusEnumeration (see chapter 9.7.2 on page 161)	Returns the result of the operation.

SetRFPower

This method can be used to set the transmitting power of a specific antenna for the current session. The unit of the transmitting power is 1/100 dBm. The set power affects the maximum range of the detection range of the antenna. The maximum permissible transmitting power depends on the antenna used and the radio regulations applicable in the respective country. Detailed information can be found in chapter 5 on page 18 and in the data sheet of the antenna used.

Min. Access Level: User

Default values: Parameter 0008_{hex} (see *Transmitting power on read (default)* in chapter 7.3 on page 58)

Input parameter

Name	Data Type	Description
Antenna	BalluffAntenna-Enumeration	Selection of the antenna whose transmitting power is to be adjusted.
Power	UInt16	Transmitting power to be set in 1/100 dBm.

Output parameter

Name	Data Type	Description
Result	AutoldOperationStatusEnumeration (see chapter 9.7.2 on page 161)	Returns the result of the operation.

GetRFPower

The method returns the transmitting power of the selected antenna set for this session in 1/100 dBm.

Input parameter

Name	Data Type	Description
Antenna	BalluffAntenna-Enumeration	Selection of the antenna whose transmitting power is to be output.

Output parameter

Name	Data Type	Description
Power	UInt16	Transmitting power for the selected antenna in 1/100 dBm.
Result	AutoldOperationStatusEnumeration (see chapter 9.7.2 on page 161)	Returns the result of the operation.

SetTagDataFormat

This method can be used to specify the format string used to format the data of individual tags in the *ReadMultipleTagDataFormatted()* (see page 145) and *ReadFormattedTagData()* (see page 144) methods. With the *WriteTagDataFormatted()* method (see page 144) the data to be written must correspond to the set format.

A detailed description of the application and the different possibilities can be found in chapter 8.11 on page 121.

Min. Access Level: Admin

Default values: Parameter 0025_{hex} (see *Format definition for ReadTagDataFormatted, ReadMultipleTagDataFormatted and WriteFormattedTagData (default)* in chapter 7.3 on page 79)

Input parameter

Name	Data Type	Description
FormatString	String	Format for the data to be formatted.
UseAsDefault	Boolean	If this value is set to <i>TRUE</i> , the set format is taken as the default value.
Result	AutoldOperationStatusEnumeration (see chapter 9.7.2 on page 161)	Returns the result of the operation.

GetTagDataFormat

This method returns the format string used to format the data of individual tags in the *ReadMultipleTagDataFormatted()* (see page 145) and *ReadFormattedTagData()* (see page 144) methods.

Return parameter

Name	Data Type	Description
FormatString	String	Format in which the tag data is formatted.
Result	AutoldOperationStatusEnumeration (see chapter 9.7.2 on page 161)	Returns the result of the operation.

SetTagSignatureFormat

The tag data can be automatically provided with a signature. Different tag data can be included in the generation of this signature as desired. The signature can be used to verify the integrity and authenticity of the data. This method can be used to enable or disable the generation and verification of the signature. The data to be included in the signature generation can also be specified. A detailed description of the application can be found in chapter 3.7 on page 12.

An example of this function is explained on page 168.

Min. Access Level: Admin

Default values: Parameter 0028_{hex} (see *Calculation format for signature generation (default)* in chapter 7.3 on page 80)

Call parameter

Name	Data Type	Description
Type	BalluffSignatureTypeEnumeration	0: None 1: Basic256Sha256
FormatString	String	Specification of data to be included for signature generation.
UseAsDefault	Boolean	If this value is set to true, the signature settings are taken as default values.

Return parameter

Name	Data Type	Description
Result	AutoldOperationStatusEnumeration (see chapter 9.7.2 on page 161)	Returns the result of the operation.

GetTagSignatureFormat

This method returns the current signature setting. If signature generation is active, the tag data used to generate the signature is also specified.

Return parameter

Name	Data Type	Description
Type	BalluffSignatureTypeEnumeration	0: None 1: Basic256Sha256
FormatString	String	Data that is used for signature generation.
Result	AutoldOperationStatusEnumeration (see chapter 9.7.2 on page 161)	Returns the result of the operation.

SetTagPassword

This method can be used to write the *access* and *kill* passwords of the data carrier. The passwords have a length of 4 bytes each (MSB first).
 For the kill command (p.197), a kill password different from 0 must have been written on the tag beforehand.

Call parameter

Name	Data Type	Description
Identifier	ScanData (see chapter 9.7.14 on page 164)	EPC of the tag.
CodeType	CodeTypeData-Type (see chapter 9.7.4 on page 162)	Specifies the type for the <i>Identifier</i> parameter.
PasswordType	RfidPassword-TypeEnumeration (see chapter 9.7.11 on page 163)	Specifies which password is to be changed. The <i>Read</i> and <i>Write</i> values are not supported on UHF devices such as the BIS U.6127 because they are not defined in the UHF EPC Gen2 V1 specification.
AccessPassword	ByteString	The current 4 byte access password of the tag.
NewPassword	ByteString	The new 4-byte-long password.

Return parameter

Name	Data Type	Description
Status	AutoldOperationStatusEnumeration (see chapter 9.7.2 on page 161)	Returns the result of the operation.

SetTIDLength

This method can be used to set the length of the TID memory area to be used for all data carriers of a particular antenna. The method is session-related.

Min. Access Level: Expert

Default values: Parameter 0004_{HEX} (see chapter 7.3 on page 49)

Input parameter

Name	Data Type	Description
Antenna	BalluffAntenna-Enumeration	Antenna where the TID length should apply to all tags.
TIDLength	Byte	Desired TID length in 2-byte words to be set. Maximum allowed length: 31 words (62 bytes)

Output parameter

Name	Data Type	Description
Result	AutoldOperationStatusEnumeration (see chapter 9.7.2 on page 161)	Returns the result of the operation.

GetTIDLength

This method returns the selected length of the TID memory area for all tags of a given antenna. The method is session-related

Input parameter

Name	Data Type	Description
Antenna	BalluffAntenna-Enumeration	Antenna for which the set TID length is to be returned.

Output parameter

Name	Data Type	Description
TIDLength	Byte	Length of the TID memory area in 2-byte words.
Result	AutoldOperationStatusEnumeration (see chapter 9.7.2 on page 161)	Returns the result of the operation.

9.6 Variables and constants

9.6.1 Device information/settings

AntennaName

Data Type	AntennaNameIdPair (see page 161)
Default value	Depending on the antenna "Antenna_1", "Antenna_2", "Antenna_3" or "Antenna_4"
Access rights	Read: User Write: Admin
007-Parameter	–
Parent	Balluff extension: AutoldDeviceType/ RuntimeParameters
Path	Root/DeviceSet/BIS_U_6127_Rfid_ Provider/RuntimeParametersGlobal/ BalluffRfidRuntimeParametersAn- tenna[1..4]

Returns the ID and the name of the corresponding antenna. The data correspond to the values of the (also global) *AntennaNames* array (see *AntennaNames* on page 156).

AntennaNames

Data Type	AntennaNameIdPair[4]
Default value	1, "Antenna_1", 2, "Antenna_2", 3, "Antenna_3", 4, "Antenna_4"
Access rights	Read: User Write: Admin
007-Parameter	–
Parent	RfidReaderDeviceType
Path	Root/DeviceSet/BIS_U_6127_Rfid_ Provider/

An array with four entries of the type *AntennaNameIdPair* (see page 161). Each entry contains the name and ID of an antenna. The values are reflected in the *AntennaName* variables of the individual antennas.

Data Type	String
Default value	1.00
Access rights	Read: User Write: –
007-Parameter	–
Parent	AutoldDeviceType
Path	Root/DeviceSet/BIS_U_6127_Rfid_ Provider/

This variable returns the version of the OPC UA Autold Spec. The version of specification used is 1.00.

DeviceInfo

Data Type	String
Default value	""
Access rights	Read: User Write: –
007-Parameter	–
Parent	AutoldDeviceType
Path	Root/DeviceSet/BIS_U_6127_Rfid_ Provider/

This variable currently has no meaning.

DeviceLocation

Data Type	Location (see page 162)
Default value	""
Access rights	Read: User Write: Admin
007-Parameter	001f _{hex}
Parent	AutoldDeviceType
Path	Root/DeviceSet/BIS_U_6127_Rfid_ Provider/

This variable sets or returns the device location. Only the *NAME* type is supported. This value corresponds to the *DeviceLocationName* variable (see page 156) and the return value of the *GetDeviceLocation()* method (see page 140).

DeviceLocationName

Data Type	String
Default value	""
Access rights	Read: User Write: Admin
007-Parameter	001f _{hex}
Parent	AutoldDeviceType
Path	Root/DeviceSet/BIS_U_6127_Rfid_ Provider/

This variable sets or returns the device location. The value corresponds to the *NAME* field in *DeviceLocation* (see page 156) and the return value of the *GetDeviceLocation()* METHOD (see page 140).

DeviceManual

Data Type	String
Default value	www.balluff.com
Access rights	Read: User Write: –
007-Parameter	–
Parent	AutoldDeviceType
Path	Root/DeviceSet/BIS_U_6127_Rfid_Provider/

This variable returns the link of the Balluff Homepage.

DeviceStatus

Data Type	DeviceStatusEnumeration (see page 162)
Default value	0: Idle
Access rights	Read: User Write: –
007-Parameter	–
Parent	AutoldDeviceType
Path	Root/DeviceSet/BIS_U_6127_Rfid_Provider/

The *DeviceStatus* returns the current status of the device. Normally this is *Idle*. If synchronous scanning mode operation is activated by an OPC-UA session with *ScanStart()*, the status changes to *Scanning*.

DeviceRevision

Data Type	String
Default value	–
Access rights	Read: User Write: –
007-Parameter	–
Parent	AutoldDeviceType
Path	Root/DeviceSet/BIS_U_6127_Rfid_Provider/

This variable provides both the hardware and software version of the device. The values correspond to *HardwareRevision* (see page 157) and *SoftwareRevision* (see page 158).

HardwareRevision

Data Type	String
Default value	–
Access rights	Read: User Write: –
007-Parameter	800e _{hex}
Parent	AutoldDeviceType
Path	Root/DeviceSet/BIS_U_6127_Rfid_Provider/

This variable specifies the hardware revision in the form of a string. It also corresponds to the hardware part of the variable *DeviceRevision* (see page 157).

Manufacturer

Data Type	String
Default value	Balluff GmbH
Access rights	Read: User Write: –
007-Parameter	–
Parent	AutoldDeviceType
Path	Root/DeviceSet/BIS_U_6127_Rfid_Provider/

This variable returns the name of the device manufacturer.

Model

Data Type	String
Default value	BIS U-6127-081-104-06-ST36
Access rights	Read: User Write: –
007-Parameter	800f _{hex}
Parent	AutoldDeviceType
Path	Root/DeviceSet/BIS_U_6127_Rfid_Provider/

This variable returns the name of the device model.

SerialNumber

Data Type	String
Default value	–
Access rights	Read: User Write: –
007-Parameter	8001 _{hex}
Parent	AutoldDeviceType
Path	Root/DeviceSet/BIS_U_6127_Rfid_Provider/

This variable specifies the serial number of the device.

SoftwareRevision

Data Type	String
Default value	–
Access rights	Read: User Write: –
007-Parameter	–
Parent	AutoldDeviceType
Path	Root/DeviceSet/BIS_U_6127_Rfid_ Provider/

This variable specifies the software version in the form of a string. It corresponds to the software part of the variable *DeviceRevision* (see page 157).

RevisionCounter

The variable currently has no meaning and always returns the value 0.

9.6.2 Scan settings

AntennaActive

Data Type	Boolean
Default value	007-Parameter 0012 _{hex}
Access rights	Read: User Write: Admin
007-Parameter	00012 _{hex}
Parent	Balluff extension: AutoldDeviceType/ RuntimeParameters
Path	Root/DeviceSet/BIS_U_6127_Rfid_ Provider/RuntimeParametersGlobal/ BalluffRfidRuntimeParametersAn- tenna[1..4]

This variable can be used to activate or deactivate the corresponding antenna globally, i.e. for all applications. This setting corresponds to parameter 0012_{hex} (see chapter 7.3 on page 49). Admin authorization is required.

AutoIncrementSendPower

Data Type	Byte
Default value	–
Access rights	Read: User Write: User
007-Parameter	0009 _{hex}
Parent	Balluff extension: AutoldDeviceType/ RuntimeParameters
Path	Root/DeviceSet/BIS_U_6127_Rfid_ Provider/RuntimeParametersGlobal/ BalluffRfidRuntimeParametersAn- tenna[1..4]

This variable specifies the automatic increase of the write power for all applications of the selected antenna.

BufferLenReadFormatted

Data Type	UInt32
Default value	500
Access rights	Read: User Write: User
007-Parameter	–
Parent	Balluff extension: AutoldDeviceType/ RuntimeParameters
Path	Root/DeviceSet/BIS_U_6127_Rfid_ Provider/RuntimeParametersGlobal/ BalluffRfidRuntimeParametersCom- mon

This variable determines how large (in bytes) the output buffer per data carrier is for the methods *ReadFormattedTagData()* (see page 144) and *ReadMultipleTagDataFormatted()* (see page 145).

CodeTypes

Data Type	UInt32[]
Default value	0
Access rights	Read: User Write: Admin
007-Parameter	–
Parent	AutoldDeviceType/RuntimeParameters
Path	Root/DeviceSet/BIS_U_6127_Rfid_ Provider/RuntimeParametersGlobal/ BalluffRfidRuntimeParametersCom- mon

This variable specifies which formats are supported for the EPC and is used to select the desired format. The following formats are supported:

RAW:BYTES	EPC binary
RAW:STRING	EPC ASCII
EPC	EPC structure (see chapter 9.7.15 on page 164)
UID	AutoID identifier according to ISO/IEC 18000-3 Mode 3, ISO/IEC 18000-63 and GS1 EPCglobal™

LastScanData

Data Type	ByteString
Default value	""
Access rights	Read: User Write: –
007-Parameter	–
Parent	AutoldDeviceType
Path	Root/DeviceSet/BIS_U_6127_Rfid_Provider/

This variable returns the data of the last detected data carrier. It is shared by all OPC UA sessions.

MinRSSI

Data Type	Int32
Default value	–128 (parameter 002f _{hex})
Access rights	Read: User Write: User
007-Parameter	–
Parent	AutoldDeviceType/RuntimeParameters
Path	Root/DeviceSet/BIS_U_6127_Rfid_Provider/RuntimeParametersGlobal/BalluffRfidRuntimeParametersAntenna[1..4]

Each tag at the corresponding antenna must be detected with at least this RSSI value to be reported as detected. In OPC UA, this value is reflected in the filters (see *SetFilter* on page 150).

The RSSI (Received Signal Strength Indicator) is a value that reflects the signal quality of a received data carrier response. Conclusions can only be drawn to a limited extent about the distance of the data carrier from the antenna.

RFPower

Data Type	SByte
Default value	0
Access rights	Read: User Write: Admin
007-Parameter	0x0008 / 4
Parent	AutoldDeviceType/RuntimeParameters
Path	Root/DeviceSet/BIS_U_6127_Rfid_Provider/RuntimeParametersGlobal/BalluffRfidRuntimeParametersAntenna[1..4]

This value specifies the transmitting power of the corresponding antenna in dBm. Only integer values are possible here. Finer settings can also be made via the web interface or the UHF Manager. The transmitting power influences the maximum range of the detection range of the antenna.

TagTypes

Data Type	UInt32[]
Default value	"EPC Class 1 Gen2 V1", "ISO 18000-63"
Access rights	Read: User Write: –
007-Parameter	–
Parent	AutoldDeviceType/RuntimeParameters
Path	Root/DeviceSet/BIS_U_6127_Rfid_Provider/RuntimeParametersGlobal/BalluffRfidRuntimeParametersAntenna[1..4]

This array returns the tag types supported by the system.

UserLed

Data Type	BalluffUserLedEnumeration
Default value	0 = off
Access rights	Read: User Write: User
007-Parameter	–
Parent	Balluff extension: AutoldDeviceType/RuntimeParameters
Path	Root/DeviceSet/BIS_U_6127_Rfid_Provider/RuntimeParametersGlobal/BalluffRfidRuntimeParametersCommon

This variable can be used to control the LED of the device.

The following values are possible:

- 0: Led off
- 1: Led lights up red
- 2: Led lights up yellow
- 3: Led lights up green

9.7 Data types

In the following subchapters, the data types of Structure, Enumeration and Union are used primarily.

With the help of a structure, several elements of any data type can be combined into one data object. Both the structure as a whole and the individual elements can be addressed.

A union also combines several elements, but only one of them can be used at a time. Since all elements can use the same memory space, the size of the memory space depends on the requirements of the largest union element.

An enumeration is a type of list. Each element is specified by a unique name and automatically assigned a number. The first element usually gets the number 0. For example, a variable of the enumeration type *Color* can take the values red, green or blue.

9.7.1 AntennaNameIdPair

This data type is a structure that assigns a readable name to an RFID antenna ID. It is used with the variables *AntennaNames* (see page 156) and *AntennaName* (see page 156).

Value	Data Type	Description
AntennaNameIdPair	Structure	
AntennaId	Int32	ID of antenna
AntennaName	String	Name of antenna

9.7.2 AutoldOperationStatusEnumeration

This data type is an enum that reflects the status of the RIFD commands. The following values are defined.

Code	Meaning
SUCCESS	Operation was successful.
MISC_ERROR_TOTAL	The operation could not be performed.
MISC_ERROR_PARTIAL	The operation was performed only partially.
PERMISSION_ERROR	The user rights are not sufficient.
PASSWORD_ERROR	Tag password is incorrect.
REGION_NOT_FOUND_ERROR	The memory area is not available at the addressed tag.
OP_NOT_POSSIBLE_ERROR	The operation is not supported by the addressed tag.
OUT_OF_RANGE_ERROR	The specified memory area is not allowed.
NO_IDENTIFIER	The operation cannot be performed because there is no tag in range.
MULTIPLE_IDENTIFIER	The command can only work with one tag, but several were selected or found.
READ_ERROR	An error occurred while reading the tag.
CODE_NOT_SUPPORTED	The code format is not correct or the value is invalid.
WRITE_ERROR	An error occurred while writing the tag.
NOT_SUPPORTED_BY_DEVICE	Command or parameters are not supported by the device.
NOT_SUPPORTED_BY_TAG	Command or parameters are not supported by the tag.
DEVICE_NOT_READY	The device is not (yet) ready for use, cable break or no antenna connected
INVALID_CONFIGURATION	The device setting is incorrect, e.g. no antenna active
RF_COMMUNICATION_ERROR	Communication error between the device and the tag
DEVICE_FAULT	Not currently used.
TAG_HAS_LOW_BATTERY	–

9.7.3 BalluffFilterOperationEnumeration

This data type is an enum that specifies which operation is to be used to apply the static filter to the data. However, currently only the *AND* operation is supported. The following values are defined:

Value	Description
0 (AND)	First filter or the new filter data are linked with the existing filters with AND. Currently only one filter is possible.
1 (OR)	Not yet supported in the current version.
2 (NAND)	Not yet supported in the current version.
3 (NOR)	Not yet supported in the current version.

9.7.4 CodeTypeDataTypes

This data type is a string that specifies how the detected data carrier is to be stored. The following strings or types are supported:

Value	Description
"RAW:BYTES"	EPC binary
"RAW:STRING"	EPC ascii
"EPC"	EPC structure (see chapter 9.7.15 on page 164)
"UID"	AutoID identifier according to ISO/IEC 18000-3 Mode 3, ISO/IEC 18000-63 and GS1 EPCglobal™

9.7.5 DeviceStatusEnumeration

This data type is an enum that provides the status of the device.

Value	Description
0	Idle: Normal status
1	Error: Device error
2	Scanning: Start of asynchronous scanning mode (see chapter <i>ScanStart</i> on page 146)
3	Busy

9.7.6 Location

The *Location* union provides the possibility to store a piece of location information in different formats. Only the *NAME* field of type *LocationName* (device location as string) is currently supported.

The selection of which field is populated with data is usually done via a separate enumeration variable of type *LocationTypeEnumeration* (see page 162).

Name	Data Type	Description
Location	Union	
NMEA	NmeaCoordinateString	Not supported.
Local	LocalCoordinate	Not supported.
WGS84	WGS84Coordinate	Not supported.
Name	LocationName	Device location as string (<i>LocationName</i> see page 162).

9.7.7 LocationName

This data type is a string that reflects the device location.

9.7.8 LocationTypeEnumeration

This enum returns the selection for the data type of the union *Location* (see page 162). This is used for example in the *GetDeviceLocation()* method (see page 140).

Value	Description
NMEA_0	Not currently supported.
LOCAL_2	Not currently supported.
WGS84_4	Not currently supported
NAME_5	String indicating the device location.

9.7.9 RfidLockOperationEnumeration

This data type defines the action to be executed in the Lock command. The following values are defined and allowed. The exact effect of the respective action depends on the selected memory area of the tag.
 A more detailed description can be found in the standards according to EPCglobal™ Class1 Generation2 and OPC UA AutoID Companion Specification 1.0.

Value	Description	
	Passwords	Memory bank
Lock_0	Write and read commands to the password are only possible with a valid access password.	It can be read without a password, but written only with a valid access password.
Unlock_1	Write and read commands to the password are possible without knowing the access password.	Both the read and write operation can be performed without a password.
Permanent-Lock_2	Write and read commands to the password are no longer possible at all. The operation is not reversible.	It can be read without a password, but written only with a valid access password. The operation is not reversible.
PermanentUnlock_3	Read and write commands to the password are possible, but the area can no longer be locked.	Both the write and read operation can be performed without a password. However, the area can no longer be locked.

9.7.10 RfidLockRegionEnumeration

This data type defines the memory area to be locked with the *LockTag()* method (see page 147). The following values are defined:

Value	Description
Kill_0	Kill password
Access_1	Access password
EPC_2	UID/EPC bank (bank 01)
TID_3	TID bank (bank 10)
User_4	User memory bank (bank 11)

9.7.11 RfidPasswordTypeEnumeration

This data type specifies which password should be changed (method: *SetTagPassword()* see chapter *SetTagPassword* on page 155). The following values are defined:

Value	Description
Access_0	Access password
Kill_1	Kill password
Read_2	Read password
Write_3	Write password

The Read_2 and Write_2 values are defined but not permitted. They are not implemented in the standard according to EPCglobal™ Class-1 Gen-2 V1.

9.7.12 RfidScanResult

This structure returns the data of a detected tag and additional information in the array of type *Sightings*. It is structured as follows.

Name	Data Type	Description
RfidScanResult	Structure	
CodeType	CodeTypeData-Type (see page 162)	Specifies the format in which the scanned data should be output under Scan-Data.
ScanData	ScanData	Data of the successfully scanned tag.
Timestamp	UtcTime	UtcTime on read.
Location	Location	Returns the location where the tag was detected.
Sightings	RfidSighting[] (see page 164)	Information about each read of the tag on an antenna: 1: Number of the antenna 2: RSSI value 3: UtcTime at read 4: Transmitting power used during read

9.7.13 RfidSighting

This structure provides additional information from the detection of a tag at a particular antenna. The structure is as follows.

Name	Data Type	Description
RfidSighting	Structure	
Antennald	Int32	Specifies the ID of the antenna where the tag was detected.
Strength	Int32	Specifies the RSSI value with which the tag was detected.
Timestamp	UtcTime	Time stamp
CurrentPower-Level	Int32	Returns the set transmitting power of the antenna.

9.7.14 ScanData

This union offers the possibility to save the scanned EPCs in different data formats. The selection of the data format is done indirectly via a separate enumeration variable of the type *CodeTypeDataType* (see page 162), which defines the format and the meaning.

Name	Data Type	Description
ScanData	Union	
ByteString	ByteString	Detected data in RAW format.
String	String	Detected data as a string.
Epc	ScanDataEpc (see page 164)	Detected data in the <i>ScanDataEpc</i> structure
Custom	BaseDataType	Manufacturer-specific data structure.

9.7.15 ScanDataEpc

This data type is a structure that offers the possibility to present the contents of the EPC bank in a structured way. It is used as a representation of the *ScanData* union and is thus used for scan results. The *CodeTypeDataType* EPC belongs to this data type (see page 162). The structure is composed as follows:

Name	Data Type	Description
ScanDataEpc	Structure	
PC	UInt16	Protocol control information according to ISO/IEC 18000-3 Mode 3, ISO/IEC 18000-63 and GS1 EPCglobal™
UId	ByteString	AutoID identifier according to ISO/IEC 18000-3 Mode 3, ISO/IEC 18000-63 and GS1 EPC-global™
XPC_W1	UInt16	Extended protocol control word 1 according to ISO/IEC 18000-3 Mode 3, ISO/IEC 18000-63 and GS1 EPCglobal™
XPC_W2	UInt16	Extended protocol control word 2 according to ISO/IEC 18000-3 Mode 3, ISO/IEC 18000-63 and GS1 EPCglobal™

9.7.16 ScanSettings

This structure defines the settings for the *Scan()* (see page 141) and *ScanStart()* (see page 146) methods. Three parameters can be used to specify how long the scan should last. The three conditions of *DURATION*, *CYCLES* and *DATAAVAILABLE* are related to each other. As soon as a condition is fulfilled, the scan operation is terminated. The structure is composed as follows:

Name	Data Type	Description
ScanSetting	Structure	
Duration	Duration	Specifies the duration of the scan process in milliseconds. The value 0 stands for <i>infinite length</i> .
Cycles	Int32	Specifies the number of scan passes. The value 0 stands for <i>infinite number</i> .
DataAvailable	Boolean	If this value is set to <i>TRUE</i> , the scan will stop as soon as data is available. With <i>FALSE</i> , only the parameters <i>Duration</i> and <i>Cycles</i> are considered.
LocationType	LocationType (see chapter 9.7.8 on page 162)	Specifies the desired type of location information in the result. Only the <i>Location-Name</i> type is supported.

9.8 Events

In this system, events of the type *RfidScanEventTyp* are used. They are used as soon as the asynchronous scanning mode (see page 146) is started from any OPC-UA session. For each detected tag, an *RFIDSCANEVENTTYP* event is generated. This event provides information about the detection as well as about the tag itself.

All sessions that have registered with the event will also have this delivered.

No event is generated for a tag that is no longer detected, since this is not defined in the AutoID Spec.

The *RfidScanEventTyp* event, which is derived from the generic *AutoldScanEventType*, contains the following data fields:

RfidScanEventType

Name	Data Type	Description
ScanResult	RfidScanResult[]	All detected tags are output with information such as EPC, timestamp, RSSI value, etc.
DeviceName	String	String with device name

Data types used

RfidScanResult

Name	Data Type	Description
CodeType	CodeTypeData (see page 162)	Specifies the format in which the scanned data should be output under <i>Scan-Data</i> .
ScanData	ScanData	Data of the successfully scanned tag.
Timestamp	UtcTime	UtcTime on read.
Location	Location	Returns the location where the tag was detected.
Sightings	RfidSighting[] (see page 164)	Information about each read of the tag on an antenna: 1: Number of the antenna 2: RSSI value 3: UtcTime at read 4: Transmitting power used during read

9.9 Examples

Various examples are shown in the following subchapters. In the examples, UaExpert is used as a client that must be installed on the PC (download at www.unified-automation.com).

9.9.1 Connection setup

See section 9.3 *Connection established via OPC UA with UaExpert* on page 135.

9.9.2 Reading and writing variables

As soon as the BIS U-6127 processor unit is connected to the UaExpert client, the objects are displayed in the *ADDRESS SPACE* window.

There are two ways to read variables (represented by an icon in the *ADDRESS SPACE*):

- ▶ Click on the desired variable in the *ADDRESS SPACE* window (in Fig. 9-18 the *DEVICENAME* variable was clicked on by way of example).
 - ⇒ In the *ATTRIBUTES* window, all information about the variables is displayed. As you can see in the figure, the current value of the variables can be seen under *VALUE – VALUE* (highlighted in blue). In this case, it would be *BISU-6127*.

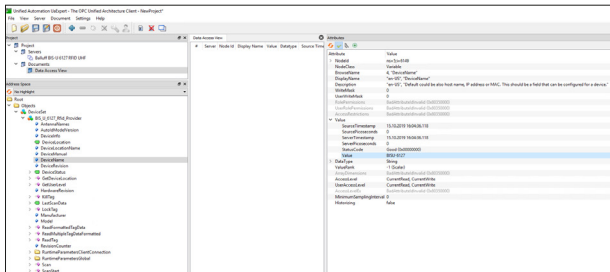


Fig. 9-18: Display of a variable in the *Attributes* window

- ▶ Drag and drop the desired variable into the *DATA ACCESS VIEW* window.
 - ⇒ As soon as the variable is in this window, further information is displayed (see Fig. 9-19). You can find the current value of the variables in the *VALUE* column.

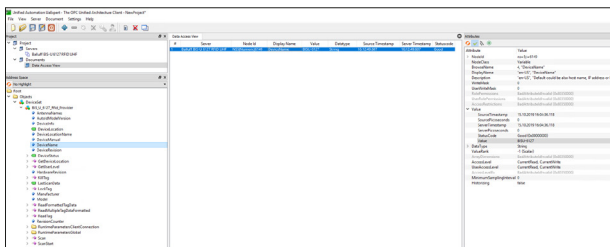


Fig. 9-19: Presentation of a variable in *DATA ACCESS VIEW*

9.9.3 Method calls

The methods are displayed in the *ADDRESS SPACE* window with violet icons. Right-clicking on a method opens a small window. The following figure shows this process using the *GetRFPower* method as an example.

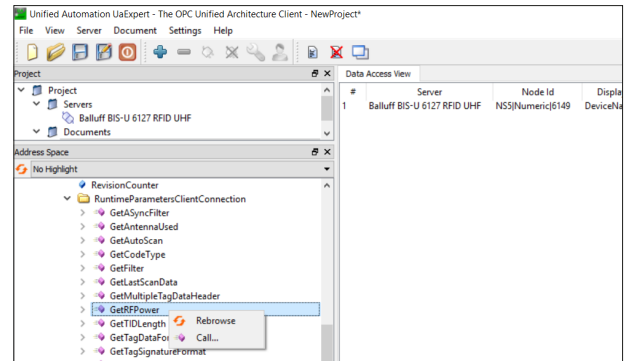


Fig. 9-20: Right-click on method

Run method

1. Click *CALL* method in the context menu.
 - ⇒ A window opens again showing the call arguments and the return parameters of the corresponding method (*GetRFPower()*, see Fig. 9-21).

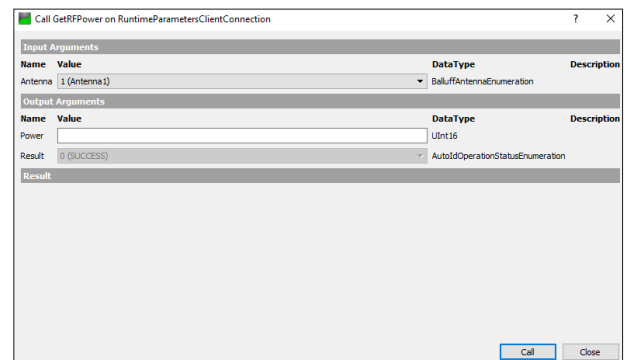


Fig. 9-21: *GetRFPower()* method call

2. Enter input parameters and confirm with *CALL*.
 - ⇒ The method is executed and the result appears in the return parameters (current example, see Fig. 9-22).

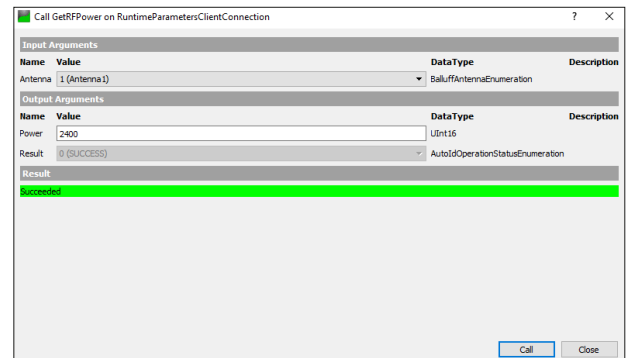


Fig. 9-22: *GetRFPower()* method result

The data read from a tag can be formatted as desired via the *ReadFormattedTagData()* method. The format can be set via the *SetTagDataFormat()* method.

In this example, the format is *%E[0.12]%S[0.3]*.



To execute the *ReadFormattedTagData* method, the call parameters of *Identifier*, *CodeType* and *Password* are required.



In this example, the tag with the EPC “08090808080808080808080808” is to be read. The CodeType used is *RAW:BYTES*, and no password is required for the read operation. The inputs therefore look like the following:



Call ReadFormattedTagData on BIS_U_6127_Rfid_Provider

Input Arguments

Name	Value	DataType	Description
Identifier	Click "...\" to display value	ScanData	
CodeType	RAIN-BYTES	CodeTypeData	
Password	Length=4, Content=00000000	ByteString	

Output Arguments

Name	Value	DataType	Description
ReadData	Length=15, Content=0809080808080808080808080800ce4	ByteString	
Status	0 (SUCCESS)	AutodOperatorStatusEnumeration	
Result	Succeeded		

Call Close

In total, data with a length of 15 bytes was read. This corresponds to the setting of the format string. This information is output via the `LENGTH` specification in the `READDATA` parameter. The read data is then specified after `CONTENT=`.

The application is described in detail in chapter 8.11 on page 121.

9.9.5 Read Multiple Tag Data Formatted

This method can be used to output data read from multiple tags in individually formatted form. The format is set using the *SetTagDataFormat()* method. In this example, the data is to be formatted according to the format string `<EPC:%E[0..12]S:%S:[0..3]>`.

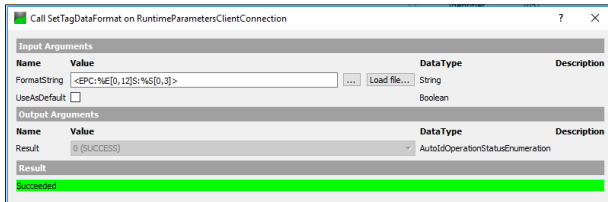


Fig. 9-27: Method *SetTagDataFormat()*

This causes the EPC with the prefix `<EPC:` and the first three bytes of the status with the prefix `S:` to be output for each detected tag. The output is terminated with `>`. The input parameters for the method are *Maxtags* and *Password*. In this case, a maximum of 5 tags should be read. An access password should not be set. The result of the scan is shown in the output parameters. If you click on the button with the three small dots, the complete data will be displayed (see Fig. 9-28).

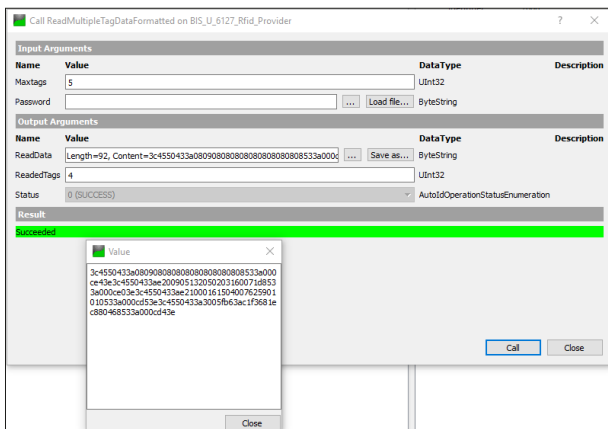


Fig. 9-28: Output parameter

In this example, a total of 68 bytes were read from 4 tags. Since the data of a tag start and end with `<` and `>`, you can now conveniently sort them (`<` corresponds to `003Chex`, `>` corresponds to `003Ehex`).

```
3c4550433a08090808080808080808533a000ce43e
3c4550433ae200905132050203160071d8533a000ce03e
3c4550433ae21000161504007625901010533a000cd53e
3c4550433a3005fb63ac1f3681ec880468533a000cd43e
```

Fig. 9-29: Tag data

This results in the following values for the four bytes:

Tag	EPC (12 bytes)	Read status	RSSI value
1st tag	08090808080808080808080808080808	0 = OK	-28
2nd tag	e200905132050203160071d8	0 = OK	-32
3rd tag	e21000161504007625901010	0 = OK	-43
4th tag	3005fb63ac1f3681ec880468	0 = OK	-44

The application is described in detail in chapter 8.11 on page 121.

9.9.6 Write Tag Data with Signature

Data to be written to a tag can be automatically signed to ensure the integrity of the data.

This example shows step-by-step how to write data with a signature to a tag. In addition, it demonstrates how to read the data and determine whether it is intact.

First, the use of the tag data signature must be enabled via the *SetTagSignatureFormat()* method. This is done by selecting the *BASIC256SHA256* signature algorithm. Additionally, it is necessary to specify the data which should be included in the signature. Usually this is the EPC and the TID of the tag. For information on the tag signature, see chapter 3.7 on page 12.

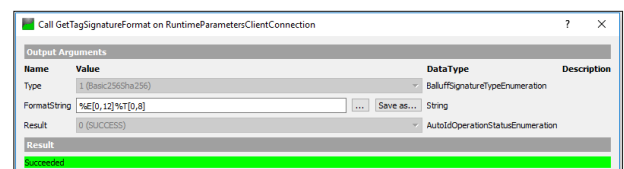


Fig. 9-30: Method *SetTagSignatureFormat()*

Any tag can now be written as usual via the *WriteTagDataFormatted()* method. To do this, the data to be written must correspond to the format string set. In this example, the format string looks like this:

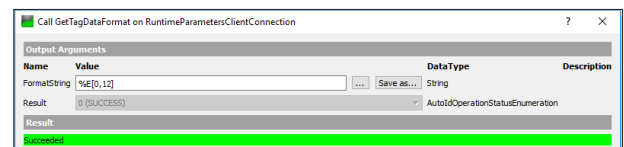


Fig. 9-31: Format string

In the example, the tag with the EPC `08090808080808080808080808080808` is to be written to. The call of the *WriteTagDataFormatted()* method is shown in Fig. 9-32.

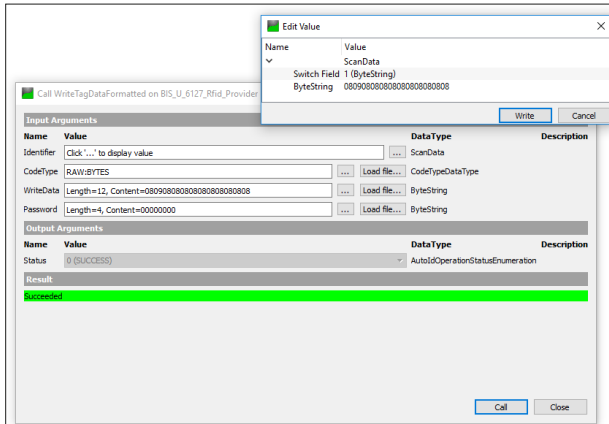


Fig. 9-32: Method WriteTagDataFormatted()

The signature is checked for all read commands that use the universal output format. The check result can be included in the output by specifying the status byte in the format string. The value 0 stands for a successful check, the value 2 means that the signature does not match the other tag data.

Fig. 9-33 shows that the signature verification was successful.

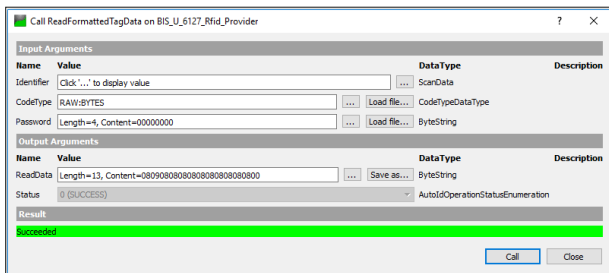


Fig. 9-33: Successful signature verification

The signature is stored in the user area. If this area is overwritten with the *WriteTag()* method, the signature verification must fail in the next read command. Fig. 9-34 shows the output with a failed signature verification.

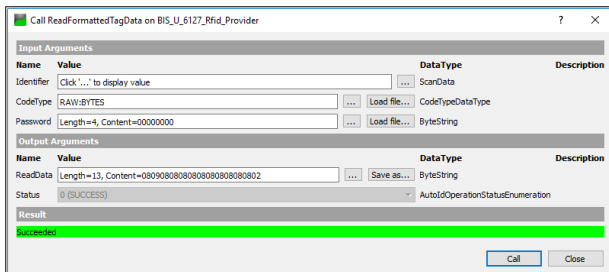


Fig. 9-34: Failed signature verification

9.9.7 Dealing with static filters

The filter for synchronous scanning mode can be set using the *SetFilter()* method.

To see the effects of the filter, a scan was first performed without the filter. As can be seen in Fig. 9-35, three tags were detected:

- 080908080808080808080808
- 3005FB63AC1F3681EC880468
- E21000161504007625901010

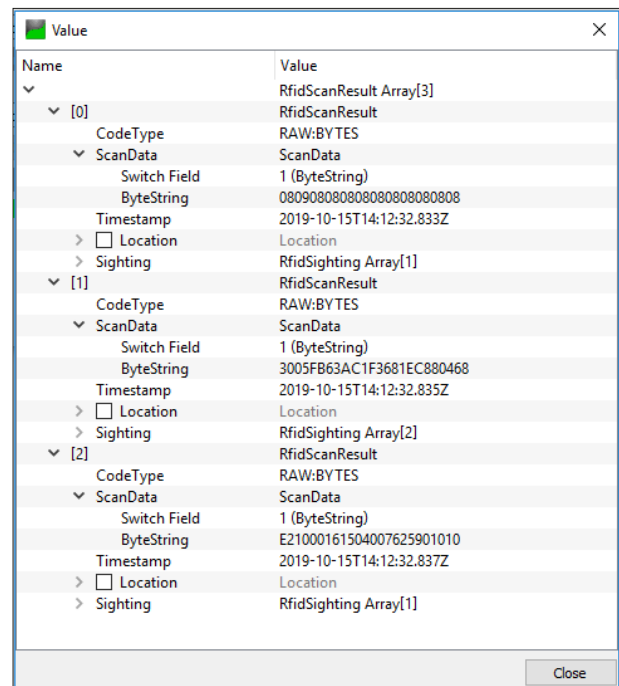


Fig. 9-35: Tag detection

For the first example, the settings that can be seen in Fig. 9-36 were set for the filter.

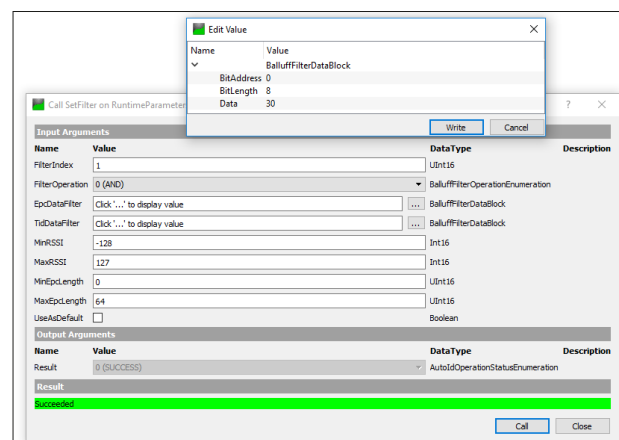


Fig. 9-36: Filter settings

This means that only tags whose EPC starts with “30” may be listed. The RSSI value and the EPC length may take any valid value.

If you now run the scan method, you get the following result (Fig. 9-37).

Name	Value
▼ [0]	RfidScanResult
CodeType	RAW:BYTES
▼ ScanData	ScanData
Switch Field	1 (ByteString)
ByteString	3005FB63AC1F3681EC880468
Timestamp	2019-10-15T15:25:50.550Z
Location	0 (Null)
Switch Field	0 (Null)
▼ Sighting	RfidSighting Array[2]
> [0]	RfidSighting
> [1]	RfidSighting

Fig. 9-37: Result of scan method

As expected, only the tag whose EPC starts with “30” is detected. All other tags are not listed.

Since the address and the length of the filter are specified in bits, you can also filter *half* bytes.

The next example shows this application. In this case, the EPCs are to be selected according to the bit address range 76...82.

- 08090808080808080808080808080808
- 3005FB63AC1F3681EC880468
- E21000161504007625901010.

The range should have the value 8080.

Name	Value	DataType	Description
Index	1	UInt16	

Name	Value	DataType	Description
EpcDataFilter	Click ... to display value	BalluffFilterDataBlock	
TidDataFilter	Click ... to display value	BalluffFilterDataBlock	
MinRSSI	-128	Int16	
MaxRSSI	127	Int16	
MinEpcLength	0	UInt16	
MaxEpcLength	64	UInt16	
Result	0 (SUCCESS)	AutoidOperationStatusEnumeration	

Result: 0 (SUCCESS)

Call GetFilter on Runtime

Fig. 9-38: Filter 8080

If you run the scan method after applying the filter, you will only get the tags whose EPC matches the filter.

Name	Value
▼ [0]	RfidScanResult
CodeType	RAW:BYTES
▼ ScanData	ScanData
Switch Field	1 (ByteString)
ByteString	08090808080808080808080808080808
Timestamp	2019-10-15T16:31:10.131Z
Location	0 (Null)
Switch Field	0 (Null)
▼ Sighting	RfidSighting Array[1]
> [0]	RfidSighting

Fig. 9-39: Filter result

9.9.8 Dealing with events

This example explains step-by-step how to use UaExpert to receive the event generated by asynchronous operation.

1. Add the *EVENT VIEW* window under *DOCUMENTS* – *ADD*.

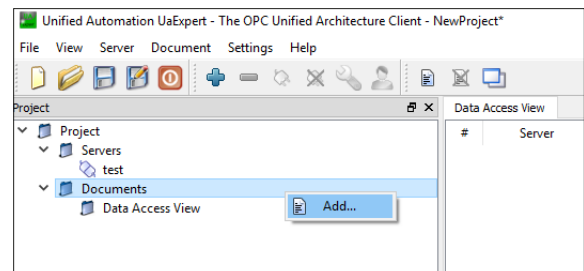


Fig. 9-40: Add Documents

2. Add the server object to the configuration by dragging and dropping to be able to register for the desired events.

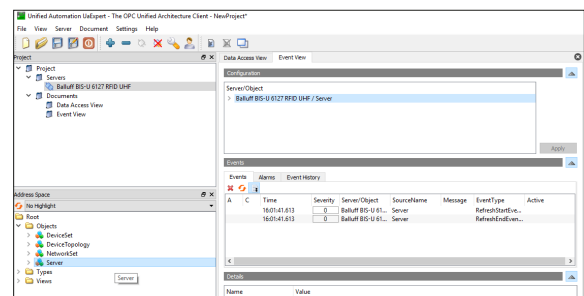


Fig. 9-41: Add server object

9

OPC UA (continued)

- To access the desired event, the *BALLUFF BIS U-6127 RFID UHF /SERVER* object must be expanded. Select the *RFIDSCANEVENTTYPE* event under *SIMPLEEVENTS - AUTOLDSCANEVENTTYPE* and accept the setting with *APPLY* (bottom right in the Event View).

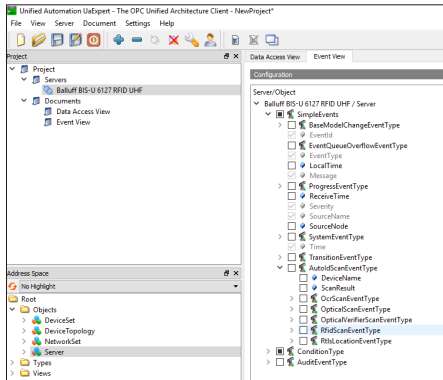


Fig. 9-42: Event View

As soon as asynchronous operation is started with the *ScanStart()* method (see page 146), an event is generated for each detected data carrier. These are displayed in the *EVENTS* window under the *EVENT* tab. The *EVENTTYPE* indicates that it is an *RFIDSCANEVENTTYPE* (see page 165). To get more information about the event, you just have to click on the event. All data are then displayed in the *DETAILS* window.

Information about the exact dates can be found under the *Events* chapter (see page 165).

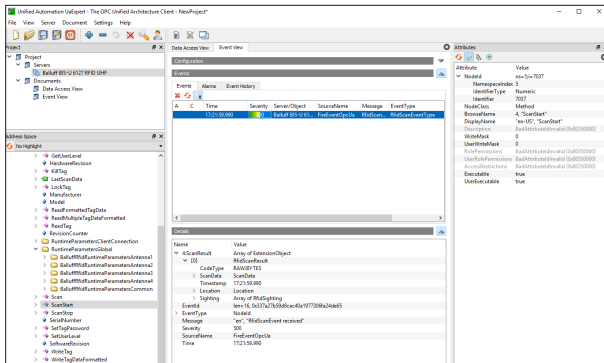


Fig. 9-43: Event Details

9.9.9 Global Session Mechanism

In OPC UA, there are session-related variables as well as global variables. The global variables are valid for all active and new sessions. An example of this is the *LASTSCANDATA* variable. It is used by all sessions.

The clients are pictured in Fig. 9-44 and Fig. 9-45. Both values of the *LASTSCANDATA* variable are identical, as expected.

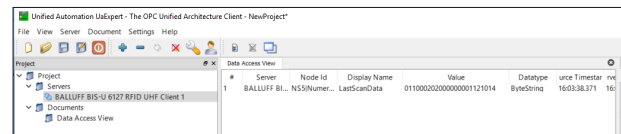


Fig. 9-44: UaExpert Client 1

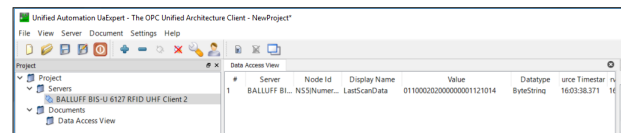


Fig. 9-45: UaExpert Client 2

If you run the scan method on client 1, only the EPC *08090808080808080808* is detected and the *LASTSCANDATA* variable is set to this value. Since all sessions use this variable, the value changes on both clients (see Fig. 9-46 and Fig. 9-47).

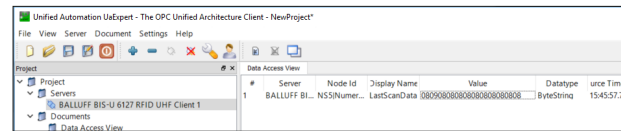


Fig. 9-46: Client 1: Variable LastScanData

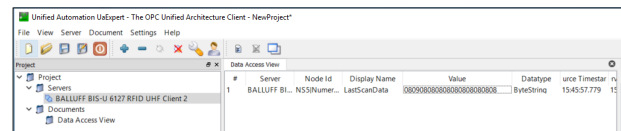


Fig. 9-47: Client 2: Variable LastScanData

However, if you want to know the last detected tag of the individual session, you have to use the *GetLastScanData()* method. This is session-related and returns the desired value. In the case of this example, the method therefore returns the value *08090808080808080808* for the client (see Fig. 9-48) and *01100020200000001121014* for client 2 (see Fig. 9-49).

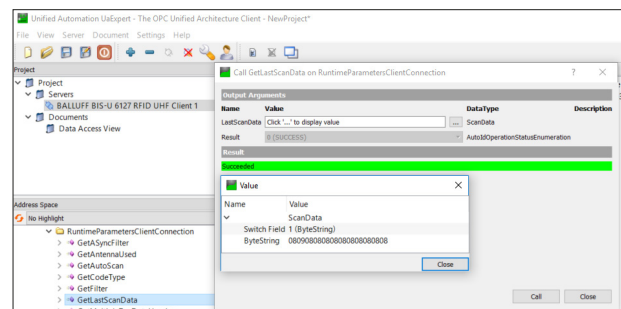


Fig. 9-48: Client 1: Method GetLastScanData

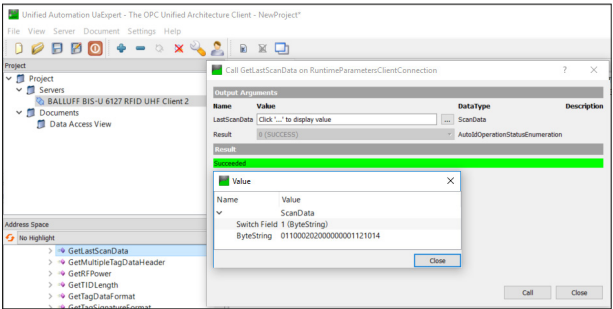


Fig. 9-49: Client 2: Method GetLastScanData

10 Accessories

Accessories are not included in the scope of delivery and must be ordered separately.



Recommended accessories can be found at www.balluff.com on the product page.

Some components for connecting and operating the device are listed below.

10.1 UHF antennas

Type	Order code
UHF Long Range Antenna (866...868 MHz)	BIS01AW
UHF Long Range Antenna (902...928 MHz)	BIS01AY
UHF Mid Range Antenna (866...868 MHz)	BIS00P0
UHF Mid Range Antenna (902...928 MHz)	BIS00TY
UHF M30 Short Range Antenna (866...868 MHz)	BIS01CP
UHF M30 Short Range Antenna (902...928 MHz)	BIS01CL

10.2 Antenna Cable

Type	Order code
Coaxial cable 1 m	BAM01HL
Coaxial cable 2 m	BAM01HM
Coaxial cable 3 m	BAM01YR
Coaxial cable 5 m	BAM01HN
Coaxial cable 10 m	BAM01HP

(other cable lengths on request)

10.3 Connection cable

Type	Order code
Power supply connection cable, M12, 2 m	BCC032F
Service/USB connection cable, M12, 2 m	BCC0KNT
Service/USB connection cable, M12, 3 m	BCC0J56
IO-Link connection cable, M12, 2 m	BCC039M
Ethernet connection cable, RJ45, 2 m	BCC0E24

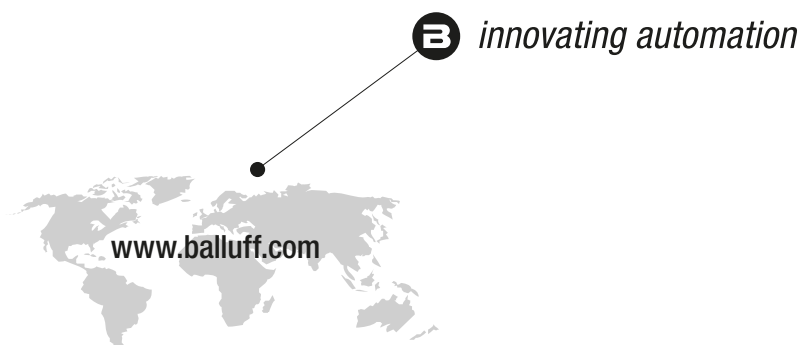
(other cable lengths on request)

10.4 Power supply/power supply unit

Type	Order code
Standard power supply 24 VDC, 5 A	BAE0112
IO-Link power supply 24 VDC, 5 A	BAE00T4

10.5 Mechanical accessories

Type	Order code
Mounting plates	BAM01KN



Headquarters

Germany

Balluff GmbH
Schurwaldstrasse 9
73765 Neuhausen a.d.F.
Phone +49 7158 173-0
Fax +49 7158 5010
balluff@balluff.de

DACH Service Center

Germany

Balluff GmbH
Schurwaldstrasse 9
73765 Neuhausen a.d.F.
Phone +49 7158 173-370
service.de@balluff.de

Southern Europe Service Center

Italy

Balluff Automation S.R.L.
Corso Cuneo 15
10078 Venaria Reale (Torino)
Phone +39 0113150711
service.it@balluff.it

Eastern Europe Service Center

Poland

Balluff Sp. z o.o.
Ul. Graniczna 21A
54-516 Wrocław
Phone +48 71 382 09 02
service.pl@balluff.pl

Americas Service Center

USA

Balluff Inc.
8125 Holton Drive
Florence, KY 41042
Toll-free +1 800 543 8390
Fax +1 859 727 4823
service.us@balluff.com

Asia Pacific Service Center

Greater China

Balluff Automation (Shanghai) Co., Ltd.
No. 800 Chengshan Rd, 8F, Building A,
Yunding International Commercial Plaza
200125, Pudong, Shanghai
Phone +86 400 820 0016
Fax +86 400 920 2622
service.cn@balluff.com.cn