



COM.GW.500 | Art.-Nr.: 2342521

Technische Daten

Nennspannung	24 V DC +/- 10%
Max. Stromaufnahme bei 24 VDC-Versorgung	4,5 A
Klasse PoE	0 IEEE 802.3af
Betriebstemperatur	-25 °C - +60 °C
Transport- und Lagerbedingungen	-40 °C - +85 °C
Verschmutzungsgrad	2
Höhenlage	< 2000 m
Relative Luftfeuchtigkeit	95% nicht kondensierend
Index der Stoßfestigkeit	3M4 IEC 60721-3-3
Funkkommunikation	WLAN: - IEEE 802.11 a/b/g/n/ac 2.4 GHz/5 GHz Drahtlos: - ISM-Band 2.400 bis 2.4835 GHz Sendeleistung: 8 dBm
I/Os Leitungslänge	Leitungslänge von max. 30 m (Vermeidung langer Leitungen) Nur in Innenräumen geeignet
I/O-Eingang	12-30 V DC
I/O-Ausgang	24 V DC, je Ausgang 500 mA

Technical Data

Nominal Voltage	24 V DC +/- 10%
Max. current consumption with 24 VDC supply	4,5 A
Rated voltage PoE	0 IEEE 802.3af
Operating temperatur	-25 °C - +60 °C
Transport and storage conditions	-40 °C - +85 °C
Altitude	2
Relative humidity	< 2000 m
Shock resistance index	95% without condensation
Radio communication	3M4 IEC 60721-3-3
I/Os cable length	WLAN: - IEEE 802.11 a/b/g/n/ac 2.4 GHz/5 GHz Wireless: - ISM-Band 2.400 bis 2.4835 GHz Transmitter power: 8 dBm
I/Os Leitungslänge	Cable length of max. 30 m (avoiding long cables) Only suitable for indoor use
I/O-Input	12-30 V DC
I/O-Output	24 V DC, per output 500 mA

Cybersicherheit

Kommunikation zwischen COM- und DAT-Modulen – 2,4 GHz ISM-Band

Zur Kommunikation zwischen COM- und DAT-Modulen wird eine **Funktechnologie gemäß Low Energy Standard Version 5.0 im 2,4 GHz ISM-Band** verwendet. Es wird **Security Mode 1, Level 4** eingesetzt, welcher die höchste Sicherheitsstufe darstellt.

Die Verbindung nutzt:

- Secure Simple Pairing (SSP) mit Authentifizierung
- Elliptic Curve Diffie-Hellman (ECDH) mit P-256-Kurve (zum Schutz vor MITM)
- AES-CCM mit 128-Bit-Schlüssel (für Verschlüsselung und Integrität)

Für jedes DAT-Modul ist ein **einzigartiger, zufällig generierter und geheimer Passkey** erforderlich.

Nur so wird sichergestellt, dass:

- Der Kommunikationspartner authentisch ist (Schutz vor Man-in-the-Middle)
- Die Verbindung vor Abhören geschützt ist (Encryption)
- Datenintegrität und -authentizität gewährleistet sind (Authentication)

Cyber Security

Communication between COM and DAT Modules – 2.4 GHz ISM band

Wireless communication between COM and DAT modules is based on a **Low Energy radio standard (version 5.0)** operating in the **2.4 GHz ISM band**. **Security Mode 1, Level 4** is strictly enforced, ensuring the highest level of security.

The connection employs:

- Authenticated Secure Simple Pairing (SSP)
- Elliptic Curve Diffie-Hellman (ECDH) using the P-256 curve (to protect against MITM attacks)
- AES-CCM encryption with a 128-bit key (for confidentiality and integrity)

Each DAT module must be configured with a **randomly generated, unique, and secret passkey**.

This security level ensures that:

- The communication partner is authenticated (MITM protection)
- Data cannot be intercepted by third parties (encryption)
- Data cannot be altered undetected (authentication)

Web-API – Authentifizierung

Die Authentifizierung erfolgt mittels **HTTP Basic Authentication**, wobei **Benutzername und Passwort** im **Base64-Format** über eine **TLS-gesicherte Verbindung** übertragen werden.

Base64 ist keine Verschlüsselung, sondern lediglich eine Kodierung. Daher ist die **Verwendung von HTTPS verpflichtend**. Die Voreinstellung **force-https** (automatische Umleitung von HTTP zu HTTPS) sollte **nicht deaktiviert** werden.

Passwörter werden auf dem COM-Modul mithilfe der **libxcrypt**-Bibliothek gehasht gespeichert. Der eingesetzte Hash-Algorithmus ist so gewählt, dass er bei akzeptabler Rechenzeit eine hohe Sicherheit gewährleistet.

Der Hash-Digest lässt **keine Rückschlüsse auf das Originalpasswort** zu.

Web API – Authentication

Client authentication to the Web API is performed using a **username and password**, which are transmitted in **Base64-encoded** form (note: not encrypted) over a **TLS-secured connection**.

Therefore, the default setting **force-https** (redirecting HTTP to HTTPS) should be strictly maintained.

Passwords are stored on the COM module using the **libxcrypt** library with strong hashing – considering a balance between processing time and device performance.

It is **not possible to reverse the password** from the resulting **hash digest**.

MQTT – TLS & Serverauthentifizierung

Der im COM-Modul enthaltene MQTT-Client nutzt **OpenSSL** in der jeweils aktuellen Version zur Absicherung der Verbindung mittels **TLS 1.3**. Die **Server-authentifizierung** erfolgt über **X.509-Zertifikate**.

Pro Verbindung kann individuell konfiguriert werden:

- **TLS aktivieren/deaktivieren**
- **Verifikation des Server-Zertifikats aktivieren/deaktivieren**

Diese Optionen ermöglichen eine flexible Sicherheitskonfiguration je nach Anwendungsfall und Infrastruktur.

MQTT – TLS and Server Authentication

The MQTT client integrated into the COM module uses the **latest version of OpenSSL** to implement **TLS 1.3 (Transport Layer Security)** and **X.509 certificates** for **server authentication**.

For each connection, it is possible to:

- **Enable or disable TLS**
- **Enable or disable server certificate verification**

This allows for flexible configuration of security settings based on the specific use case or environment.

Modbus – Sicherheit (ACL & DoS-Schutz)

Der integrierte Modbus-Server des COM-Moduls implementiert eine **Access Control List (ACL)** auf Basis von **IP-Adressen**, um unautorisierten Zugriff zu unterbinden.

Zur Abwehr potenzieller **Denial-of-Service-Angriffe (DoS)** durch fehlerhafte oder böswillige Clients ist zusätzlich ein **Rate Limiter** aktiviert, der die Anzahl eingehender Anfragen pro Zeitfenster begrenzt.

Diese Maßnahmen erhöhen die Robustheit und Sicherheit des Modbus-Kommunikationskanals.

Modbus Server – Access Control & DoS Protection

The Modbus server integrated into the COM module is protected by an **IP address-based Access Control List (ACL)** to prevent unauthorized access.

In addition, a **rate limiter** is in place to mitigate the effects of **misconfigured or malicious devices**, helping to reduce the risk of **Denial-of-Service (DoS) attacks**.