phi.krausnaimer.com

Fiche technique | Datasheet

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

Caractéristiques techniques

Tension nominale	24 V DC +/- 10%
Consommation de courant maximale avec alimentation 24 V DC	4,5 A
Classe PoE	0 IEEE 802.3af
Température de fonctionnement	-25 °C - +60 °C
Conditions de transport et de stockage	-40 °C - +85 °C
Degré de pollution	2
Altitude	< 2000 m
Humidité relative	95 % sans condensation
Indice de résistance aux chocs	3M4 IEC 60721-3-3
Communication radio	**WLAN:** ▪ IEEE 802.11 a/b/g/n/ac ▪ 2.4 GHz/5 GHz **Sans fil :** ▪ Bande ISM 2.400 à 2.4835 GHz **Puissance d'émission:** 8 dBm
Longueur de câble des E/S	Longueur de câble maximale de 30 m (éviter les longues lignes) Convient uniquement à une utilisation en intérieur
Entrée E/S	12-30 V DC
Sortie E/S	24 V DC, 500 mA par sortie

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
Pollution degree	2
Altitude	< 2000 m
Relative humidity	95% without condensation
Shock resistance index	3M4 IEC 60721-3-3
Radio communication	**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 cable length	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

Cybersécurité

Communication entre les modules COM et DAT – Communication sans fil dans la bande ISM de 2,4 GHz

La communication sans fil entre les modules COM et DAT repose sur une norme radio **Low Energy (version 5.0)** fonctionnant dans la bande ISM de **2,4 GHz. Le mode de sécurité 1, niveau 4,** est strictement appliqué, garantissant le niveau de sécurité le plus élevé.

La connexion utilise :

- **Appairage sécurisé simple authentifié (SSP)**
- **Elliptic Curve Diffie-Hellman (ECDH)** utilisant la courbe P-256 (pour la protection contre les attaques MITM)
- **Chiffrement AES-CCM** avec une clé de 128 bits (pour la confidentialité et l'intégrité)

Chaque module DAT doit être configuré avec une clé d'accès secrète, **unique et générée aléatoirement.**

Ce niveau de sécurité garantit que :

- Le partenaire de communication est authentifié (protection contre les attaques MITM)
- Les données ne peuvent pas être interceptées par des tiers (chiffrement)
- Les données ne peuvent pas être modifiées sans être détectées (authentification

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)

API Web – Authentification

L'authentification du client auprès de l'API Web s'effectue au moyen d'un nom d'utilisateur et d'un mot de passe, transmis sous forme encodée en **Base64 (remarque : non chiffrée)** via une connexion sécurisée par **TLS.**

Par conséquent, le paramètre par défaut **force-https** (redirection de HTTP vers HTTPS) doit impérativement être maintenu.

Les mots de passe sont stockés sur le module COM à l'aide de la bibliothèque **libxcrypt** avec un hachage fort, en tenant compte d'un équilibre entre le temps de traitement et les performances de l'appareil.

Il n'est pas possible de reconstituer le mot de passe à partir de l'empreinte de hachage obtenue.

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 et authentification du serveur

Le client MQTT intégré au module COM utilise la dernière version d'OpenSSL pour mettre en œuvre **TLS 1.3 (Transport Layer Security)** ainsi que des certificats X.509 pour l'authentification du serveur.

Pour chaque connexion, il est possible de :

- **activer ou désactiver TLS**
- **activer ou désactiver la vérification du certificat du serveur**

Cela permet une configuration flexible des paramètres de sécurité en fonction du cas d'usage ou de l'environnement concerné.

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.

Serveur Modbus – Contrôle d'accès et protection contre les attaques DoS

Le serveur Modbus intégré au module COM est protégé par une liste de **contrôle d'accès (ACL)** basée sur les adresses IP afin d'empêcher les accès non autorisés.

En outre, un limiteur de débit est mis en place afin d'atténuer les effets d'appareils mal configurés ou malveillants, contribuant ainsi à réduire le risque d'attaques par **déni de service (DoS).**

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**.