Grundfos Connect

Notes relatives à la sécurité

GRUNDFOS

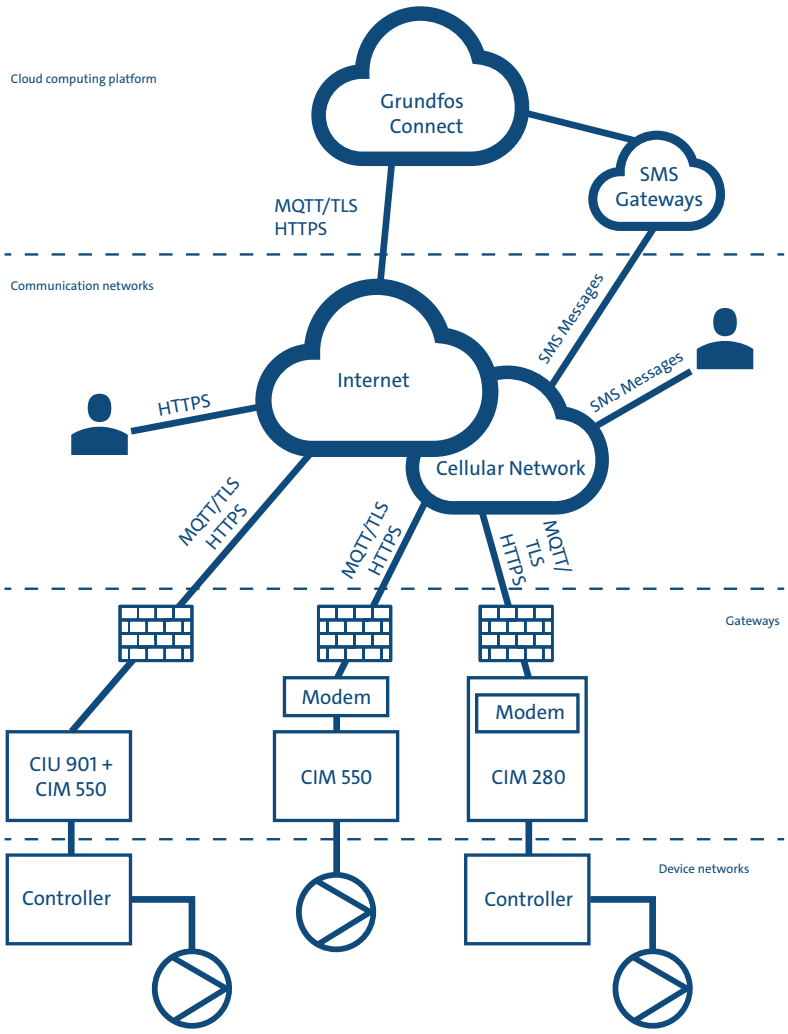
Possibility in every drop

Introduction

Grundfos Connect est un système en ligne prêt à l'emploi offrant une alternative efficace et rentable aux systèmes SCADA plus coûteux. Il vous permet de surveiller & contrôler vos appareils où que vous soyez. Il dispose d'un certain nombre de fonctions de sécurité qui vous offrent à la fois protection et sérennité.

Ce document en détaille les caractéristiques.

Architecture de sécurité



Architecture de sécurité

Comme schématisé ci-dessus, l'architecture de Grundfos Connect comprend une plateforme informatique sur laquelle fonctionne Grundfos Connect : plusieurs réseaux de communication, des passerelles contrôlant la connexion ainsi que l'infrastructure physique des systèmes localisés contrôlant les pompes.
Toutes les données TCP/IP envoyées vers et depuis les appareils connectés au réseau sont systématiquement cryptées.

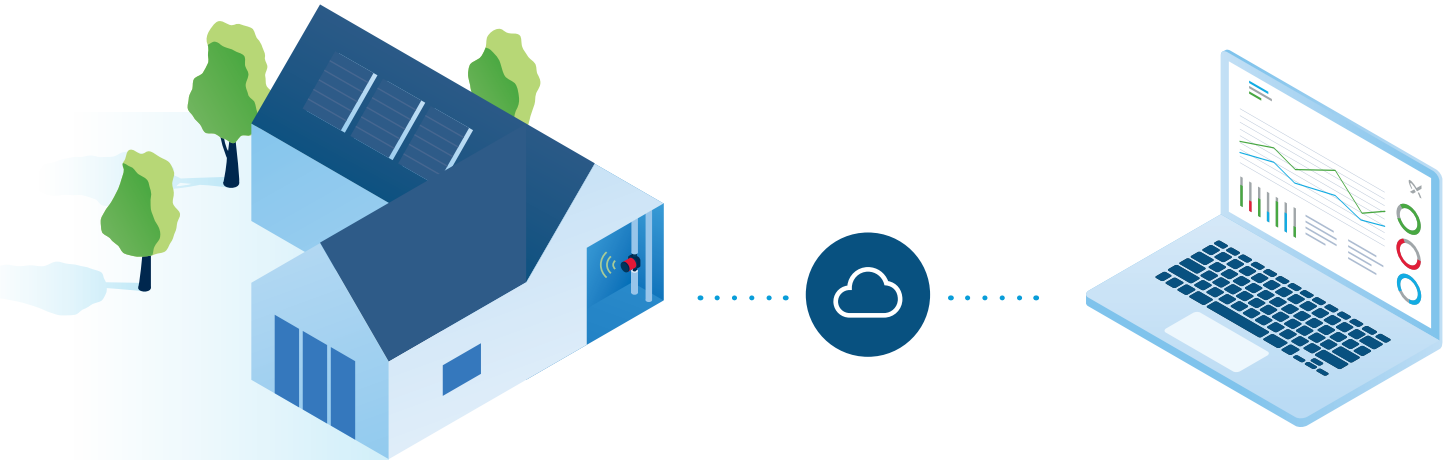
Dans ce livre blanc, vous découvrirez les principes mis en oeuvre par Grundfos Connect en matière de cybersécurité et de sécurité de l'information.

Comment cela fonctinone-t-il ?

Grundfos Connect se compose de quatre niveaux qui lui permettent de se connecter rapidement et en toute sécurité à vos systèmes.

- **Plateforme logicielle en cloud**
- **Réseaux internet & cellulaires**
- **Passerelles de communication**
- **Equipements à surveiller**

Grundfos Connect



Plateforme logicielle en cloud

Grundfos Connect est composé d'un certain nombre de services backend : Un service de terminal IoT[1] et un service d'authentification. Le service de terminal IoT gère la communication générale avec les appareils, tandis que le service d'authentification gère l'authentification des appareils et sélectionne le terminal IoT que les appareils doivent utiliser pour la communication. Grundfos Connect utilise un système d'authentification mutuelle basé sur des certificats X.509.

Les services backend comprennent également des services de stockage, de gestion des accès, de notification et des passerelles SMS spécialisées pour envoyer des messages aux utilisateurs.

Les services backend sont hébergés dans une infrastructure cloud évolutive, protégée par des technologies de sécurité de dernière génération, telles que des "reverse-proxies" avec filtrage & analyse du trafic "Layer-7", des Web Application Firewalls (WAF) et des mécanismes de protection contre les attaques par déni de service distribuée (DDoS).

Réseaux internet & cellulaires

Grundfos Connect utilise l'Internet ou le réseau cellulaire, en fonction des exigences du client et de l'infrastructure physique disponible.

Les passerelles initient des connexions HTTPS à travers le réseau pour se connecter au service d'authentification. HTTPS est la version sécurisée de HTTP qui utilise Transport Level Security (TLS).
Lorsqu'un terminal IoT lui est attribué, la passerelle se connecte au terminal IoT à l'aide de MQTT/TLS pour poursuivre la communication avec Grundfos Connect.
Les passerelles utilisent un système d'authentification mutuelle basé sur des certificats X.509 où le serveur et le client sont tous deux authentifiés. Les utilisateurs accèdent à Grundfos Connect à l'aide d'un client Web. Le client Web utilise HTTPS et peut être utilisé partout où il y a un accès à Internet. L'authentification de l'utilisateur est assurée par le fournisseur d'identité Grundfos (Global Login). Vous pouvez inviter des utilisateurs supplémentaires appartenant à votre organisation et ils devront suivre le processus de création dans Global Login.

Grundfos Connect enverra des courriels ou des SMS aux utilisateurs qui se sont abonnés aux alertes.

1 Internet of Things ou Internet des Objets

Passerelles de communication

Les directives de Grundfos concernant les produits connectés sont disponibles sur grundfos.com et doivent toujours être respectées pour votre sécurité.

Le CIM 280 est une interface utilisée pour la transmission de données via un réseau 3G ou 4G, tandis que le CIM 550 est utilisé sur les réseaux basés sur Ethernet.
Le CIM 280 et le CIM 550 transfèrent des données entre le réseau sur lequel se trouve l'appareil et Grundfos Connect par le biais de connexions TLS sécurisées. Ils peuvent être installés dans différentes configurations physiques, par exemple dans un produit Grundfos doté d'un emplacement CIM ou dans une passerelle de communication CIU 900/901.

Les passerelles sont attribuées aux utilisateurs dans le cadre d'un processus nécessitant un accès physique à l'équipement.

Utilisation de pare feu

Comme les passerelles initient toujours la connexion à Grundfos Connect, aucune connexion entrante ne doit être autorisée à travers le pare-feu.
Si vous utilisez un pare-feu externe, assurez-vous qu'il autorise les connexions sortantes via HTTPS et MQTT/TLS.

Équipements à surveiller

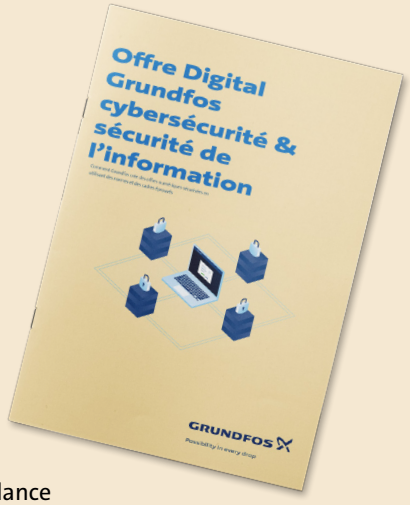
Les équipements à surveiller correspond aux équipements fonctionnels, tels que les contrôleurs, les pompes et les autres relais et capteurs, ils sont placés dans l'architecture du système. Ils peuvent communiquer entre eux, ainsi qu'avec les passerelles du système, par l'intermédiaire de Fieldbus en série. Aucune communication dans cette section n'est basée sur TCP/IP.

Résumé

Communication de l'appareil : Communication via Fieldbus en série (pas de TCP/IP)
Communication WAN : HTTPS et MQTT/TLS (utilisant TLS 1.2) via réseau ethernet ou cellulaire (3G/4G)
Communication avec l'utilisateur : HTTPS (utilisant TLS 1.2) et email/SMS pour les notifications

Authentication Grundfos Connect : Certificats X.509
Authentication utilisateur : Nom d'utilisateur / mot de passe
Authentication passerelle : Certificats X. 509

Mise à jour logiciel : Protégée par TLS
Disponibilité : Mise en place de services d'application virtualisés redondants
Opérations : essai d'intrusion (pentest), modèle de menace, enregistrement et surveillance continus.



© Grundfos Holding A/S 03.2024

Des questions
Contactez :

Hubert Claeyssens
Ventes digitales
WU FRANCE
hclaeyssens@grundfos.com

Pompes Grundfos Distribution S.A.S.
57 rue de Malacombe
FR- 38070 St-Quentin-Fallavier
Tél: 04 74 82 15 15
www.grundfos.fr

GRUNDFOS