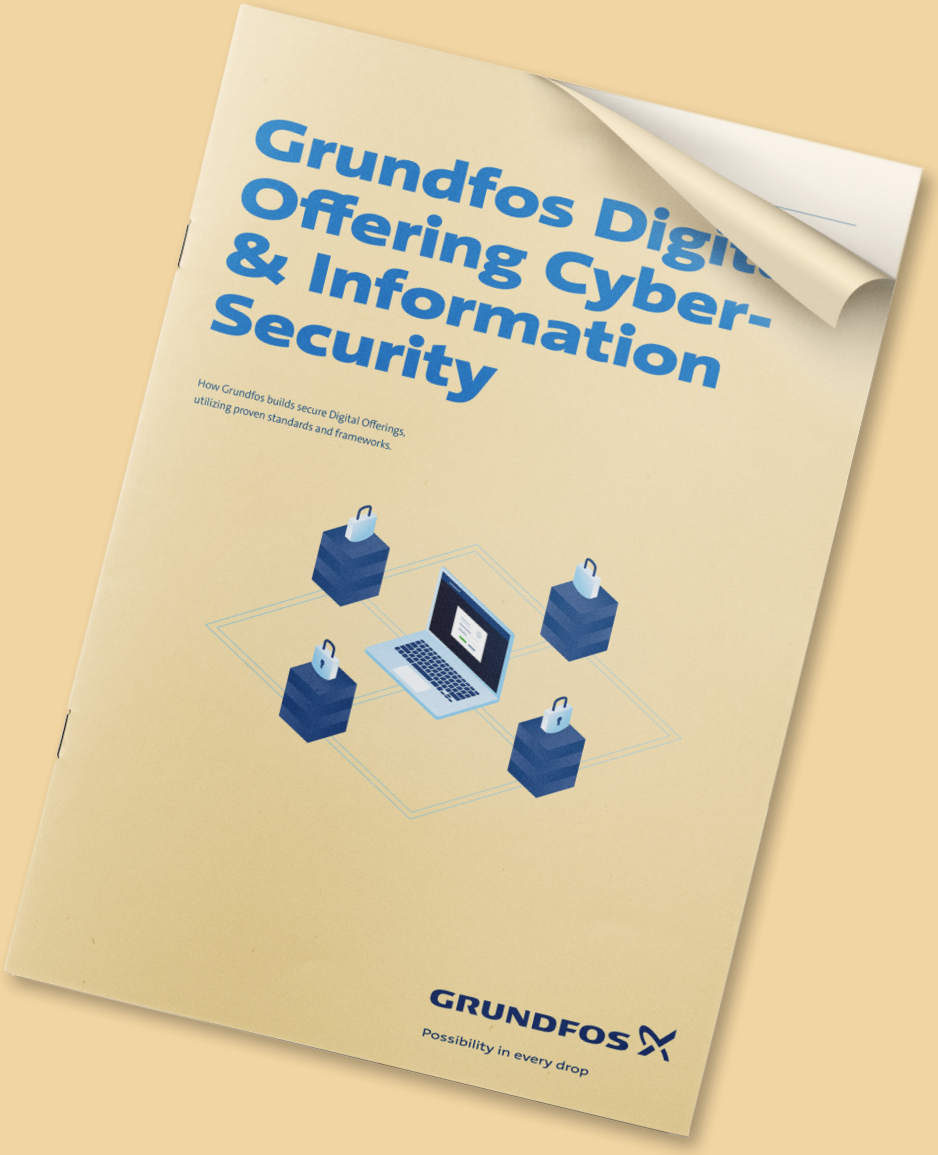
Grundfos Connect Asset Monitor

Aviso de segurança da aplicação



GRUNDFOS

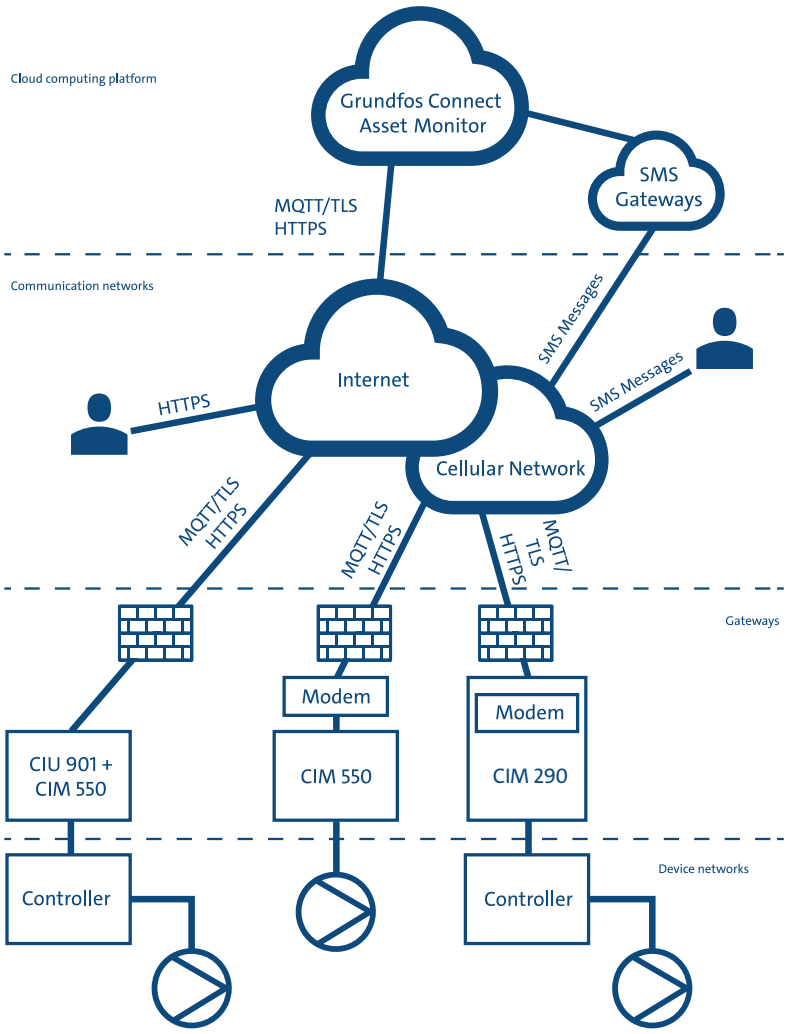
Possibility in every drop

Introdução

O Grundfos Connect Asset Monitor é um sistema “plug & play” baseado na Internet, que oferece uma alternativa eficiente e rentável aos sistemas SCADA mais dispendiosos. Proporciona-lhe controlo total dos seus dispositivos Grundfos, onde quer que esteja. Tem várias funcionalidades de segurança que lhe oferecem proteção e tranquilidade.

Este documento explica essas funcionalidades em detalhe.

A Arquitetura de Segurança



Arquitetura de Segurança

Como ilustrado acima, a arquitetura de segurança do Asset Monitor inclui uma plataforma de computação na qual o dispositivo de monitorização de ativos é executado, diversas redes de comunicação, gateways que controlam a ligação e a infraestrutura física dos sistemas localizados que controlam as bombas.

Todos os dados TCP/IP enviados de e para dispositivos ligados à rede são permanentemente encriptados.

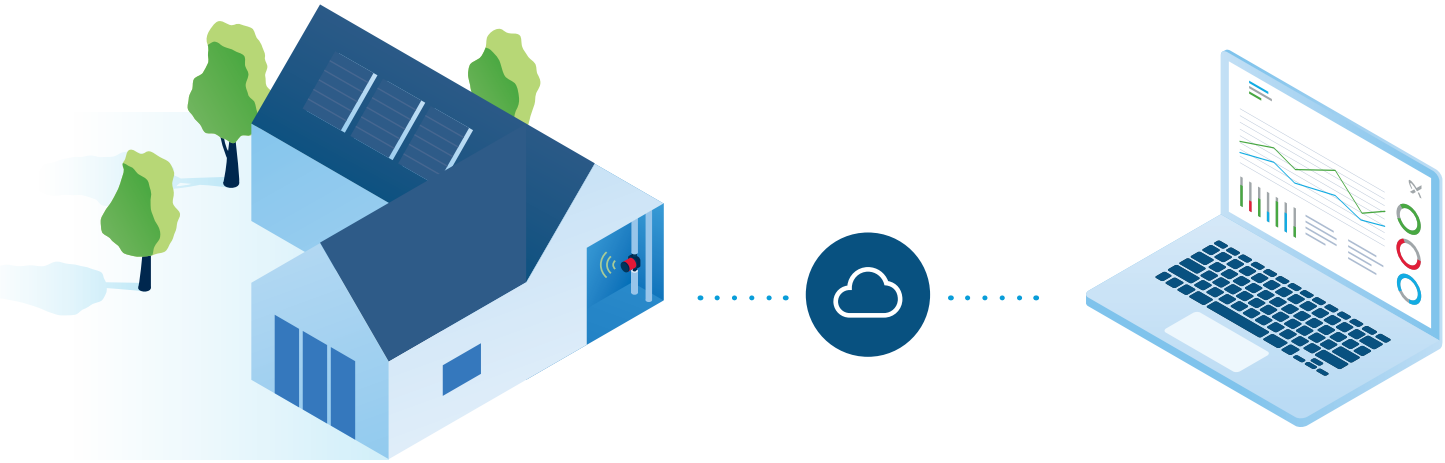
Pode ler mais sobre os princípios cumpridos pelo Asset Monitor no artigo técnico sobre cibersegurança e segurança da informação da Grundfos, disponível em Grundfos.com/pt.

Como funciona

O Asset Monitor tem quatro componentes que o ajudam a ligar-se rápida e de forma segura aos seus sistemas.

- **Plataforma de computação na cloud**
- **Redes de comunicação**
- **Gateways**
- **Redes de dispositivos**

Grundfos Connect Asset Monitor



Plataforma de computação na cloud

O Asset Monitor é composto por vários serviços de backend: Um serviço de ponto terminal IoT e um serviço de autenticação. O serviço de ponto terminal IoT gere a comunicação geral com os dispositivos, enquanto o serviço de autenticação trata da autenticação dos dispositivos e seleciona qual ponto terminal IoT os dispositivos devem usar para comunicação. O Asset Monitor utiliza um esquema de autenticação mútua baseado em certificados X.509.

Os serviços de backend incluem também serviços de armazenamento, autorização e notificação; e gateways de SMS especializados podem enviar mensagens de texto aos utilizadores do sistema.

Os serviços de backend são alojados numa infraestrutura na cloud altamente escalável, protegida por tecnologias de segurança modernas e da próxima geração, como proxies reversos com filtragem e análise de tráfego Layer7, firewalls de aplicações web (WAF) e mecanismos de proteção contra negação de serviço distribuído (DDoS).

Redes de comunicação

O Asset Monitor utiliza a Internet ou a rede móvel, dependendo dos requisitos do cliente e da infraestrutura física disponível.

Os gateways iniciam ligações HTTPS através da rede para se ligarem ao serviço de autenticação. HTTPS é a versão segura do HTTP que utiliza segurança ao nível de transporte (TLS). Quando atribuído a um ponto terminal IoT, o gateway liga-se ao mesmo usando MQTT/TLS para continuar a comunicação com o Asset Monitor.
Os gateways utilizam um esquema de autenticação mútua baseado em certificados X.509, em que tanto o servidor como o cliente são autenticados.

Os utilizadores acedem ao Asset Monitor através de um cliente web. O cliente web utiliza HTTPS e pode ser usado em qualquer lugar com acesso à internet. A autenticação do utilizador é assegurada através do fornecedor de identidade Grundfos (Global Login). Pode convidar utilizadores adicionais da sua organização e estes terão de passar pelo processo de criação no Global Login.

O Asset Monitor enviará e-mails ou mensagens de texto aos utilizadores que subscreveram os alertas.

Gateways

As diretrizes da Grundfos para lidar com produtos ligados estão disponíveis em grundfos.com e devem ser sempre cumpridas para garantir a sua segurança.

O CIM 290 é uma interface utilizada para transmissão de dados através de uma rede 3G ou 4G, enquanto o CIM 550 é utilizado em redes baseadas em Ethernet.
Tanto o CIM 290 como o CIM 550 transferem dados entre a rede onde o dispositivo se encontra e o Asset Monitor através de ligações TLS seguras. Podem ser instalados em diferentes configurações físicas, como num produto Grundfos com slot para CIM ou numa unidade de interface CIU 900/901.

O processo de atribuição dos gateways aos utilizadores requer acesso físico ao equipamento.

Utilização de firewalls

Como os gateways iniciam sempre a ligação ao Asset Monitor, nenhuma ligação de entrada deverá ser permitida através do firewall.
Ao utilizar uma firewall externa, certifique-se de que permite ligações de saída via HTTPS e MQTT/TLS.

Redes de dispositivos

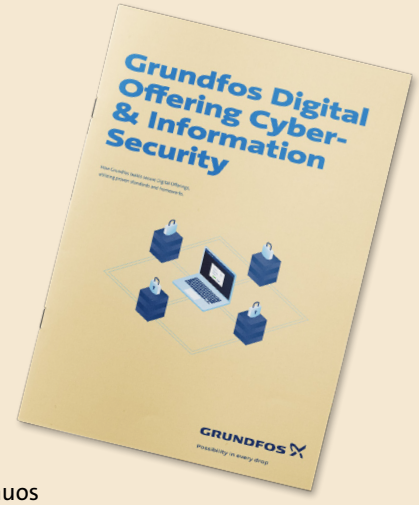
A secção de rede de dispositivos é onde todo o hardware funcional – como controladores, bombas e outros dispositivos – é colocado na arquitetura do sistema. Podem comunicar entre si, bem como com os gateways do sistema, através de fieldbus de série. Nenhuma da comunicação nesta secção é baseada em TCP/IP.

Resumo

Comunicação entre dispositivos: comunicação fieldbus de série (não TCP/IP)
Comunicação WAN: HTTPS e MQTT/TLS (utilizando TLS 1.2)
via Ethernet ou rede móvel (3G/4G)
Comunicação com o utilizador: HTTPS (utilizando TLS 1.2)
e e-mail/SMS para notificações

Autenticação do Grundfos Connect Asset Monitor: Certificados X.509
Autenticação do utilizador: Nome de utilizador / palavra-passe
Autenticação do Gateway: X. 509 certificados

Atualização de software: “Over-the-air” protegido por TLS
Disponibilidade: Configuração de serviços da aplicação virtualizada redundante
Operações: Teste de penetração, modelo de ameaça e logging e monitorização contínuos



Tem dúvidas?
Não hesite em contactar-nos:

Michael Sandholm
Responsável de produto
Desenvolvimento Digital
msandholm@grundfos.com

Bombas Grundfos Portugal S.A.
Rua Calvet de Magalhães, 241
2770-153 Paço de Arcos, Portugal
Tel: (+351) 21 440 76 00
www.grundfos.com/pt

GRUNDFOS