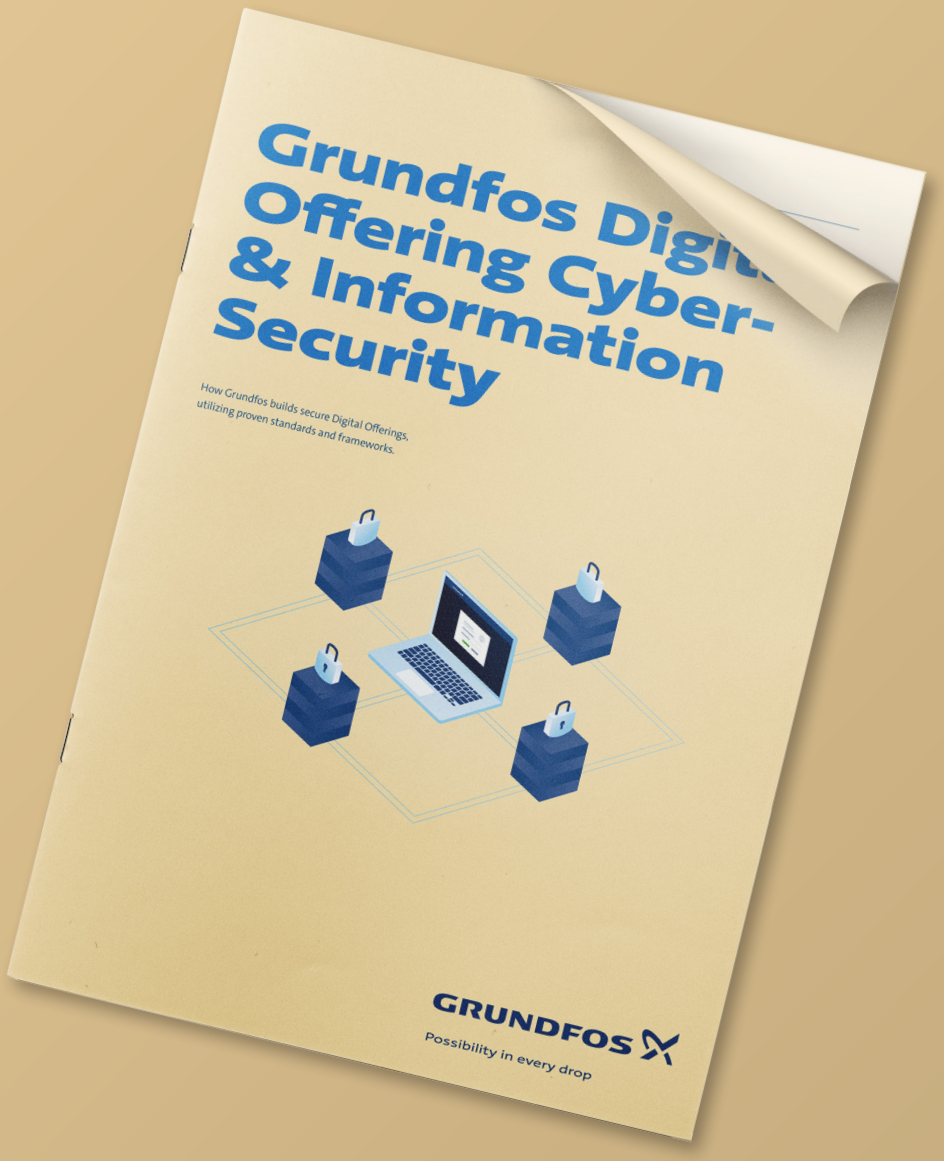
Grundfos Connect Asset Monitor

Security Application Note



GRUNDFOS

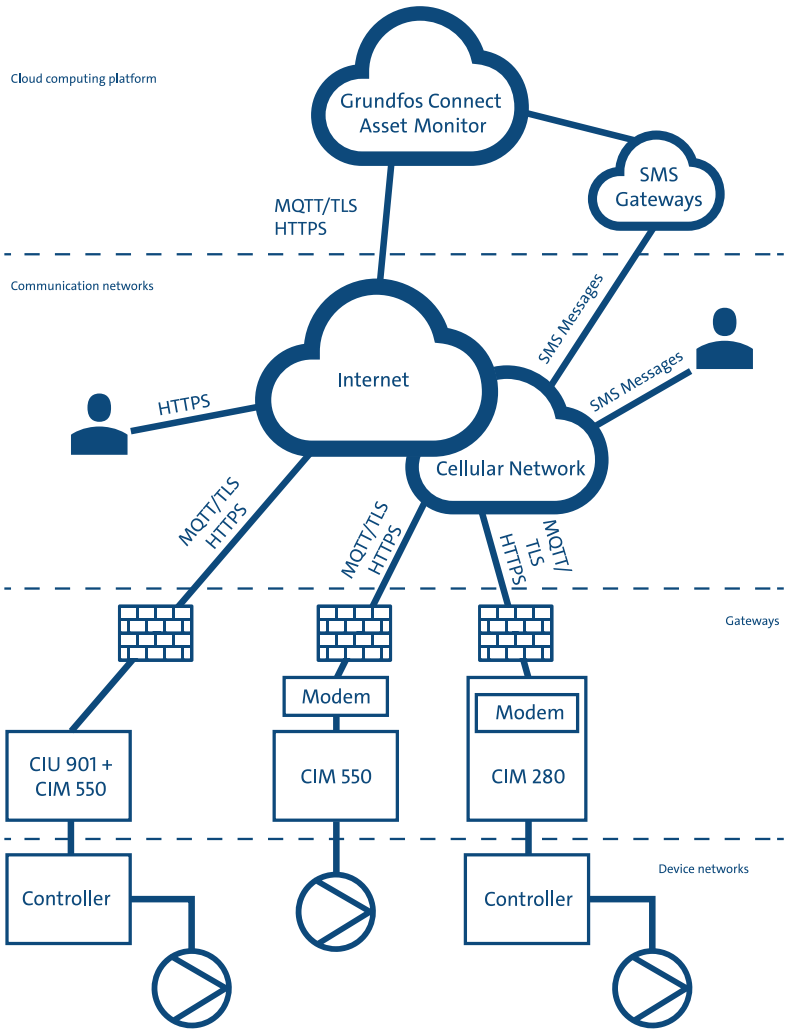
Possibility in every drop

Introduction

Grundfos Connect Asset Monitor is a plug & play internet-based system, that gives you an efficient and cost-effective alternative to more costly SCADA systems. It gives you complete control over your Grundfos devices, no matter where you are. It has a number of security features that give you both protection and peace of mind.

This document details what they are.

The Security Architecture



Security architecture

As shown above, the Asset Monitor security architecture includes a computing platform on which Asset Monitor runs, multiple communication networks, gateways that control the connection, and the physical infrastructure of the localized systems which control the pumps.
All TCP/IP data sent to and from devices connected to the network are encrypted at all times.

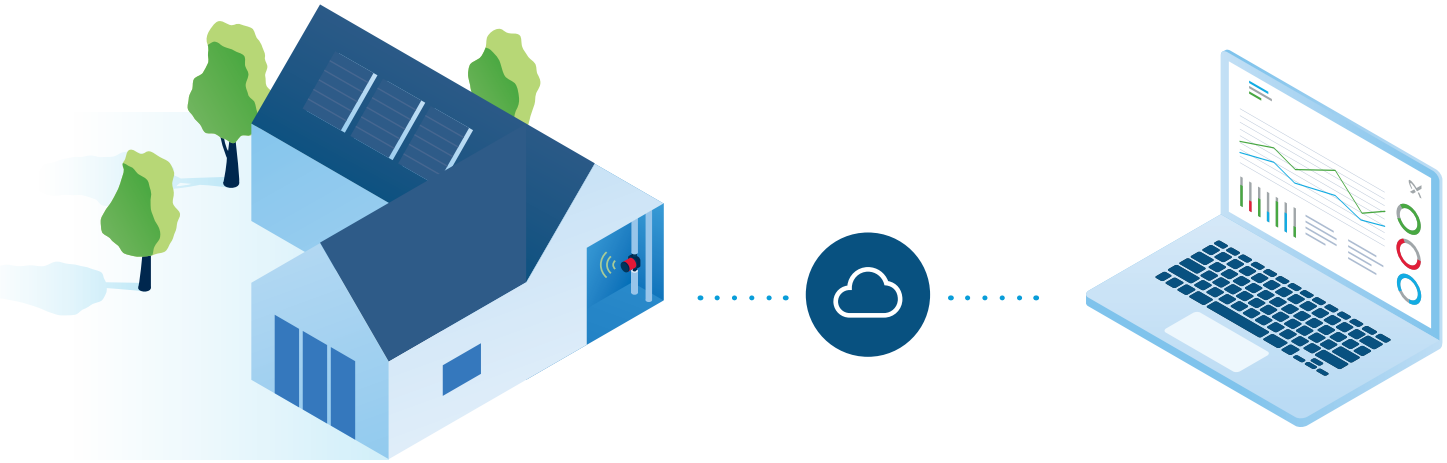
You can read more about the principles that Asset Monitor abides by in the Grundfos cyber and information security whitepaper found at Grundfos.us.

How it works

There are four components to Asset Monitor which help it to connect quickly and securely to your systems.

- **Cloud computing platform**
- **Communication networks**
- **Gateways**
- **Device networks**

Grundfos Connect Asset Monitor



Cloud computing platform

Asset Monitor is made up of a number of backend services: An IoT endpoint service and an authentication service. The IoT endpoint service handles the general communication with devices while the authentication service handles authentication of devices and selects which IoT endpoint the devices should use for communication. Asset Monitor uses a mutual authentication scheme based on X.509 certificates.

The backend services also include storage, authorization, and notification services, and specialist SMS gateways can send text messages to system users.

The backend services are hosted in a highly scalable cloud infrastructure, protected by modern and next-gen security technologies, such as reverse proxies with Layer7 filtering and traffic analysis, Web Application Firewalls (WAF) and Distributed Denial of Service (DDoS) protection mechanisms.

Communication networks

Asset Monitor uses the internet or the cellular network, depending on the customer's requirements and the available physical infrastructure.

Gateways initiate HTTPS connections through the network to connect with the authentication service. HTTPS is the secure version of HTTP that uses Transport Level Security (TLS).

When assigned an IoT endpoint, the gateway will connect to the IoT endpoint using MQTT/TLS to continue the communication with Asset Monitor.
Gateways use a mutual authentication scheme based on X.509 certificates where both server and client are authenticated.

Users access Asset Monitor with a web client. The web client uses HTTPS and can be used anywhere with internet access. User Authentication is ensured via the Grundfos identity provider (Global Login). You can invite additional users belonging to your organization and they will have to go through the creation process in Global Login.

Asset Monitor will send emails or texts to users who has subscribed to alerts.

Gateways

Grundfos guidelines for dealing with connected products are available at grundfos.com and should always be followed for your security.

The CIM 280 is an interface used for data transmission via a 3G or 4G network, while the CIM 550 is used on ethernet-based networks.
Both the CIM 280 and the CIM 550 transfer data between the network the device is on and Asset Monitor through secure TLS connections. They can be installed in different physical configurations, such as in a Grundfos product with a CIM slot or in a CIU 900/901 interface unit.

Gateways are assigned to users in a process that requires physical access to the equipment.

Using firewalls

As the gateways always initiate the connection to Asset Monitor, no inbound connections should be allowed through the firewall.
When using an external firewall, be sure that it allows outgoing connections through HTTPS, and MQTT/TLS.

Device networks

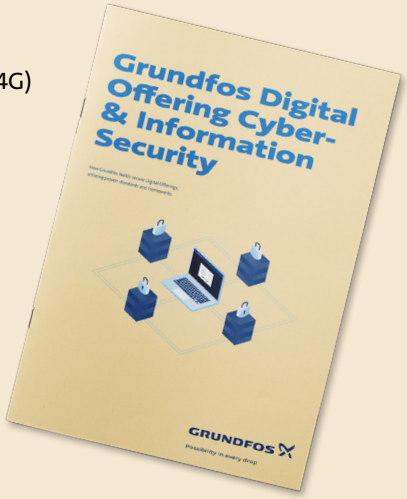
The device network section is where all working hardware, such as controllers, pumps, and other devices are placed onto the system architecture. They can communicate with each other, as well as the system gateways, through serial fieldbuses. No communication in this section is TCP/IP based.

Summary

Device communication: Serial fieldbus communication (not TCP/IP)
WAN communication: HTTPS and MQTT/TLS (using TLS 1.2) over ethernet or cellular (3G/4G)
User communication: HTTPS (using TLS 1.2) and email/SMS for notifications

Grundfos Connect Assets Monitor authentication: X.509 certificates
User authentication: Username / password
Gateway authentication: X. 509 certificates

Software update: Over-the-air protected by TLS
Availability: Redundant virtualized application services setup
Operations: Penetration test, threat model, and continuous logging and monitoring



Any questions?
Feel free to contact:

Michael Sandholm
Product Owner
Digital Development
msandholm@grundfos.us

GRUNDFOS
902 Koomey Road
US-77423, Brookshire, TX
Tel: 630-236-5500
www.grundfos.us

GRUNDFOS