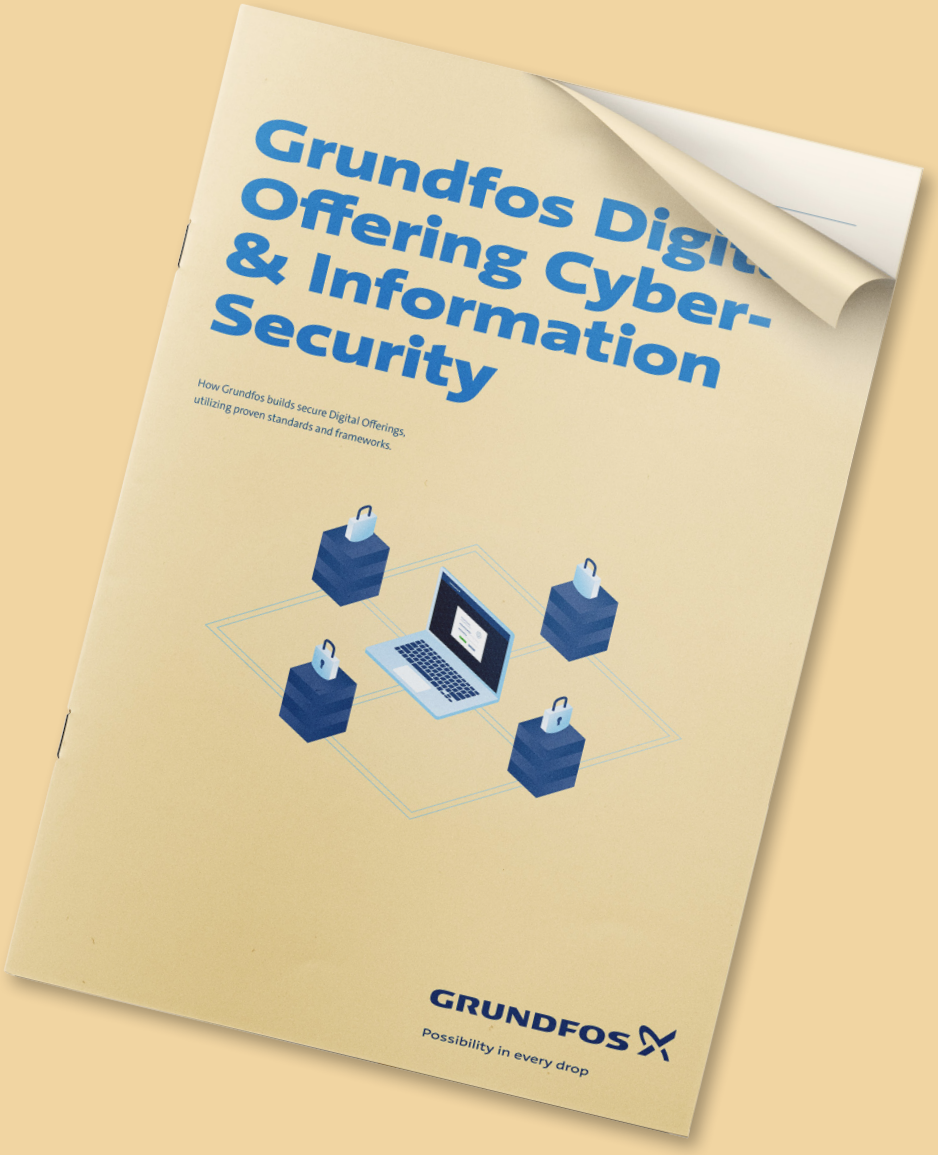
Grundfos Connect Asset Monitor

Nota de la aplicación sobre seguridad



GRUNDFOS

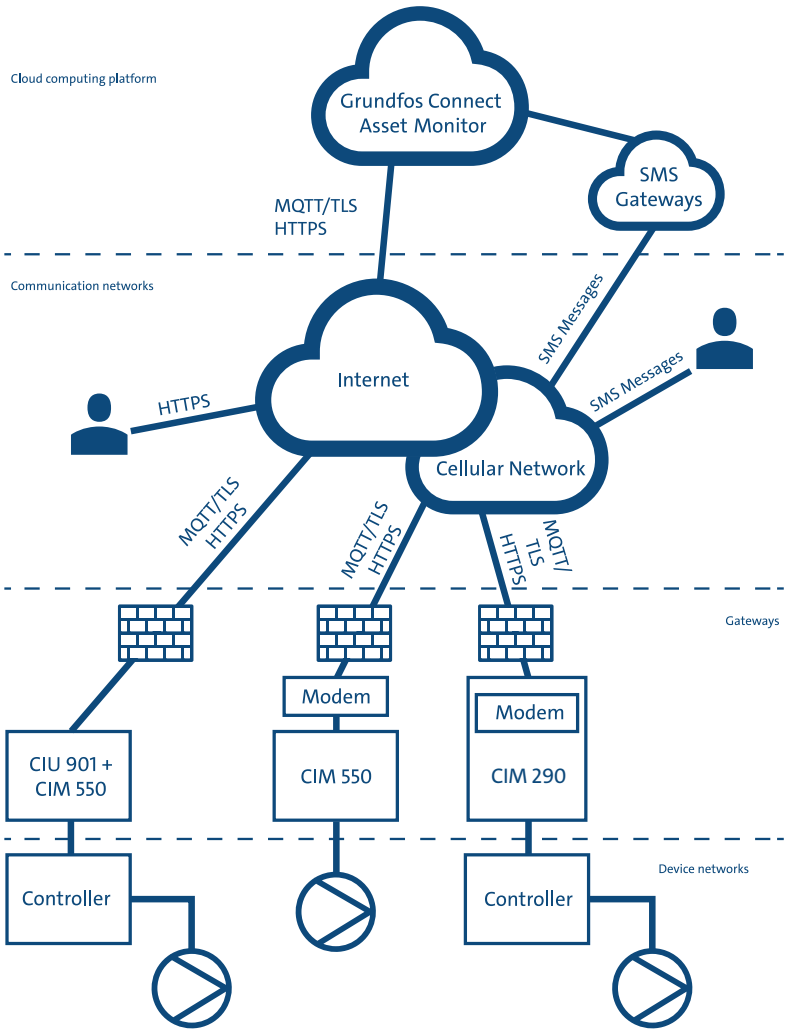
Possibility in every drop

Introducción

Grundfos Connect Asset Monitor es un sistema *plug-and-play* basado en Internet que brinda una alternativa eficiente y rentable a sistemas SCADA más caros. Te da un control total sobre tus dispositivos Grundfos, sin importar dónde estés. Cuenta con una serie de características de seguridad que te proporcionan tanto protección como tranquilidad.

Este documento detalla cuáles son.

La arquitectura de seguridad



Arquitectura de seguridad

Como se muestra arriba, la arquitectura de seguridad de Asset Monitor incluye una plataforma de computación donde se ejecuta Asset Monitor, múltiples redes de comunicación, pasarelas de comunicación que controlan la conexión y la infraestructura física de los sistemas localizados que controlan las bombas.
Todos los datos TCP/IP enviados hacia y desde los dispositivos conectados a la red están cifrados en todo momento.

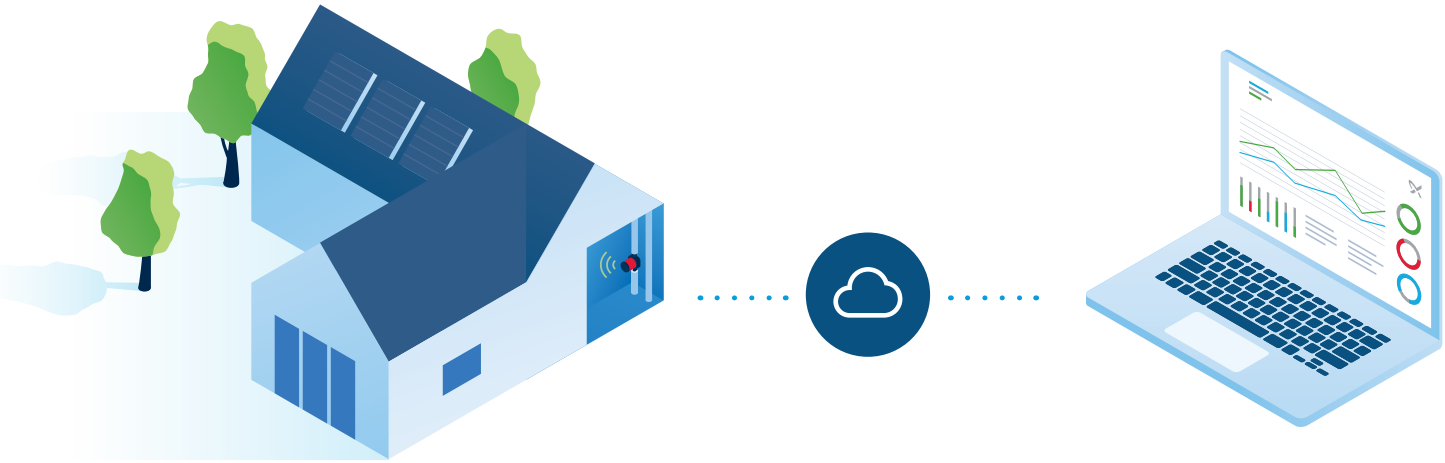
Puedes leer más sobre los principios que rigen Asset Monitor en el artículo técnico sobre ciberseguridad y seguridad de la información de Grundfos, disponible en Grundfos.com.

Cómo funciona

Hay cuatro componentes en Asset Monitor que ayudan a conectar de forma rápida y segura con tus sistemas.

- **Plataforma de computación en la nube**
- **Redes de comunicación**
- **Pasarelas de comunicación**
- **Redes de dispositivos**

Grundfos Connect Asset Monitor



Plataforma de computación en la nube

Asset Monitor se compone de varios servicios *backend:* un servicio de punto final de IoT y un servicio de autenticación. El servicio de punto final de IoT gestiona la comunicación general con los dispositivos, mientras que el servicio de autenticación gestiona la autenticación de los dispositivos y selecciona qué punto final de IoT deben usar para comunicarse. Asset Monitor usa un esquema de autenticación mutua basada en certificados X.509.

Los servicios *backend* también incluyen almacenamiento, autorización y servicios de notificación, y pasarelas de comunicación SMS especializadas que pueden enviar mensajes de texto a los usuarios del sistema.

Los servicios *backend* se encuentran alojados en una infraestructura en la nube altamente escalable, protegida por tecnologías de seguridad modernas y de última generación, como los proxies inversos con filtrado Layer 7 y análisis de tráfico, *firewall* de aplicaciones web (WAF) y mecanismos de protección contra denegación de servicio distribuida (DDoS).

Redes de comunicación

Asset Monitor utiliza Internet o la red móvil, en función de los requisitos del cliente y de la infraestructura física disponible.

Las pasarelas de comunicación inician conexiones HTTPS a través de la red para conectar con el servicio de autenticación. HTTPS es la versión segura de HTTP que utiliza seguridad de nivel de transporte (TLS).
Cuando se le asigna un punto final de IoT, la pasarela de comunicación se conectará al punto final de IoT utilizando MQTT/TLS para continuar la comunicación con Asset Monitor. Las pasarelas de comunicación utilizan un esquema de autenticación mutua basado en certificados X.509 donde se autentican tanto el servidor como el cliente.

Los usuarios acceden a Asset Monitor con un cliente web. El cliente web utiliza HTTPS y se puede usar en cualquier lugar con acceso a Internet. La autenticación de usuarios se asegura a través del proveedor de identidad de Grundfos (Global Login). Puedes invitar a usuarios adicionales que pertenezcan a tu organización y tendrán que pasar por el proceso de creación en Global Login.

Asset Monitor enviará correos electrónicos o mensajes de texto a los usuarios que se hayan suscrito a las alertas.

Pasarelas de comunicación

Las directrices de Grundfos para tratar con productos conectados están disponibles en grundfos.com y deben seguirse siempre por tu seguridad.

La CIM 290 es una interfaz que se utiliza para la transmisión de datos a través de una red 3G o 4G, mientras que la CIM 550 se utiliza en redes basadas en Ethernet.
Tanto la CIM 290 como la CIM 550 transfieren datos entre la red en la que está el dispositivo y Asset Monitor a través de conexiones TLS seguras. Se pueden instalar en diferentes configuraciones físicas, como en un producto Grundfos con una ranura CIM o en una unidad de interfaz CIU 900/901.

Las pasarelas de comunicación se asignan a usuarios en un proceso que requiere acceso físico al equipo.

Uso de firewalls

Dado que las pasarelas de comunicación siempre inician la conexión con Asset Monitor, no se deben permitir conexiones entrantes a través del *firewall*.
Al usar un *firewall* externo, asegúrate de que permite conexiones salientes a través de HTTPS y MQTT/TLS.

Redes de dispositivos

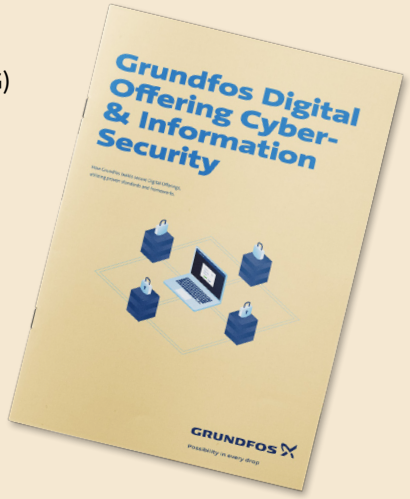
La sección de redes de dispositivos es donde todo el hardware operativo, como controladores, bombas y otros dispositivos, se ubica en la arquitectura del sistema. Pueden comunicarse entre sí, así como con las pasarelas de comunicación del sistema, a través de Fieldbus en serie. Ninguna comunicación de esta sección está basada en TCP/IP.

Resumen

Comunicación de dispositivos: Comunicación de Fieldbus en serie (no TCP/IP)
Comunicación WAN: HTTPS y MQTT/TLS (usando TLS 1.2) sobre Ethernet o móvil (3G/4G)
Comunicación de usuarios: HTTPS (usando TLS 1.2) y correo electrónico/SMS para las notificaciones

Autenticación de Grundfos Connect Asset Monitor: Certificados X.509
Autenticación de usuarios: Nombre de usuario/contraseña
Autenticación de pasarela de comunicación: Certificados X. 509

Actualización de software: Inalámbrica protegida por TLS
Disponibilidad: Configuración de servicios de aplicaciones virtualizadas redundantes
Operaciones: Prueba de penetración, modelo de amenazas y registro y monitorización continuos



¿Tienes alguna duda?
No dudes en contactar con:

Michael Sandholm
Product Owner
Desarrollo Digital
msandholm@grundfos.com

Bombas GRUNDFOS España, S.A.
Camino de la Fuentecilla, s/n
ES-28110 Algete España
Tel.: +34 91 848 8800
www.grundfos.com/es

GRUNDFOS