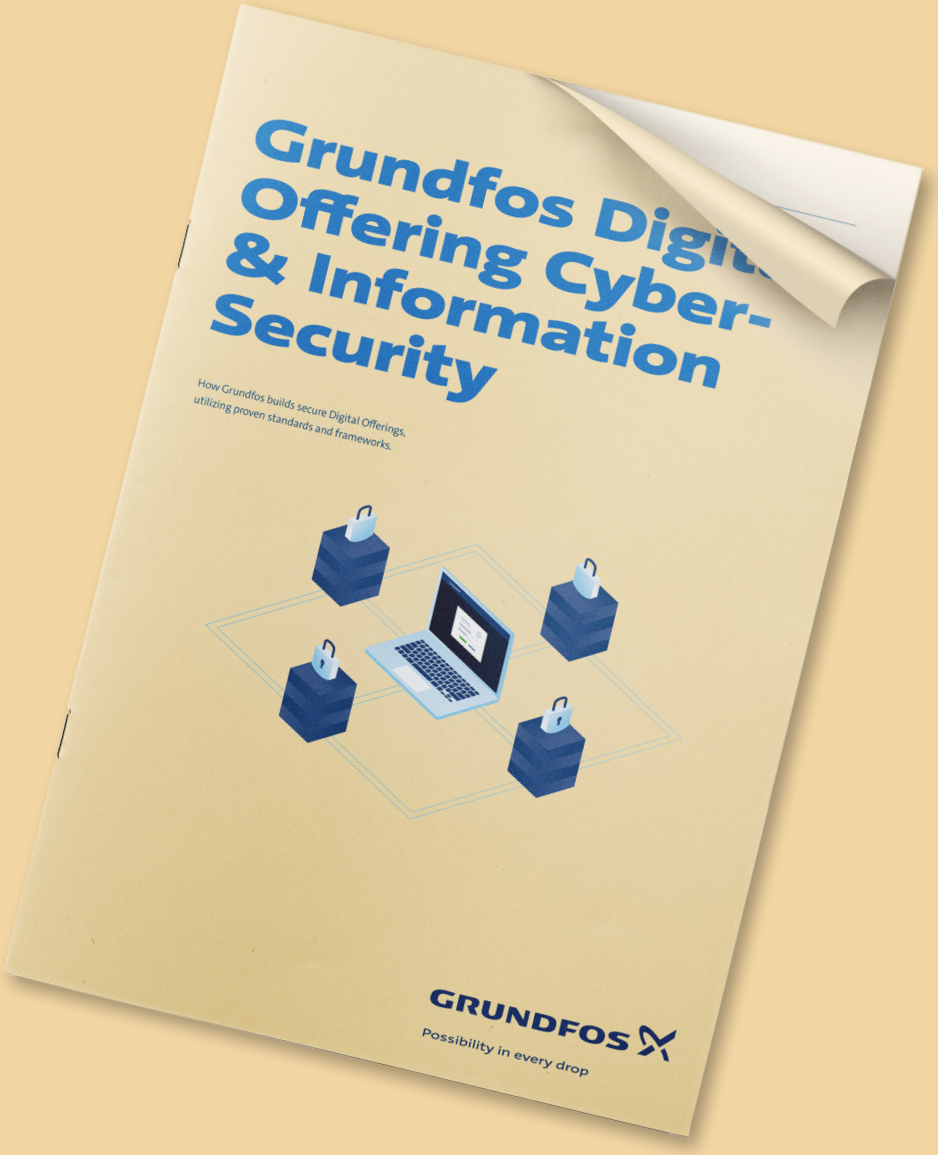
Grundfos Connect Asset Monitor

Anwendungshinweis zur Sicherheit



GRUNDFOS

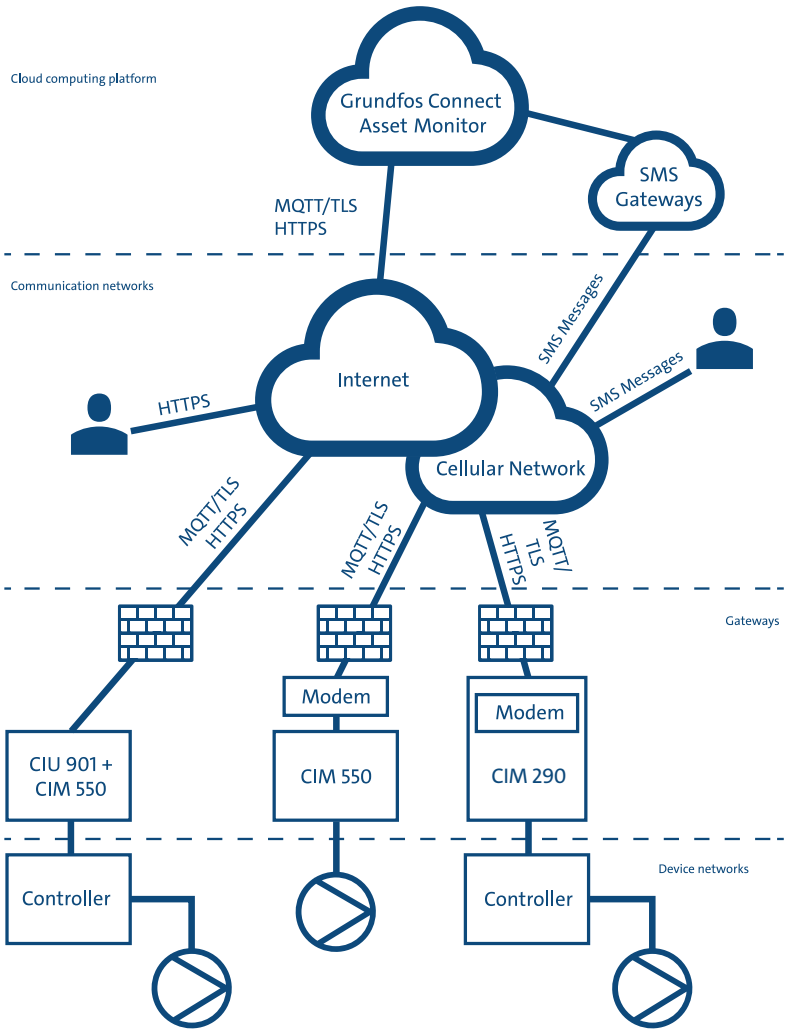
Possibility in every drop

Einführung

Grundfos Connect Asset Monitor ist als internetbasiertes Plug&Play-System eine effiziente und kostengünstige Alternative zu teureren SCADA-Systemen. Sie erhalten damit die vollständige Kontrolle über Ihre Grundfos-Geräte, und zwar von überall her. Es verfügt über eine Reihe von Sicherheitsfunktionen, die Ihnen Schutz und einen sorgenfreien Betrieb bieten.

Diese Funktionen werden in diesem Dokument beschrieben.

Die Sicherheitsarchitektur



Sicherheitsarchitektur

Wie oben gezeigt, umfasst die Sicherheitsarchitektur von Grundfos Connect Asset Monitor eine Computing-Plattform, auf der Grundfos Connect Asset Monitor läuft, mehrere Kommunikationsnetzwerke, Gateways zur Steuerung der Verbindung sowie die physische Infrastruktur der lokalen Systeme, die die Pumpen steuern.
Alle TCP/IP-Daten, die an und von Geräten gesendet werden, die mit dem Netzwerk verbunden sind, sind jederzeit verschlüsselt.

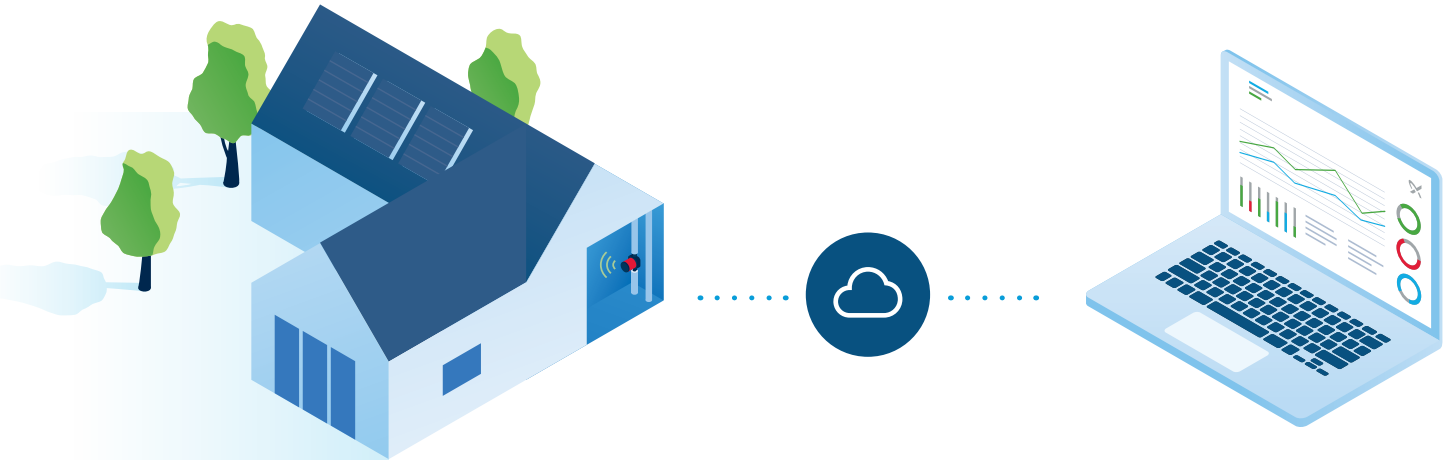
Mehr über die Grundprinzipien von Grundfos Connect Asset Monitor können Sie im Grundfos Whitepaper zur Cyber- und Informationssicherheit auf Grundfos.de nachlesen.

Funktionsweise

Grundfos Connect Asset Monitor besteht aus vier Komponenten, mit denen sich die Software schnell und sicher mit Ihren Anlagen verbinden kann.

- **Cloud-Computing-Plattform**
- **Kommunikationsnetzwerke**
- **Gateways**
- **Gerätenetzwerke**

Grundfos Connect Asset Monitor



Cloud-Computing-Plattform

Grundfos Connect Asset Monitor besteht aus einer Reihe von Backend-Diensten: Ein IoT-Endpunktdienst und ein Authentifizierungsdienst. Der IoT-Endpunktdienst ist für die allgemeine Kommunikation mit Geräten zuständig, während der Authentifizierungsdienst die Geräte authentifiziert und auswählt, welchen IoT-Endpunkt die Geräte für die Kommunikation verwenden sollen. Grundfos Connect Asset Monitor verwendet für die gegenseitige Authentifizierung ein Schema, das auf X.509-Zertifikaten basiert.

Zu den Backend-Diensten gehören außerdem Speicher-, Autorisierungs- und Benachrichtigungsdienste. Zudem können spezialisierte SMS-Gateways Textnachrichten an Systemanwender senden.

Die Backend-Dienste werden in einer hochskalierbaren Cloud-Infrastruktur gehostet, die durch moderne Sicherheitstechnologien der nächsten Generation geschützt ist, unter anderem Reverse Proxys mit Layer7-Filterung und Verkehrsanalyse, Web Application Firewalls (WAF) und DDoS-Schutzmechanismen (Distributed Denial of Service).

Kommunikationsnetzwerke

Grundfos Connect Asset Monitor nutzt das Internet oder das Mobilfunknetz je nach den Anforderungen des Kunden und der verfügbaren physischen Infrastruktur.

Gateways initiieren HTTPS-Verbindungen über das Netzwerk, um eine Verbindung mit dem Authentifizierungsdienst herzustellen. HTTPS ist die sichere Version von HTTP und verwendet Transport Level Security (TLS).
Wenn dem Gateway ein IoT-Endpunkt zugewiesen wurde, stellt das Gateway die Verbindung mit dem IoT-Endpunkt über MQTT/TLS her, um mit Grundfos Connect Asset Monitor zu kommunizieren.
Gateways verwenden für die gegenseitige Authentifizierung ein auf X.509-Zertifikaten basierendes Schema, bei dem sowohl Server als auch Client authentifiziert werden.

Nutzer greifen über einen Webclient auf Grundfos Connect Asset Monitor zu. Der Webclient verwendet HTTPS und kann überall verwendet werden, wo Internetzugang besteht. Die Benutzerauthentifizierung erfolgt über den Grundfos-Identitätsanbieter (Global Login). Sie können zusätzliche Nutzer Ihrer Organisation einladen, die den Erstellungsprozess in Global Login durchlaufen müssen.

Grundfos Connect Asset Monitor sendet E-Mails oder SMS an Nutzer, die Benachrichtigungen abonniert haben.

Gateways

Grundfos-Richtlinien für den Umgang mit angeschlossenen Produkten stehen auf grundfos.de zur Verfügung und sollten zu Ihrer Sicherheit immer befolgt werden.

Das CIM 290 ist eine Schnittstelle für die Datenübertragung über ein 3G- oder 4G-Netz, während das CIM 550 in Ethernet-basierten Netzen eingesetzt wird.
Sowohl das CIM 290 als auch das CIM 550 übertragen Daten zwischen dem Netzwerk (in dem sich das Gerät befindet) und Grundfos Connect Asset Monitor über sichere TLS-Verbindungen. Sie können in verschiedenen physischen Konfigurationen installiert werden, beispielsweise in einem Grundfos-Produkt mit CIM-Steckplatz oder in einer Schnittstelleneinheit CIU 900/901.

Gateways werden den Nutzern in einem Prozess zugewiesen, bei dem die Geräte physisch zugänglich sein müssen.

Verwendung von Firewalls

Da immer die Gateways die Verbindung mit Grundfos Connect Asset Monitor initiieren, sollten keine eingehenden Verbindungen über die Firewall zugelassen werden.
Wenn Sie eine externe Firewall verwenden, stellen Sie sicher, dass sie ausgehende Verbindungen über HTTPS und MQTT/TLS zulässt.

Gerätenetzwerke

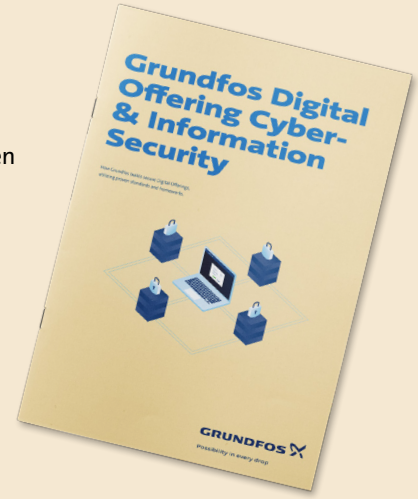
Im Bereich für Gerätenetzwerke wird sämtliche funktionsfähige Hardware wie Steuerungen, Pumpen und andere Geräte in die Systemarchitektur eingebunden. Sie können über serielle Feldbusse miteinander sowie mit den Systemgateways kommunizieren. Keine Kommunikation in diesem Bereich basiert auf TCP/IP.

Zusammenfassung

Gerätekommunikation: Kommunikation über seriellen Feldbus (nicht TCP/IP)
WAN-Kommunikation: HTTPS und MQTT/TLS (mit TLS 1.2) über Ethernet oder Mobilfunk (3G/4G)
Benutzerkommunikation: HTTPS (mit TLS 1.2) und E-Mail/SMS für Benachrichtigungen

Grundfos Connect Asset Monitor-Authentifizierung: X.509-Zertifikate
Benutzerauthentifizierung: Benutzername/Passwort
Gateway-Authentifizierung: X. 509-Zertifikate

Software-Update: Over-the-Air, durch TLS geschützt
Verfügbarkeit: Redundante, virtualisierte Anwendungsdienste
Betrieb: Penetrationstest, Bedrohungsmodell sowie kontinuierliche Protokollierung und Überwachung



Haben Sie Fragen?
Zögern Sie nicht, uns zu kontaktieren:

Michael Sandholm
Product Owner
Digital Development
msandholm@grundfos.com

Grundfos Pumpen Vertrieb Ges.m.b.H.
Grundfosstraße 2
AT-5082 Grödig
Tel. +43 6246 883 0
www.grundfos.at

GRUNDFOS