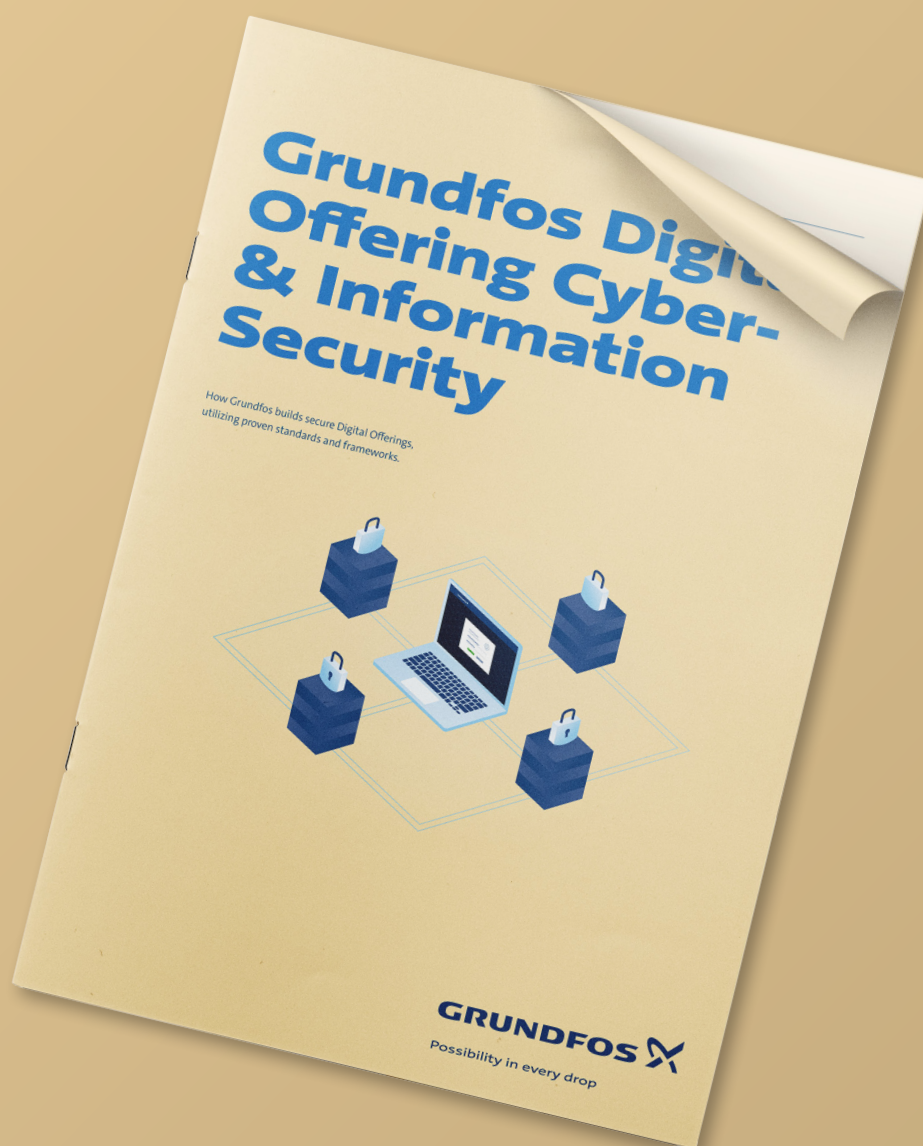


# Grundfos Connect Asset Monitor

Nota applicativa sulla sicurezza



**GRUNDFOS** 

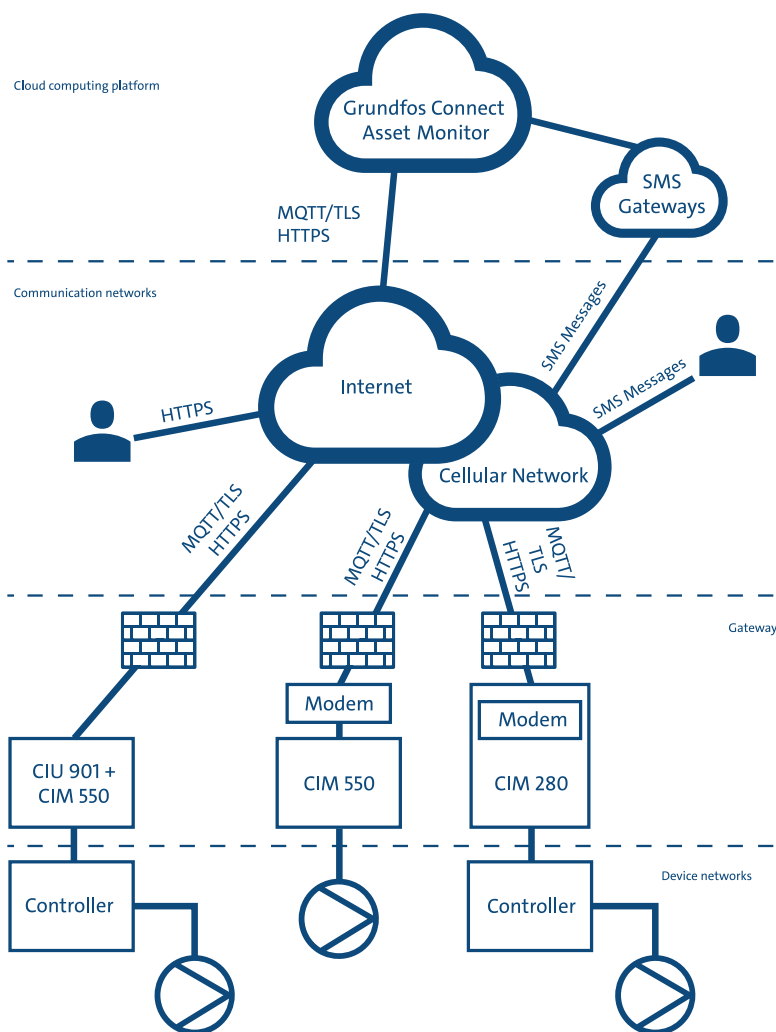
Possibility in every drop

## **Introduzione**

Grundfos Connect Asset Monitor è un sistema plug & play progettato per garantire un monitoraggio affidabile ed efficiente degli asset, grazie all'accesso da remoto. Una soluzione smart che rappresenta una valida alternativa ai tradizionali sistemi SCADA, riducendo sia la complessità che i costi di implementazione. Con Grundfos Connect Asset Monitor hai pieno controllo sui tuoi dispositivi Grundfos, ovunque ti trovi. Il sistema integra funzionalità di sicurezza avanzate, pensate per offrire protezione operativa e tranquillità gestionale.

In questo documento trovi tutti i dettagli.

# Architettura del Sistema di Sicurezza



## Architettura del Sistema di Sicurezza

Come illustrato sopra, l'architettura del sistema di sicurezza di Asset Monitor prevede una piattaforma di elaborazione sulla quale il sistema viene eseguito, diverse reti di comunicazione, gateway che gestiscono le connessioni e un'infrastruttura fisica dei sistemi locali che controllano le pompe. La trasmissione di tutti i dati TCP/IP da e verso i dispositivi connessi alla rete è costantemente protetta tramite crittografia.

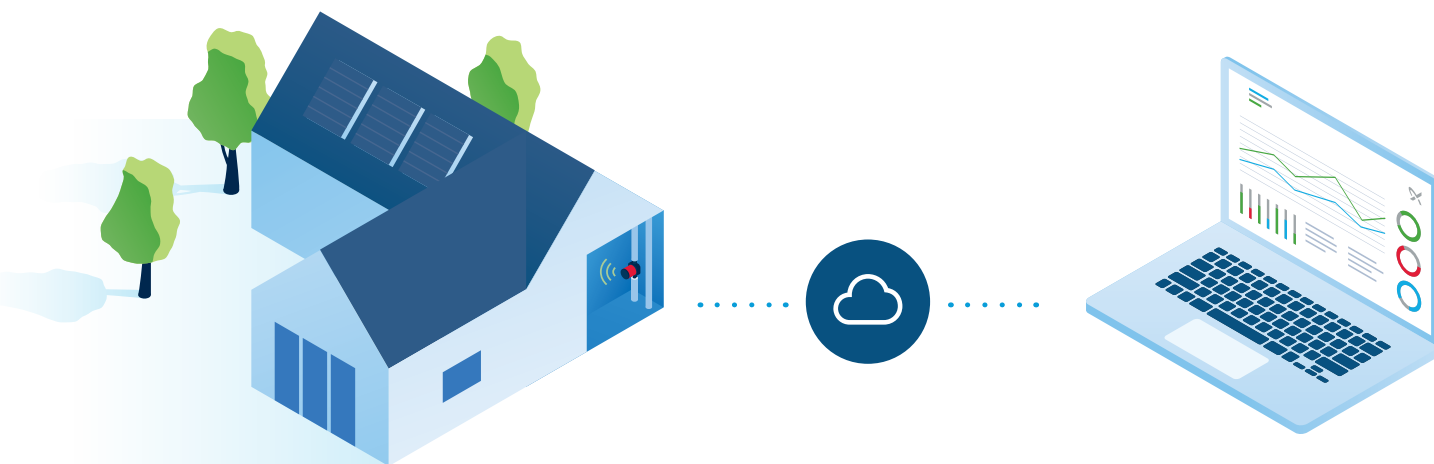
Approfondisci le linee guida di Asset Monitor nel documento tecnico Grundfos dedicato alla sicurezza informatica, disponibile su [Grundfos.it](http://Grundfos.it).

## Come funziona

Asset Monitor dispone di quattro componenti principali che facilitano una connessione rapida e sicura ai sistemi:

- **Piattaforma cloud**
- **Reti di comunicazione**
- **Gateway di rete**
- **Rete dei dispositivi**

# Grundfos Connect Asset Monitor



## Piattaforma cloud

Asset Monitor è composto da due diversi servizi backend: un servizio endpoint IoT e un servizio di autenticazione. Il servizio endpoint IoT gestisce la comunicazione generale con i dispositivi, mentre il servizio di autenticazione si occupa dell'autenticazione dei dispositivi e della selezione dell'endpoint IoT da utilizzare per la comunicazione. Asset Monitor utilizza un sistema di autenticazione reciproca basato su certificati X.509.

I servizi backend includono anche funzionalità di archiviazione, autorizzazione e notifiche. Inoltre, gateway SMS specializzati possono inviare messaggi di testo agli utenti del sistema.

I servizi backend sono ospitati in un'infrastruttura cloud altamente scalabile, protetta da tecnologie di sicurezza moderne e di nuova generazione, come proxy inversi con filtraggio Layer 7 e analisi del traffico, firewall per applicazioni web (WAF) e meccanismi di protezione contro attacchi DDoS (Distributed Denial of Service).

## Reti di comunicazione

Asset Monitor utilizza la rete Internet o la rete cellulare, a seconda delle esigenze del cliente e dell'infrastruttura fisica disponibile.

I gateway avviano connessioni HTTPS attraverso la rete per collegarsi al servizio di autenticazione. HTTPS è la versione sicura di HTTP che utilizza il protocollo TLS (Transport Level Security). Una volta assegnato un endpoint IoT, il gateway si connette a quest'ultimo utilizzando il protocollo MQTT su TLS per proseguire la comunicazione con Asset Monitor. I gateway utilizzano un sistema di autenticazione reciproca basato su certificati X.509, in cui sia il server che il client vengono autenticati.

Gli utenti accedono ad Asset Monitor tramite un'interfaccia web. L'interfaccia utilizza una connessione HTTPS ed è accessibile ovunque ci sia una connessione internet. L'autenticazione degli utenti è garantita tramite l'identity provider di Grundfos (Global Login). È possibile invitare altri utenti appartenenti alla tua organizzazione, i quali dovranno completare la registrazione dell'account tramite Global Login.

Asset Monitor invierà email o SMS agli utenti che hanno attivato gli avvisi.

### Gateway di rete

Le linee guida Grundfos per la gestione dei prodotti connessi sono disponibili su [grundfos.com](http://grundfos.com) e vanno sempre seguite per garantire la sicurezza degli utenti.

La CIM 280 è un'interfaccia per la trasmissione dati su rete 3G o 4G, a differenza della CIM 550, che utilizza la rete ethernet. Sia la CIM 280 che la 550 trasferiscono i dati tra la rete a cui è connesso il dispositivo e Asset Monitor tramite connessioni sicure TLS. Possono essere installati in diverse configurazioni, ad esempio in un prodotto Grundfos con slot CIM o in un'unità di interfaccia CIU 900/901.

Per assegnare un gateway a un utente è necessario intervenire fisicamente sui dispositivi.

### Uso di firewall

Poiché i gateway stabiliscono connessioni in uscita verso Asset Monitor, non è necessario autorizzare connessioni in entrata attraverso il firewall.

Nel caso si utilizzi un firewall esterno, è importante assicurarsi che siano abilitate le connessioni in uscita tramite i protocolli HTTPS e MQTT/TLS.

### Rete dei dispositivi

La sezione della rete dei dispositivi rappresenta il livello dell'architettura di sistema in cui vengono integrati tutti i componenti hardware operativi, come controller e pompe. Questi elementi possono comunicare tra loro e con i gateway di sistema tramite Fieldbus. Nessuna comunicazione avviene tramite protocolli TCP/IP.

### Riepilogo

**Comunicazione con i dispositivi:** Comunicazione seriale con Fieldbus (non TCP/IP)

**Comunicazione WAN:** HTTPS e MQTT/TLS (utilizzando TLS 1.2) su ethernet o cellulare (3G/4G)

**Comunicazione con l'utente:** HTTPS (utilizzando TLS 1.2) e e-mail/SMS per le notifiche

**Autenticazione Grundfos Connect Assets Monitor:** certificati X.509

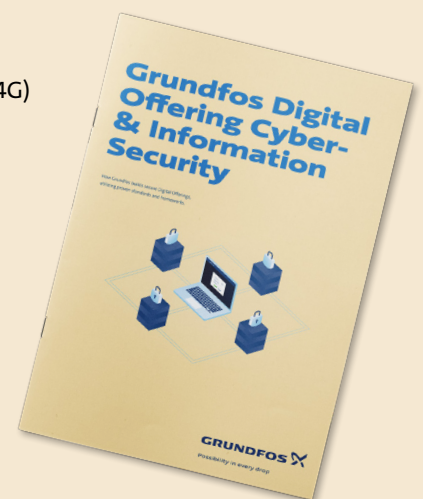
**Autenticazione utente:** Nome utente / password

**Autenticazione gateway:** X. Certificati 509

**Aggiornamento software:** Over-the-air con protocollo TLS

**Disponibilità:** I servizi applicativi sono configurati in modo ridondante su un'infrastruttura virtuale, per garantire continuità operativa.

**Operazioni:** Test di penetrazione, analisi delle minacce e monitoraggio continuo



**Domande?**

Non esitare a contattarci:

**Michael Sandholm**  
Product Owner  
Digital Development  
[msandholm@grundfos.it](mailto:msandholm@grundfos.it)