Grundfos Connect Asset Monitor

Notă privind securitatea aplicației

GRUNDFOS

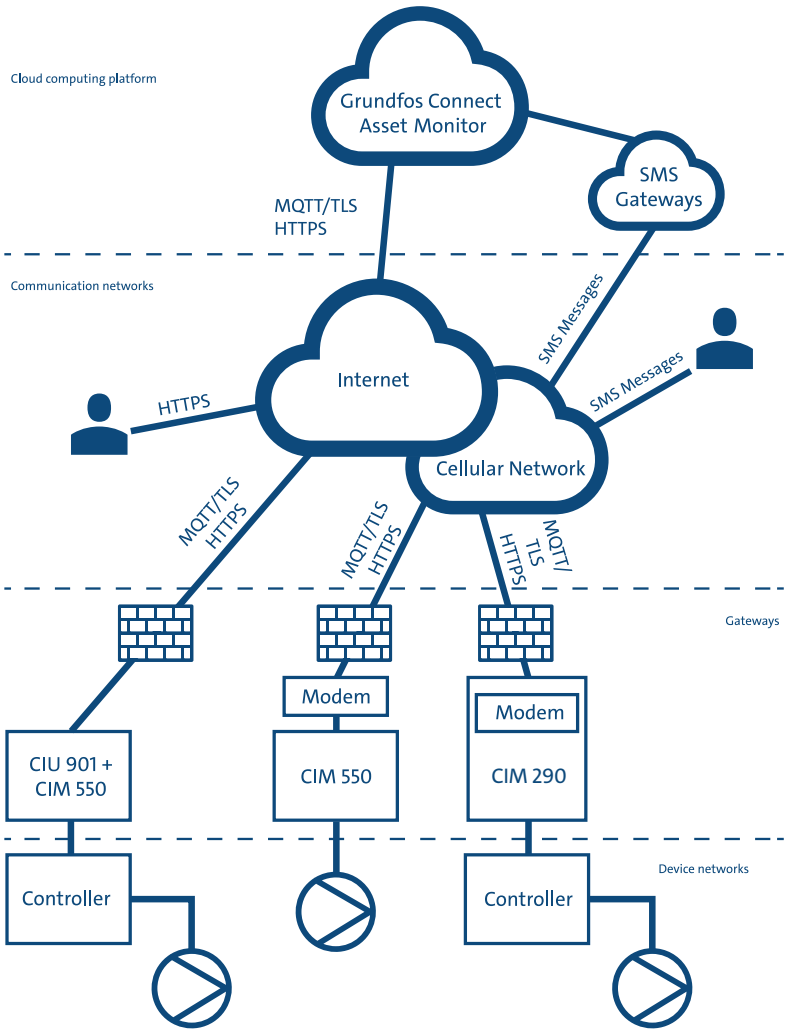
Possibility in every drop

Introducere

Grundfos Connect Asset Monitor este un sistem tip plug-and-play bazat pe Internet, care vă oferă o alternativă eficientă și rentabilă la sistemele SCADA mai scumpe. Aveți control complet asupra dispozitivelor Grundfos, indiferent unde vă aflați. Sistemul are o serie de elemente de securitate care vă oferă atât protecție, cât și liniște.

Acest document prezintă în detaliu aceste elemente.

Arhitectura de securitate



Arhitectură de securitate

După cum s-a explicat anterior, arhitectura de securitate a soluției Asset Monitor include o platformă digitală pe care rulează Asset Monitor, mai multe rețele de comunicații, gateway-uri care controlează conexiunea și infrastructura fizică a sistemelor localizate ce controlează pompele. Toate datele TCP/IP trimise către și de la dispozitivele conectate la rețea sunt criptate tot timpul.

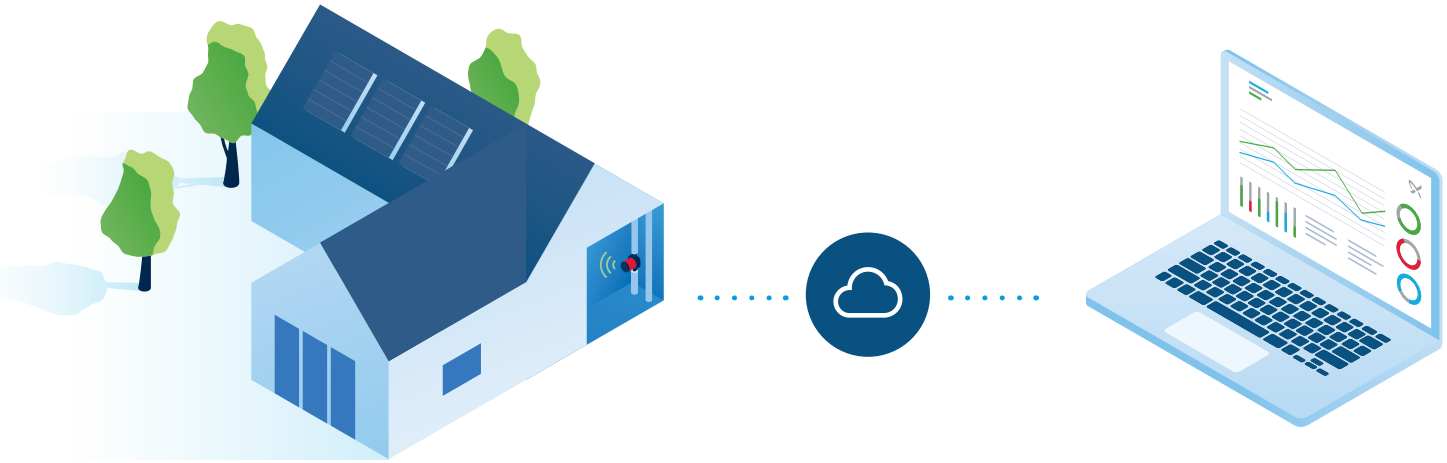
Puteți citi mai multe despre principiile pe care le respectă Asset Monitor în cartea albă publicată de Grunfos referitoare la securitatea cibernetică și a informațiilor, disponibilă pe Grundfos.ro.

Cum funcționează

Asset Monitor are patru componente cu ajutorul cărora se poate conecta rapid și sigur la sistemele dumneavoastră.

- **Platformă de cloud computing**
- **Rețele de comunicații**
- **Gateway-uri**
- **Rețele de dispozitive**

Grundfos Connect Asset Monitor



Platformă de cloud computing
Asset Monitor este alcătuit din mai multe servicii de backend: un serviciu endpoint de tip IoT și un serviciu de autentificare. Serviciul endpoint de tip IoT se ocupă de comunicarea generală cu dispozitivele, în timp ce serviciul de autentificare se ocupă de autentificarea dispozitivelor și selectează ce endpoint IoT trebuie să utilizeze dispozitivele pentru comunicare. Asset Monitor utilizează o schemă de autentificare reciprocă bazată pe certificate X.509.

Serviciile de backend includ, de asemenea, servicii de stocare, autorizare și notificare, iar gateway-urile SMS specializate pot trimite mesaje text utilizatorilor sistemului.

Serviciile de backend sunt găzduite într-o infrastructură de cloud cu scalabilitate ridicată, protejată prin tehnologii de securitate moderne și de ultimă generație, cum ar fi proxy-uri inverse cu filtrare Layer7 și analiză de trafic, mecanisme de protecție precum Web Application Firewalls (WAF) și DDoS (Distributed Denial of Service).

Rețele de comunicații
Asset Monitor utilizează Internetul sau rețeaua celulară, în funcție de cerințele clientului și de infrastructura fizică disponibilă.

Gateway-urile inițiază conexiuni HTTPS prin rețea pentru a se conecta la serviciul de autentificare. HTTPS este versiunea securizată a protocolului HTTP care utilizează Transport Level Security (TLS).
Când se alocă un endpoint de tip IoT, gateway-ul se conectează la endpoint-ul de tip IoT cu MQTT/TLS pentru a continua comunicarea cu Asset Monitor.
Gateway-urile utilizează o schemă de autentificare reciprocă bazată pe certificate X.509, în care sunt autentificate atât serverul, cât și clientul.

Utilizatorii accesează Asset Monitor cu un client web. Clientul web folosește HTTPS și poate fi utilizat oriunde există acces la Internet. Autentificarea utilizatorului este realizată prin intermediul furnizorului de identitate Grundfos (Global Login - Autentificare globală). Puteți să invitați utilizatori suplimentari din organizația dumneavoastră și aceștia trebuie să parcurgă pașii pentru Global Login.

Asset Monitor va trimite e-mailuri sau mesaje text utilizatorilor care s-au abonat la alerte.

Gateway-uri

Instrucțiunile Grundfos privind gestionarea produselor conectate sunt disponibile pe grundfos.com și pentru siguranța dumneavoastră, ele trebuie respectate întotdeauna.

CIM 290 este o interfață utilizată pentru transmiterea de date printr-o rețea 3G sau 4G, în timp ce CIM 550 se utilizează în rețelele bazate pe Ethernet.
Atât CIM 290, cât și CIM 550 transferă date între rețeaua unde se află dispozitivul și Asset Monitor prin conexiuni TLS securizate. Acestea pot fi instalate în diferite configurații fizice, cum ar fi într-un produs Grundfos cu un slot CIM sau într-o unitate de interfață CIU 900/901.

Gateway-urile sunt alocate utilizatorilor în cadrul unui proces care necesită acces fizic la echipament.

Utilizarea de firewall-uri

Întrucât gateway-urile inițiază întotdeauna conexiunea la Asset Monitor, nu trebuie permise conexiuni de intrare prin firewall.
Când utilizați un firewall extern, asigurați-vă că acesta permite conexiuni de ieșire prin HTTPS și MQTT/TLS.

Rețele de dispozitive

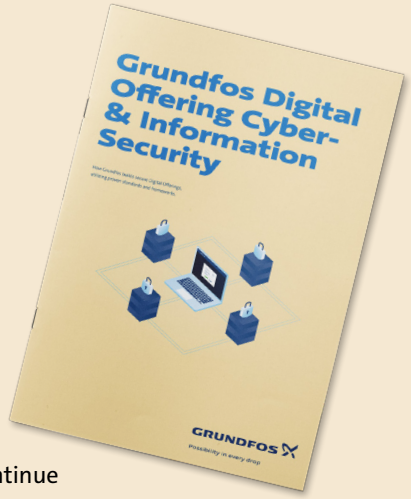
Secțiunea „rețea de dispozitive” este locul unde toate echipamentele de lucru, cum ar fi controlere, pompe și alte dispozitive sunt plasate în arhitectura sistemului. Acestea pot comunica între ele, precum și cu gateway-urile de sistem, prin magistrale de câmp seriale. Nicio comunicare din această secțiune nu este bazată pe TCP/IP.

Rezumat

Comunicare între dispozitive: Comunicare prin magistrală serială (nu prin TCP/IP)
Comunicare WAN: HTTPS și MQTT/TLS (folosind TLS 1.2) prin Ethernet sau rețea celulară (3G/4G)
Comunicare cu utilizatorul: HTTPS (folosind TLS 1.2) și e-mail/SMS pentru notificări

Autentificare în Grundfos Connect Assets Monitor: Certificate X.509
Autentificare utilizator: Nume de utilizator/parolă
Autentificare gateway: Certificate X. 509

Actualizare software: Over-the-air (wireless), protejată de TLS
Disponibilitate: Configurare de servicii de aplicații virtualizate redundante
Operațiuni: Test de penetrare, model de amenințare și înregistrare și monitorizare continue



Aveți întrebări?
Nu ezitați să contactați:

Michael Sandholm
Proprietar al produsului
Dezvoltare digitală
msandholm@grundfos.ro

Grundfos Pompe Romania S.R.L.
S-Park, Tipografilor st. 11-15
Building A2, Floor 2 Sector 1
Bucharest Romania
Tel: (+40) 21 2004 100
www.grundfos.ro

GRUNDFOS