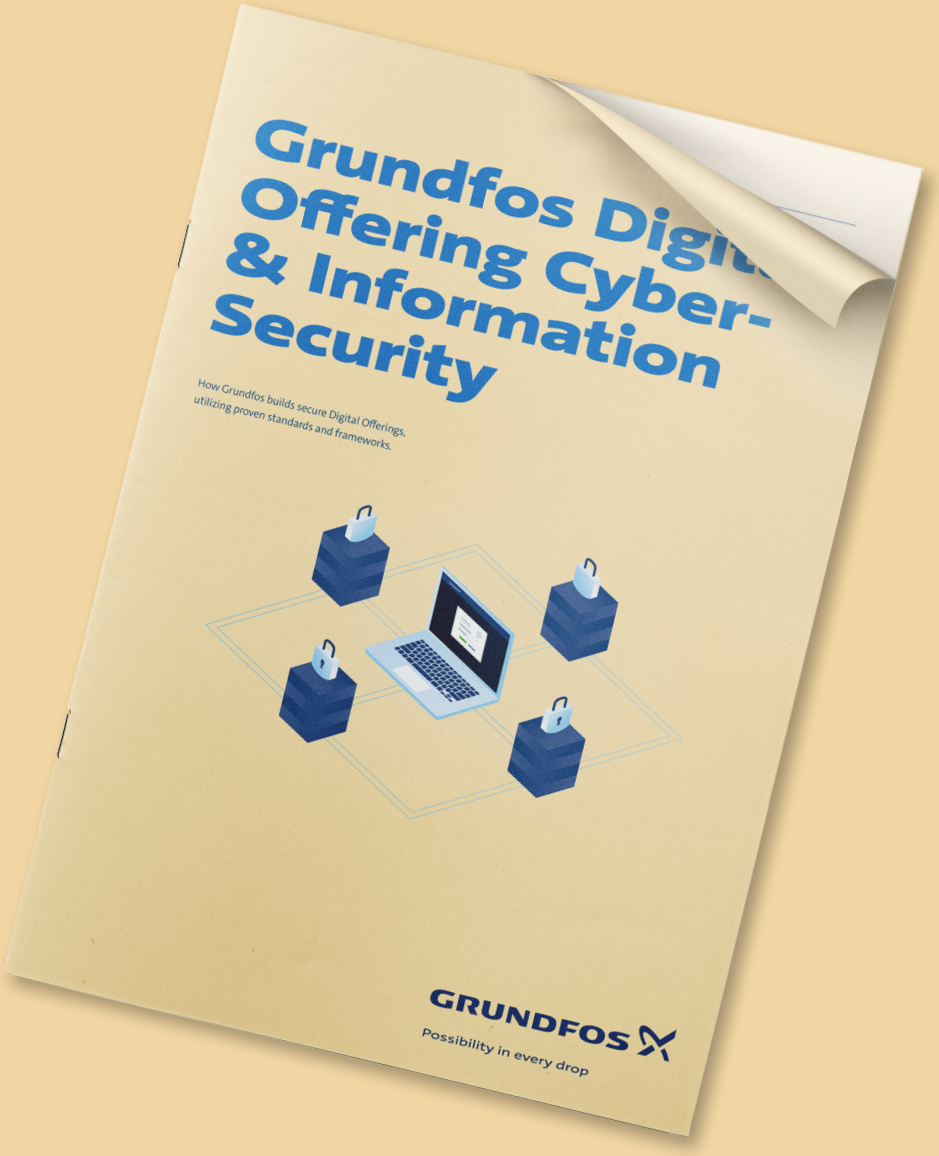
Grundfos Connect Asset Monitor

Napomena o bezbednosnoj primeni



GRUNDFOS

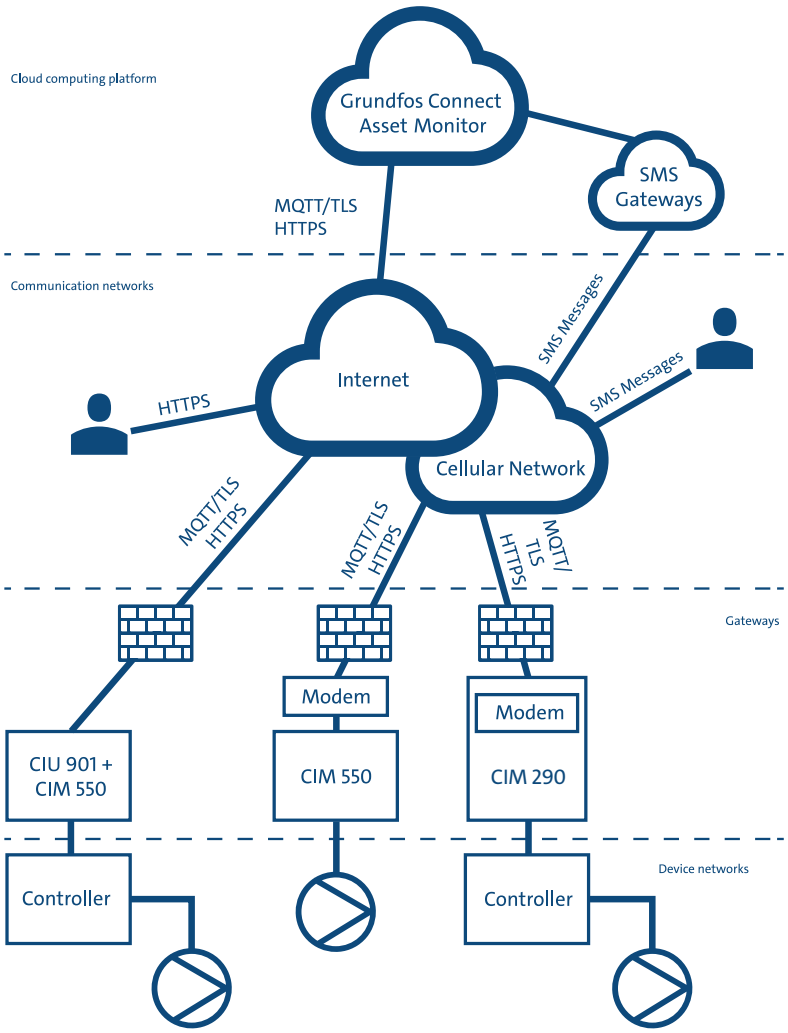
Possibility in every drop

Uvod

Grundfos Connect Asset Monitor je „plug & play“ sistem baziran na internetu, koji vam pruža efikasnu i isplativu alternativu skupljim SCADA sistemima. Daje vam potpunu kontrolu nad vašim Grundfos uređajima, bez obzira gde se nalazite. Ima niz bezbednosnih funkcija koje vam pružaju i zaštitu i duševni mir.

Ovaj dokument detaljno opisuje o čemu je tačno reč.

Bezbednosna arhitektura



Bezbednosna arhitektura

Kao što je gore prikazano, bezbednosna arhitektura Asset Monitor sistema uključuje računarsku platformu na kojoj Asset Monitor radi, više komunikacionih mreža, mrežne prolaze koje kontrolišu vezu i fizičku infrastrukturu lokalizovanih sistema koji kontrolišu pumpe.
Svi TCP/IP podaci poslati na i sa uređaja povezanih na mrežu su u svakom trenutku šifrovani.

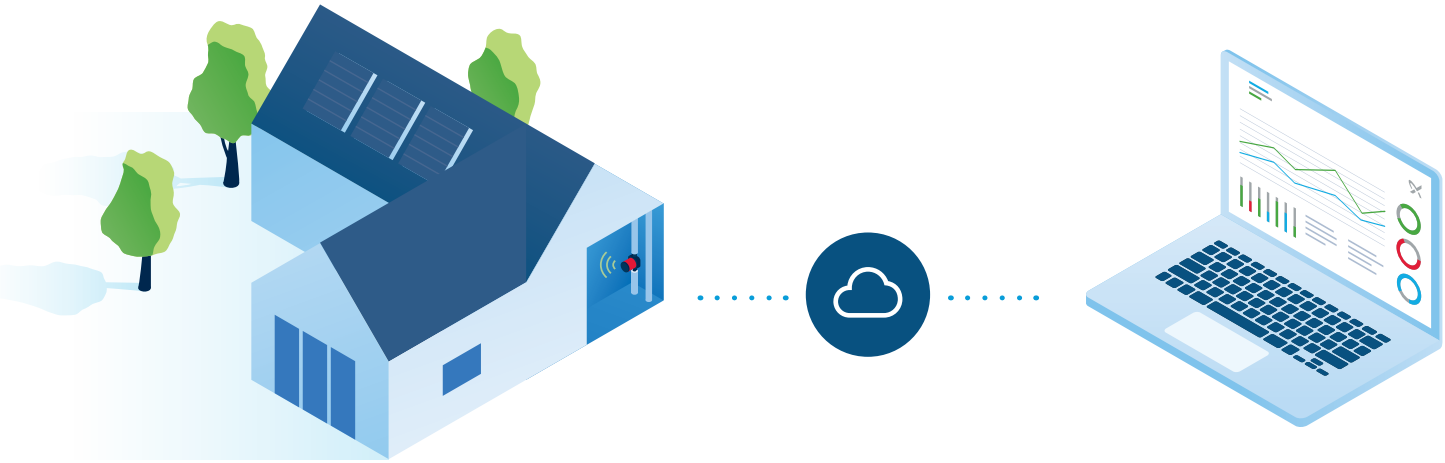
Više o principima kojih se Asset Monitor pridržava možete pročitati u Grundfos dokumentu o sajber i informacionoj bezbednosti koji se nalazi na Grundfos.com.

Kako funkcioniše

Asset Monitor ima četiri komponente koje mu pomažu da se brzo i bezbedno poveže sa vašim sistemima.

- **Računarska platforma u oblaku**
- **Komunikacione mreže**
- **Mrežni prolazi**
- **Mreže uređaja**

Grundfos Connect Asset Monitor



Računarska platforma u oblaku

Asset Monitor se sastoji od niza bekend servisa: IoT servisa krajnje tačke i servisa za autentifikaciju. IoT servis krajnje tačke obrađuje opštu komunikaciju sa uređajima, dok servis za autentifikaciju obrađuje autentifikaciju uređaja i bira koju IoT krajnju tačku uređaj treba da koristi za komunikaciju. Asset Monitor koristi šemu međusobne autentifikacije zasnovanu na X.509 sertifikatima.

Bekend servisi takođe uključuju usluge skladištenja, autorizacije i obaveštavanja, a specijalizovani SMS mrežni prolazi mogu da šalju tekstualne poruke korisnicima sistema.

Bekend servisi se nalaze u visoko skalabilnoj infrastrukturi u oblaku, zaštićenoj modernim i bezbednosnim tehnologijama sledeće generacije, kao što su obrnuti proksiji sa filtriranjem i analizom saobraćaja Layer7, zaštitni zidovi veb aplikacija (WAF) i mehanizmi zaštite od distribuiranog uskraćivanja usluge (DDoS).

Komunikacione mreže

Asset Monitor koristi internet ili mobilnu mrežu, u zavisnosti od zahteva klijenta i dostupne fizičke infrastrukture.

Mrežni prolazi pokreću HTTPS veze preko mreže kako bi se povezali sa servisom za autentifikaciju. HTTPS je bezbedna verzija HTTP-a koja koristi Transport Level Security (TLS). Kada mu se dodeli IoT krajnja tačka, mrežni prolaz će se povezati sa IoT krajnjom tačkom koristeći MQTT/TLS da bi nastavio komunikaciju sa Asset Monitor sistemom. Mrežni prolazi koriste šemu međusobne autentifikacije zasnovanu na X.509 sertifikatima gde su i server i klijent autentifikovani.

Korisnici pristupaju Asset Monitor sistemu pomoću veb klijenta. Veb klijent koristi HTTPS i može se koristiti bilo gde sa pristupom internetu. Autentifikacija korisnika je obezbeđena putem Grundfos provajdera identiteta (Global Login). Možete pozvati dodatne korisnike koji pripadaju vašoj organizaciji i oni će morati da prođu kroz proces kreiranja u Global Login sistemu.

Asset Monitor će slati imejlove ili SMS-ove korisnicima koji su se pretplatili na upozorenja.

Mrežni prolazi

Grundfos smernice za rukovanje povezanim proizvodima dostupne su na grundfos.com i uvek ih treba poštovati radi vaše bezbednosti.

CIM 290 je interfejs koji se koristi za prenos podataka putem 3G ili 4G mreže, dok se CIM 550 koristi na mrežama zasnovanim na eternetu.
I CIM 290 i CIM 550 prenose podatke između mreže na kojoj se uređaj nalazi i Asset Monitor-a putem bezbednih TLS veza. Mogu se instalirati u različitim fizičkim konfiguracijama, kao što je u Grundfos proizvodu sa CIM slotom ili u CIU 900/901 interfejs jedinici.

Mrežni prolazi se dodeljuju korisnicima u procesu koji zahteva fizički pristup opremi.

Korišćenje zaštitnih zidova

Pošto mrežni prolazi uvek iniciraju vezu sa Asset Monitor sistemom, ne smeju se dozvoliti dolazne veze kroz zaštitni zid.
Kada koristite spoljni zaštitni zid, uverite se da on dozvoljava odlazne veze putem HTTPS i MQTT/TLS.

Mreže uređaja

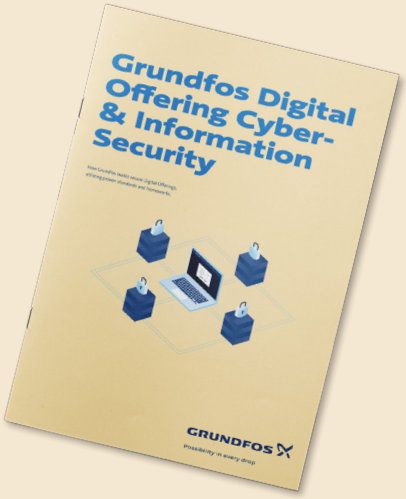
Odeljak mreže uređaja je mesto gde se sav radni hardver, kao što su kontroleri, pumpe i drugi uređaji, postavlja na sistemsku arhitekturu. Mogu da komuniciraju jedni sa drugima, kao i sa sistemskim mrežnim prolazima, putem serijskih magistrala. Nijedna komunikacija u ovom odeljku nije zasnovana na TCP/IP-u.

Rezime

Komunikacija uređaja: Serijska komunikacija preko fieldbus-a (ne TCP/IP)
WAN komunikacija: HTTPS i MQTT/TLS (koristeći TLS 1.2) preko eterneta ili mobilne mreže (3G/4G)
Komunikacija sa korisnikom: HTTPS (koristeći TLS 1.2) i e-pošta/SMS za obaveštenja

Autentifikacija Grundfos Connect Assets Monitor sistema: X.509 sertifikati
Autentifikacija korisnika: Korisničko ime / lozinka
Autentifikacija putem mrežnog prolaza: X. 509 sertifikati

Ažuriranje softvera: Zaštićeno preko mreže putem TLS-a
Dostupnost: Podešavanje redundantnih virtuelizovanih aplikacijskih usluga
Operacije: Test penetracije, model pretnji i kontinuirano evidentiranje i praćenje



0326/WU/A017410-Brandbox

Grundfos Srbija D.O.O.
Omladinskih brigada 90V
11070 New Belgrade, Serbia
Tel: (+381) 11 2258 740
www.grundfos.rs

GRUNDFOS