Grundfos Connect Asset Monitor

Notering beträffande säkerhetsapplikationen

GRUNDFOS

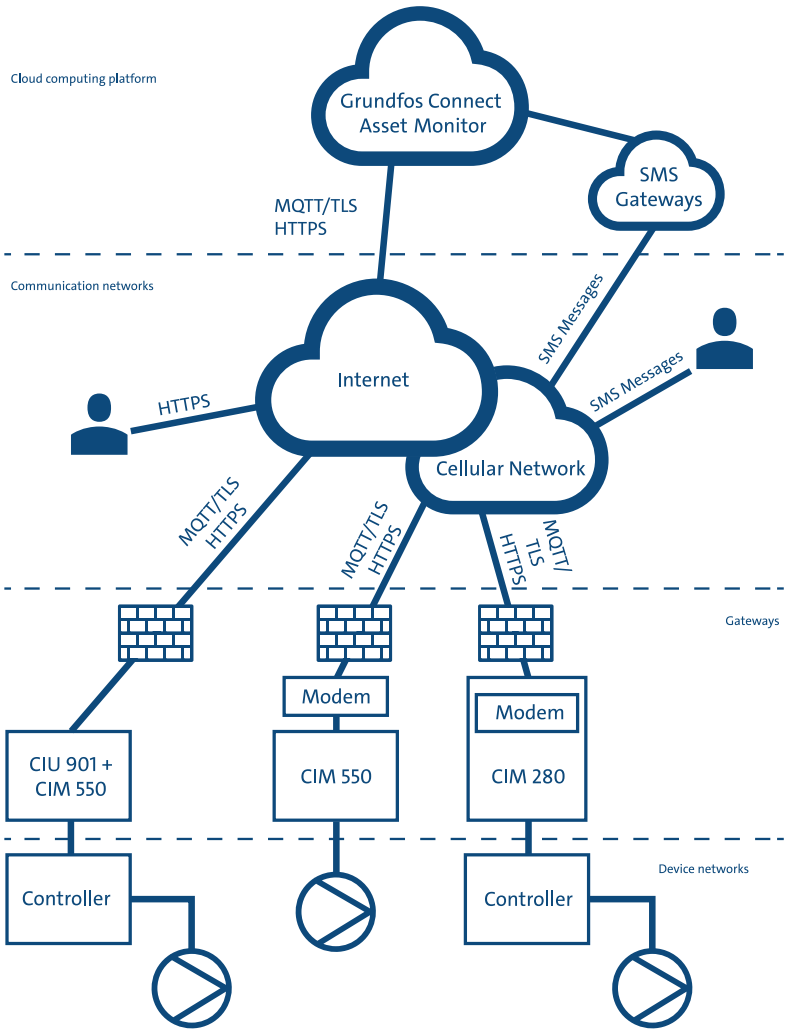
Possibility in every drop

Inledning

Grundfos Connect Asset Monitor är ett molnbaserat plug & play-system som ger dig ett säkert och kostnadseffektivt alternativ till dyrare SCADA-system. Det ger dig fullständig kontroll över dina Grundfos-enheter, oavsett var du befinner dig. Den har ett antal säkerhetsfunktioner som ger dig både skydd och trygghet.

Detta dokument beskriver dessa funktioner.

Säkerhetsarkitekturen



Säkerhetsarkitekturen

Som visas ovan omfattar säkerhetsarkitekturen för Asset Monitor en datorplattform på vilken Asset Monitor körs, flera kommunikationsnät och gateways som styr anslutningen och den fysiska infrastrukturen för de lokala system som styr pumparna.
Alla TCP/IP-data som skickas till och från enheter anslutna till nätverket krypteras hela tiden.

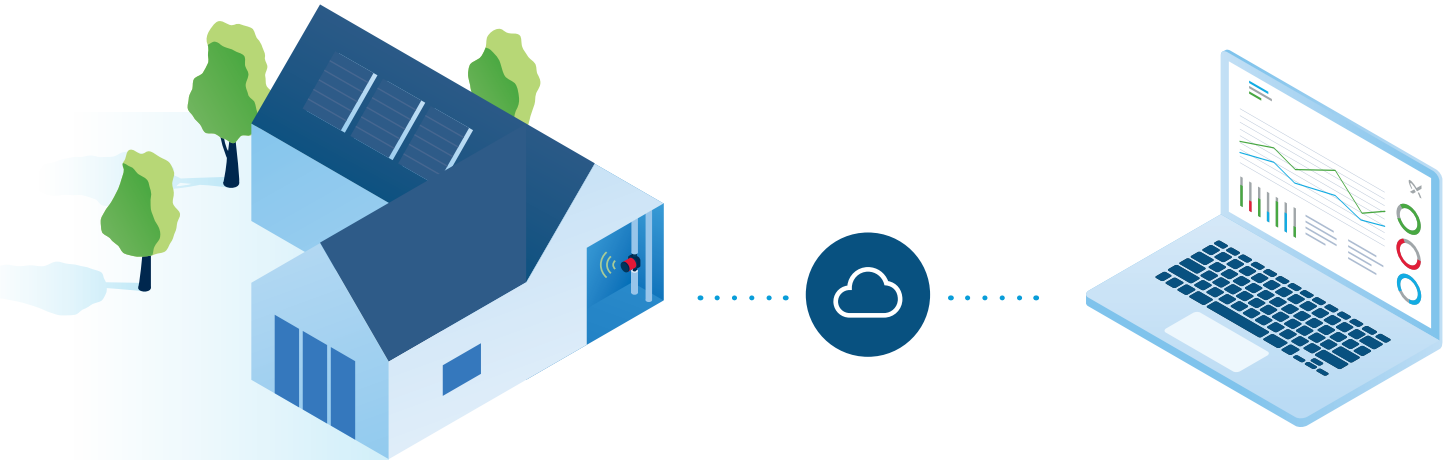
Du kan läsa mer om de principer som Asset Monitor följer i Grundfos whitepaper om cyber- och informationssäkerhet som finns på Grundfos.se.

Så här fungerar det

Asset Monitor har fyra komponenter som hjälper det att snabbt och säkert ansluta till dina system.

- **Molntjänst**
- **Kommunikationsnätverk**
- **Gateways**
- **Enhetsnätverk**

Grundfos Connect Asset Monitor



Molntjänst

Asset Monitor består av ett antal backend-tjänster:
En IoT-slutpunktstjänst och en autentiseringstjänst.
IoT-slutpunktstjänsten hanterar den allmänna kommunikationen med enheterna, medan autentiseringstjänsten hanterar autentiseringen av enheterna och väljer vilken IoT-slutpunkt enheterna ska använda för kommunikation. Asset Monitor använder ett ömsesidigt autentiseringssystem baserat på X.509-certifikat.

Backend-tjänsterna omfattar även lagring, auktorisering och meddelandetjänster, och specialiserade SMS-gateways kan skicka textmeddelanden till systemanvändare.

Backend-tjänsterna finns i en mycket skalbar molninfrastruktur, skyddad av modern och nästa generations säkerhetsteknik, som omvända proxyservrar med Layer7-filtrering och trafikanalys, webbapplikationsbrandväggar (WAF) och skyddsmekanismer mot distribuerade överbelastningsattacker (DDoS).

Kommunikationsnätverk

Asset Monitor använder internet eller mobilnätet, beroende på kundens krav och tillgänglig fysisk infrastruktur.

Gateways startar HTTPS-anslutningar via nätverket för att ansluta till autentiseringstjänsten. HTTPS är den säkra versionen av HTTP som använder Transport Level Security (TLS).
När en IoT-slutpunkt tilldelas kommer gatewayen att ansluta till IoT-slutpunkten med MQTT/TLS för att fortsätta kommunikationen med Asset Monitor.
Gateways använder ett ömsesidigt autentiseringssystem baserat på X.509-certifikat där både servern och klienten autentiseras.

Användare kommer åt Asset Monitor med hjälp av en webbklient. Webbklienten använder HTTPS och kan användas var som helst där det finns tillgång till internet. Användarautentisering säkras via Grundfos identitetsleverantör (Global Login). Du kan bjuda in fler användare som tillhör din organisation, och de måste gå igenom registreringsprocessen i Global Login.

Asset Monitor skickar e-post eller meddelanden till användare som prenumererar på varningar.

Gateways

Grundfos riktlinjer för hantering av anslutna produkter finns tillgängliga på grundfos.se och bör alltid följas för din säkerhets skull.

CIM 290 är ett gränssnitt som används för dataöverföring via ett 3G- eller 4G-nätverk, medan CIM 550 används på Ethernet-baserade nätverk.
Både CIM 290 och CIM 550 överför data mellan nätverket som enheten är ansluten till och Asset Monitor via säkra TLS-anslutningar. De kan installeras i olika fysiska konfigurationer, till exempel i en Grundfos-produkt med ett CIM-uttag eller i en CIU 900/901-gränssnittsenhet.

Gateways tilldelas användare i en process som kräver fysisk åtkomst till utrustningen.

Användning av brandväggar

Eftersom gateways alltid startar anslutningen till Asset Monitor bör inga inkommande anslutningar tillåtas genom brandväggen.
När du använder en extern brandvägg måste du se till att den tillåter utgående anslutningar via HTTPS och MQTT/TLS.

Enhetsnätverk

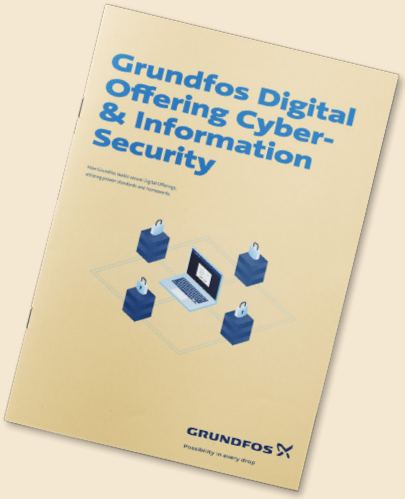
Enhetsnätverkssektionen är där all fungerande maskinvara, som styrenheter, pumpar och andra enheter, placeras i systemarkitekturen. De kan kommunicera med varandra, liksom med systemgatewayerna, via seriella fieldbus-lösningar, ingen kommunikation i den här sektionen är TCP/IP-baserad.

Sammanfattning

Kommunikation mellan enheter: Seriell fieldbus-kommunikation (inte TCP/IP)
WAN-kommunikation:
HTTPS och MQTT/TLS (med TLS 1.2) via Ethernet eller mobilnät (3G/4G)
Användarkommunikation: HTTPS (med TLS 1.2) och e-post/SMS för meddelanden

Autentisering av Grundfos Connect Assets Monitor: X.509-certifikat
Användarautentisering: Användarnamn/lösenord
Gateway-autentisering: X. 509-certifikat

Uppdatering av programvara: Trådlös överföring skyddad av TLS
Tillgänglighet: Redundant installation av virtualiserade applikationstjänster
Åtgärder: Penetrationstest, hotmodellering och kontinuerlig loggning och övervakning



Några frågor?
Kontakta oss gärna:

Michael Sandholm
Produktägare
Digital utveckling
msandholm@grundfos.se

Grundfos AB
Box 333 (Lunnagårdsg. 6)
431 24 Mölndal
Tel: (+46) 771 32 23 00
www.grundfos.se

GRUNDFOS