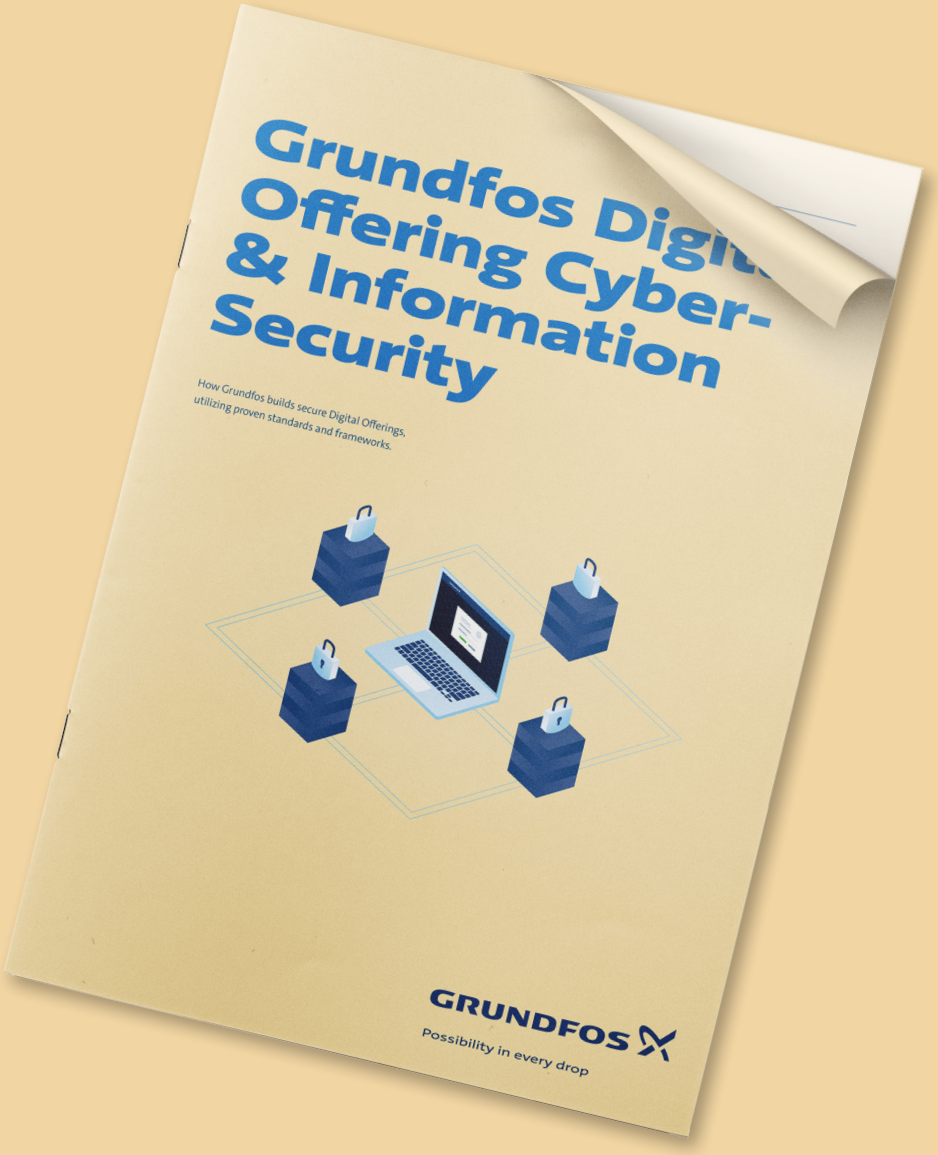
Grundfos Connect Asset Monitor

Turvallisuusohje



GRUNDFOS

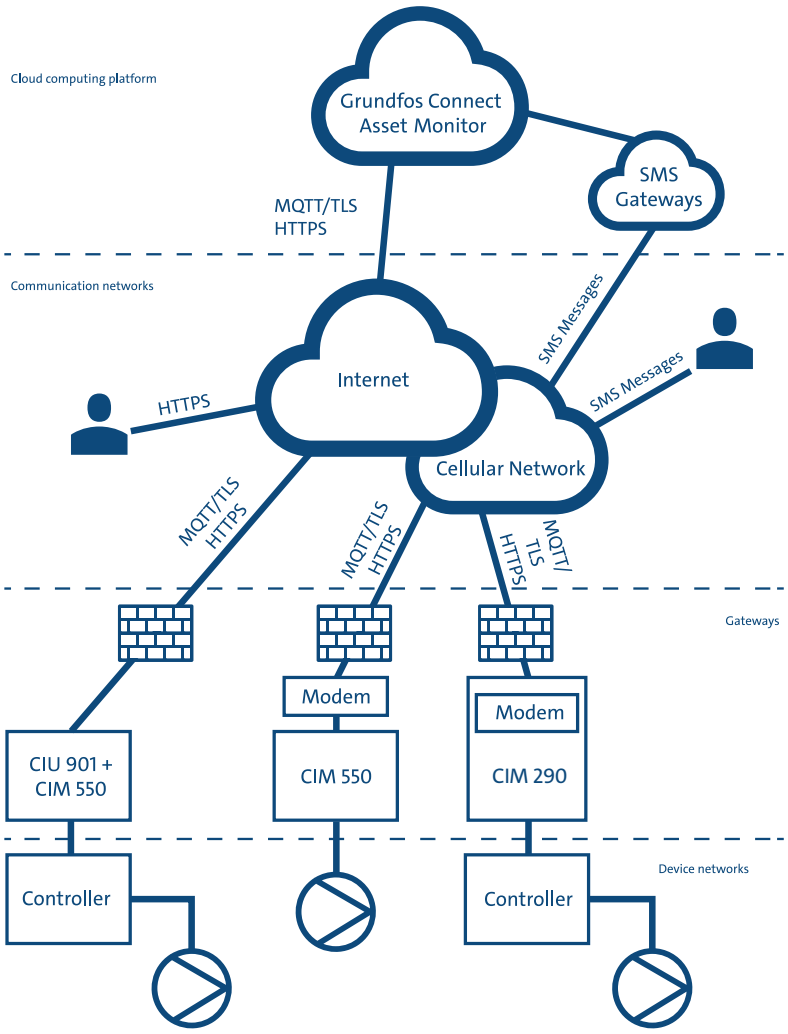
Possibility in every drop

Johdanto

Käyttövalmis, internetpohjainen Grundfos Connect Asset Monitor on suorituskykyinen ja kustannustehokas vaihtoehto kalliimmille SCADA-järjestelmille. Sen avulla voit hallita Grundfos-laitteitasi sijainnistasi riippumatta. Ratkaisun lukuisilla turvaominaisuuksilla saat sekä suojausta että mielenrauhaa.

Tässä asiakirjassa kerrotaan niistä lisää.

Turvallisuusarkkitehtuuri



Turvallisuusarkkitehtuuri

Asset Monitorin turvallisuusarkkitehtuuri sisältää yllä olevan kuvauksen mukaisesti laskenta-alustan, jolla Asset Monitor toimii, useita tiedonsiirtoverkkoja, yhdyskäytäviä, jotka ohjaavat liikennettä, sekä pumppuja ohjaavien paikallisten järjestelmien fyysisen infrastruktuurin.
Kaikki verkostoon yhdistettyihin laitteisiin ja niistä lähetettävä TCP/IP-data salataan jatkuvasti.

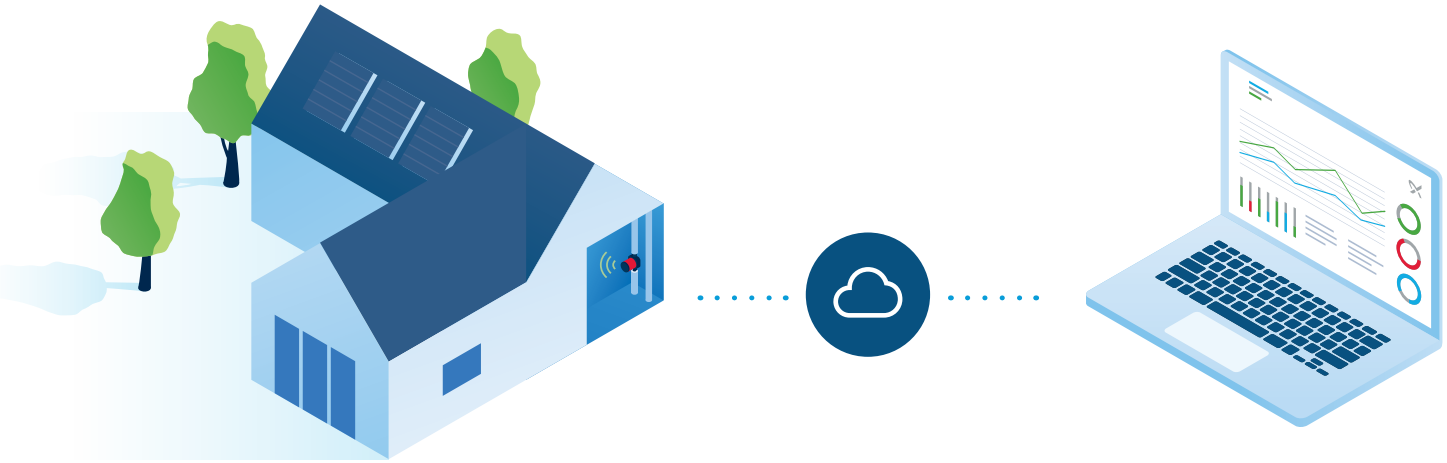
Voit lukea lisää Asset Monitorin toimintaperiaatteista Grundfosin kyber- ja tietoturvaraportista, joka on saatavilla Grundfos.com-sivustolla.

Toimintaperiaate

Asset Monitorissa on neljä komponenttia, joiden avulla se muodostaa yhteyden järjestelmiisi nopeasti ja turvallisesti.

- **Pilvipalvelualusta**
- **Tiedonsiirtoverkot**
- **Yhdyskäytävät**
- **Laiteverkot**

Grundfos Connect Asset Monitor



Pilvipalvelualusta

Asset Monitor koostuu useista taustapalveluista: IoT-päätepistepalvelu ja todennuspalvelu. IoT-päätepistepalvelu vastaa yleisestä tiedonsiirrosta laitteiden kanssa, kun taas todennuspalvelu vastaa laitteiden todentamisesta ja valitsee, mitä IoT-päätepistettä laitteet käyttävät tiedonsiirtoon. Asset Monitor käyttää molemminpuolista todennusmenetelmää X.509-varmenteilla.

Taustapalveluihin kuuluvat myös tallennustila-, valtuutus- ja ilmoituspalvelut, ja erillisten SMS-yhdyskäytävien kautta voidaan lähettää tekstiviestejä järjestelmän käyttäjille.

Taustapalveluita ylläpidetään erittäin skaalattavassa pilvi-infrastruktuurissa, jota suojataan nykyaikaisilla uuden sukupolven tietoturvateknologioilla, kuten Layer7-suodatusta ja liikenneanalyysiä käyttävillä käänteisillä välityspalvelimilla, verkkosovelluksen palomuureilla (WAF) ja hajautettujen palvelunestohyökkäysten (DDoS) suojausmekanismeilla.

Tiedonsiirtoverkot

Asset Monitor käyttää internetiä tai mobiiliverkkoa asiakkaan tarpeiden ja käytettävissä olevan fyysisen infrastruktuurin mukaan.

Yhdyskäytävät käynnistävät HTTPS-yhteydet verkon kautta, jotta todennuspalveluun saadaan yhteys. HTTPS on HTTP:n turvallinen versio, jossa käytetään Transport Level Security (TLS) -suojausta.
Kun yhdyskäytävälle määritetään IoT-päätepiste, se muodostaa yhteyden IoT-päätepisteeseen MQTT/TLS:n avulla, jotta tiedonsiirtoa voidaan jatkaa Asset Monitorin kanssa.
Yhdyskäytävät käyttävät molemminpuolista X.509-varmenteisiin perustuvaa todennusmenetelmää, jossa sekä palvelin että asiakas todennetaan.

Käyttäjät käyttävät Asset Monitoria verkkosovelluksella. Verkkosovellus käyttää HTTPS:ää, ja sitä voidaan käyttää missä tahansa, missä on internetyhteys. Käyttäjien todentaminen varmistetaan Grundfosin tunnistetietojen palveluntarjoajan Global Loginin kautta. Voit kutsua lisää organisaatioosi kuuluvia käyttäjiä, joiden tulee luoda tili Global Loginissa.

Asset Monitor lähettää sähköposti- tai tekstiviestejä käyttäjille, jotka ovat tilanneet hälytykset.

Yhdyskäytävät

Grundfosin ohjeet liitettyjen tuotteiden käsittelyyn ovat saatavilla grundfos.com-sivustolla, ja niitä tulee aina noudattaa turvallisuussyistä.

CIM 290 -liittymää käytetään tiedonsiirtoon 3G- tai 4G-verkon kautta, kun taas CIM 550 toimii Ethernet-pohjaisissa verkoissa.
Sekä CIM 290 että CIM 550 siirtävät dataa laitteen verkon ja Asset Monitorin välillä suojattujen TLS-yhteyksien kautta. Ne voidaan asentaa Grundfos-laitteeseen, jossa on CIM-paikka, tai CIU 900/901 -tiedonsiirtoyksikköön.

Yhdyskäytävät määritetään käyttäjille prosessissa, joka edellyttää fyysistä pääsyä laitteelle.

Palomuurien käyttö

Koska yhdyskäytävät aloittavat aina yhteyden muodostamisen Asset Monitoriin, saapuvia yhteyksiä ei tulisi sallia palomuurin kautta.
Kun käytät ulkoista palomuuria, varmista, että se sallii lähtevät yhteydet HTTPS:n ja MQTT/TLS:n kautta.

Laiteverkot

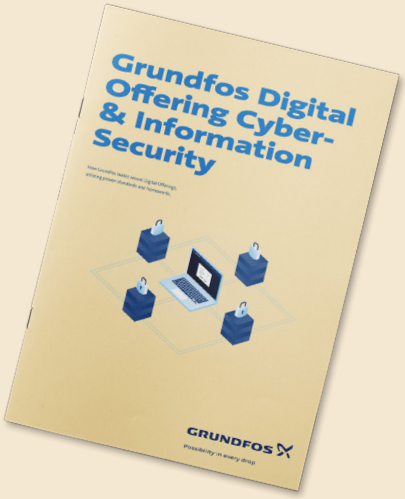
Laiteverkko-osa on se kohta, jossa kaikki käytettävät laitteistot, kuten säätimet ja pumput, sijoitetaan järjestelmäarkkitehtuuriin. Ne voivat siirtää tietoja sekä keskenään että järjestelmän yhdyskäytävien kanssa sarjakenttäväylien kautta. Laiteverkoissa tapahtuvassa tietoliikenteessä ei käytetä TCP/IP-protokollaa.

Yhteenveto

Laitteiden tiedonsiirto: sarjatiedonsiirto kenttäväylän kautta (ei TCP/IP)
WAN-tiedonsiirto: HTTPS ja MQTT/TLS (käyttäen TLS 1.2:ta) Ethernetin tai matkapuhelinverkon (3G/4G) kautta
Käyttäjäviestintä: HTTPS (käyttäen TLS 1.2:ta) ja sähköposti-/tekstiviesti-ilmoitukset

Grundfos Connect Assets Monitor -todennus: X.509-varmenteet
Käyttäjien todentaminen: käyttäjätunnus/salasana
Yhdyskäytävätodennus: X.509-varmenteet

Ohjelmistopäivitys: OTA-suojaus TLS:llä
Saatavuus: virtualisoidut sovelluspalvelut
Toiminta: penetraatiotestaus, uhkamallinnus sekä jatkuva kirjaaminen ja valvonta



Kysyttävää?
Ota yhteyttä:

Michael Sandholm
Product Owner
digitaalinen kehitys
msandholm@grundfos.com

Oy Grundfos Pumput AB
Trukkikuja 1
01360 Vantaa
Puh. +358 (0) 207 889 500
www.grundfos.fi

GRUNDFOS