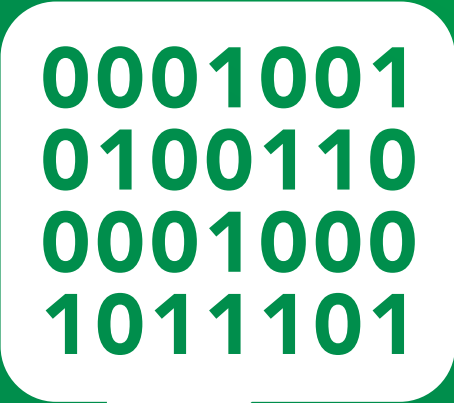


# Avtal om Robust & Säker IoT

Bilaga 3

Tjänstespecifikationer



```
0001001
0100110
0001000
1011101
```

# Innehåll

<b>Inledning</b>	<b>3</b>
<b>3.1 Infrastruktur</b>	<b>3</b>
3.1.1 Radionät	3
3.1.2 Plattformer	3
3.1.2.1 Plattform LoRa	4
<b>3.2 Säkerhet</b>	<b>5</b>
3.2.1 Informationssäkerhetsarbetet	5
3.2.2 Ledningssystem för Driftsäkerhet	6
3.2.3 Arkitektur vid byggande av OT/IoT-system	7
<b>3.3 Hårdvara</b>	<b>8</b>
3.3.1 IoT-Enheter	8

# Inledning

Denna bilaga definierar tjänstespecifikationer för infrastruktur, Säkerhet och Hårdvara.

Kapitlet om infrastruktur beskriver de olika former av nätinфраstruktur som tillhandahålls för IoT. Varje nät beskrivs med egen underbilaga.

Kapitlet om säkerhet beskriver säkerhet och dess tillhörande informations säkerhetsarbete som hanteras för IoT-systemet. Säkerhet gäller samtliga infrastrukturplattformar som finns specificerad i 3.1. Säkerhetsarbetet utgår från vägledning för Robust & Säker IoT.

Kapitlet om hårdvara tekniska datablad av produkter som tillhandahålls av nätägare och systemägaren av IoT-system. Bilaga kan innehålla ett antal underbilagor som exempelvis Bilaga 3.3.1 IoT-enhet och Bilaga 3.3.2 Säkerhetsprodukter

## 3.1 Infrastruktur

### 3.1.1 Radionät

Nätet benämnd Stadshubben är ett av Umeå Energi etablerat radiobaserat LoRa-nät som möjliggör uppkoppling (aktivering) av IOT-sensorer baserat på LoRa-teknik för insamling av mätdata.

Stadshubben tar emot radiosignaler från sensorer och förmedlar sensor-data via nätverksservern benämnd Stadshubbsplattformen till det gränssnitt Kunden ansluter mot Stadshubbsplattformen.

Stadshubben består av ett antal radiomottagare som möjliggör att radiosignalerna från och till en sensor inom täckningsområdet tas upp och vidareförmedlas via ett API till av Kunden vald applikation. Aktivering och avaktivering av förbindelser till sensorer sker via Umeå Energis Regionala Stadshubbsplattform.

Den Regionala Stadshubbens täckningsområde omfattar Umeå Kommun. Kunden är införstådd med att täckningsgraden (styrkan på radiosignalen) kan variera inom olika delar av täckningsområdet.

### 3.1.2 Plattformar

Umeå Energi kan till Kunden leverera en Dashboard där kunden hanterar och visualisera sina sensorer. I Dashboarden kan man hantera regelverk på vad och på vilket sätt sensorerna ska mäta samt hantering av notiser och larm. I Dashboarden finns även en projektmodul med möjlighet sortera sensorer, sätta mål, ta in insikter och få fram resultat utifrån förutbestämda hypoteser.

- Dashboard
- Visualisering sensorer
- Obegränsat med sensorer
- Lagring sensorvärden
- Inställning regelverk sensorer
- Hantering notiser och larm
- Modul projekt/piloter
- API Dashboard

### 3.1.2.1 Plattform LoRa

Umeå Energi tillhandahåller en plattform för LoRaWAN från Aqility med benämningen Thingpark.

Nedan följer en enklare teknisk beskrivning över plattformen ThingPark samt en enklare beskrivning av hur man hanterar ett eget konto med tillgång till dess Webportal. Mer detaljerat tekniskt innehåll kan bifogas vid behov.

- Stadshubben består av ett antal radiomottagare (Gateways) som möjliggör att radiosignalerna från och till en sensor inom täckningsområdet tas upp och vidareförmedlas till Umeå Energi:s Regionala plattform i ThingPark.
- I Thingpark kan Kunden köpa och koppla produkter (connectivity plans) till sina sensorer samt löpande hantera sina sensorer.
- Via Thingpark kan Kunden, via ett API, skicka sensors värden till en av Kunden vald applikation. API för ThingPark kan bifogas vid behov.

Dessa verktyg har kunden tillgång till

- Device manager
- Används för hantering av sensorer
- Lägga upp nya sensorer
- Koppla destinationer (routing profiles)
- Sensors signalstyrka
- Lokalisering vid senaste sändning
- Överblick/status på alla sensorer
- Överblick över alla produkter (connectivity plans)
- Rutin: TPW\_v5.1 - User\_Guide – Device\_Manager.pdf

Wireless logger

- Visar nätverkstrafik i realtid
- Används för felsökning för att se om sensor skickar data
- Rutin: TPW\_v5.1 - User\_Guide – Wireless\_Logger.pdf

Network survey

- Sensorers uppkoppling mot gateway
- Sensordata i råformat
- Historisk lokalisering av sensor
- Rutin:TPW\_v5.1 - User\_Guide – Network\_Survey.pdf

## 3.2 Säkerhet

Kapitlet säkerhet beskriver säkerhet och dess tillhörande informationssäkerhetsarbete som hanteras för OT och IoT-systemet. Säkerhet gäller samtliga infrastrukturplattformar som finns specificerad i 3.1. Säkerhetsarbetet utgår från vägledning för Robust & Saker IoT.

### Vad är skillnaden med OT och IoT

**IoT** Sakernas internet eller Internet of Things – IoT är ett samlingsbegrepp för saker som har en inbyggd elektronik och uppkoppling. IoT är helt enkelt saker som kan prata med varandra och dela med sig av viktig information till oss människor.

**OT** (Operational technology) är driftsystem och driftsteknologi – datorsystem som styr och övervakar industriella processer. Det är som IT (datorsystem för ex. administration) fast på fabriksgolvet, elnätet, vården eller i den smarta/digitaliserade samhället.

Detta kapitel hanterar både OT och Kritisk IoT för samhällsnyttiga digitala tjänster.

### 3.2.1 Informationssäkerhetsarbetet

Informationssäkerhet utgår från vägledning Robust & Saker IoT. Vägledningen utgår från standarder och regelverk inom de olika delområden som berörs i vägledningen till exempel:

- ENISA Good practices for IoT and Smart Infrastructures
- ENISA Baseline Security Recommendations for IoT
- MSB 245, 2011 MSB:s vägledning för risk- och sårbarhetsanalyser
- MSB 2017–1554 NCS3 Studie – IoT-relaterade risker och strategier
- ISO/IEC 30141 Internet of Things Reference architecture
- ISO/IEC 15408–1:2009 Generella säkerhetsmodeller
- ISO/IEC TR 15446:2017 Vägledning för produktion av skyddsprofiler och säkerhetsmål
- ISO/IEC 31010:2019 Risk management - Risk assessment techniques

Verktyg som används för säkerhetsarbetet är:

- KRAVANALYS ROBUST OCH SÄKER IoT
- RSA- MALL ROBUST OCH SÄKER IoT

Arbetet utgår från en generisk modell av ett IoT-system som består av sju huvuddelar:

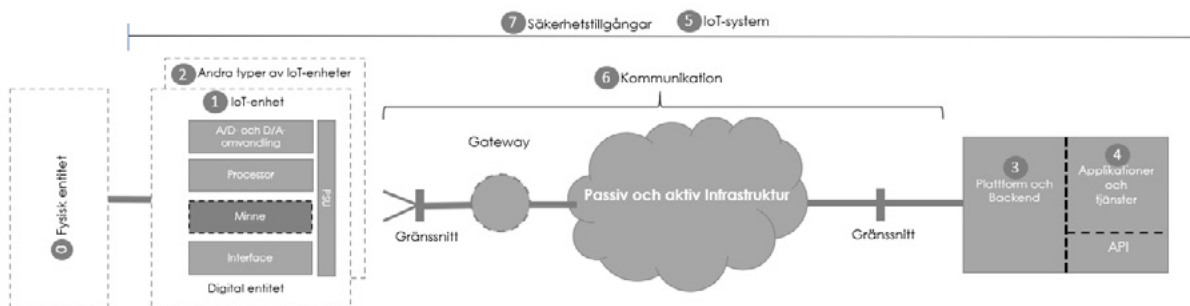


Bild: Konceptuellt IoT-system

Som bilden visar så består ett IoT-system av IoT-enheter, Andra typer av IoT-enheter, plattform och backend, Applikationer och tjänster (API), Systemägare av IoT-system, kommunikation samt säkerhetstillgångar. Samtliga dessa roller har säkerhetskrav. Dessa finns beskrivet

vägledningen för Robust & säker IoT. Det finns också minimikrav och hjälpmedel för att hantera alla säkerhetsfrågor.

Utifrån den konceptuella bilden ritas ett realiserat OT/IoT-systemet upp och på så sätt går det att koppla kravbilder till funktioner och roller. Nedan ser du ett exempel på koppling. Exemplet visar övervakning av gods med data för position, temperatur, tider och larm.

De gråa bollarna med siffror representerar roller inom vägledningen som ska hanteras och beskrivas säkerhetsmässigt.

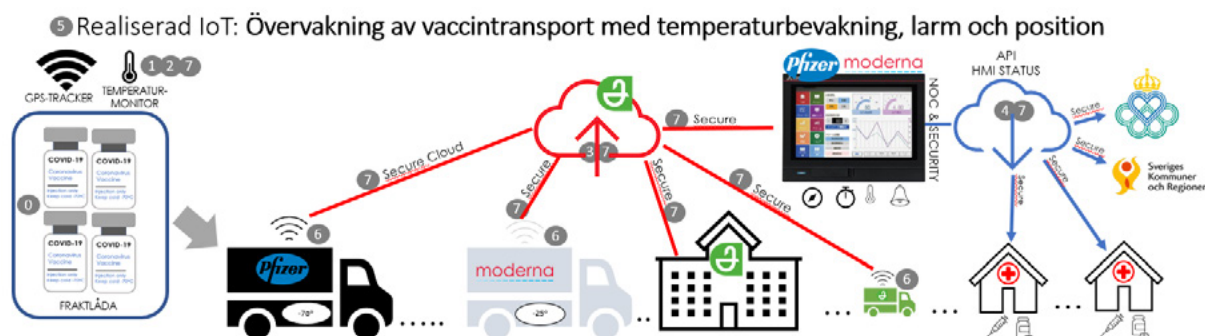


Bild: Realiserad IoT

### 3.2.2 Ledningssystem för Driftsäkerhet

Syftet med ledningssystemet är att säkerställa att driftsäkerhetsarbetet bedrivs långsiktigt, kontinuerligt och systematiskt för att fortlöpande kunna utveckla och säkra kvaliteten i stadsnätets nät och tjänster så att stadsnätet uppfyller driftsäkerhetskrav från ledningen, myndigheter och kunder.

Ledningssystemet för driftsäkerhet ska ge stöd för driftorganisationens:

- Ledning
- Planering
- Kontroll
- Uppföljning
- Utvärdering
- Förbättringar

Dokumentets tillämpningsområde utgörs av stadsnätets nät och tjänster, inkluderande stödsystem för övervakning och larm.

Dokumentet har som utgångspunkt:

- Stadsnätets Ledningssystem (företagsspecifik)
- Lag (2003:389) om elektronisk kommunikation
- PTSFS 2015:2 och PTSFS 2020:1 Post- och telestyrelsens föreskrifter om krav på driftsäkerhet

Arbetet omfattar såväl normala driftsförhållanden som extraordinära händelser.

### 3.2.3 Arkitektur vid byggande av OT/IoT-system

Säkerhet handlar om att ge enkel åtkomst till data för de i organisationen som behöver det för att göra sitt jobb bättre, men samtidigt skydda uppgifterna genom att förhindra tillgång till informationen av utomstående som inte ska se, ändra eller ta bort den.

Det är viktigt att separera verksamhetssystem IT från OT och IoT-systemet. I verksamhetssystem hanteras information och i OT-system hanteras funktion och data. Det är olika regelverk som styr säkerhet och sättet att förhålla sig till innehållet i systemen.

Ett tydligt gränssnitt definieras och kan också därför kontrolleras mellan IT- och OT/IoT-system. Gränssnittet kan vara en brandvägg, datadiod eller både och.

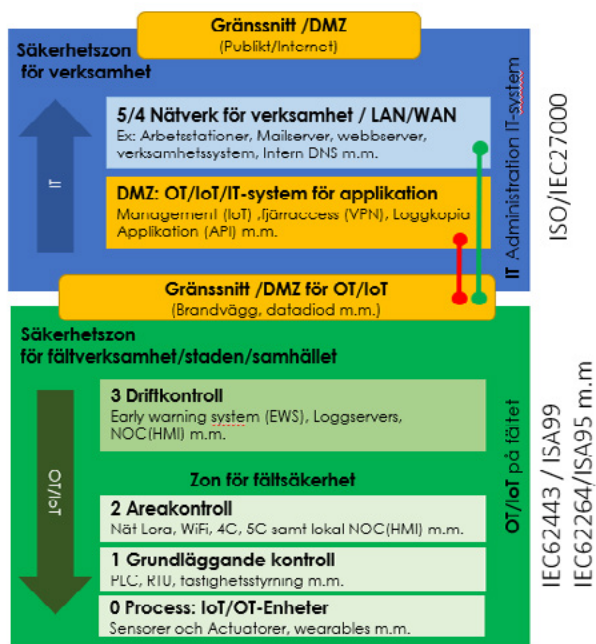


Bild: Purdue-modellen för OT och applicerbar för kritisk IoT

#### Några råd och guidelines är:

- Standarder för dataskydd, datasäkerhet finns redan. För OT och IoT använd IEC62443, ISA 99, IEC62265 samt ISA 95
- Standarderna för OT/IoT-säkerhet (IEC62443 / ISA99) skiljer sig från de för IT-säkerhet (ISO / IEC27000) eftersom affärssystemens behov skiljer sig från behoven för anläggning/fältautomationen och datainsamling.
- Rekommendationen är att hålla systemarkitekturen enkel.
- Paketera inte ihop verksamhetssystem med OT/IoT-system.
- Tätt kopplade system är svåra att hantera.
- Använd en skiktad arkitektur enligt IEC62443 / ISA99 och ICS-CERT för djupförvar. Upprätthåll en arkitektur baserad på Purdue-modellen (ISA95 / IEC62264) som redan finns på de flesta moderna anläggningar för kritisk styrning genom OT/IoT.
- Systemlagren ska vara separata, ändå ansluten eftersom Purdue-modellen är förgrenad via DMZ.

- IT-avdelningen hanterar nivå 4/5-verksamhetssystem och applikationspaket.
- OT/IoT hanterar lager 0 - 3. Operativsystem exempelvis distribuerade kontrollsystem (DCS), OT/IoT-datalagring och OT/IoT-analys-beräkning, algoritmer och AI, OT/IoT-kommunikation samt alla sensorer och aktuatorer/ställdon.

## 3.3 Hårdvara

### 3.3.1 IoT-Enheter

Umeå Energi tillhandahåller sensorer från olika sensortillverkare utifrån kundens behov. Generellt fungerar de flesta sensorerna från de större tillverkarna i vår nätverksserver och dashboard.

Umeå Energi validerar succesivt upp nya sensorer utifrån kundens behov vilket gör att sensorlistan för godkända sensorer ökar.

Vid vissa specifika behov av sensorer kan det behövas en dialog för alternativa lösningar för att kunna mäta kundens behov med hjälp av sensorer.